O2OA V5.1 安全评估报告

该报告包含有关 web 应用程序的重要安全信息。

安全报告

该报告由 IBM Security AppScan Standard 创建 9.0.3.12, 规则： 17339
扫描开始时间： 2020/8/4 13:01:14

目录

介绍

摘要

按问题类型分类的问题

介绍

该报告包含由 IBM Security AppScan Standard 执行的 Web 应用程序安全性扫描的结果。

低严重性问题：	52
参考严重性问题：	8
报告中包含的严重性问题总数：	60
扫描中发现的严重性问题总数：	60

常规信息

扫描文件名称：	0804
扫描开始时间：	2020/8/4 13:01:14
测试策略：	Default（已修改）

主机	develop.o2oa.net
端口	80
操作系统：	未知
Web 服务器：	未知
应用程序服务器：	任何

主机	develop.o2oa.net
端口	20020
操作系统：	未知
Web 服务器：	未知
应用程序服务器：	任何

主机	develop.o2oa.net
端口	20030
操作系统：	未知
Web 服务器：	未知
应用程序服务器：	任何

登陆设置

登陆方法：	记录的登录
并发登陆：	已启用
JavaScript 执行文件：	已禁用
会话中检测：	已启用
会话中模式：	gggggggggg|hhhhhhhhhhhhhhh|jjjjjjjjjjjj
跟踪或会话标识 cookie：	x-token
跟踪或会话标识参数：	->"captcha"
登陆序列：	http://develop.o2oa.net:20030/x_program_center/jaxrs/distribute/assemble/source/develop.o2oa.net?v=5.1.1&kdfh24ru= http://develop.o2oa.net:20030/x_program_center/jaxrs/distribute/assemble/source/develop.o2oa.net?v=5.1.1&kdfh24ru= http://develop.o2oa.net:20020/x_organization_assemble_authentication/jaxrs/authentication?v=5.1.1&kdfh24rv= http://develop.o2oa.net:20020/x_organization_assemble_authentication/jaxrs/authentication?v=5.1.1&kdfh24rv= http://develop.o2oa.net:20020/x_organization_assemble_personal/jaxrs/definition/loginStyleList?v=5.1.1&kdfh24rw= http://develop.o2oa.net:20020/x_organization_assemble_personal/jaxrs/definition/loginStyleList?v=5.1.1&kdfh24rw= http://develop.o2oa.net:20020/x_organization_assemble_authentication/jaxrs/authentication/mode?v=5.1.1 http://develop.o2oa.net:20020/x_organization_assemble_authentication/jaxrs/authentication/mode?v=5.1.1 http://develop.o2oa.net:20020/x_organization_assemble_authentication/jaxrs/authentication/mode?v=5.1.1 http://develop.o2oa.net:20020/x_organization_assemble_personal/jaxrs/regist/mode?v=5.1.1 http://develop.o2oa.net:20020/x_organization_assemble_personal/jaxrs/regist/mode?v=5.1.1 http://develop.o2oa.net:20020/x_organization_assemble_authentication/jaxrs/authentication/captcha/width/120/height/50?v=5.1.1 http://develop.o2oa.net:20020/x_organization_assemble_authentication/jaxrs/authentication/bind?v=5.1.1 http://develop.o2oa.net:20020/x_organization_assemble_authentication/jaxrs/authentication/oauth/list?v=5.1.1 http://develop.o2oa.net:20020/x_organization_assemble_authentication/jaxrs/authentication/oauth/list?v=5.1.1 http://develop.o2oa.net:20020/x_organization_assemble_authentication/jaxrs/authentication/captcha/width/120/height/50?v=5.1.1 http://develop.o2oa.net:20020/x_organization_assemble_authentication/jaxrs/authentication/bind?v=5.1.1 http://develop.o2oa.net/x_desktop/index.html http://develop.o2oa.net:20030/x_program_center/jaxrs/distribute/assemble/source/develop.o2oa.net?v=5.1.1&kdfh28db= http://develop.o2oa.net:20030/x_program_center/jaxrs/distribute/assemble/source/develop.o2oa.net?v=5.1.1&kdfh28db= http://develop.o2oa.net:20020/x_organization_assemble_authentication/jaxrs/authentication?v=5.1.1&kdfh28dc= http://develop.o2oa.net:20020/x_organization_assemble_authentication/jaxrs/authentication?v=5.1.1&kdfh28dc= http://develop.o2oa.net:20020/x_organization_assemble_personal/jaxrs/definition/loginStyleList?v=5.1.1&kdfh28dd= http://develop.o2oa.net:20020/x_organization_assemble_personal/jaxrs/definition/loginStyleList?v=5.1.1&kdfh28dd= http://develop.o2oa.net:20020/x_organization_assemble_authentication

```
/jaxrs/authentication/mode?v=5.1.1
http://develop.o2oa.net:20020/x_organization_assemble_authentication
/jaxrs/authentication/mode?v=5.1.1
http://develop.o2oa.net:20020/x_organization_assemble_personal/jaxrs
/regist/mode?v=5.1.1
http://develop.o2oa.net:20020/x_organization_assemble_authentication
/jaxrs/authentication/bind?v=5.1.1
http://develop.o2oa.net:20020/x_organization_assemble_authentication
/jaxrs/authentication/oauth/list?v=5.1.1
http://develop.o2oa.net:20020/x_organization_assemble_authentication
/jaxrs/authentication/captcha/width/120/height/50?v=5.1.1
http://develop.o2oa.net/x_desktop/index.html
http://develop.o2oa.net:20030/x_program_center/jaxrs/distribute/asse
mble/source/develop.o2oa.net?v=5.1.1&kdfh2aq0=
http://develop.o2oa.net:20030/x_program_center/jaxrs/distribute/asse
mble/source/develop.o2oa.net?v=5.1.1&kdfh2aq0=
http://develop.o2oa.net:20020/x_organization_assemble_authentication
/jaxrs/authentication?v=5.1.1&kdfh2aq1=
http://develop.o2oa.net:20020/x_organization_assemble_authentication
/jaxrs/authentication?v=5.1.1&kdfh2aq1=
http://develop.o2oa.net:20020/x_organization_assemble_personal/jaxrs
/definition/loginStyleList?v=5.1.1&kdfh2aq2=
http://develop.o2oa.net:20020/x_organization_assemble_personal/jaxrs
/definition/loginStyleList?v=5.1.1&kdfh2aq2=
http://develop.o2oa.net:20020/x_organization_assemble_authentication
/jaxrs/authentication/mode?v=5.1.1
http://develop.o2oa.net:20020/x_organization_assemble_authentication
/jaxrs/authentication/mode?v=5.1.1
http://develop.o2oa.net:20020/x_organization_assemble_authentication
/jaxrs/authentication/mode?v=5.1.1
http://develop.o2oa.net:20020/x_organization_assemble_personal/jaxrs
/regist/mode?v=5.1.1
http://develop.o2oa.net:20020/x_organization_assemble_personal/jaxrs
/regist/mode?v=5.1.1
http://develop.o2oa.net:20020/x_organization_assemble_authentication
/jaxrs/authentication/captcha/width/120/height/50?v=5.1.1
http://develop.o2oa.net:20020/x_organization_assemble_authentication
/jaxrs/authentication/bind?v=5.1.1
http://develop.o2oa.net:20020/x_organization_assemble_authentication
/jaxrs/authentication/oauth/list?v=5.1.1
http://develop.o2oa.net:20020/x_organization_assemble_authentication
/jaxrs/authentication/oauth/list?v=5.1.1
http://develop.o2oa.net:20020/x_organization_assemble_authentication
/jaxrs/authentication/captcha/width/120/height/50?v=5.1.1
http://develop.o2oa.net:20020/x_organization_assemble_authentication
/jaxrs/authentication/bind?v=5.1.1
http://develop.o2oa.net:20020/x_organization_assemble_authentication
/jaxrs/authentication/captcha?v=5.1.1&kdfh2aq3=
http://develop.o2oa.net:20020/x_organization_assemble_authentication
/jaxrs/authentication/captcha?v=5.1.1&kdfh2aq3=
http://develop.o2oa.net/x_desktop/index.html
http://develop.o2oa.net:20030/x_program_center/jaxrs/distribute/asse
mble/source/develop.o2oa.net?v=5.1.1&kdfh2isk=
http://develop.o2oa.net:20030/x_program_center/jaxrs/distribute/asse
mble/source/develop.o2oa.net?v=5.1.1&kdfh2isk=
http://develop.o2oa.net:20020/x_organization_assemble_authentication
/jaxrs/authentication?v=5.1.1&kdfh2isl=
http://develop.o2oa.net:20020/x_organization_assemble_authentication
/jaxrs/authentication?v=5.1.1&kdfh2isl=
http://develop.o2oa.net:20020/x_organization_assemble_personal/jaxrs
/definition/forceLayout?v=5.1.1&kdfh2ism=
http://develop.o2oa.net:20020/x_organization_assemble_personal/jaxrs
/definition/forceLayout?v=5.1.1&kdfh2ism=
http://develop.o2oa.net:20020/x_organization_assemble_personal/jaxrs
/custom/layout?v=5.1.1&kdfh2isn=
http://develop.o2oa.net:20020/x_organization_assemble_personal/jaxrs
/custom/layout?v=5.1.1&kdfh2isn=
http://develop.o2oa.net/o2_core/o2/xAction/services/x_organization_a
ssemble_control.json?v=5.1.1
http://develop.o2oa.net/o2_core/o2/xDesktop/$Default/blue/layout-
pc.html
http://develop.o2oa.net/o2_core/o2/widget/$Menu/flatStyle/css.wcss?
v=5.1.1
http://develop.o2oa.net/o2_core/o2/widget/$Menu/flatUser/css.wcss?
v=5.1.1
http://develop.o2oa.net/o2_core/o2/xDesktop/$Default/styles.json?
v=5.1.1
http://develop.o2oa.net/o2_core/o2/widget/$ScrollBar/hide/css.wcss?
v=5.1.1
http://develop.o2oa.net/o2_core/o2/xDesktop/$Default/icons.json?
v=5.1.1
http://develop.o2oa.net/x_component_Homepage/$Main/default/view.html
http://develop.o2oa.net/x_component_Homepage/$Main/default/taskConte
nt.html
http://develop.o2oa.net/o2_core/o2/xDesktop/$Default/blue/layout-
message-pc.html
http://develop.o2oa.net:20020/x_processplatform_assemble_surface/des
cribe/api.json?v=5.1.1
http://develop.o2oa.net:20020/x_processplatform_assemble_surface/des
cribe/api.json?v=5.1.1
http://develop.o2oa.net:20020/x_processplatform_assemble_surface/jax
rs/review/v2/count?v=5.1.1
http://develop.o2oa.net:20020/x_processplatform_assemble_surface/jax
rs/draft/list/(0)/next/1?v=5.1.1
http://develop.o2oa.net/x_component_Homepage/$Main/default/inforCont
ent.html
http://develop.o2oa.net/o2_core/o2/widget/$ScrollBar/xDesktop_Messag
e/css.wcss?v=5.1.1
http://develop.o2oa.net:20020/x_processplatform_assemble_surface/jax
rs/work/count/083ad4d3-4df1-4f88-b79b-36b810b5c80b?v=5.1.1
http://develop.o2oa.net/x_component_Homepage/$Main/default/fileConte
nt.html
http://develop.o2oa.net:20020/x_processplatform_assemble_surface/jax
rs/draft/list/(0)/next/1?v=5.1.1
http://develop.o2oa.net:20020/x_processplatform_assemble_surface/jax
rs/review/v2/count?v=5.1.1
http://develop.o2oa.net/x_component_Homepage/$Main/default/calendarC
ontent.html
http://develop.o2oa.net:20020/x_processplatform_assemble_surface/jax
rs/task/list/my/paging/1/size/12?v=5.1.1
http://develop.o2oa.net/x_component_Homepage/$Main/default/meetingCo
ntent.html
http://develop.o2oa.net:20020/x_cms_assemble_control/describe/api.js
on?v=5.1.1
http://develop.o2oa.net:20020/x_cms_assemble_control/describe/api.js
on?v=5.1.1
http://develop.o2oa.net:20020/x_file_assemble_control/describe/api.j
son?v=5.1.1
http://develop.o2oa.net:20020/x_file_assemble_control/describe/api.j
son?v=5.1.1
http://develop.o2oa.net/x_component_Homepage/$Main/default/allInfor.
html
http://develop.o2oa.net:20020/x_cms_assemble_control/jaxrs/appinfo/l
ist/user/view?v=5.1.1
http://develop.o2oa.net:20020/x_meeting_assemble_control/describe/ap
i.json?v=5.1.1
```

```
http://develop.o2oa.net:20020/x_meeting_assemble_control/describe/api.json?v=5.1.1
http://develop.o2oa.net:20020/x_processplatform_assemble_surface/jaxrs/work/count/083ad4d3-4df1-4f88-b79b-36b810b5c80b?v=5.1.1
http://develop.o2oa.net:20020/x_file_assemble_control/jaxrs/attachment/list/top?v=5.1.1
http://develop.o2oa.net:20020/x_processplatform_assemble_surface/jaxrs/task/list/my/paging/1/size/12?v=5.1.1
http://develop.o2oa.net:20020/x_hotpic_assemble_control/describe/api.json?v=5.1.1
http://develop.o2oa.net:20020/x_meeting_assemble_control/jaxrs/meeting/list/invited/wait?v=5.1.1
http://develop.o2oa.net:20020/x_hotpic_assemble_control/describe/api.json?v=5.1.1
http://develop.o2oa.net:20020/x_cms_assemble_control/jaxrs/document/filter/list/1/size/12?v=5.1.1
http://develop.o2oa.net/o2_core/o2/widget/$Calendar/homepage/css.wcss?v=5.1.1
http://develop.o2oa.net:20020/x_hotpic_assemble_control/jaxrs/user/hotpic/filter/list/page/1/count/6?v=5.1.1
http://develop.o2oa.net:20020/x_file_assemble_control/jaxrs/attachment/list/top?v=5.1.1
http://develop.o2oa.net:20020/x_cms_assemble_control/jaxrs/appinfo/list/user/view?v=5.1.1
http://develop.o2oa.net/o2_core/o2/widget/$Calendar/homepage/container.html
http://develop.o2oa.net/o2_core/o2/widget/$Calendar/homepage/day.html
http://develop.o2oa.net:20020/x_calendar_assemble_control/describe/api.json?v=5.1.1
http://develop.o2oa.net:20020/x_calendar_assemble_control/describe/api.json?v=5.1.1
http://develop.o2oa.net:20020/x_calendar_assemble_control/jaxrs/event/list/filter?v=5.1.1
http://develop.o2oa.net:20020/x_meeting_assemble_control/jaxrs/meeting/list/invited/wait?v=5.1.1
http://develop.o2oa.net:20020/x_calendar_assemble_control/jaxrs/event/list/filter/sample?v=5.1.1
http://develop.o2oa.net:20020/x_hotpic_assemble_control/jaxrs/user/hotpic/filter/list/page/1/count/6?v=5.1.1
http://develop.o2oa.net:20020/x_calendar_assemble_control/jaxrs/event/list/filter?v=5.1.1
http://develop.o2oa.net:20020/x_calendar_assemble_control/jaxrs/event/list/filter/sample?v=5.1.1
http://develop.o2oa.net:20020/x_cms_assemble_control/jaxrs/document/filter/list/1/size/12?v=5.1.1
http://develop.o2oa.net:20020/x_meeting_assemble_control/jaxrs/meeting/list/coming/month/1?v=5.1.1
http://develop.o2oa.net:20020/x_meeting_assemble_control/jaxrs/meeting/list/coming/month/1?v=5.1.1
http://develop.o2oa.net/x_component_Homepage/$Main/default/hotpic.html
```

摘要

问题类型 13

TOC

	问题类型	问题的数量
低	“Content-Security-Policy”头缺失或不安全	5
低	“X-Content-Type-Options”头缺失或不安全	5
低	“X-XSS-Protection”头缺失或不安全	5
低	Oracle 日志文件信息泄露	4
低	发现压缩目录	25
低	归档文件下载	2
低	过度许可的 CORS 访问测试	3
低	会话 cookie 中缺少 HttpOnly 属性	1
低	临时文件下载	2
参	发现电子邮件地址模式	1
参	发现可能的服务器路径泄露模式	1
参	客户端（JavaScript）Cookie 引用	1
参	应用程序错误	5

有漏洞的 URL 18

TOC

	URL	问题的数量
低	http://develop.o2oa.net/	2
低	http://develop.o2oa.net/o2_core/o2/lp/zh-cn.js	3
低	http://develop.o2oa.net/o2_core/o2/widget/Menu.min.js	2
低	http://develop.o2oa.net/o2_lib/Decimal.js	3
低	http://develop.o2oa.net/x_desktop/js/x.min.js	3
低	http://develop.o2oa.net/x_desktop/index.html	1
低	http://develop.o2oa.net/x_desktop/res/config/config.json	1
低	http://develop.o2oa.net:20020/x_hotpic_assemble_control/jaxrs/user/hotpic/filter/	12

低	http://develop.o2oa.net:20020/x_processplatform_assemble_surface/jaxrs/work/count/	12
低	http://develop.o2oa.net:20020/x_hotpic_assemble_control/jaxrs/user/hotpic/filter/list/	5
低	http://develop.o2oa.net:20020/x_organization_assemble_personal/jaxrs/definition/forceLayout	2
低	http://develop.o2oa.net:20020/x_processplatform_assemble_surface/jaxrs/work/count/083ad4d3-4df1-4f88-b79b-36b810b5c80b	3
低	http://develop.o2oa.net:20020/x_organization_assemble_authentication/jaxrs/authentication	1
低	http://develop.o2oa.net:20020/x_organization_assemble_authentication/jaxrs/authentication/check/credential/huqi	1
低	http://develop.o2oa.net:20030/x_program_center/jaxrs/distribute/assemble/source/develop.o2oa.net	2
参	http://develop.o2oa.net/o2_core/o2.min.js	3
参	http://develop.o2oa.net:20020/x_calendar_assemble_control/jaxrs/event/list/filter	2
参	http://develop.o2oa.net:20020/x_calendar_assemble_control/jaxrs/event/list/filter/sample	2

修订建议 12

TOC

	修复任务	问题的数量
低	除去 Web 站点中的电子邮件地址	1
低	除去客户端中的业务逻辑和安全逻辑	1
低	除去虚拟目录中的旧版本文件	4
低	除去压缩目录文件或限制对它的访问	25
低	关闭跟踪，限制对日志文件的访问，或者将其除去	4
低	将服务器配置为使用安全策略的“Content-Security-Policy”头	5
低	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头	5
低	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头	5
低	为 Web 服务器或 Web 应用程序下载相关的安全补丁	1
低	向所有会话 cookie 添加“HttpOnly”属性	1
低	修改“Access-Control-Allow-Origin”头以仅获取允许的站点	3
低	验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常	5

安全风险 8

TOC

	风险	问题的数量
低	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名	23

	和/或敏感文件位置	
低	可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息	18
低	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息	25
低	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息	4
低	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务	1
参	可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息	1
参	此攻击的最坏情形取决于在客户端所创建的 cookie 的上下文和角色	1
参	可能会收集敏感的调试信息	5

原因 8

TOC

	原因	问题的数量
低	Web 应用程序编程或配置不安全	44
低	Web 服务器或应用程序服务器是以不安全的方式配置的	4
低	在生产环境中留下临时文件	4
低	Web 应用程序设置了缺少 HttpOnly 属性的会话 cookie	1
参	未安装第三方产品的最新补丁或最新修补程序	1
参	Cookie 是在客户端创建的	1
参	未对入局参数值执行适当的边界检查	5
参	未执行验证以确保用户输入与预期的数据类型匹配	5

WASC 威胁分类

TOC

威胁	问题的数量
可预测资源位置	4
信息泄露	56

按问题类型分类的问题

低 “Content-Security-Policy”头缺失或不安全 5 TOC

问题 1 / 5 TOC

“Content-Security-Policy”头缺失或不安全	
严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net/o2_core/o2/lp/zh-cn.js
实体：	zh-cn.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用安全策略的“Content-Security-Policy”头

推理： AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

未经处理的测试响应：

```
...

Referer: http://develop.o2oa.net/x_desktop/index.html
Connection: keep-alive
Host: develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Last-Modified: Tue, 28 Jul 2020 07:56:47 GMT
Connection: keep-alive
Server: nginx/1.14.1
Accept-Ranges: bytes
Vary: Accept-Encoding, User-Agent
Content-Length: 16837
Date: Tue, 04 Aug 2020 05:02:52 GMT
Content-Type: application/javascript
```

```
o2.LP = window.LP || {
    "name": "名称",
    "description": "描述",
    "searchKey": "请输入搜索关键字",
    "desktop_style": "桌面风格",
    "flat_style": "扁平风格"
};

o2.LP.process = {
    "unnamed": "未命名",

...
```

问题 2 / 5

TOC

“Content-Security-Policy”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net/x_desktop/js/x.min.js
实体：	x.min.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用安全策略的“Content-Security-Policy”头

推理： AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

未经处理的测试响应：

```
...

Referer: http://develop.o2oa.net/x_desktop/index.html
Connection: keep-alive
Host: develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Last-Modified: Tue, 28 Apr 2020 03:57:27 GMT
Connection: keep-alive
Server: nginx/1.14.1
Accept-Ranges: bytes
Vary: Accept-Encoding, User-Agent
Content-Length: 839
Date: Tue, 04 Aug 2020 05:02:52 GMT
Content-Type: application/javascript

layout.addReady((function(){!function(e){e.inBrowser=!1,e.desktop.type="layout";var
o=$("browser_loading");MWF.xDesktop.getUserLayout((function(){e.userLayout=e.userLayout||{};var
t=new URI(window.location.href),a=t.getData("view"),p=t.getData("style");p&&
(e.userLayout.flatStyle=p),a||(a=e.userLayout&&e.userLayout.viewMode?
e.userLayout.viewMode:"homepage"),a=a.toLowerCase(),a=-1!==
["layout","desktop"].indexOf(a)?"Layout":"Default",e.viewMode=a.capitalize(),$("appContent").dest
roy(),MWF.require("MWF.xDesktop."+e.viewMode,(function(){e.desktop=new MWF.xDesktop[e.viewMode]
("layout_main",{}),e.desktop.load(),e.desktop.openApplication||
(e.desktop.openApplication=e.openApplication),e.desktop.refreshApp||
(e.desktop.refreshApp=e.refreshApp)})),o&&new Fx.Tween(o).start("opacity",0).chain((function()
{o.destroy(),o=null}))}))}(layout)}));
...
```

问题 3 / 5

TOC

“Content-Security-Policy”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net/
实体：	(Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用安全策略的“Content-Security-Policy”头

推理： AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

未经处理的测试响应：

```
...

Connection: keep-alive
Host: develop.o2oa.net
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
authorization: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Last-Modified: Fri, 19 Jun 2020 02:28:22 GMT
Connection: keep-alive
Server: nginx/1.14.1
Accept-Ranges: bytes
Vary: Accept-Encoding, User-Agent
Content-Length: 282
Date: Tue, 04 Aug 2020 05:02:52 GMT
Content-Type: text/html

<!DOCTYPE html>
<html>
<head>
 <meta charset="UTF-8"/>
 <meta property="qc:admins" content="1556771456600414672564530" />
 <meta http-equiv="refresh" content="0;url=./x_desktop/index.html"/>
</head>
<body style="margin:0;font-size: 1.0em;font-family:Microsoft Yahei"></body>
</html>


...
```

```
...

Referer: http://develop.o2oa.net/
Connection: Keep-Alive
Host: develop.o2oa.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
authorization: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g
Accept-Language: en-US
x-token: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Last-Modified: Fri, 19 Jun 2020 02:28:23 GMT
x-ua-compatible: IE=edge
Connection: keep-alive
Server: nginx/1.14.1
Accept-Ranges: bytes
Vary: Accept-Encoding, User-Agent
Content-Length: 5202
Date: Tue, 04 Aug 2020 05:02:19 GMT
Content-Type: text/html

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xml:lang="zh-CN" xmlns="http://www.w3.org/1999/xhtml">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
    <link rel="stylesheet" type="text/css" href="css/style.css?v=-87026e5" charset="UTF-8" />
    <link rel="stylesheet" href="css/mBoxNotice.css?v=-f060151" charset="UTF-8" />
    <link rel="stylesheet" href="css/mBoxTooltip.css?v=-4e9e25a" charset="UTF-8" />
    <title>O2</title>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
...
```

问题 4 / 5

TOC

“Content-Security-Policy”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net/o2_lib/Decimal.js
实体：	Decimal.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用安全策略的“Content-Security-Policy”头

推理： AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

未经处理的测试响应：

```
...

Referer: http://develop.o2oa.net/x_desktop/index.html
Connection: keep-alive
Host: develop.o2oa.net
```

```
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Last-Modified: Tue, 28 Apr 2020 03:57:25 GMT
Connection: keep-alive
Server: nginx/1.14.1
Accept-Ranges: bytes
Vary: Accept-Encoding, User-Agent
Content-Length: 23334
Date: Tue, 04 Aug 2020 05:02:52 GMT
Content-Type: application/javascript

/*! decimal.js v4.0.1 https://github.com/MikeMcl/decimal.js/LICENCE */
(function(n){"use strict";function l(n){for(var t,e,f=1,r=n.length,u=n[0]+"";f<r;f++)...

...
```

问题 5 / 5

TOC

“Content-Security-Policy”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net/o2_core/o2/widget/Menu.min.js
实体：	Menu.min.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用安全策略的“Content-Security-Policy”头

推理： AppScan 检测到 Content-Security-Policy 响应头缺失或具有不安全策略，这可能会更大程度地暴露于各种跨站点注入攻击之下

未经处理的测试响应：

```
...

Connection: keep-alive
Host: develop.o2oa.net
X-Requested-With: XMLHttpRequest
Accept: text/javascript, text/html, application/xml, text/xml, */*
authorization: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Last-Modified: Fri, 19 Jun 2020 02:28:22 GMT
Connection: keep-alive
Server: nginx/1.14.1
Accept-Ranges: bytes
Vary: Accept-Encoding, User-Agent
Content-Length: 10217
Date: Tue, 04 Aug 2020 05:02:52 GMT
```

```
Content-Type: application/javascript

o2.widget=o2.widget||{},o2.widget.Menu=new Class({Implements:
[Options,Events],Extends:o2.widget.Common,options:
{style:"default",event:"contextmenu",disable:...

...
```

低 “X-Content-Type-Options”头缺失或不安全 5 TOC

问题 1 / 5 TOC

“X-Content-Type-Options”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net/o2_core/o2/lp/zh-cn.js
实体：	zh-cn.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

推理： AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

未经处理的测试响应：

```
...

Referer: http://develop.o2oa.net/x_desktop/index.html
Connection: keep-alive
Host: develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Last-Modified: Tue, 28 Jul 2020 07:56:47 GMT
Connection: keep-alive
Server: nginx/1.14.1
Accept-Ranges: bytes
Vary: Accept-Encoding, User-Agent
Content-Length: 16837
Date: Tue, 04 Aug 2020 05:02:52 GMT
Content-Type: application/javascript

o2.LP = window.LP || {
    "name": "名称",
    "description": "描述",
    "searchKey": "请输入搜索关键字",
    "desktop_style": "桌面风格",
    "flat_style": "扁平风格"
};

o2.LP.process = {
    "unnamed": "未命名",

...
```

问题 2 / 5

TOC

“X-Content-Type-Options”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net/x_desktop/js/x.min.js
实体：	x.min.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

推理： AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

未经处理的测试响应：

```
...

Referer: http://develop.o2oa.net/x_desktop/index.html
Connection: keep-alive
Host: develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Last-Modified: Tue, 28 Apr 2020 03:57:27 GMT
Connection: keep-alive
Server: nginx/1.14.1
Accept-Ranges: bytes
Vary: Accept-Encoding, User-Agent
Content-Length: 839
Date: Tue, 04 Aug 2020 05:02:52 GMT
Content-Type: application/javascript

layout.addReady((function(){!function(e){e.inBrowser=!1,e.desktop.type="layout";var
o=$("browser_loading");MWF.xDesktop.getUserLayout((function(){e.userLayout=e.userLayout||{};var
t=new URI(window.location.href),a=t.getData("view"),p=t.getData("style");p&&
(e.userLayout.flatStyle=p),a||(a=e.userLayout&&e.userLayout.viewMode?
e.userLayout.viewMode:"homepage"),a=a.toLowerCase(),a=-1!==
["layout","desktop"].indexOf(a)?"Layout":"Default",e.viewMode=a.capitalize(),$("appContent").dest
roy(),MWF.require("MWF.xDesktop."+e.viewMode,(function(){e.desktop=new MWF.xDesktop[e.viewMode]
("layout_main",{}),e.desktop.load(),e.desktop.openApplication||
(e.desktop.openApplication=e.openApplication),e.desktop.refreshApp||
(e.desktop.refreshApp=e.refreshApp)})),o&&new Fx.Tween(o).start("opacity",0).chain((function()
{o.destroy(),o=null}))})})(layout)}));
...
```

问题 3 / 5

TOC

“X-Content-Type-Options”头缺失或不安全	
严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net/o2_lib/Decimal.js
实体：	Decimal.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

推理： AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

未经处理的测试响应：

```
...

Referer: http://develop.o2oa.net/x_desktop/index.html
Connection: keep-alive
Host: develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Last-Modified: Tue, 28 Apr 2020 03:57:25 GMT
Connection: keep-alive
Server: nginx/1.14.1
Accept-Ranges: bytes
Vary: Accept-Encoding, User-Agent
Content-Length: 23334
Date: Tue, 04 Aug 2020 05:02:52 GMT
Content-Type: application/javascript

/*! decimal.js v4.0.1 https://github.com/MikeMcl/decimal.js/LICENCE */
(function(n){"use strict";function l(n){for(var t,e,f=1,r=n.length,u=n[0]+"";f<r;f++)...

...
```

问题 4 / 5

TOC

“X-Content-Type-Options”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net/x_desktop/index.html
实体：	index.html (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

推理： AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

未经处理的测试响应：

```
...

Referer: http://develop.o2oa.net/
Connection: Keep-Alive
Host: develop.o2oa.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
authorization: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjjynyKX8qw5g
Accept-Language: en-US
x-token: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjjynyKX8qw5g


HTTP/1.1 200 OK
Last-Modified: Fri, 19 Jun 2020 02:28:23 GMT
x-ua-compatible: IE=edge
Connection: keep-alive
Server: nginx/1.14.1
Accept-Ranges: bytes
Vary: Accept-Encoding, User-Agent
Content-Length: 5202
Date: Tue, 04 Aug 2020 05:02:52 GMT
Content-Type: text/html

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xml:lang="zh-CN" xmlns="http://www.w3.org/1999/xhtml">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
    <link rel="stylesheet" type="text/css" href="css/style.css?v=-87026e5" charset="UTF-8" />
    <link rel="stylesheet" href="css/mBoxNotice.css?v=-f060151" charset="UTF-8" />
    <link rel="stylesheet" href="css/mBoxTooltip.css?v=-4e9e25a" charset="UTF-8" />
    <title>O2</title>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
...
```

问题 5 / 5

TOC

“X-Content-Type-Options”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net/
实体：	(Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头

推理： AppScan 检测到“X-Content-Type-Options”响应头缺失或具有不安全值，这可能会更大程度地暴露于偷渡式下载攻击之下

未经处理的测试响应：

```
...

Connection: keep-alive
Host: develop.o2oa.net
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
authorization: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Last-Modified: Fri, 19 Jun 2020 02:28:22 GMT
Connection: keep-alive
Server: nginx/1.14.1
Accept-Ranges: bytes
Vary: Accept-Encoding, User-Agent
Content-Length: 282
Date: Tue, 04 Aug 2020 05:02:52 GMT
Content-Type: text/html

<!DOCTYPE html>
<html>
<head>
 <meta charset="UTF-8"/>
 <meta property="qc:admins" content="1556771456600414672564530" />
 <meta http-equiv="refresh" content="0;url=./x_desktop/index.html"/>
</head>
<body style="margin:0;font-size: 1.0em;font-family:Microsoft Yahei"></body>
</html>


...

...

Referer: http://develop.o2oa.net/
Connection: Keep-Alive
Host: develop.o2oa.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
authorization: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g
Accept-Language: en-US
x-token: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Last-Modified: Fri, 19 Jun 2020 02:28:23 GMT
x-ua-compatible: IE=edge
Connection: keep-alive
Server: nginx/1.14.1
Accept-Ranges: bytes
```

```
Vary: Accept-Encoding, User-Agent
Content-Length: 5202
Date: Tue, 04 Aug 2020 05:02:19 GMT
Content-Type: text/html

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xml:lang="zh-CN" xmlns="http://www.w3.org/1999/xhtml">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
    <link rel="stylesheet" type="text/css" href="css/style.css?v=-87026e5" charset="UTF-8" />
    <link rel="stylesheet" href="css/mBoxNotice.css?v=-f060151" charset="UTF-8" />
    <link rel="stylesheet" href="css/mBoxTooltip.css?v=-4e9e25a" charset="UTF-8" />
    <title>O2</title>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
...
```

低 “X-XSS-Protection”头缺失或不安全 5

TOC

问题 1 / 5

TOC

“X-XSS-Protection”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net/o2_core/o2/lp/zh-cn.js
实体：	zh-cn.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

推理： AppScan 检测到 X-XSS-Protection 响应头缺失或具有不安全值，这可能会造成跨站点脚本编制攻击

未经处理的测试响应：

```
...

Referer: http://develop.o2oa.net/x_desktop/index.html
Connection: keep-alive
Host: develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Last-Modified: Tue, 28 Jul 2020 07:56:47 GMT
Connection: keep-alive
```

```
Server: nginx/1.14.1
Accept-Ranges: bytes
Vary: Accept-Encoding, User-Agent
Content-Length: 16837
Date: Tue, 04 Aug 2020 05:02:52 GMT
Content-Type: application/javascript

o2.LP = window.LP || {
    "name": "名称",
    "description": "描述",
    "searchKey": "请输入搜索关键字",
    "desktop_style": "桌面风格",
    "flat_style": "扁平风格"
};

o2.LP.process = {
    "unnamed": "未命名",

...
```

问题 2 / 5

TOC

“X-XSS-Protection”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net/x_desktop/js/x.min.js
实体：	x.min.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

推理： AppScan 检测到 X-XSS-Protection 响应头缺失或具有不安全值，这可能会造成跨站点脚本编制攻击

未经处理的测试响应：

```
...

Referer: http://develop.o2oa.net/x_desktop/index.html
Connection: keep-alive
Host: develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Last-Modified: Tue, 28 Apr 2020 03:57:27 GMT
Connection: keep-alive
Server: nginx/1.14.1
Accept-Ranges: bytes
Vary: Accept-Encoding, User-Agent
Content-Length: 839
Date: Tue, 04 Aug 2020 05:02:52 GMT
Content-Type: application/javascript
```

```
layout.addReady((function(){!function(e){e.inBrowser=!1,e.desktop.type="layout";var
o=$("browser_loading");MWF.xDesktop.getUserLayout((function(){e.userLayout=e.userLayout||{};var
t=new URI(window.location.href),a=t.getData("view"),p=t.getData("style");p&&
(e.userLayout.flatStyle=p),a||(a=e.userLayout&&e.userLayout.viewMode?
e.userLayout.viewMode:"homepage"),a=a.toLowerCase(),a=-1!==
["layout","desktop"].indexOf(a)?"Layout":"Default",e.viewMode=a.capitalize(),$("appContent").dest
roy(),MWF.require("MWF.xDesktop."+e.viewMode,(function(){e.desktop=new MWF.xDesktop[e.viewMode]
("layout_main",{}),e.desktop.load(),e.desktop.openApplication||
(e.desktop.openApplication=e.openApplication),e.desktop.refreshApp||
(e.desktop.refreshApp=e.refreshApp)}))),o&&new Fx.Tween(o).start("opacity",0).chain((function()
{o.destroy(),o=null}))}}))}(layout)}));
...
```

问题 3 / 5

TOC

“X-XSS-Protection”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net/o2_core/o2/widget/Menu.min.js
实体：	Menu.min.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

推理： AppScan 检测到 X-XSS-Protection 响应头缺失或具有不安全值，这可能会造成跨站点脚本编制攻击

未经处理的测试响应：

```
...

Connection: keep-alive
Host: develop.o2oa.net
X-Requested-With: XMLHttpRequest
Accept: text/javascript, text/html, application/xml, text/xml, */*
authorization: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Last-Modified: Fri, 19 Jun 2020 02:28:22 GMT
Connection: keep-alive
Server: nginx/1.14.1
Accept-Ranges: bytes
Vary: Accept-Encoding, User-Agent
Content-Length: 10217
Date: Tue, 04 Aug 2020 05:02:52 GMT
Content-Type: application/javascript

o2.widget=o2.widget||{},o2.widget.Menu=new Class({Implements:
[Options,Events],Extends:o2.widget.Common,options:
{style:"default",event:"contextmenu",disable:...

...
```

问题 4 / 5

TOC

“X-XSS-Protection”头缺失或不安全	
严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net/o2_lib/Decimal.js
实体：	Decimal.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

推理： AppScan 检测到 X-XSS-Protection 响应头缺失或具有不安全值，这可能会造成跨站点脚本编制攻击

未经处理的测试响应：

```
...

Referer: http://develop.o2oa.net/x_desktop/index.html
Connection: keep-alive
Host: develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Last-Modified: Tue, 28 Apr 2020 03:57:25 GMT
Connection: keep-alive
Server: nginx/1.14.1
Accept-Ranges: bytes
Vary: Accept-Encoding, User-Agent
Content-Length: 23334
Date: Tue, 04 Aug 2020 05:02:52 GMT
Content-Type: application/javascript

/*! decimal.js v4.0.1 https://github.com/MikeMcl/decimal.js/LICENCE */
(function(n){"use strict";function l(n){for(var t,e,f=1,r=n.length,u=n[0]+"";f<r;f++)...

...
```

问题 5 / 5

TOC

“X-XSS-Protection”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net/x_desktop/res/config/config.json
实体：	config.json (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头

推理： AppScan 检测到 X-XSS-Protection 响应头缺失或具有不安全值，这可能会造成跨站点脚本编制攻击

未经处理的测试响应：

```
...

Connection: keep-alive
Host: develop.o2oa.net
X-Requested-With: XMLHttpRequest
Accept: application/json
authorization: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Last-Modified: Mon, 27 Jul 2020 02:07:20 GMT
Connection: keep-alive
Server: nginx/1.14.1
Accept-Ranges: bytes
Vary: Accept-Encoding, User-Agent
Content-Length: 521
Date: Tue, 04 Aug 2020 05:02:52 GMT
Content-Type: application/json

{

"center": [

{

"port": "20030",

"host": ""


...
```

低 Oracle 日志文件信息泄露 4 TOC

Oracle 日志文件信息泄露

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_processplatform_assemble_surface/jaxrs/work/count/
实体：	sqlnet.log (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值：	关闭跟踪，限制对日志文件的访问，或者将其除去

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: GET
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Vary: Accept-Encoding, User-Agent
Content-Length: 244
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "824817160"

...

...

Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "824817160"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAu3lZUQ-L4bKOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:04:51 GMT
x-token: HeEoZIVgPjRSFT_gQ92UAu3lZUQ-L4bKOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{

"type": "success",

"data": {

"task": 0,

"taskCompleted": 0,

...
```

问题 2 / 4

TOC

Oracle 日志文件信息泄露

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_hotpic_assemble_control/jaxrs/user/hotpic/filter/
实体：	sqlnet.trc (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值：	关闭跟踪，限制对日志文件的访问，或者将其除去

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: PUT
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Vary: Accept-Encoding, User-Agent
Content-Length: 132
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"

...

...

Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAhFlYbuaku1hOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:05:09 GMT
x-token: HeEoZIVgPjRSFT_gQ92UAhFlYbuaku1hOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{
```

```
"type": "success",

"message": "",

"date": "2020-08-04 13:05:09",

"spent": 2,

...
```

问题 3 / 4

TOC

Oracle 日志文件信息泄露

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_processplatform_assemble_surface/jaxrs/work/count/
实体：	sqlnet.trc (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值：	关闭跟踪，限制对日志文件的访问，或者将其除去

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: GET
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Vary: Accept-Encoding, User-Agent
Content-Length: 244
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "824817160"

...

...

Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "824817160"
```

```
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAu3lZUQ-L4bKOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:04:51 GMT
x-token: HeEoZIVgPjRSFT_gQ92UAu3lZUQ-L4bKOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{

"type": "success",

"data": {

"task": 0,

"taskCompleted": 0,

...
```

问题 4 / 4

TOC

Oracle 日志文件信息泄露

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_hotpic_assemble_control/jaxrs/user/hotpic/filter/
实体：	sqlnet.log (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 服务器或应用程序服务器是以不安全的方式配置的
固定值：	关闭跟踪，限制对日志文件的访问，或者将其除去

推理： AppScan 请求的文件可能不是应用程序的合法部分。响应状态为“200 OK”。这表示测试成功检索了所请求的文件的内容。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: PUT
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Vary: Accept-Encoding, User-Agent
Content-Length: 132
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"
```

```
...

...

Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAhFlYbuaku1hOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:05:09 GMT
x-token: HeEoZIVgPjRSFT_gQ92UAhFlYbuaku1hOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{

"type": "success",

"message": "",

"date": "2020-08-04 13:05:09",

"spent": 2,

...
```

低 发现压缩目录 25

TOC

问题 1 / 25

TOC

发现压缩目录

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_hotpic_assemble_control/jaxrs/user/hotpic/filter/
实体：	filter.gz (Page)
风险：	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	除去压缩目录文件或限制对它的访问

推理： AppScan 接收到响应状态“200 OK”，而且内容类型与请求的文件扩展名匹配。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
```

```
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: PUT
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Content-Length: 132
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAhFlYbuaku1hOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net

...

...

Access-Control-Allow-Origin: http://develop.o2oa.net
Content-Length: 132
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAhFlYbuaku1hOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:05:09 GMT
x-token: HeEoZIVgPjRSFT_gQ92UAhFlYbuaku1hOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{

"type": "success",

"message": "",

"date": "2020-08-04 13:05:09",

"spent": 1,

...
```

问题 2 / 25

TOC

发现压缩目录

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_processplatform_assemble_surface/jaxrs/work/count/
实体：	count.zip (Page)
风险：	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	除去压缩目录文件或限制对它的访问

推理： AppScan 接收到响应状态“200 OK”，而且内容类型与请求的文件扩展名匹配。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: GET
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Content-Length: 244
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "824817160"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAu3lZUQ-L4bKOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net

...

...

Access-Control-Allow-Origin: http://develop.o2oa.net
Content-Length: 244
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "824817160"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAu3lZUQ-L4bKOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:04:51 GMT
x-token: HeEoZIVgPjRSFT_gQ92UAu3lZUQ-L4bKOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{

"type": "success",

"data": {

"task": 0,

"taskCompleted": 0,

...
```

问题 3 / 25

TOC

发现压缩目录

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_processplatform_assemble_surface/jaxrs/work/count/
实体：	count.gz (Page)
风险：	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	除去压缩目录文件或限制对它的访问

推理： AppScan 接收到响应状态“200 OK”，而且内容类型与请求的文件扩展名匹配。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: GET
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Content-Length: 244
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "824817160"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAu3lZUQ-L4bKOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net

...

...

Access-Control-Allow-Origin: http://develop.o2oa.net
Content-Length: 244
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "824817160"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAu3lZUQ-L4bKOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:04:51 GMT
x-token: HeEoZIVgPjRSFT_gQ92UAu3lZUQ-L4bKOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8
```

```
{

"type": "success",

"data": {

"task": 0,

"taskCompleted": 0,

...
```

问题 4 / 25

TOC

发现压缩目录

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_hotpic_assemble_control/jaxrs/user/hotpic/filter/list/
实体：	list.war (Page)
风险：	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	除去压缩目录文件或限制对它的访问

推理： AppScan 接收到响应状态“200 OK”，而且内容类型与请求的文件扩展名匹配。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: PUT
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Vary: Accept-Encoding, User-Agent
Content-Length: 132
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"

...

...

Vary: Accept-Encoding, User-Agent
```

```
Content-Length: 132
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAnQacD1Vuo2AOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:05:11 GMT
x-token: HeEoZIVgPjRSFT_gQ92UAnQacD1Vuo2AOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{

"type": "success",

"message": "",

"date": "2020-08-04 13:05:11",

"spent": 3,

...
```

问题 5 / 25

TOC

发现压缩目录

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_processplatform_assemble_surface/jaxrs/work/count/
实体：	count.rar (Page)
风险：	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	除去压缩目录文件或限制对它的访问

推理： AppScan 接收到响应状态“200 OK”，而且内容类型与请求的文件扩展名匹配。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: GET
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Content-Length: 244
```

```
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "824817160"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAu3lZUQ-L4bKOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net

...

...

Access-Control-Allow-Origin: http://develop.o2oa.net
Content-Length: 244
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "824817160"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAu3lZUQ-L4bKOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:04:51 GMT
x-token: HeEoZIVgPjRSFT_gQ92UAu3lZUQ-L4bKOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{

"type": "success",

"data": {

"task": 0,

"taskCompleted": 0,

...
```

问题 6 / 25

TOC

发现压缩目录

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_hotpic_assemble_control/jaxrs/user/hotpic/filter/
实体：	filter.rar (Page)
风险：	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	除去压缩目录文件或限制对它的访问

推理： AppScan 接收到响应状态“200 OK”，而且内容类型与请求的文件扩展名匹配。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
```

```
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: PUT
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Content-Length: 132
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAhFlYbuaku1hOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net

...

...

Access-Control-Allow-Origin: http://develop.o2oa.net
Content-Length: 132
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAhFlYbuaku1hOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:05:10 GMT
x-token: HeEoZIVgPjRSFT_gQ92UAhFlYbuaku1hOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{

"type": "success",

"message": "",

"date": "2020-08-04 13:05:10",

"spent": 5,

...
```

问题 7 / 25

TOC

发现压缩目录

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_processplatform_assemble_surface/jaxrs/work/count/
实体：	count.ace (Page)
风险：	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	除去压缩目录文件或限制对它的访问

推理： AppScan 接收到响应状态“200 OK”，而且内容类型与请求的文件扩展名匹配。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: GET
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Content-Length: 244
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "824817160"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAu3lZUQ-L4bKOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net

...

...
-begin_highlight_tag--
"type": "success",

"data": {

"task": 0,

"taskCompleted": 0,

"--end_highlight_tag--read": 0,

"readCompleted": 0,

"review": 0

 },

"message": "",

...
```

问题 8 / 25

TOC

发现压缩目录

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_hotpic_assemble_control/jaxrs/user/hotpic/filter/
实体：	filter.ace (Page)
风险：	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	除去压缩目录文件或限制对它的访问

推理： AppScan 接收到响应状态“200 OK”，而且内容类型与请求的文件扩展名匹配。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: PUT
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Vary: Accept-Encoding, User-Agent
Content-Length: 132
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"

...

...

Vary: Accept-Encoding, User-Agent
Content-Length: 132
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UApFDyzE07TNBOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:05:10 GMT
x-token: HeEoZIVgPjRSFT_gQ92UApFDyzE07TNBOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{

"type": "success",

"message": "",

"date": "2020-08-04 13:05:10",

"spent": 1,

...
```

问题 9 / 25

TOC

发现压缩目录

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_processplatform_assemble_surface/jaxrs/work/count/
实体：	count.lha (Page)
风险：	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	除去压缩目录文件或限制对它的访问

推理： AppScan 接收到响应状态“200 OK”，而且内容类型与请求的文件扩展名匹配。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: GET
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Vary: Accept-Encoding, User-Agent
Content-Length: 244
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "824817160"

...

...

Vary: Accept-Encoding, User-Agent
Content-Length: 244
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "824817160"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAu3lZUQ-L4bKOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:04:51 GMT
x-token: HeEoZIVgPjRSFT_gQ92UAu3lZUQ-L4bKOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{
```

```
"type": "success",

"data": {

"task": 0,

"taskCompleted": 0,

...
```

问题 10 / 25

TOC

发现压缩目录	
严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_processplatform_assemble_surface/jaxrs/work/count/
实体：	count.lzh (Page)
风险：	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	除去压缩目录文件或限制对它的访问

推理： AppScan 接收到响应状态“200 OK”，而且内容类型与请求的文件扩展名匹配。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: GET
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Content-Length: 244
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "824817160"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAu3lZUQ-L4bKOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net

...

...
-begin_highlight_tag--
"type": "success",

"data": {
```

```
"task": 0,

"taskCompleted": 0,

"--end_highlight_tag--read": 0,

"readCompleted": 0,

"review": 0

 },

"message": "",

...
```

问题 11 / 25

TOC

发现压缩目录

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_processplatform_assemble_surface/jaxrs/work/count/
实体：	count.tar (Page)
风险：	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	除去压缩目录文件或限制对它的访问

推理： AppScan 接收到响应状态“200 OK”，而且内容类型与请求的文件扩展名匹配。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: GET
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: close
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Vary: Accept-Encoding, User-Agent
Content-Length: 244
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "824817160"

...
```

```
...

Vary: Accept-Encoding, User-Agent
Content-Length: 244
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "824817160"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAu3lZUQ-L4bKOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:04:51 GMT
x-token: HeEoZIVgPjRSFT_gQ92UAu3lZUQ-L4bKOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{

"type": "success",

"data": {

"task": 0,

"taskCompleted": 0,

...
```

问题 12 / 25

TOC

发现压缩目录

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_processplatform_assemble_surface/jaxrs/work/count/
实体：	count.arj (Page)
风险：	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	除去压缩目录文件或限制对它的访问

推理： AppScan 接收到响应状态“200 OK”，而且内容类型与请求的文件扩展名匹配。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: GET
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: close
```

```
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Vary: Accept-Encoding, User-Agent
Content-Length: 244
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "824817160"

...

...

Vary: Accept-Encoding, User-Agent
Content-Length: 244
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "824817160"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAu3lZUQ-L4bKOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:04:51 GMT
x-token: HeEoZIVgPjRSFT_gQ92UAu3lZUQ-L4bKOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{

"type": "success",

"data": {

"task": 0,

"taskCompleted": 0,

"read": 0,

"readCompleted": 0,

"review": 0


...
```

问题 13 / 25

TOC

发现压缩目录

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_hotpic_assemble_control/jaxrs/user/hotpic/filter/list/
实体：	list.wim (Page)
风险：	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	除去压缩目录文件或限制对它的访问

推理： AppScan 接收到响应状态“200 OK”，而且内容类型与请求的文件扩展名匹配。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: PUT
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Vary: Accept-Encoding, User-Agent
Content-Length: 133
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"

...

...

Vary: Accept-Encoding, User-Agent
Content-Length: 133
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAnQacD1Vuo2AOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:05:11 GMT
x-token: HeEoZIVgPjRSFT_gQ92UAnQacD1Vuo2AOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{

"type": "success",

"message": "",

"date": "2020-08-04 13:05:11",

"spent": 11,

...
```

发现压缩目录

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_processplatform_assemble_surface/jaxrs/work/count/
实体：	count.arc (Page)
风险：	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	除去压缩目录文件或限制对它的访问

推理： AppScan 接收到响应状态“200 OK”，而且内容类型与请求的文件扩展名匹配。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: GET
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Vary: Accept-Encoding, User-Agent
Content-Length: 244
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "824817160"

...

...

Vary: Accept-Encoding, User-Agent
Content-Length: 244
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "824817160"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAu3lZUQ-L4bKOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:04:51 GMT
x-token: HeEoZIVgPjRSFT_gQ92UAu3lZUQ-L4bKOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{

"type": "success",

"data": {

"task": 0,

"taskCompleted": 0,

...
```

问题 15 / 25

TOC

发现压缩目录	
严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_hotpic_assemble_control/jaxrs/user/hotpic/filter/
实体：	filter.lha (Page)
风险：	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	除去压缩目录文件或限制对它的访问

推理： AppScan 接收到响应状态“200 OK”，而且内容类型与请求的文件扩展名匹配。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: PUT
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Vary: Accept-Encoding, User-Agent
Content-Length: 132
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"

...

...

Vary: Accept-Encoding, User-Agent
Content-Length: 132
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UApFDyzE07TNBOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:05:10 GMT
x-token: HeEoZIVgPjRSFT_gQ92UApFDyzE07TNBOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{
```

```
"type": "success",

"message": "",

"date": "2020-08-04 13:05:10",

"spent": 1,

...
```

问题 16 / 25

TOC

发现压缩目录

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_processplatform_assemble_surface/jaxrs/work/count/
实体：	count.tar.gz (Page)
风险：	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	除去压缩目录文件或限制对它的访问

推理： AppScan 接收到响应状态“200 OK”，而且内容类型与请求的文件扩展名匹配。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: GET
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Vary: Accept-Encoding, User-Agent
Content-Length: 244
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "824817160"

...

...

Vary: Accept-Encoding, User-Agent
Content-Length: 244
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
```

```
Access-Control-Expose-Headers: x-token, c-token
ETag: "824817160"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAu3lZUQ-L4bKOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:04:51 GMT
x-token: HeEoZIVgPjRSFT_gQ92UAu3lZUQ-L4bKOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{

"type": "success",

"data": {

"task": 0,

"taskCompleted": 0,

...
```

问题 17 / 25

TOC

发现压缩目录	
严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_hotpic_assemble_control/jaxrs/user/hotpic/filter/
实体：	filter.lzh (Page)
风险：	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	除去压缩目录文件或限制对它的访问

推理： AppScan 接收到响应状态“200 OK”，而且内容类型与请求的文件扩展名匹配。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: PUT
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Vary: Accept-Encoding, User-Agent
Content-Length: 132
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
```

```
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"

...

...

Vary: Accept-Encoding, User-Agent
Content-Length: 132
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UApFDyzE07TNBOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:05:10 GMT
x-token: HeEoZIVgPjRSFT_gQ92UApFDyzE07TNBOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{

"type": "success",

"message": "",

"date": "2020-08-04 13:05:10",

"spent": 4,

...
```

问题 18 / 25

TOC

发现压缩目录

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_hotpic_assemble_control/jaxrs/user/hotpic/filter/
实体：	filter.zip (Page)
风险：	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	除去压缩目录文件或限制对它的访问

推理： AppScan 接收到响应状态“200 OK”，而且内容类型与请求的文件扩展名匹配。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: PUT
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
```

```
HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Content-Length: 132
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAhFlYbuaku1hOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net

...

...

Access-Control-Allow-Origin: http://develop.o2oa.net
Content-Length: 132
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAhFlYbuaku1hOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:05:09 GMT
x-token: HeEoZIVgPjRSFT_gQ92UAhFlYbuaku1hOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{

"type": "success",

"message": "",

"date": "2020-08-04 13:05:09",

"spent": 1,

...
```

问题 19 / 25

TOC

发现压缩目录

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_hotpic_assemble_control/jaxrs/user/hotpic/filter/list/
实体：	list.ear (Page)
风险：	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	除去压缩目录文件或限制对它的访问

推理： AppScan 接收到响应状态“200 OK”，而且内容类型与请求的文件扩展名匹配。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: PUT
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Vary: Accept-Encoding, User-Agent
Content-Length: 132
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"

...

...

Vary: Accept-Encoding, User-Agent
Content-Length: 132
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAnQacD1Vuo2AOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:05:11 GMT
x-token: HeEoZIVgPjRSFT_gQ92UAnQacD1Vuo2AOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{

"type": "success",

"message": "",

"date": "2020-08-04 13:05:11",

"spent": 2,

...
```

问题 20 / 25

TOC

发现压缩目录

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_hotpic_assemble_control/jaxrs/user/hotpic/filter/
实体：	filter.tar (Page)
风险：	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	除去压缩目录文件或限制对它的访问

推理： AppScan 接收到响应状态“200 OK”，而且内容类型与请求的文件扩展名匹配。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: PUT
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Vary: Accept-Encoding, User-Agent
Content-Length: 132
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"

...

...

Vary: Accept-Encoding, User-Agent
Content-Length: 132
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UApFDyzE07TNBOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:05:10 GMT
x-token: HeEoZIVgPjRSFT_gQ92UApFDyzE07TNBOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{

"type": "success",

"message": "",

"date": "2020-08-04 13:05:10",

"spent": 3,

...
```

问题 21 / 25

TOC

发现压缩目录

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_hotpic_assemble_control/jaxrs/user/hotpic/filter/list/
实体：	list.ar (Page)
风险：	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	除去压缩目录文件或限制对它的访问

推理： AppScan 接收到响应状态“200 OK”，而且内容类型与请求的文件扩展名匹配。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: PUT
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Vary: Accept-Encoding, User-Agent
Content-Length: 132
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"

...

...

Vary: Accept-Encoding, User-Agent
Content-Length: 132
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAj-P2BLi3LUBOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:05:12 GMT
x-token: HeEoZIVgPjRSFT_gQ92UAj-P2BLi3LUBOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{
```

```
"type": "success",

"message": "",

"date": "2020-08-04 13:05:12",

"spent": 2,

...
```

问题 22 / 25

TOC

发现压缩目录

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_hotpic_assemble_control/jaxrs/user/hotpic/filter/
实体：	filter.arj (Page)
风险：	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	除去压缩目录文件或限制对它的访问

推理： AppScan 接收到响应状态“200 OK”，而且内容类型与请求的文件扩展名匹配。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: PUT
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Vary: Accept-Encoding, User-Agent
Content-Length: 132
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"

...

...

Vary: Accept-Encoding, User-Agent
Content-Length: 132
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
```

```
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UApFDyzE07TNBOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:05:10 GMT
x-token: HeEoZIVgPjRSFT_gQ92UApFDyzE07TNBOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{

"type": "success",

"message": "",

"date": "2020-08-04 13:05:10",

"spent": 2,

...
```

问题 23 / 25

TOC

发现压缩目录

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_hotpic_assemble_control/jaxrs/user/hotpic/filter/
实体：	filter.arc (Page)
风险：	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	除去压缩目录文件或限制对它的访问

推理： AppScan 接收到响应状态“200 OK”，而且内容类型与请求的文件扩展名匹配。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: PUT
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Vary: Accept-Encoding, User-Agent
Content-Length: 132
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
```

```
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"

...

...

Vary: Accept-Encoding, User-Agent
Content-Length: 132
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UApFDyzE07TNBOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:05:10 GMT
x-token: HeEoZIVgPjRSFT_gQ92UApFDyzE07TNBOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{

"type": "success",

"message": "",

"date": "2020-08-04 13:05:10",

"spent": 2,

...
```

问题 24 / 25

TOC

发现压缩目录

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_hotpic_assemble_control/jaxrs/user/hotpic/filter/
实体：	filter.tar.gz (Page)
风险：	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	除去压缩目录文件或限制对它的访问

推理： AppScan 接收到响应状态“200 OK”，而且内容类型与请求的文件扩展名匹配。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: PUT
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
```

```
HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Vary: Accept-Encoding, User-Agent
Content-Length: 132
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"

...

...

Vary: Accept-Encoding, User-Agent
Content-Length: 132
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UApFDyzE07TNBOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:05:10 GMT
x-token: HeEoZIVgPjRSFT_gQ92UApFDyzE07TNBOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{

"type": "success",

"message": "",

"date": "2020-08-04 13:05:10",

"spent": 2,

...
```

问题 25 / 25

TOC

发现压缩目录	
严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_hotpic_assemble_control/jaxrs/user/hotpic/filter/list/
实体：	list.tar.lzma (Page)
风险：	可能会检索服务器端脚本的源代码，这可能会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	除去压缩目录文件或限制对它的访问

推理： AppScan 接收到响应状态“200 OK”，而且内容类型与请求的文件扩展名匹配。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: PUT
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Vary: Accept-Encoding, User-Agent
Content-Length: 133
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"

...

...

Vary: Accept-Encoding, User-Agent
Content-Length: 133
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "634125391"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAnQacD1Vuo2AOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:05:11 GMT
x-token: HeEoZIVgPjRSFT_gQ92UAnQacD1Vuo2AOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{

"type": "success",

"message": "",

"date": "2020-08-04 13:05:11",

"spent": 27,

...
```

低 归档文件下载 2 TOC

问题 1 / 2 TOC

归档文件下载

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_organization_assemble_personal/jaxrs/definition/forceLayout
实体：	forceLayout (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

推理： AppScan 接收到响应状态“200 OK”，而且内容类型与请求的文件扩展名匹配。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: GET
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Vary: Accept-Encoding, User-Agent
Content-Length: 146
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "856364347"

...

...

Vary: Accept-Encoding, User-Agent
Content-Length: 146
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "856364347"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAvtQAvj-9AeSOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:05:22 GMT
x-token: HeEoZIVgPjRSFT_gQ92UAvtQAvj-9AeSOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{

"type": "success",

"data": "",

"message": "",

"date": "2020-08-04 13:05:22",

...
```

问题 2 / 2

TOC

归档文件下载

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_processplatform_assemble_surface/jaxrs/work/count/083ad4d3-4df1-4f88-b79b-36b810b5c80b
实体：	083ad4d3-4df1-4f88-b79b-36b810b5c80b (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

推理： AppScan 接收到响应状态“200 OK”，而且内容类型与请求的文件扩展名匹配。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: GET
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Vary: Accept-Encoding, User-Agent
Content-Length: 244
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "824817160"

...

...

Vary: Accept-Encoding, User-Agent
Content-Length: 244
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "824817160"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAgKEEhkOcscVOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:05:26 GMT
x-token: HeEoZIVgPjRSFT_gQ92UAgKEEhkOcscVOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{

"type": "success",
"data": {

"task": 0,

"taskCompleted": 0,

...
```

低 过度许可的 CORS 访问测试 3 TOC

问题 1 / 3 TOC

过度许可的 CORS 访问测试	
严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20030/x_program_center/jaxrs/distribute/assemble/source/develop.o2oa.net
实体：	develop.o2oa.net (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	修改“Access-Control-Allow-Origin”头以仅获取允许的站点

推理： AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

未经处理的测试响应：

```
...

Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json; charset=utf-8


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: *
Vary: Accept-Encoding, User-Agent
Content-Length: 4792
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "2486136150"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAkfElwIMIVKbOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:02:54 GMT
x-token: HeEoZIVgPjRSFT_gQ92UAkfElwIMIVKbOBWG66Z0IlyjynyKX8qw5g
```

```
...
```

问题 2 / 3

TOC

过度许可的 CORS 访问测试	
严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_organization_assemble_authentication/jaxrs/authentication/check/credential/huqi
实体：	huqi (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	修改“Access-Control-Allow-Origin”头以仅获取允许的站点

推理： AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

未经处理的测试响应：

```
...

Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json; charset=utf-8


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: *
Vary: Accept-Encoding, User-Agent
Content-Length: 167
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "4126181196"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAqGZUGXfzKk5OBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:02:57 GMT
x-token: HeEoZIVgPjRSFT_gQ92UAqGZUGXfzKk5OBWG66Z0IlyjynyKX8qw5g

...
```

问题 3 / 3

TOC

过度许可的 CORS 访问测试

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_organization_assemble_authentication/jaxrs/authentication
实体：	authentication (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置 可能会劝说初级用户提供诸如用户名、密码、信用卡号、社会保险号等敏感信息
原因：	Web 应用程序编程或配置不安全
固定值：	修改“Access-Control-Allow-Origin”头以仅获取允许的站点

推理： AppScan 检测到“Access-Control-Allow-Origin”头的许可权太多

未经处理的测试响应：

```
...

Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAsoDcGlLWekGOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json; charset=utf-8


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: *
Vary: Accept-Encoding, User-Agent
Content-Length: 2452
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "2116402561"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAjOm5srj4MqrOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:02:55 GMT
x-token: HeEoZIVgPjRSFT_gQ92UAjOm5srj4MqrOBWG66Z0IlyjynyKX8qw5g

...
```

低 会话 cookie 中缺少 HttpOnly 属性 1 TOC

问题 1 / 1

TOC

会话 cookie 中缺少 HttpOnly 属性

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20030/x_program_center/jaxrs/distribute/assemble/source/develop.o2oa.net
实体：	x-token (Cookie)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于模仿合法用户，从而使黑客能够以该用户身份查看或变更用户记录以及执行事务
原因：	Web 应用程序设置了缺少 HttpOnly 属性的会话 cookie
固定值：	向所有会话 cookie 添加“HttpOnly”属性

推理： AppScan 发现所用的会话 cookie 没有“HttpOnly”属性。

原始响应

```
...

Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Vary: Accept-Encoding, User-Agent
Content-Length: 4792
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "2486136150"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAuz9TL6S-X1KOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:04:25 GMT
x-token: HeEoZIVgPjRSFT_gQ92UAuz9TL6S-X1KOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{

"type": "success",

...
```

低 临时文件下载 2 TOC

问题 1 / 2

TOC

临时文件下载

严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_processplatform_assemble_surface/jaxrs/work/count/083ad4d3-4df1-4f88-b79b-36b810b5c80b
实体：	083ad4d3-4df1-4f88-b79b-36b810b5c80b (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

推理： AppScan 接收到响应状态“200 OK”，而且内容类型与请求的文件扩展名匹配。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: GET
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Vary: Accept-Encoding, User-Agent
Content-Length: 244
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "824817160"

...

...

Vary: Accept-Encoding, User-Agent
Content-Length: 244
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "824817160"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAgKEEhkOcscVOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:05:26 GMT
x-token: HeEoZIVgPjRSFT_gQ92UAgKEEhkOcscVOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{

"type": "success",

"data": {

"task": 0,

"taskCompleted": 0,

...
```

问题 2 / 2

TOC

临时文件下载	
严重性：	低
CVSS 分数：	5.0
URL：	http://develop.o2oa.net:20020/x_organization_assemble_personal/jaxrs/definition/forceLayout
实体：	forceLayout (Page)
风险：	可能会下载临时脚本文件，这会泄露应用程序逻辑及其他诸如用户名和密码之类的敏感信息
原因：	在生产环境中留下临时文件
固定值：	除去虚拟目录中的旧版本文件

推理： AppScan 接收到响应状态“200 OK”，而且内容类型与请求的文件扩展名匹配。

未经处理的测试响应：

```
...

Access-Control-Request-Headers: authorization,content-type,x-requested-with,x-token
Origin: http://develop.o2oa.net
Accept: */*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Access-Control-Request-Method: GET
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g


HTTP/1.1 200 OK
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Vary: Accept-Encoding, User-Agent
Content-Length: 146
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "856364347"

...

...

Vary: Accept-Encoding, User-Agent
Content-Length: 146
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
ETag: "856364347"
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAvtQAvj-9AeSOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE
Date: Tue, 04 Aug 2020 05:05:22 GMT
x-token: HeEoZIVgPjRSFT_gQ92UAvtQAvj-9AeSOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json;charset=utf-8

{

"type": "success",
"data": "",

"message": "",

"date": "2020-08-04 13:05:22",

...
```

参 发现电子邮件地址模式 1 TOC

问题 1 / 1 TOC

发现电子邮件地址模式	
严重性：	参考
CVSS 分数：	0.0
URL：	http://develop.o2oa.net/o2_core/o2.min.js
实体：	o2.min.js (Page)
风险：	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置
原因：	Web 应用程序编程或配置不安全
固定值：	除去 Web 站点中的电子邮件地址

推理： 响应包含可能是专用的电子邮件地址。

未经处理的测试响应：

```
...
...ate such as MM/DD/YYYY (i.e. "12/31/1999")',email:'Please enter a valid email address. For
example "fred@domain.com".',url:"Please enter a valid URL such as
http://www.example.com.",currencyDollar:"Please enter a va...

...

...
...os MM/DD/YYYY in (bv. "12/31/1999")',email:'Voer asseblief \'n geldige e-pos adres in.
Byvoorbeeld "fred@domain.com".',url:"Voer asseblief 'n geldige bronadres (URL) soos
http://www.example.com in.",currencyDollar:"...

...

...
... "31/12/1999")',email:'Per favor, introdueix una adreÃ§a de correu electronic valida. Per
exemple, "fred@domain.com".',url:"Per favor introdueix una URL valida com
http://www.example.com.",currencyDollar:"Per favor ...

...

...
...o MM / DD / RRRR (tj. "12/31/1999")',email:'Zadejte prosÃm platnou e-mailovou adresu. NapÅÃ-
klad "fred@domain.com".',url:"Zadejte prosÃm platnou URL adresu jako
http://www.example.com.",currencyDollar:"Zadejte pr...

...

...
...riv dato i formatet DD-MM-YYYY (f.eks. "31-12-1999")',email:'Skriv en gyldig e-mail adresse.
F.eks "fred@domain.com".',url:'Skriv en gyldig URL adresse. F.eks
"http://www.example.com".',currencyDollar:"Skriv et gldi...

...
```

```
...
...12.1999&quot;)",email:"Geben Sie bitte eine g&uuml;ltige E-Mail Adresse ein. Wie zum Beispiel
&quot;maria@bernasconi.ch&quot;.",url:"Geben Sie bitte eine g&uuml;ltige URL ein. Wie zum
Beispiel http://www.example.com.",c...

...

...
...TT.MM.JJJJ ein (z.B. "31.12.1999").',email:'Geben Sie bitte eine gÃ¼ltige E-Mail-Adresse ein
(z.B. "max@mustermann.de").',url:'Geben Sie bitte eine gÃ¼ltige URL ein (z.B.
"http://www.example.com").',currencyDollar:"Ge...

...

...
...µ Î¼Î¹Î± ÎÎ³ÎºÏÏÎ· Î´Î¹ÎµÏÎ¸ÏÎ½ÏÎ· Î·Î»ÎµÎºÏÏÎ¿Î½Î¹ÎºÎ¿Ï ÏÎ±ÏÏÎ´ÏÎ¿Î¼ÎµÎ¯Î¿Ï (Ï.Ï.
"fred@domain.com").',url:"Î Î±ÏÎ±ÎºÎ±Î»Î¿ÏÎ¼Îµ, ÎµÎ¹ÏÎ¬Î³ÎµÏÎµ Î¼Î¹Î± ÎÎ³ÎºÏÏÎ· URL Î´Î¹ÎµÏÎ¸Ï
Î½ÏÎ·, ÏÏÏ...

...

...
...YYYY (p.e. "31/12/1999")',email:'Por favor, ingrese una direcciÃ³n de e-mail vÃ¡lida. Por
ejemplo, "fred@dominio.com".',url:"Por favor ingrese una URL vÃ¡lida como
http://www.example.com.",currencyDollar:"Por favor i...

...

...
...1/12/1999")',email:'Por favor, introduce una direcci&oacute;n de email v&aacute;lida. Por
ejemplo, "fred@domain.com".',url:"Por favor introduce una URL v&aacute;lida como
http://www.example.com.",currencyDollar:"Por...

...

...
...jul MM.DD.YYYY (nÃ¤iteks: "12.31.1999").',email:'Palun sisestage kehtiv e-maili aadress (nÃ
¤iteks: "fred@domain.com").',url:"Palun sisestage kehtiv URL (nÃ¤iteks:
http://www.example.com).",currencyDollar:"Palun sise...

...

...
.../1999").',email:'ÙØ·ÙØ§ ÛÚ© Ø¢Ø¯Ø±Ø³ Ø§ÛÙÛÙ ÙØ¹ØªØ¨Ø± ÙØ§Ø±Ø¯ Ú©ÙÛØ¯. Ø¨Ø±Ø§Û ÙØ«Ø§Ù
"fred@domain.com".',url:"ÙØ·ÙØ§ ÛÚ© URL ÙØ¹ØªØ¨Ø± ÙØ§ÙÙØ¯ http://www.example.com ÙØ§Ø±Ø¯
Ú©ÙÛØ¯.",currency...

...

...
...v (kuten "12/31/1999")',email:'Ole hyvÃ¤ ja anna kelvollinen sÃ¤hkÃ¶postiosoite (kuten
esimerkiksi "matti@meikalainen.com").',url:"Ole hyvÃ¤ ja anna kelvollinen URL, kuten esimerkiksi
http://www.example.com.",currencyDoll...

...

...
... : "31/11/1999").',email:'Veuillez saisir une adresse de courrier &eacute;lectronique. Par
exemple "fred@domaine.com".',url:"Veuillez saisir une URL, comme
http://www.exemple.com.",currencyDollar:"Veuillez saisir une...

...

...
...YY (××× "12/31/1999")',email:'× × ××××× ××ª×××ª ×××××× ×××§××ª. ××××××:
"fred@domain.com".',url:"× × ××××× ××ª×××ª ××ª×¨ ×××§××ª, ×××
http://www.example.com.",currencyDolla...

...

...
...ÃÃÃ.HH.NN. formÃ¡ban. (pl. "1999.12.31.")',email:'ValÃ³s e-mail cÃm megadÃ¡sa szÃ¼ksÃ©ges (pl.
"fred@domain.hu").',url:"ValÃ³s URL megadÃ¡sa szÃ¼ksÃ©ges (pl.
http://www.example.com).",currencyDollar:"ValÃ³s pÃ©...

...
```

```
...
...nel formato MM/GG/AAAA (es.: "12/31/1999")',email:'Inserire un indirizzo email valido. Per
esempio "nome@dominio.com".',url:'Inserire un indirizzo valido. Per esempio
"http://www.example.com".',currencyDollar:'Inseri...

...

...
...formaat MM/DD/YYYY (bijvoorbeeld "12/31/1999")',email:'Vul een geldig e-mailadres in.
Bijvoorbeeld "fred@domein.nl".',url:"Vul een geldige URL in, zoals http...
```

参 发现可能的服务器路径泄露模式 1 TOC

问题 1 / 1 TOC

发现可能的服务器路径泄露模式

严重性：	参考
CVSS 分数：	0.0
URL：	http://develop.o2oa.net/o2_core/o2.min.js
实体：	o2.min.js (Page)
风险：	可能会检索 Web 服务器安装的绝对路径，这可能会帮助攻击者开展进一步攻击和获取有关 Web 应用程序文件系统结构的信息
原因：	未安装第三方产品的最新补丁或最新修补程序
固定值：	为 Web 服务器或 Web 应用程序下载相关的安全补丁

推理： 响应包含服务器上文件的绝对路径和/或文件名。

未经处理的测试响应：

```
...
...\\))?)".replace(/<combinator>/,"["+h(">+~`!@$%^&={}\\;</")+"]").replace(/<unicode>/g,"(?:
[\\w\\u00a1-\\uFFFF-]|\\\\[^\\s0-9a-f])").replace(/<unicode1>/g,"(?:[:\\w\\u00a1-\\uFFFF--
end_hi...

...

...
...eturn new RegExp("(?:"+e.getMsg(t).map((function(e){return e.substr(0,3)})).join("|")+")[a-
z]*")},m=--begin_highlight_tag--{d:/[0-2]?[0-9]|3[01]/,H:/[01]?[0-9]|2[0-3]/--begin_highligh...

...

...
...function(e,t){var i=m[t];return i?(n.push(t),"("+i.source+")"):t})).replace(/\[a-z\]/gi,"[a-
z\\u00c0-\\uffff;&]");return{format:t,re:new RegExp("^"+i+"$","i"),handler:function(t)
{t=t.slice(1).associate(n);var...

...

...
...)||this.className).clean().replace(/'(\\.|[^'])*'|"(\\.|[^"])*"/g,(function(e){return
e.replace(" ","\\x20")})).split(" ")}},Element.Properties.validatorProps={set:function(e){return
this.eliminate("$moo:va...

...
```

参 客户端（JavaScript）Cookie 引用 1 TOC

问题 1 / 1 TOC

客户端（JavaScript）Cookie 引用

严重性：	参考
CVSS 分数：	0.0
URL：	http://develop.o2oa.net/o2_core/o2.min.js
实体：	/*! (Page)
风险：	此攻击的最坏情形取决于在客户端所创建的 cookie 的上下文和角色
原因：	Cookie 是在客户端创建的
固定值：	除去客户端中的业务逻辑和安全逻辑

推理： AppScan 在 JavaScript 中找到对 cookie 的引用。

原始响应

```
...
... this.options.secure&&(e+="; secure"),this.options.httpOnly&&(e+=";
HttpOnly"),this.options.document.cookie=this.key+"="+e,this},read:function(){var
e=this.options.document.cookie.match("(?:^|;)\\s*"+this.key....

...

...
...vent(e,(function(){s[l]||r--,s[l]=arguments,r||(t.call(o,n,a,s),r=i,s=new Array(i))}))})))}}))}
(),Hash.Cookie=new Class({Extends:Cookie,options:{autoSave:!0},initialize:function(e,t)
{this.parent(e,t),this.load()...

...
```

参 应用程序错误 5 TOC

问题 1 / 5

TOC

应用程序错误

严重性：	参考
CVSS 分数：	0.0
URL：	http://develop.o2oa.net:20020/x_processplatform_assemble_surface/jaxrs/work/count/083ad4d3-4df1-4f88-b79b-36b810b5c80b
实体：	[GUID] (Parameter)
风险：	可能会收集敏感的调试信息
原因：	未对入局参数值执行适当的边界检查 未执行验证以确保用户输入与预期的数据类型匹配
固定值：	验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常

推理： 应用程序以错误消息响应，表示可能会泄露敏感信息的未定义状态。

未经处理的测试响应：

```
...

X-Requested-With: XMLHttpRequest
Origin: http://develop.o2oa.net
Accept: text/html,application/json,*/*
authorization: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Accept-Language: en-US,en;q=0.9
x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json; charset=utf-8


HTTP/1.1 500 Internal Server Error
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Content-Length: 241
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAtQY0SpXTqAUOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE

...
```

问题 2 / 5

TOC

应用程序错误

严重性：	参考
CVSS 分数：	0.0
URL：	http://develop.o2oa.net:20020/x_calendar_assemble_control/jaxrs/event/list/filter
实体：	->"startTime" (Parameter)
风险：	可能会收集敏感的调试信息
原因：	未对入局参数值执行适当的边界检查 未执行验证以确保用户输入与预期的数据类型匹配
固定值：	验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常

推理： 应用程序以错误消息响应，表示可能会泄露敏感信息的未定义状态。

未经处理的测试响应：

```
...

x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json; charset=UTF-8

{
 "startTime": "'",
 "endTime": "2020-09-06 00:00:00",
 "createPerson": "huqi@huqi@P"
}

HTTP/1.1 500 Internal Server Error
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Content-Length: 369
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAhmLvTxSAUQWOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE

...
```

问题 3 / 5

TOC

应用程序错误

严重性：	参考
CVSS 分数：	0.0
URL：	http://develop.o2oa.net:20020/x_calendar_assemble_control/jaxrs/event/list/filter
实体：	->"endTime" (Parameter)
风险：	可能会收集敏感的调试信息
原因：	未对入局参数值执行适当的边界检查 未执行验证以确保用户输入与预期的数据类型匹配
固定值：	验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常

推理： 应用程序以错误消息响应，表示可能会泄露敏感信息的未定义状态。

未经处理的测试响应：

```
...

x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json; charset=UTF-8

{
 "startTime": "2020-07-26 00:00:00",
 "endTime": "\u0000",
 "createPerson": "huqi@huqi@P"
}

HTTP/1.1 500 Internal Server Error
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Content-Length: 371
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAtsiwLOGUxcBOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE

...
```

问题 4 / 5

TOC

应用程序错误

严重性：	参考
CVSS 分数：	0.0
URL：	http://develop.o2oa.net:20020/x_calendar_assemble_control/jaxrs/event/list/filter/sample
实体：	->"endTime" (Parameter)
风险：	可能会收集敏感的调试信息
原因：	未对入局参数值执行适当的边界检查 未执行验证以确保用户输入与预期的数据类型匹配
固定值：	验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常

推理： 应用程序以错误消息响应，表示可能会泄露敏感信息的未定义状态。

未经处理的测试响应：

```
...

x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json; charset=UTF-8

{
 "startTime": "2020-08-04 00:00:00",
 "endTime": "\u0000",
 "createPerson": "huqi@huqi@P"
}

HTTP/1.1 500 Internal Server Error
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Content-Length: 370
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAhmLvTxSAUQWOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE

...
```

问题 5 / 5

TOC

应用程序错误

严重性：	参考
CVSS 分数：	0.0
URL：	http://develop.o2oa.net:20020/x_calendar_assemble_control/jaxrs/event/list/filter/sample
实体：	->"startTime" (Parameter)
风险：	可能会收集敏感的调试信息
原因：	未对入局参数值执行适当的边界检查 未执行验证以确保用户输入与预期的数据类型匹配
固定值：	验证参数值是否在其预计范围和类型内。不要输出调试错误消息和异常

推理： 应用程序以错误消息响应，表示可能会泄露敏感信息的未定义状态。

未经处理的测试响应：

```
...

x-token: HeEoZIVgPjRSFT_gQ92UAoJb-dJ_t5ZcOBWG66Z0IlyjynyKX8qw5g
Content-Type: application/json; charset=UTF-8

{
 "startTime": "'",
 "endTime": "2020-08-05 00:00:00",
 "createPerson": "huqi@huqi@P"
}

HTTP/1.1 500 Internal Server Error
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.14.1
Access-Control-Allow-Origin: http://develop.o2oa.net
Content-Length: 369
Access-Control-Allow-Headers: x-requested-with, x-request, x-token, c-token, Content-Type,
Content-Length, x-cipher, x-client, x-debugger, Authorization
Access-Control-Expose-Headers: x-token, c-token
Set-Cookie: x-token=HeEoZIVgPjRSFT_gQ92UAhmLvTxSAUQWOBWG66Z0IlyjynyKX8qw5g; path=/;
domain=.o2oa.net
Access-Control-Allow-Methods: GET, POST, OPTIONS, PUT, DELETE, HEAD, TRACE

...
```