Web 应用程序报告

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 HCL AppScan Standard 创建 10.0.7
扫描开始时间： 2022/6/22 15:17:02

目录

介绍

摘要

按问题类型分类的问题

修复方法

- API Improper Assets Management
- 检测到弱密码：并非所有密码套件均支持完全前向保密
- 弱密码套件 - ROBOT 攻击：服务器支持易受攻击的密码套件
- “Content-Security-Policy”头缺失
- “X-Content-Type-Options”头缺失或不安全
- “X-XSS-Protection”头缺失或不安全
- HTTP Strict-Transport-Security 头缺失或不安全
- 发现可高速缓存的 SSL 页面
- 发现信用卡号模式（MasterCard）
- 检测到 SHA-1 密码套件
- 检测到隐藏目录
- 敏感身份验证（基本）信息泄露
- 在应用程序中发现不必要的 Http 响应头
- 支持较老的 TLS 版本
- "Referral Policy" Security 头缺失
- JSON 中反映的未清理用户输入
- 发现电子邮件地址模式
- 发现可能的服务器路径泄露模式
- 发现内部 IP 泄露模式
- 客户端（JavaScript）Cookie 引用

介绍

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

高严重性问题：	1
中等严重性问题：	2
低严重性问题：	11
参考严重性问题：	15
报告中包含的严重性问题总数：	29
扫描中发现的严重性问题总数：	29

常规信息

扫描文件名称：	CMD-S-0622
扫描开始时间：	2022/6/22 15:17:02
测试策略：	Default
测试优化级别：	快

主机	cmduat.segway-ninebot.com
端口	443
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
会话中检测：	已启用
会话中模式：	`200\s+OK`
跟踪或会话 ID cookie：	
跟踪或会话 ID 参数：	

登陆序列：	`https://cmduat.segway-ninebot.com/login`
	`https://cmduat.segway-ninebot.com/api/rdp-system/i18n/message?locale=zh`
	`https://cmduat.segway-ninebot.com/api/rdp-auth/oauth/token`
	`https://cmduat.segway-ninebot.com/api/rdp-system/client-route/list`

https://cmduat.segway-ninebot.com/api/rdp-user/user/menus
https://cmduat.segway-ninebot.com/api/rdp-system/dict-biz/list
https://cmduat.segway-ninebot.com/api/rdp-system/client/list
https://cmduat.segway-ninebot.com/api/rdp-system/client-route/list
https://cmduat.segway-ninebot.com/api/rdp-user/user/menus
https://cmduat.segway-ninebot.com/api/rdp-project/taskNodeClass/listClassNodes
https://cmduat.segway-ninebot.com/api/rdp-notify/message/self/unread/page?size=10&current=1
https://cmduat.segway-ninebot.com/api/rdp-project/projectTask/queryProjectTask
https://cmduat.segway-ninebot.com/api/rdp-project/projectTask/queryProjectTask
https://cmduat.segway-ninebot.com/api/rdp-cpm-meta//projectInfo/selectAllProjectInfo

摘要

问题类型 20

TOC

	问题类型	问题的数量
高	API Improper Assets Management	1
中	检测到弱密码：并非所有密码套件均支持完全前向保密	1
中	弱密码套件 - ROBOT 攻击：服务器支持易受攻击的密码套件	1
低	“Content-Security-Policy”头缺失	1
低	“X-Content-Type-Options”头缺失或不安全	1
低	“X-XSS-Protection”头缺失或不安全	1
低	HTTP Strict-Transport-Security 头缺失或不安全	1
低	发现可高速缓存的 SSL 页面	1
低	发现信用卡号模式（MasterCard）	1
低	检测到 SHA-1 密码套件	1
低	检测到隐藏目录	1
低	敏感身份验证（基本）信息泄露	1
低	在应用程序中发现不必要的 Http 响应头	1
低	支持较老的 TLS 版本	1
参	"Referral Policy" Security 头缺失	1
参	JSON 中反映的未清理用户输入	3
参	发现电子邮件地址模式	2
参	发现可能的服务器路径泄露模式	4
参	发现内部 IP 泄露模式	2
参	客户端（JavaScript）Cookie 引用	3

有漏洞的 URL 10

TOC

	URL	问题的数量
高	https://cmduat.segway-ninebot.com/api/rdp-system/i18n/message	2
中	https://cmduat.segway-ninebot.com/login	5
低	https://cmduat.segway-ninebot.com/	6
低	https://cmduat.segway-ninebot.com/assets/js/chunk-vendors.50b76844.js	5
低	https://cmduat.segway-ninebot.com/assets/js/index.40582c4f.js	1

参	https://cmduat.segway-ninebot.com/api/rdp-auth/oauth/token	3
参	https://cmduat.segway-ninebot.com/cdn/libs/rz-ui/0.3.22/rzui.umd.min.js	4
参	https://cmduat.segway-ninebot.com/cdn/libs/designer/0.3.58/designer.umd.min.js	1
参	https://cmduat.segway-ninebot.com/cdn/libs/element-ui/2.13.1/index.js	1
参	https://cmduat.segway-ninebot.com/cdn/libs/axios/0.19.2/axios.min.js	1

修订建议 18

TOC

	修复任务	问题的数量
高	Inventory all API hosts and document important aspects of each one of them, focusing on the API environment (e.g., production, staging, test, development), who should have network access to the host (e.g., public, internal, partners) and the API version.When newer versions of API's include security improvements, perform risk analysis to make the decision of the mitigation actions required for the older version API's	1
中	更改服务器的受支持密码套件	3
低	保护敏感信息，避免意外泄露	1
低	查看危险字符注入的可能解决方案	3
低	除去 Web 站点中的电子邮件地址	2
低	除去 Web 站点中的内部 IP 地址	2
低	除去 Web 站点中的信用卡号	1
低	除去客户端中的业务逻辑和安全逻辑	3
低	对禁止的资源发布“404 - Not Found”响应状态代码，或者将其完全除去	1
低	对证书使用不同签名算法。请参阅“修订建议”以获取特定服务器指示信息。	1
低	将服务器配置为使用安全策略的 "Referrer Policy" 头	1
低	将服务器配置为使用安全策略的“Content-Security-Policy”头	1
低	将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头	1
低	将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头	1
低	请勿允许敏感信息泄漏。	1
低	实施具有长“max-age”的 HTTP Strict-Transport-Security 策略	1
低	通过在响应中添加“Cache-Control: no-store”和“Pragma: no-cache”标题，可以阻止高速缓存 SSL 页面。	1
低	为 Web 服务器或 Web 应用程序下载相关的安全补丁	4

安全风险 7

TOC

	风险	问题的数量
高	API Improper Assets Management may lead to gain access to sensitive data, or even takeover the server through old, unpatched API versions.	1
中	可能会窃取或操纵客户会话和 cookie，它们可能用于假冒合法用户，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	7
低	可能会收集有关 Web 应用程序的敏感信息，如用户名、密码、机器名和/或敏感文件位置	13
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	5

低	可能会检索有关站点文件系统结构的信息，这可能会帮助攻击者映射此 Web 站点	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	4	
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	3	

原因 13

TOC

	原因	问题的数量
高	API endpoints are vulnerable to Improper Assets Management since the non-production versions of the API (for example, staging, testing, devlopment, or earlier versions) that are not as well protected as the production API or the older API's and their libraries remain exposed/unpatched.	1
中	Web 服务器或应用程序服务器配置方式不安全	1
中	检测到支持 TLS-RSA 密钥交换的密码套件。具有 TLS 实现缺陷的 Web 服务器或应用程序服务器可能容易受到 ROBOT 攻击。即使存在这个问题也并不一定意味着容易受到攻击。请遵循咨询指南。	1
低	Web 应用程序编程或配置不安全	11
低	浏览器可能已将敏感信息高速缓存	1
低	Web 服务器或应用程序服务器是以不安全的方式配置的	3
参	不安全的 Web 应用程序编程或配置	1
参	当攻击者向受害者的浏览器发送恶意代码（大多数情况下使用 JavaScript）时，会出现跨站脚本攻击 (XSS) 漏洞。易受攻击的 Web 应用程序可能会在不进行过滤或编码的情况下将不受信任的数据嵌入到输出中。这样，攻击者便可以向该应用程序注入恶意脚本，并在响应中返回该脚本。然后，在受害者的浏览器上运行该脚本。	3
参	尤其是，未对用户输入或不受信任的数据正确执行危险字符的清理。	3
参	在反射型攻击中，攻击者诱骗最终用户将包含恶意代码的请求发送到易受攻击的 Web 服务器，然后该服务器将攻击反射回最终用户的浏览器。	3
参	服务器直接从 HTTP 请求接收恶意数据，并将其反射回 HTTP 响应。发送恶意内容的最常见方法是将其作为参数添加到公开发布或通过电子邮件直接发送给受害者的 URL 中。包含恶意脚本的 URL 构成了许多网络钓鱼方案的核心，被诱骗的受害者访问指向易受攻击站点的 URL。然后，该站点将恶意内容反射回受害者，接着受害者的浏览器会执行该内容。	3
参	未安装第三方产品的最新补丁或最新修补程序	4
参	Cookie 是在客户端创建的	3

WASC 威胁分类

TOC

威胁	问题的数量
Improper Assets Management Vulnerability of API	1
服务器配置错误	4
跨站点脚本编制	3
信息泄露	21

按问题类型分类的问题

高 API Improper Assets Management 1 TOC

问题 1 / 1 TOC

API Improper Assets Management

严重性：	高
CVSS 分数：	7.5
URL：	https://cmduat.segway-ninebot.com/api/rdp-system/i18n/message
实体：	message (Page)
风险：	API Improper Assets Management may lead to gain access to sensitive data, or even takeover the server through old, unpatched API versions.
原因：	API endpoints are vulnerable to Improper Assets Management since the non-production versions of the API (for example, staging, testing, devlopment, or earlier versions) that are not as well protected as the production API or the older API's and their libraries remain exposed/unpatched.
固定值：	Inventory all API hosts and document important aspects of each one of them, focusing on the API environment (e.g., production, staging, test, development), who should have network access to the host (e.g., public, internal, partners) and the API version.When newer versions of API's include security improvements, perform risk analysis to make the decision of the mitigation actions required for the older version API's

推理： 测试结果似乎指示存在漏洞，因为测试响应成功（返回 200 OK），这表明应用程序/API 访问成功。

中 检测到弱密码：并非所有密码套件均支持完全前向保密 1 TOC

问题 1 / 1 TOC

检测到弱密码：并非所有密码套件均支持完全前向保密

严重性：	中
CVSS 分数：	5.8
URL：	https://cmduat.segway-ninebot.com/login
实体：	cmduat.segway-ninebot.com (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于假冒合法用户，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 服务器或应用程序服务器配置方式不安全
固定值：	更改服务器的受支持密码套件

推理： 通过使用此处列出的各个弱密码套件成功创建 SSL 连接，AppScan 可以确定该站点使用的是弱密码套件。

验证套件是否使用此处列出的加密型弱密码套件。

服务器支持以下较弱的密码套件：

ID	名称	SSL 版本
47	TLS_RSA_WITH_AES_128_CBC_SHA	TLS 1.2
53	TLS_RSA_WITH_AES_256_CBC_SHA	TLS 1.2
60	TLS_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2
61	TLS_RSA_WITH_AES_256_CBC_SHA256	TLS 1.2
65	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	TLS 1.2
132	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	TLS 1.2
156	TLS_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2
157	TLS_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2
186	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256	TLS 1.2
192	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256	TLS 1.2
49232	TLS_RSA_WITH_ARIA_128_GCM_SHA256	TLS 1.2
49233	TLS_RSA_WITH_ARIA_256_GCM_SHA384	TLS 1.2
49308	TLS_RSA_WITH_AES_128_CCM	TLS 1.2
49309	TLS_RSA_WITH_AES_256_CCM	TLS 1.2
49312	TLS_RSA_WITH_AES_128_CCM_8	TLS 1.2
49313	TLS_RSA_WITH_AES_256_CCM_8	TLS 1.2

中 弱密码套件 - ROBOT 攻击：服务器支持易受攻击的密码套件 1 TOC

问题 1 / 1 TOC

弱密码套件 - ROBOT 攻击：服务器支持易受攻击的密码套件

严重性：	中
CVSS 分数：	6.4
URL：	https://cmduat.segway-ninebot.com/login
实体：	cmduat.segway-ninebot.com (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于假冒合法用户，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：	检测到支持 TLS-RSA 密钥交换的密码套件。具有 TLS 实现缺陷的 Web 服务器或应用程序服务器可能容易受到 ROBOT 攻击。即使存在这个问题也并不一定意味着容易受到攻击。请遵循咨询指南。
固定值：	更改服务器的受支持密码套件

推理： 通过使用此处列出的各个弱密码套件成功创建 SSL 连接，AppScan 可以确定该站点使用的是弱密码套件。

验证套件是否使用此处列出的加密型弱密码套件。

服务器支持以下较弱的密码套件：

ID	名称	SSL 版本
47	TLS_RSA_WITH_AES_128_CBC_SHA	TLS 1.2
53	TLS_RSA_WITH_AES_256_CBC_SHA	TLS 1.2
60	TLS_RSA_WITH_AES_128_CBC_SHA256	TLS 1.2
61	TLS_RSA_WITH_AES_256_CBC_SHA256	TLS 1.2
65	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	TLS 1.2
132	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	TLS 1.2
156	TLS_RSA_WITH_AES_128_GCM_SHA256	TLS 1.2
157	TLS_RSA_WITH_AES_256_GCM_SHA384	TLS 1.2
186	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256	TLS 1.2
192	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256	TLS 1.2
49232	TLS_RSA_WITH_ARIA_128_GCM_SHA256	TLS 1.2
49233	TLS_RSA_WITH_ARIA_256_GCM_SHA384	TLS 1.2
49308	TLS_RSA_WITH_AES_128_CCM	TLS 1.2
49309	TLS_RSA_WITH_AES_256_CCM	TLS 1.2
49312	TLS_RSA_WITH_AES_128_CCM_8	TLS 1.2
49313	TLS_RSA_WITH_AES_256_CCM_8	TLS 1.2

低 “Content-Security-Policy”头缺失 1 TOC

问题 1 / 1 TOC

“Content-Security-Policy”头缺失

严重性：	低
CVSS 分数：	5.0
URL：	https://cmduat.segway-ninebot.com/
实体：	cmduat.segway-ninebot.com (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: https://cmduat.segway-ninebot.com/login
Host: cmduat.segway-ninebot.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
r-auth: bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0ZW5hbnRfaWQiOiIwMDAwMDAiLCJwd2RfdXBkYXRlX3RpbWUiOjE2NTQ4MjY2NDUwMDAsInVzZXJfbmFtZSI6IkFsZXggSGUiLCJyZWFsX25hbWUiOiJBbGV4IEhlIiwiYXZhdGFyIjoiIiwiYXV0aG9yaXRpZXMiOlsiMSJdLCJyb2xlX2lkcyI6IjEiLCJjbGllbnRfaWQiOiJjcG1fbWV0YSIsInJvbGVfbmFtZSI6ImFkbWluaXN0cmF0b3IiLCJsaWNlbnNlIjoicG93ZXJlZCBieSBSZHAiLCJ1c2VyX2lkIjoiMTIlODU5NTQzNTQ1NjM0NDA2NiIsInNjb3BlIjpbImFsbCJ...


HTTP/1.1 200 OK
Server: openresty
Date: Wed, 22 Jun 2022 07:21:09 GMT
Content-Type: application/javascript
Content-Length: 312
Connection: keep-alive
Last-Modified: Tue, 14 Jun 2022 02:46:30 GMT
ETag: "62a7f686-138"
Accept-Ranges: bytes

(window.webpackJsonp=window.webpackJsonp||[]).push([["chunk-2d0b30b7"],{2762:function(e,n,t){"use strict";t.r(n);var a=
{data:function(){return{}}},u=t("2877"),c=Object(u.a)(a,(function(){var e=this.$createElement;return(this._self._c||e)
("downloadTemplate")}),[],!1,null,"903e2e9a",null);n.default=c.exports}}]);
...
```

低 “X-Content-Type-Options”头缺失或不安全 1 TOC

问题 1 / 1

TOC

“X-Content-Type-Options”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	https://cmduat.segway-ninebot.com/
实体：	cmduat.segway-ninebot.com (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: https://cmduat.segway-ninebot.com/login
Host: cmduat.segway-ninebot.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
r-auth: bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0ZW5hbnRfaWQiOiIwMDAwMDAiLCJwd2RfdXBkYXRlX3RpbWUiOjE2NTQ4MjY2NDUwMDAsInVzZXJfbmFtZSI6IkFsZXggSGUiLCJyZWFsX25hbWUiOiJBbGV4IEhlIiwiYXZhdGFyIjoiIiwiYXV0aG9yaXRpZXMiOlsiMSJdLCJyb2xlX2lkcyI6IjEiLCJjbGllbnRfaWQiOiJjcG1fbWV0YSIsInJvbGVfbmFtZSI6ImFkbWluaXN0cmF0b3IiLCJsaWNlbnNlIjoicG93ZXJlZCBieSBSZHAiLCJ1c2VyX2lkIjoiMTI1ODU5NTQzNTQ1NjM0NDA2NiIsInNjb3BlIjpbImFsbCJ...


HTTP/1.1 200 OK
Server: openresty
Date: Wed, 22 Jun 2022 07:20:56 GMT
Content-Type: application/javascript
Content-Length: 336
Connection: keep-alive
Last-Modified: Tue, 14 Jun 2022 02:46:30 GMT
ETag: "62a7f686-150"
Accept-Ranges: bytes

(window.webpackJsonp=window.webpackJsonp||[]).push([["chunk-2d21ab1b"],{bd36:function(n,e,t){"use strict";t.r(e);var r=
{name:"reportForm",props:["code"]},s=t("2877"),o=Object(s.a)(r,(function(){var
n=this.$createElement;return(this._self._c||n)("div",{staticClass:"supplierInformation"})})),
[],!1,null,null,null);e.default=o.exports}}]);
...
```

低 “X-XSS-Protection”头缺失或不安全 1

TOC

问题 1 / 1

TOC

“X-XSS-Protection”头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	https://cmduat.segway-ninebot.com/
实体：	cmduat.segway-ninebot.com (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: https://cmduat.segway-ninebot.com/login
Host: cmduat.segway-ninebot.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36
r-auth: bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0ZW5hbnRfaWQiOiIwMDAwMDAiLCJwd2RfdXBkYXRlX3RpbWUiOjE2NTQ4MjY2NDUwMDAsInVzZXJfbmFtZSI6IkFsZXggSGUiLCJyZWFsX25hbWUiOiJBbGV4IEhlIiwiYXZhdGFyIjoiIiwiYXV0aG9yaXRpZXMiOlsiMSJdLCJyb2xlX2lkcyI6IjEiLCJjbGllbnRfaWQiOiJjcG1fbWV0YSIsInJvbGVfbmFtZSI6ImFkbWluaXN0cmF0b3IiLCJsaWNlbnNlIjoicG93ZXJlZCBieSBSZHAiLCJ1c2VyX2lkIjoiMTI1ODU5NTQzNTQ1NjM0NDA2NiIsInNjb3BlIjpbImFsbCJ...


HTTP/1.1 200 OK
Server: openresty
Date: Wed, 22 Jun 2022 07:20:56 GMT
Content-Type: application/javascript
Content-Length: 336
Connection: keep-alive
Last-Modified: Tue, 14 Jun 2022 02:46:30 GMT
ETag: "62a7f686-150"
Accept-Ranges: bytes

(window.webpackJsonp=window.webpackJsonp||[]).push([["chunk-2d21ab1b"],{bd36:function(n,e,t){"use strict";t.r(e);var r=
{name:"reportForm",props:["code"]},s=t("2877"),o=Object(s.a)(r,(function(){var
n=this.$createElement;return(this._self._c||n)("div",{staticClass:"supplierInformation"})})),
[],!1,null,null,null);e.default=o.exports}}]);
...
```

低 HTTP Strict-Transport-Security 头缺失或不安全 1

TOC

问题 1 / 1

TOC

HTTP Strict-Transport-Security 头缺失或不安全

严重性：	低
CVSS 分数：	5.0
URL：	https://cmduat.segway-ninebot.com/
实体：	cmduat.segway-ninebot.com (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：	实施具有长“max-age”的 HTTP Strict-Transport-Security 策略

推理： AppScan 检测到 HTTP Strict-Transport-Security 响应头缺失或者“max-age”不足

未经处理的测试响应：

```
HTTP/1.1 200 OK
Server: openresty
Date: Wed, 22 Jun 2022 07:20:56 GMT
Content-Type: application/javascript
Content-Length: 336
Connection: keep-alive
Last-Modified: Tue, 14 Jun 2022 02:46:30 GMT
ETag: "62a7f686-150"
Accept-Ranges: bytes

(window.webpackJsonp=window.webpackJsonp||[]).push([["chunk-2d21ab1b"],{bd36:function(n,e,t){"use strict";t.r(e);var r=
{name:"reportForm",props:["code"]},s=t("2877"),o=Object(s.a)(r,(function(){var
n=this.$createElement;return(this._self._c||n)("div",{staticClass:"supplierInformation"})}),
[],!1,null,null,null);e.default=o.exports}}]);...
```

低 发现可高速缓存的 SSL 页面 1

TOC

问题 1 / 1

TOC

发现可高速缓存的 SSL 页面

严重性：	低
CVSS 分数：	5.0
URL：	https://cmduat.segway-ninebot.com/api/rdp-system/i18n/message
实体：	message (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：	浏览器可能已将敏感信息高速缓存
固定值：	通过在响应中添加“Cache-Control: no-store”和“Pragma: no-cache”标题，可以阻止高速缓存 SSL 页面。

推理： 应用程序已进行响应，指示该页面应进行高速缓存，但未设置高速缓存控件（可以设置“Cache-Control: no-store”、“Cache-Control: no-cache”或“Pragma: no-cache”来防止高速缓存）。

未经处理的测试响应：

```
HTTP/1.1 200 OK
Server: openresty
Date: Wed, 22 Jun 2022 07:25:07 GMT
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Rdp-TraceId: Ignored_Trace
X-Frame-Options: SAMEORIGIN

{
 "code": 200,
 "success": true,
 "data": {
         "common": {
                 "changeLang": "        中英文切换",
                 "home": "        简体中文",
                 "title": "en"
         }        ,
         "user": {
...
```

低 发现信用卡号模式（MasterCard） 1 TOC

问题 1 / 1 TOC

发现信用卡号模式（MasterCard）

严重性：	低
CVSS 分数：	5.0
URL：	https://cmduat.segway-ninebot.com/assets/js/chunk-vendors.50b76844.js
实体：	chunk-vendors.50b76844.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 站点中的信用卡号

推理： 响应包含完整的 MasterCard 信用卡号。
未经处理的测试响应：

```
...
...e=r.n(Xe),$e=r(35),Ke=r.n($e),Je=r(49),Qe=r.n(Je),tr=r(130),er=r.n(tr),rr={"
":.3329986572265625,a:.5589996337890625,A:.6569992065429687,b:.58599853515625,B:.6769989013671875,c:.5469985961914062,C:.72
79998779296875,d...

...

...
...6899993896484375,l:.23499908447265624,L:.5879989624023437,m:.854998779296875,M:.8819992065429687,n:.5589996337890625,N:.
7189987182617188,o:.58599853515625,O:.7669998168945312,p:.58599853515625,P:.6419998168945312,q:....

...

...
...ject.defineProperty(e,"__esModule",{value:!0}),e.default=void 0,e.default={"
":.3329986572265625,a:.5589996337890625,A:.6569992065429687,b:.58599853515625,B:.6769989013671875,c:.5469985961914062,C:.72
79998779296875,d...
```

```
...

...
...6899993896484375,l:.23499908447265624,L:.5879989624023437,m:.854998779296875,M:.8819992065429687,n:.5589996337890625,N:.
7189987182617188,o:.58599853515625,O:.7669998168945312,p:.58599853515625,P:.6419998168945312,q:....

...
```

低 检测到 SHA-1 密码套件 1 TOC

问题 1 / 1 TOC

检测到 SHA-1 密码套件

严重性：	低
CVSS 分数：	4.3
URL：	https://cmduat.segway-ninebot.com/login
实体：	cmduat.segway-ninebot.com (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于假冒合法用户，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 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：	更改服务器的受支持密码套件

推理： 通过使用此处列出的各个弱密码套件成功创建 SSL 连接，AppScan 可以确定该站点使用的是弱密码套件。

验证套件是否使用此处列出的加密型弱密码套件。

服务器支持以下较弱的密码套件：

ID	名称	SSL 版本
47	TLS_RSA_WITH_AES_128_CBC_SHA	TLS 1.0
53	TLS_RSA_WITH_AES_256_CBC_SHA	TLS 1.0
65	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	TLS 1.0
132	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	TLS 1.0
49171	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLS 1.0
49172	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLS 1.0
47	TLS_RSA_WITH_AES_128_CBC_SHA	TLS 1.1
53	TLS_RSA_WITH_AES_256_CBC_SHA	TLS 1.1
65	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	TLS 1.1
132	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	TLS 1.1
49171	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLS 1.1
49172	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLS 1.1

47	TLS_RSA_WITH_AES_128_CBC_SHA	TLS 1.2
53	TLS_RSA_WITH_AES_256_CBC_SHA	TLS 1.2
65	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	TLS 1.2
132	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	TLS 1.2
49171	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLS 1.2
49172	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLS 1.2

低 检测到隐藏目录 1 TOC

问题 1 / 1 TOC

检测到隐藏目录

严重性:	低
CVSS 分数:	5.0
URL:	https://cmduat.segway-ninebot.com/
实体:	assets/ (Page)
风险:	可能会检索有关站点文件系统结构的信息，这可能会帮助攻击者映射此 Web 站点
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:	对禁止的资源发布“404 - Not Found”响应状态代码，或者将其完全除去

推理: 测试尝试了检测服务器上的隐藏目录。403 Forbidden 响应暴露了存在此目录，即使不允许对其进行访问。
未经处理的测试响应:

```
...

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
r-auth: bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0ZW5hbnRfaWQiOiIwMDAwMDAiLCJwd2RfdXBkYXRlX3RpbWUiOjE2NTQ4MjY2NDUwMDAsInVzZXJfbmFtZSI6IkFsZXggSGUiLCJyZWFsX25hbWUiOiJBbGV4IEhlIiwiYXZhdGFyIjoiIiwiYXV0aG9yaXRpZXMiOlsiMSJdLCJyb2xlX2lkcyI6IjEiLCJjbGllbnRfaWQiOiJjcG1fbWV0YSIsInJvbGVfbmFtZSI6ImFkbWluaXN0cmF0b3IiLCJsaWNlbnNlIjoicG93ZXJlZCBieSBSZHAiLCJ1c2VyX2lkIjoiMTIlODU5NTQzNTQ1NjM0NDA2NiIsInNjb3BlIjpbImFsbCJ...
Host: cmduat.segway-ninebot.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36


HTTP/1.1 403 Forbidden
Server: openresty
Date: Wed, 22 Jun 2022 07:23:12 GMT
Content-Type: text/html
Content-Length: 555
Connection: keep-alive


...
```

低 敏感身份验证（基本）信息泄露 1

TOC

问题 1 / 1

TOC

敏感身份验证（基本）信息泄露	
严重性：	低
CVSS 分数：	5.0
URL：	https://cmduat.segway-ninebot.com/assets/js/index.40582c4f.js
实体：	index.40582c4f.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：	保护敏感信息，避免意外泄露

推理： 应用程序已发送一个暴露了与认证相关敏感信息的响应。
未经处理的测试响应：

```
...
...Type,mt.a.defaults.headers.common["X-Requested-With"]="XMLHttpRequest",mt.a.defaults.headers.common.
```

低 在应用程序中发现不必要的 Http 响应头 1

TOC

问题 1 / 1

TOC

在应用程序中发现不必要的 Http 响应头	
严重性：	低
CVSS 分数：	5.0
URL：	https://cmduat.segway-ninebot.com/login
实体：	cmduat.segway-ninebot.com (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：	请勿允许敏感信息泄漏。

推理： 响应包含不必要的头，这可能会帮助攻击者计划进一步攻击。
未经处理的测试响应：

```
...
```

```
r-auth: bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0ZW5hbnRfaWQiOiIwMDAwMDAiLCJwd2RfdXBkYXRlX3RpbWUiOjE2NTQ4MjY2NDUwMDAsInVzZXJfbmFtZSI6IkFsZXggSGUiLCJyZWFsX25hbWUiOiJBbGV4IEhlIiwiYXZhdGFyIjoiIiwiYXV0aG9yaXRpZXMiOlsiMSJdLCJyb2xlX2lkcyI6IjEiLCJjbGllbnRfaWQiOiJjcG1fbWV0YSIsInJvbGVfbmFtZSI6ImFkbWluaXN0cmF0b3IiLCJsaWNlbnNlIjoicG93ZXJlZCBieSBSZHAiLCJ1c2VyX2lkIjoiMTI1ODU5NTQzNTQ1NjM0NDA2NiIsInNjb3BlIjpbImFsbCJ...
Host: cmduat.segway-ninebot.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36


HTTP/1.1 200 OK
Server: openresty
Date: Wed, 22 Jun 2022 07:20:56 GMT
Content-Type: text/html
Content-Length: 2474
Connection: keep-alive
Vary: Accept-Encoding
Last-Modified: Tue, 14 Jun 2022 02:46:30 GMT
ETag: "62a7f686-9aa"
Accept-Ranges: bytes


...
```

低 支持较老的 TLS 版本 1

TOC

问题 1 / 1

TOC

支持较老的 TLS 版本

严重性：	低
CVSS 分数：	5.0
URL：	https://cmduat.segway-ninebot.com/login
实体：	cmduat.segway-ninebot.com (Page)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于假冒合法用户，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 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：	对证书使用不同签名算法。请参阅“修订建议”以获取特定服务器指示信息。

推理： AppScan 发现服务器支持较老的 TLS 版本（TLSv1.0 或 TLSv1.1）

未经处理的测试响应：

```
HTTP/1.1 200 OK
Server: openresty
Date: Wed, 22 Jun 2022 07:18:01 GMT
Content-Type: text/html
Content-Length: 2474
Connection: keep-alive
Vary: Accept-Encoding
Last-Modified: Tue, 14 Jun 2022 02:46:30 GMT
ETag: "62a7f686-9aa"
Accept-Ranges: bytes

<!DOCTYPE html><html lang=en><head><meta charset=utf-8><meta update="Tue Jun 14 2022 10:45:13 GMT+0800 (China Standard Time)"><meta http-equiv=X-UA-Compatible content="IE=edge"><meta name=viewport content="width=device-width,initial-scale=1"><link rel=icon href=/logo.png><title>九号电动工程管家</title><link href=/assets/css/chunk-3747e792.120cf1e4.css rel=prefetch><link href=/assets/css/chunk-4a199e48.5f922224.css rel=prefetch><link href=/assets/css/chunk-6bbaf443.20625f77.css
```

rel=prefetch><link href=/assets/css/chunk-6bea370e.dead598c.css rel=prefetch><link href=/assets/css/chunk-b99a48b4.744baf95.css rel=prefetch><link href=/assets/css/chunk-df293294.98b96b86.css rel=prefetch><link href=/assets/css/common.0107074c.css rel=prefetch><link href=/assets/js/chunk-2d0b30b7.5363d1fc.js rel=prefetch><link href=/assets/js/chunk-2d21ab1b.6d640a77.js rel=prefetch><link href=/assets/js/chunk-3747e792.0e0a1a6d.js rel=prefetch><link href=/assets/js/chunk-4a199e48.2f74b586.js rel=prefetch><link href=/assets/js/chunk-6bbaf443.227b7327.js rel=prefetch><link href=/assets/js/chunk-6bea370e.add63f94.js rel=prefetch><link href=/assets/js/chunk-b99a48b4.e09c6021.js rel=prefetch><link href=/assets/js/chunk-df293294.cc949f3f.js rel=prefetch><link href=/assets/js/common.56dfdf75.js rel=prefetch><link href=/assets/css/chunk-vendors.17ce05f9.css rel=preload as=style><link href=/assets/css/index.cc9d40cf.css rel=preload as=style><link href=/assets/js/chunk-vendors.50b76844.js rel=preload as=script><link href=/assets/js/index.40582c4f.js rel=preload as=script><link href=/assets/css/chunk-vendors.17ce05f9.css rel=stylesheet><link href=/assets/css/index.cc9d40cf.css rel=stylesheet></head><body><noscript>We're sorry but 九号电动工程管家 doesn't work properly without JavaScript enabled. Please enable it to continue.<...

参 "Referral Policy" Security 头缺失 1

TOC

问题 1 / 1

TOC

"Referral Policy" Security 头缺失	
严重性:	参考
CVSS 分数:	0.0
URL:	https://cmduat.segway-ninebot.com/
实体:	cmduat.segway-ninebot.com (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:	不安全的 Web 应用程序编程或配置
固定值:	将服务器配置为使用安全策略的 "Referrer Policy" 头

推理: AppScan 检测到 Referrer Policy 响应头缺失或具有不安全的策略，这可能会增加暴露于各种跨站点注入攻击的风险

未经处理的测试响应:

```
HTTP/1.1 200 OK
Server: openresty
Date: Wed, 22 Jun 2022 07:21:00 GMT
Content-Type: text/css
Content-Length: 323
Connection: keep-alive
Last-Modified: Tue, 14 Jun 2022 02:46:30 GMT
ETag: "62a7f686-143"
Accept-Ranges: bytes...
```

参 JSON 中反映的未清理用户输入 3

TOC

问题 1 / 3

TOC

JSON 中反映的未清理用户输入

严重性：	参考
CVSS 分数：	0.0
URL：	https://cmduat.segway-ninebot.com/api/rdp-auth/oauth/token
实体：	grant_type (Global)
风险：	可能会窃取或操纵客户会话和 cookie，它们可能用于假冒合法用户，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：	当攻击者向受害者的浏览器发送恶意代码（大多数情况下使用 JavaScript）时，会出现跨站脚本攻击 (XSS) 漏洞。易受攻击的 Web 应用程序可能会在不进行过滤或编码的情况下将不受信任的数据嵌入到输出中。这样，攻击者便可以向该应用程序注入恶意脚本，并在响应中返回该脚本。然后，在受害者的浏览器上运行该脚本。 尤其是，未对用户输入或不受信任的数据正确执行危险字符的清理。 在反射型攻击中，攻击者诱骗最终用户将包含恶意代码的请求发送到易受攻击的 Web 服务器，然后该服务器将攻击反射回最终用户的浏览器。 服务器直接从 HTTP 请求接收恶意数据，并将其反射回 HTTP 响应。发送恶意内容的最常见方法是将其作为参数添加到公开发布或通过电子邮件直接发送给受害者的 URL 中。包含恶意脚本的 URL 构成了许多网络钓鱼方案的核心，被诱骗的受害者访问指向易受攻击站点的 URL。然后，该站点将恶意内容反射回受害者，接着受害者的浏览器会执行该内容。
固定值：	查看危险字符注入的可能解决方案

推理： 测试结果似乎指示存在脆弱性，因为“全局验证”功能发现在响应中嵌入了脚本，该脚本可能是由先前的测试注入的。

未经处理的测试响应：

```
...
lX2lkcyI6IjEiLCJjbGllbnRfaWQiOiJjcG1fbWV0YSIsInJvbGVfbmFtZSI6ImFkbWluaXN0cmF0b3IiLCJsaWNlbnNlIjoicG93ZXJlZCBieSBSZHAiLCJ1c2
VyX2lkIjoiMTI1ODU5NTQzNTQ1NjM0NDA2NiIsInNjb3BlIjpbImFsbCJdLCJuaWNrX25hbWUiOiJBbGV4IEhlIiwib2F1dGhfaWQiOiIiLCJleHAiOjE2NTY3N
DYzNTQsImRlcHRfaWQiOiIiLCJqdGkiOiI4OWFiYmFkZi02NzMwLTRkMGQtYjM1Zi01ODEyZGFkNjMxMzAiLCJhY2NvdW50IjoiQWxleCBIZSJ9.dvk11Uw9ARy
v_FLThMoP8MJGTNO698rAzyhfDa...
Content-Length: 99

username=Alex%20He&password=**CONFIDENTIAL 0**&grant_type=password<script>alert(483)</script>&scope=all

HTTP/1.1 200 OK
Server: openresty
Date: Wed, 22 Jun 2022 07:25:21 GMT
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Expires: 0
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
X-XSS-Protection: 1; mode=block
Pragma: no-cache
X-Frame-Options: DENY
X-Frame-Options: SAMEORIGIN

...

...

X-Frame-Options: DENY
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000 ; includeSubDomains

{
 "code": 400,
 "success": false,
 "data": null,
 "message": "Unsupported grant type: password<script>alert(483)</script>"
}
...
```

JSON 中反映的未清理用户输入

严重性:	参考
CVSS 分数:	0.0
URL:	https://cmduat.segway-ninebot.com/api/rdp-auth/oauth/token
实体:	token (Global)
风险:	可能会窃取或操纵客户会话和 cookie，它们可能用于假冒合法用户，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:	当攻击者向受害者的浏览器发送恶意代码（大多数情况下使用 JavaScript）时，会出现跨站脚本攻击 (XSS) 漏洞。易受攻击的 Web 应用程序可能会在不进行过滤或编码的情况下将不受信任的数据嵌入到输出中。这样，攻击者便可以向该应用程序注入恶意脚本，并在响应中返回该脚本。然后，在受害者的浏览器上运行该脚本。 尤其是，未对用户输入或不受信任的数据正确执行危险字符的清理。 在反射型攻击中，攻击者诱骗最终用户将包含恶意代码的请求发送到易受攻击的 Web 服务器，然后该服务器将攻击反射回最终用户的浏览器。 服务器直接从 HTTP 请求接收恶意数据，并将其反射回 HTTP 响应。发送恶意内容的最常见方法是将其作为参数添加到公开发布或通过电子邮件直接发送给受害者的 URL 中。包含恶意脚本的 URL 构成了许多网络钓鱼方案的核心，被诱骗的受害者访问指向易受攻击站点的 URL。然后，该站点将恶意内容反射回受害者，接着受害者的浏览器会执行该内容。
固定值:	查看危险字符注入的可能解决方案

推理: 测试结果似乎指示存在脆弱性，因为“全局验证”功能发现在响应中嵌入了脚本，该脚本可能是由先前的测试注入的。

未经处理的测试响应:

```
...
bGV4IEhlIiwib2F1dGhfaWQiOiIiLCJleHAiOjE2NTY3NDYzNTQsImRlcHRfaWQiOiIiLCJqdGkiOiI4OWFiYmFkZi02NzMwLTRkMGQtYjM1Zi01ODEyZGFkNjM
xMzAiLCJhY2NvdW50IjoiQWxleCBIZSJ9.dvk11Uw9ARyv_FLThMoP8MJGTNO698rAzyhfDayD_rI
Content-Length: 250

username=%3E%22%27%3E%3Cscript%3Ealert%28211%29%3C%2Fscript%3E&password=%3E%22%27%3E%3Cscript%3Ealert%28211%29%3C%2Fscript%
3E&grant_type=%3E%22%27%3E%3Cscript%3Ealert%28211%29%3C%2Fscript%3E&scope=%3E%22%27%3E%3Cscript%3Ealert%28211%29%3C%2Fscrip
t%3E

HTTP/1.1 200 OK
Server: openresty
Date: Wed, 22 Jun 2022 07:25:05 GMT
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Expires: 0
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
X-XSS-Protection: 1; mode=block
Pragma: no-cache
X-Frame-Options: DENY
X-Frame-Options: SAMEORIGIN

...

...

X-Frame-Options: DENY
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000 ; includeSubDomains

{
 "code": 400,
 "success": false,
 "data": null,
 "message": "Invalid scope: >\"'><script>alert(211)</script>"
}
...
```

JSON 中反映的未清理用户输入

严重性:	参考
CVSS 分数:	0.0
URL:	https://cmduat.segway-ninebot.com/api/rdp-auth/oauth/token
实体:	scope (Global)
风险:	可能会窃取或操纵客户会话和 cookie，它们可能用于假冒合法用户，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:	当攻击者向受害者的浏览器发送恶意代码（大多数情况下使用 JavaScript）时，会出现跨站脚本攻击 (XSS) 漏洞。易受攻击的 Web 应用程序可能会在不进行过滤或编码的情况下将不受信任的数据嵌入到输出中。这样，攻击者便可以向该应用程序注入恶意脚本，并在响应中返回该脚本。然后，在受害者的浏览器上运行该脚本。 尤其是，未对用户输入或不受信任的数据正确执行危险字符的清理。 在反射型攻击中，攻击者诱骗最终用户将包含恶意代码的请求发送到易受攻击的 Web 服务器，然后该服务器将攻击反射回最终用户的浏览器。 服务器直接从 HTTP 请求接收恶意数据，并将其反射回 HTTP 响应。发送恶意内容的最常见方法是将其作为参数添加到公开发布或通过电子邮件直接发送给受害者的 URL 中。包含恶意脚本的 URL 构成了许多网络钓鱼方案的核心，被诱骗的受害者访问指向易受攻击站点的 URL。然后，该站点将恶意内容反射回受害者，接着受害者的浏览器会执行该内容。
固定值:	查看危险字符注入的可能解决方案

推理: 测试结果似乎指示存在脆弱性，因为“全局验证”功能发现在响应中嵌入了脚本，该脚本可能是由先前的测试注入的。

未经处理的测试响应:

```
...
lX2lkcyI6IjEiLCJjbGllbnRfaWQiOiJjcG1fbWV0YSIsInJvbGVfbmFtZSI6ImFkbWluaXN0cmF0b3IiLCJsaWNlbnNlIjoicG93ZXJlZCBieSBSZHAiLCJ1c2
VyX2lkIjoiMTI1ODU5NTQzNTQ1NjM0NDA2NiIsInNjb3BlIjpbImFsbCJdLCJuaWNrX25hbWUiOiJBbGV4IEhlIiwib2FldGhfaWQiOiIiLCJleHAiOjE2NTY3N
DYzNTQsImRlcHRfaWQiOiIiLCJqdGkiOiI4OWFiYmFkZi02NzMwLTRkMGQtYjM1Zi01ODEyZGFkNjMxMzAiLCJhY2NvdW50IjoiQWxleCBIZSJ9.dvk11Uw9ARy
v_FLThMoP8MJGTNO698rAzyhfDa...
Content-Length: 99

username=Alex%20He&password=**CONFIDENTIAL 0**&grant_type=password&scope=all<script>alert(481)</script>

HTTP/1.1 200 OK
Server: openresty
Date: Wed, 22 Jun 2022 07:25:21 GMT
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Expires: 0
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
X-XSS-Protection: 1; mode=block
Pragma: no-cache
X-Frame-Options: DENY
X-Frame-Options: SAMEORIGIN

...

...

X-Frame-Options: DENY
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000 ; includeSubDomains

{
 "code": 400,
 "success": false,
 "data": null,
 "message": "Invalid scope: all<script>alert(481)</script>"
}
...
```

问题 1 / 2

TOC

发现电子邮件地址模式

严重性：	参考
CVSS 分数：	0.0
URL：	https://cmduat.segway-ninebot.com/assets/js/chunk-vendors.50b76844.js
实体：	chunk-vendors.50b76844.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：

```
...
..._where":"/var/lib/jenkins/workspace/jhke-ninebot-sims-fe","author":{"name":"Fedor
Indutny","email":"fedor@indutny.com"},"bugs":{"url":"https://github.com/indutny/elliptic/issues"},"dependencies":
{"bn.js":"^4.4.0","bro...

...

...
...cense":"MIT","main":"lib/elliptic.js","name":"elliptic","repository":
{"type":"git","url":"git+ssh://git@github.com/indutny/elliptic.git"},"scripts":{"jscs":"jscs benchmarks/*.js lib/*.js
lib/**/*.js lib/**/**/*.js ...

...

...
...where":"/var/lib/jenkins/workspace/jhke-ninebot-sims-fe","author":{"name":"Brian
McKelvey","email":"theturtle32@gmail.com","url":"https://github.com/theturtle32"},"browser":"lib/browser.js","bugs":
{"url":"https://github.com/theturtle32/WebSocket-Node/issues"},"config":{"verbose":false},"contributors":[{"name":"Iñaki
Baz Castillo","email":"ibc@aliax.net","url":"http://dev.sipdoc.net"}],"dependencies":
{"bufferutil":"^4.0.1","debug":"^2.2.0","es5-ext":"...

...

...
...name":"element-ui","peerDependencies":{"vue":"^2.5.17"},"repository":
{"type":"git","url":"git+ssh://git@github.com/ElemeFE/element.git"},"scripts":{"bootstrap":"yarn || npm
i","build:file":"node build/bin/iconInit....

...
```

问题 2 / 2

TOC

发现电子邮件地址模式

严重性：	参考
CVSS 分数：	0.0
URL：	https://cmduat.segway-ninebot.com/cdn/libs/rz-ui/0.3.22/rzui.umd.min.js
实体：	rzui.umd.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：

```
...
...abstract away many browser irregularities. Check the documentation,\n *  grep for things, or ask on
javascript@lists.facebook.com before writing yet\n *  another copy of \"event || window.event\".\n *\n */\n\nvar _populated
= fal...

...
```

参 发现可能的服务器路径泄露模式 4

TOC

问题 1 / 4

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：	https://cmduat.segway-ninebot.com/cdn/libs/designer/0.3.58/designer.umd.min.js
实体：	designer.umd.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：

```
...
...          errStr = \'Parse error on line \'+(yylineno+1)+":\\n"+this.lexer.showPosition()+"\\nExpecting
"+expected.join(\', \') + ", got \'" + this.terminals_[symbol]+ "\'";\n          } else {\n    ...

...

...
...}W\d{2}/,!1],["YYYYDDD",/\d{7}/],["YYYYMM",/\d{6}/,!1],["YYYY",/\d{4}/,!1]],pt=[["HH:mm:ss.SSSS",/\d\d:\d\d:\d\d\.\d+/],
```

```
["HH:mm:ss,SSSS",/\d\d:\d\d:\d\d,\d+/],["HH:mm:ss",/\d
```

问题 2 / 4

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:	https://cmduat.segway-ninebot.com/cdn/libs/element-ui/2.13.1/index.js
实体:	index.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:

```
...
...nction(e){return e.trim()}).filter(function(e){return e}).some(function(e){return/\..+$/.test(e)?r===e:/\/\*$/.test(e)?
s===e.replace(/\/\*$/,""):!!/^[^\/]+\/[^\/]+$/.test(e)&&i===e})})):this.$emit("file",...

...
```

问题 3 / 4

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:	https://cmduat.segway-ninebot.com/assets/js/chunk-vendors.50b76844.js
实体:	chunk-vendors.50b76844.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:

```
...
...tion(t){e(t),r.emit("close")}))}},2801:function(t){t.exports=JSON.parse('{"_args":
[["elliptic@6.5.3","/var/lib/jenkins/workspace/jhke-ninebot-sims-
fe"]],"_development":true,"_from":"elliptic@6.5.3","_id":"el...

...
```

```
...
...cdh"],"_resolved":"http://192.168.1.181:4873/elliptic/-/elliptic-
6.5.3.tgz","_spec":"6.5.3","_where":"/var/lib/jenkins/workspace/jhke-ninebot-sims-fe","author":{"name":"Fedor
Indutny","email":"fedor@indutny....

...

...
...return t.objectMode?16:16384}}},ba0c:function(t){t.exports=JSON.parse('{"_args":
[["websocket@1.0.33","/var/lib/jenkins/workspace/jhke-ninebot-sims-
fe"]],"_development":true,"_from":"websocket@1.0.33","_id":"...

...

...
...],"_resolved":"http://192.168.1.181:4873/websocket/-/websocket-
1.0.33.tgz","_spec":"1.0.33","_where":"/var/lib/jenkins/workspace/jhke-ninebot-sims-fe","author":{"name":"Brian
McKelvey","email":"theturtle32@g...

...

...
...stroyed=!0}},t}();e.default=c},f6f8:function(t){t.exports=JSON.parse('{"_args":[["element-
ui@2.14.1","/var/lib/jenkins/workspace/jhke-ninebot-sims-fe"]],"_from":"element-ui@2.14.1","_id":"element-ui@2.14.1",...

...

...
..."_resolved":"http://192.168.1.181:4873/element-ui/-/element-ui-
2.14.1.tgz","_spec":"2.14.1","_where":"/var/lib/jenkins/workspace/jhke-ninebot-sims-fe","bugs":
{"url":"https://github.com/ElemeFE/element/issues...

...
```

问题 4 / 4

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:	https://cmduat.segway-ninebot.com/cdn/libs/rz-ui/0.3.22/rzui.umd.min.js
实体:	rzui.umd.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:

```
...
... f: F\n      };\n    }\n\n    throw new TypeError(\"Invalid attempt to iterate non-iterable instance.\\nIn order to be
iterable, non-array objects must have a [Symbol.iterator]() method.\");\n  }\n\n  var it...

...

...

"use strict";
eval("__webpack_require__.r(__webpack_exports__);\n/* harmony export (binding) */
__webpack_require__.d(__webpack_exports__, \"default\", function() { return _nonIterableRest; });\nfunction
_nonIterableRest() {\n  throw new TypeError(\"Invalid attempt to destructure non-iterable instance.\\nIn order to be
iterable, non-array objects must have a [Symbol.iterator]() method.\");\n}\n\n//#
sourceURL=webpack://rzui/./node_modules/@babel/runtime/helpers/esm/nonIterableRest.js?");
```

```
...

...

"use strict";
eval("__webpack_require__.r(__webpack_exports__);\n/* harmony export (binding) */
__webpack_require__.d(__webpack_exports__, \"default\", function() { return _nonIterableSpread; });\nfunction
_nonIterableSpread() {\n  throw new TypeError(\"Invalid attempt to spread non-iterable instance.\\nIn order to be iterable,
non-array objects must have a [Symbol.iterator]() method.\");\n}\n\n//#
sourceURL=webpack://rzui/./node_modules/@babel/runtime/helpers/esm/nonIterableSpread.js?");
...

...

eval("function _nonIterableRest() {\n  throw new TypeError(\"Invalid attempt to destructure non-iterable instance.\\nIn
order to be iterable, non-array objects must have a [Symbol.iterator]() method.\");\n}\n\nmodule.exports =
_nonIterableRest;\n\n//# sourceURL=webpack://rzui/./node_modules/@babel/runtime/helpers/nonIterableRest.js?");
...

...

eval("function _nonIterableSpread() {\n  throw new TypeError(\"Invalid attempt to spread non-iterable instance.\\nIn order
to be iterable, non-array objects must have a [Symbol.iterator]() method.\");\n}\n\nmodule.exports =
_nonIterableSpread;\n\n//# sourceURL=webpack://rzui/./node_modules/@babel/runtime/helpers/nonIterableSpread.js?");
...

...
...: \"0 0 348.333 348.333\"\n      }\n    },\n    [\n      _c(\"path\", {\n        attrs: {\n          d:\n
\"M336.559 68.611L231.016 174.165l105.543 105.549c15.699 15.705 15.699 41.145 0 56.85-7...

...

...
...: \"0 0 292.362 292.362\"\n      }\n    },\n    [\n      _c(\"path\", {\n        attrs: {\n          d:\n
\"M286.935 69.377c-3.614-3.617-7.898-5.424-12.848-5.424H18.274c-4.952 0-9.233 1.807-12....

...

...
...der = h(\"div\", {\n          \"class\": \"vue-treeselect__option-arrow-placeholder\"\n        }, [\"\\xA0\"]);\n
return arrowPlaceholder;\n      }\n\n      return null;\n    },\n    renderLabelContai...

...

...
...\": row.id,\n          \"value\": self.selectedRadioRow.id\n          }\n          }, [\"\\xA0\"])]);\n          }\n
}].concat(columns);\n      }\n\n      return columns;\n    }\n  },\n  m...

...

...
.../ max;\n\n  if (max === min) {\n    h = 0; // achromatic\n  } else {\n    switch (max) {\n      case r:\n        h = (g
- b) / d + (g < b ? 6 : 0);\n        break;\n      case g:\n        h = (b - r) / d + 2;\n        break;\n      case b:\n
h = (r - g) / d + 4;\n        break;\n    }\n    h /= 6;\n  }\n\n  return { h: h * 360, s: ...

...

...
... in a path array with directory names there\n// must be no slashes, empty elements, or device names (c:\) in the
array\n// (so also no leading and trailing slashes - it does not distinguish\n// relative ...

...

...
...unction _nonIterableSpread() { throw new TypeError(\"Invalid attempt to spread non-iterable instance.\\nIn order to be
iterable, non-array objects must have a [Symbol.iterator]() method.\"); }\n\nfunction _u...

...

...
...unction _nonIterableSpread() { throw new TypeError(\"Invalid attempt to spread non-iterable instance.\\nIn order to be
iterable, non-array objects must have a [Symbol.iterator]() method.\"); }\n\nfunction _u...

...

...
...unction _nonIterableSpread() { throw new TypeError(\"Invalid attempt to spread non-iterable instance.\\nIn order to be
iterable, non-array objects must have a [Symbol.iterator]() method.\"); }\n\nfunction _u...

...

...
...unction _nonIterableSpread() { throw new TypeError(\"Invalid attempt to spread non-iterable instance.\\nIn ord...
```

问题 1 / 2 TOC

发现内部 IP 泄露模式	
严重性：	参考
CVSS 分数：	0.0
URL：	https://cmduat.segway-ninebot.com/assets/js/chunk-vendors.50b76844.js
实体：	chunk-vendors.50b76844.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 站点中的内部 IP 地址

推理： AppScan 在响应中发现了看似为内部 IP 地址的内容。
未经处理的测试响应：

```
...
...ec":null,"fetchSpec":"6.5.3"},"_requiredBy":["/browserify-sign","/create-
ecdh"],"_resolved":"http://192.168.1.181:4873/elliptic/-/elliptic-
6.5.3.tgz","_spec":"6.5.3","_where":"/var/lib/jenkins/workspace/jhke-nineb...

...

...
...Spec":"1.0.33","saveSpec":null,"fetchSpec":"1.0.33"},"_requiredBy":
["/stompjs"],"_resolved":"http://192.168.1.181:4873/websocket/-/websocket-
1.0.33.tgz","_spec":"1.0.33","_where":"/var/lib/jenkins/workspace/jhke-n...

...

...
...i","rawSpec":"2.14.1","saveSpec":null,"fetchSpec":"2.14.1"},"_requiredBy":
["/"],"_resolved":"http://192.168.1.181:4873/element-ui/-/element-ui-
2.14.1.tgz","_spec":"2.14.1","_where":"/var/lib/jenkins/workspace/jhke...

...
```

问题 2 / 2 TOC

发现内部 IP 泄露模式

严重性：	参考
CVSS 分数：	0.0
URL：	https://cmduat.segway-ninebot.com/cdn/libs/rz-ui/0.3.22/rzui.umd.min.js
实体：	rzui.umd.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 站点中的内部 IP 地址

推理： AppScan 在响应中发现了看似为内部 IP 地址的内容。
未经处理的测试响应：

```
...
...eated: function created() {\n    var _this = this;\n\n    // 导入从阿里图库中下的svg文件\n    var url =
'http://192.168.1.248:10002/common/cdn/libs/fonts/iconfont.svg';\n    this.getText(url).then(function (data) {\n
var...

...
```

参 客户端（JavaScript）Cookie 引用 3 TOC

问题 1 / 3 TOC

客户端（JavaScript）Cookie 引用

严重性：	参考
CVSS 分数：	0.0
URL：	https://cmduat.segway-ninebot.com/assets/js/chunk-vendors.50b76844.js
实体：	(window.webpackJsonp=window.webpackJsonp||[]).push([["chunk-vendors"],{"0040":function(t,e,r){"use s... (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

```
HTTP/1.1 200 OK
Server: openresty
Date: Wed, 22 Jun 2022 07:21:04 GMT
Content-Type: application/javascript
Content-Length: 2168722
Connection: keep-alive
Vary: Accept-Encoding
Last-Modified: Tue, 14 Jun 2022 02:46:30 GMT
```

```
ETag: "62a7f686-211792"
Accept-Ranges: bytes

(window.webpackJsonp=window.webpackJsonp||[]).push([["chunk-vendors"],{"0040":function(t,e,r){"use
strict";t.exports=function(t){return{filterToEnabled:function(e,r){var n={main:[],facade:[]};return e?"string"==typeof e&&
(e=[e]):e=[],t.forEach((function(t){t&&("websocket"===t.transportName&&!1===r.websocket||(e.length&&-
1===e.indexOf(t.transportName)?t.transportName:t.enabled(r)?
(t.transportName,n.main.push(t),t.facadeTransport&&n.facade.push(t.facadeTransport)):t.transportName))})),n}}}},"009a":func
tion(t,e,r){"use strict";r.r(e),r.d(e,"blue",(function(){return x})),r.d(e,"cyan",(function(){return w})),r.d(e,"geekblue",
(function(){return M})),r.d(e,"generate",(function(){return c})),r.d(e,"gold",(function(){return g})),r.d(e,"green",
(function(){return b})),r.d(e,"grey",(function(){return k})),r.d(e,"lime",(function(){return y})),r.d(e,"magenta",
(function(){return S})),r.d(e,"orange",(function(){return v})),r.d(e,"presetDarkPalettes",(function(){return
l})),r.d(e,"presetPalettes",(function(){return f})),r.d(e,"presetPrimaryColors",(function(){return h})),r.d(e,"purple",
(function(){return _})),r.d(e,"red",(function(){return d})),r.d(e,"volcano",(function(){return p})),r.d(e,"yellow",
(function(){return m}));var n=r("66cb"),i=r.n(n),o=[{index:7,opacity:.15},{index:6,opacity:.25},{index:5,opacity:.3},
{index:5,opacity:.45},{index:5,opacity:.65},{index:5,opacity:.85},{index:4,opacity:.9},{index:3,opacity:.95},
{index:2,opacity:.97},{index:1,opacity:.98}];function a(t,e,r){var n;return(n=Math.round(t.h)>=60&&Math.round(t.h)<=240?r?
Math.round(t.h)-2*e:Math.round(t.h)+2*e:r?Math.round(t.h)+2*e:Math.round(t.h)-2*e)<0?n+=360:n>=360&&(n-=360),n}function
s(t,e,r){return 0===t.h&&0===t.s?t.s:((n=r?t.s-.16*e:4===e?t.s+.16:t.s+.05*e)>1&&(n=1),r&&5===e&&n>.1&&(n=.1),n<.06&&
(n=.06),Number(n.toFixe...
```

问题 2 / 3

TOC

客户端（JavaScript）Cookie 引用

严重性：	参考
CVSS 分数：	0.0
URL：	https://cmduat.segway-ninebot.com/cdn/libs/axios/0.19.2/axios.min.js
实体：	/* axios v0.19.2 | (c) 2020 by Matt Zabriskie */ (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

```
HTTP/1.1 200 OK
Server: openresty
Date: Wed, 22 Jun 2022 07:21:00 GMT
Content-Type: application/javascript
Content-Length: 13993
Connection: keep-alive
Vary: Accept-Encoding
Last-Modified: Tue, 14 Jun 2022 02:46:30 GMT
ETag: "62a7f686-36a9"
Accept-Ranges: bytes

/* axios v0.19.2 | (c) 2020 by Matt Zabriskie */
!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t():"function"==typeof define&&define.amd?
define([],t):"object"==typeof exports?exports.axios=t():e.axios=t()}(this,function(){return function(e){function t(r)
{if(n[r])return n[r].exports;var o=n[r]={exports:{},id:r,loaded:!1};return
e[r].call(o.exports,o,o.exports,t),o.loaded=!0,o.exports}var n={};return t.m=e,t.c=n,t.p="",t(0)}([function(e,t,n)
{e.exports=n(1)},function(e,t,n){"use strict";function r(e){var t=new s(e),n=i(s.prototype.request,t);return
o.extend(n,s.prototype,t),o.extend(n,t),n}var o=n(2),i=n(3),s=n(4),a=n(22),u=n(10),c=r(u);c.Axios=s,c.create=function(e)
{return r(a(c.defaults,e))},c.Cancel=n(23),c.CancelToken=n(24),c.isCancel=n(9),c.all=function(e){return
Promise.all(e)},c.spread=n(25),e.exports=c,e.exports.default=c},function(e,t,n){"use strict";function r(e){return"[object
Array]"===j.call(e)}function o(e){return"undefined"==typeof e}function i(e){return
null!==e&&!o(e)&&null!==e.constructor&&!o(e.constructor)&&"function"==typeof
e.constructor.isBuffer&&e.constructor.isBuffer(e)}function s(e){return"[object ArrayBuffer]"===j.call(e)}function a(e)
{return"undefined"!=typeof FormData&&e instanceof FormData}function u(e){var t;return t="undefined"!=typeof
ArrayBuffer&&ArrayBuffer.isView?ArrayBuffer.isView(e):e&&e.buffer&&e.buffer instanceof ArrayBuffer}function c(e)
{return"string"==typeof e}function f(e){return"number"==typeof e}function p(e){return null!==e&&"object"==typeof e}function
d(e){return"[object Date]"===j.call(e)}function l(e){return"[object File]"===j.call(e)}function h(e){re...
```

客户端（JavaScript）Cookie 引用

严重性：	参考
CVSS 分数：	0.0
URL：	https://cmduat.segway-ninebot.com/cdn/libs/rz-ui/0.3.22/rzui.umd.min.js
实体：	(function webpackUniversalModuleDefinition(root, factory) { (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

```
HTTP/1.1 200 OK
Server: openresty
Date: Wed, 22 Jun 2022 07:21:09 GMT
Content-Type: application/javascript
Content-Length: 5917571
Connection: keep-alive
Vary: Accept-Encoding
Last-Modified: Tue, 14 Jun 2022 02:46:30 GMT
ETag: "62a7f686-5a4b83"
Accept-Ranges: bytes

(function webpackUniversalModuleDefinition(root, factory) {
 if(typeof exports === 'object' && typeof module === 'object')
        module.exports = factory(require("vue"));
 else if(typeof define === 'function' && define.amd)
        define([], factory);
 else if(typeof exports === 'object')
        exports["rzui"] = factory(require("vue"));
 else
        root["rzui"] = factory(root["Vue"]);
...
```

修复方法

API Improper Assets Management

TOC

原因：

API endpoints are vulnerable to Improper Assets Management since the non-production versions of the API (for example, staging, testing, devlopment, or earlier versions) that are not as well protected as the production API or the older API's and their libraries remain exposed/unpatched.

风险：

API Improper Assets Management may lead to gain access to sensitive data, or even takeover the server through old, unpatched API versions.

修订建议：

常规

Document API hosts and important aspects of each one of them, focusing on the API environment (e.g., production, staging, test, development), as well as access control to each respective version. When newer versions of API's include security improvements, perform a risk analysis to take a decision of the mitigation and actions required to protect older versions

CWE:

1059

外部引用：

API Security

检测到弱密码：并非所有密码套件均支持完全前向保密

TOC

原因：

Web 服务器或应用程序服务器配置方式不安全

风险：

一旦主机的私钥被泄露，攻击者便可通过生成密钥来解密安全通信
AppScan 检测到不支持完全前向保密 (PFS) 的弱密码套件
如果主机不支持 PFS，则在大多数情况下，当客户机与服务器建立连接时，客户机使用服务器的公钥对预主密钥进行加密，然后将其发送到服务器。然后，服务器使用其私钥来解密预主密钥，以便客户机和服务器可以使用预主密钥生成会话密钥。如果主机的私钥被泄露，攻击者可以解密预主密钥，然后生成用于安全通信的密钥。有可能会出现这种情况，因为系统不会为客户机和服务器之间的每个通信会话生成唯一的会话密钥。例如，当使用 DHE - Diffie-Hellman Ephemeral 或 ECDHE - Elliptic Curve Diffie-Hellman Ephemeral 临时密钥交换时，可以实现此类通信。使用 PFS，客户机和服务器之间的每个新会话都会生成新的随机密钥，以创建预主密钥。因此，即使其中一个密钥被泄露，攻击者也只能破解客户机和服务器之间的一个会话，而不是之前的所有通信会话。

受影响产品：

不支持 DHE 和 ECDHE 密钥交换的密码套件

修订建议：

常规

通过使用带有 Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) 和 Diffie-Hellman Ephemeral (DHE) 密钥交换的密码套件来支持 PFS。

CWE:

327

外部引用：

维基百科：完全前向保密
RFC：完全前向保密

弱密码套件 - ROBOT 攻击：服务器支持易受攻击的密码套件

TOC

原因：

检测到支持 TLS-RSA 密钥交换的密码套件。具有 TLS 实现缺陷的 Web 服务器或应用程序服务器可能容易受到 ROBOT 攻击。即使存在这个问题也并不一定意味着容易受到攻击。请遵循咨询指南。

风险：

攻击者可以获得解密后的 RSA 密文或使用服务器的私钥对任意消息进行签名。这种攻击允许攻击者解密易受攻击主机的记录流量。
“ROBOT – Bleichenbacher 的 Oracle 威胁回归”攻击适用于 TLS-RSA 密钥交换，以 TLS_RSA 开头的所有密码套件名称都使用该密钥交换。攻击可能会利用易受攻击的服务器，该服务器根据密文有效性以不同的消息进行响应。该攻击依赖于 RSA 的灵活性，允许拥有 RSA 公钥的任何人乘以加密的明文，并采用 PKCS #1 v1.5 填充格式，使攻击者有较高的概率创建有效消息。
在支持使用 RSA 加密（TLS_RSA 密码）的 TLS 密码模式的 TLS 实现中，存在缺陷的主机容易受到 ROBOT 攻击。

受影响产品：

如需受影响产品的列表，请参阅 https://robotattack.org/#patches

修订建议：

常规

如果您使用的是易受攻击的产品，请检查修补程序和更新
修补程序和受影响的产品列表可能会不时更改。有修补程序和受影响产品的更多信息，请参阅 https://robotattack.org/#patches
此外，还建议在 TLS 中完全弃用基于 RSA 加密的密钥交换，因为它不提供前向保密。

CWE:

203

外部引用：

F5：BIG-IP SSL 漏洞
Citrix：Citrix NetScaler 应用交付控制器 (ADC) 和 NetScaler 网关中的 TLS 填充 Oracle 漏洞
Radware：CVE-2017-17427
Cisco ACE 和 Cisco ASA：对影响 Cisco 产品的 TLS 发起的 Bleichenbacher 攻击
Bouncy Castle：1.59 测试版 9
Bouncy Castle：修补/提交
Erlang：OTP 18.3.4.7
Erlang：OTP 19.3.6.4
Erlang：OTP 20.1.7
WolfSSL：Github PR/修补程序
Palo Alto Networks：PAN-OS 暴露于 ROBOT 攻击
IBM GSKit：IBM i 受 GSKIT 漏洞影响
IBM GSKit：IBM HTTP Server 中的信息泄露
IBM GSKit：WebSphere MQ 容易通过有效和无效 PKCS#1 填充之间的差异来泄露边信道信息
Unisys ClearPath MCP：MCP TLS 易受 ROBOT 攻击
Symantec IntelligenceCenter 和 Symantec SSL 漏洞 (SSLV)：SA160 Bleichenbacher 的 Oracle 威胁回归 (ROBOT)
Cavium Nitro/Octeon：CVE-2017-17428
FortiGuard SSL 深度检测和 FortiGuard VIP SSL：PSIRT 咨询 FG-IR-17-302
Haskell-TLS：对 RSA 错误（可能是 Bleichenbacher/ROBOT 攻击）的回答不一致
MatrixSSL：CVE-2016-6883
Java / JSSE : Oracle 重要修补程序更新公告 - 2012 年 10 月
ROBOT 攻击的详细信息

“Content-Security-Policy”头缺失

TOC

原因：

Web 应用程序编程或配置不安全

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
CSP 值缺失或不当会导致 Web 应用程序容易受到 XSS、点击劫持等的攻击。
“Content-Security-Policy”头旨在修改浏览器呈现页面的方式，从而防止各种跨站点注入，包括跨站点脚本编制。以不会妨碍 Web 站点正常运行的方式正确设置头值非常重要。例如，如果头设置为阻止执行内联 JavaScript，则 Web 站点不得在其页面中使用内联 JavaScript。
要防止跨站点脚本编制攻击、跨框架脚本编制攻击和点击劫持，请务必使用正确的值设置以下策略：
“default-src”和“frame-ancestors”策略*或*“script-src”、“object-src”和“frame-ancestors”策略
对于“default-src”、“script-src”和“object-src”，应避免使用不安全的值，例如“*”、“data:”、“unsafe-inline”或“unsafe-eval”。
对于“frame-ancestors”，应避免使用不安全的值，例如“*”或“data:”。
请参考以下链接以获取更多信息。
请注意，“Content-Security-Policy”包括四种不同的测试。 验证是否正在使用“Content-Security-Policy”头的常规测试以及检查“Frame-Ancestors”、“Object-Src”和“Script-Src”是否正确配置的三个附加测试。

受影响产品：

此问题可能影响不同类型的产品

修订建议：

常规

配置服务器以发送“Content-Security-Policy”头。
建议将 Content-Security-Policy 头配置为其指令的安全值，如下所示：
对于“default-src”、“script-src”和“object-src”，需要使用诸如“none”、“self”、https://any.example.com 之类的安全值。
对于“frame-ancestors”，需要使用诸如“self”、“none”或 https://any.example.com 之类的安全值。
在任何情况下都不得使用“unsafe-inline”和“unsafe-eval”。使用 nonce/hash 只会被视为短期解决方法。
关于 Apache，请参阅：
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
关于 IIS，请参阅：
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
关于 nginx，请参阅：
http://nginx.org/en/docs/http/ngx_http_headers_module.html

CWE:

1032

外部引用：

一些安全头的列表
内容安全策略简介
MDN Web 文档 - 内容安全策略

“X-Content-Type-Options”头缺失或不安全

TOC

原因：

Web 应用程序编程或配置不安全

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。
“X-Content-Type-Options”头（具有“nosniff”值）防止 IE 和 Chrome 忽略响应的内容类型。
此操作可能防止不可信内容（例如，用户上载内容）在用户浏览器上执行（例如，在恶意命名之后）。

受影响产品：

此问题可能影响不同类型的产品

修订建议：

常规

将服务器配置为针对所有外发请求发送具有值“nosniff”的“X-Content-Type-Options”头。
关于 Apache，请参阅：
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
关于 IIS，请参阅：
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
关于 nginx，请参阅：
http://nginx.org/en/docs/http/ngx_http_headers_module.html

CWE:

200

外部引用：

有用 HTTP 头列表
减少 MIME 类型安全风险

“X-XSS-Protection”头缺失或不安全

TOC

原因：

Web 应用程序编程或配置不安全

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。
值为‘1’的“X-XSS-Protection”报头强制跨站点脚本编制过滤器进入启用模式，即使用户已禁用。
此过滤器内置于最新版本的 Web 浏览器（IE 8 +、Chrome 4+）中，在缺省情况下通常为已启用状态。虽然此过滤器不是第一个也不是唯一一个针对跨站点脚本编制的防御程序，但它可以作为额外保护层。

受影响产品：

此问题可能影响不同类型的产品

修订建议：

常规

配置您的服务器，以确保在所有传出请求上发送值为“1”（即已启用）的“X-XSS-Protection”报头。
关于 Apache，请参阅：
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
关于 IIS，请参阅：
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
关于 nginx，请参阅：
http://nginx.org/en/docs/http/ngx_http_headers_module.html

CWE:

200

外部引用：

有用 HTTP 头列表
IE XSS 过滤器

HTTP Strict-Transport-Security 头缺失或不安全

TOC

原因：

Web 应用程序编程或配置不安全

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。
HTTP 严格传输安全 (HSTS) 是防止安全的 (HTTPS) 网站降级为不安全的 HTTP 网站的一种机制。该机制可让 Web 服务器指导其客户机（Web 浏览器或其他用户代理程序）在与该服务器交互时使用安全的 HTTPS 连接，禁止使用不安全的 HTTP 协议。
请务必将'max-age'设置为一个足够高的值，以防止过早地回到不安全连接。
HTTP 严格传输安全策略由服务器使用名为"Strict-Transport-Security"的响应头传达给其客户机。此响应头的值是一个时间段，在此时间段内客户机应仅以 HTTPS 访问服务器。其他响应头属性包括"includeSubDomains"和"preload"。

受影响产品：

此问题可能影响不同类型的产品。

修订建议：

常规

通过将"Strict-Transport-Security"响应头添加到 Web 应用程序响应来实施 HTTP 严格传输安全策略。
有关更多信息，请参阅
https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html

CWE:

200

外部引用：

OWASP"HTTP 严格传输安全"
HSTS 规范

发现可高速缓存的 SSL 页面

TOC

原因：

浏览器可能已将敏感信息高速缓存

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
缺省情况下，大部分 Web 浏览器都配置成会在使用期间高速缓存用户的页面。 这表示也会高速缓存 SSL 页面。不建议让 Web 浏览器保存任何 SSL 信息，因为当有漏洞存在时，可能会危及这个信息。

受影响产品：

该问题可能会影响各种类型的产品。

修订建议：

常规

在所有 SSL 页面及含有敏感数据的所有页面上，禁用高速缓存。
通过使用你您 SSL 页面标题中的“Cache-Control: no-store”和“Pragma: no-cache”或“Cache-Control: no-cache”响应伪指令来实现此操作。
Cache-Control: private - 此伪指令可向代理指示某个页面中包含私有信息，因此不能由共享高速缓存进行高速缓存。但是，它不会指示浏览器阻止高速缓存此页面。
Cache-Control：no-cache - 此伪指令也可向代理指示某个页面中包含私有信息，因此不能高速缓存。它还会指示浏览器重新验证服务器以检查是否有新的版本可用。这意味着浏览器可能会存储敏感页面或要在重新验证中使用的信息。某些浏览器不一定会跟踪 RFC，因此可能会将 no-cache 视为 no-store。
Cache-Control：no-store - 这是最安全的伪指令。它同时指示代理和浏览器不要高速缓存此页面或将其存储为它们的高速缓存文件夹。
Pragma: no-cache - 对于不支持高速缓存控制标题的较旧浏览器，该伪指令是必需的。

CWE:

525

发现信用卡号模式（MasterCard）

TOC

原因：

Web 应用程序编程或配置不安全

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
AppScan 检测到包含完整 MasterCard 信用卡号码的响应。
基于安全和隐私权考虑，信用卡号码不应出现在 web 页面中。

受影响产品：

该问题可能会影响各种类型的产品。

修订建议：

常规

请克制，避免将信用卡号码包含在 web 站点中。

CWE:

200

检测到 SHA-1 密码套件

TOC

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

风险：

它可能窃取或操纵客户会话和 cookie，这可能用于假冒合法用户，从使攻击者能够查看或更改用户记录，并以该用户的身份执行事务。
服务器支持 SHA-1 密码套件。
NIST 在 2011 年淘汰了 SHA-1，但是许多应用程序仍然依赖它。
直到目前 (2017) 为止，已知只有推论上的攻击是针对 SHA-1，这就是为何许多应用程序仍然依赖它的原因。
最近，CWI Amsterdam 和 Google Research 团队（[1] 和 [2]）才引入实际的攻击。

受影响产品：

该问题可能会影响各种类型的产品。

修订建议：

常规

安全密码套件最佳实践：
[1]
链接：现代兼容性
[2]
链接：SSL 和 TLS 部署最佳实践：使用安全密码套件

CWE:

327

外部引用：

[1] SHATTERED
[2] 完整 SHA-1 的第一个冲突

检测到隐藏目录

TOC

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

风险：

可能会检索有关站点文件系统结构的信息，这可能会帮助攻击者映射此 Web 站点
Web 应用程序显现了站点中的目录。虽然目录并没有列出其内容，但此信息可以帮助攻击者发展对站点进一步的攻击。例如，知道目录名称之后，攻击者便可以猜测它的内容类型，也许还能猜出其中的文件名或子目录，并尝试访问它们。
内容的敏感度越高，此问题也可能越严重。

受影响产品：

该问题可能会影响各种类型的产品。

修订建议：

常规

如果不需要禁止的资源，请将其从站点中除去。
可能的话，请发出改用“404 — 找不到”响应状态代码，而不是“403 — 禁止”。这项更改会将站点的目录模糊化，可以防止泄漏站点结构。

CWE:

200

敏感身份验证（基本）信息泄露

TOC

原因：

Web 应用程序编程或配置不安全

风险：

可以收集有关 Web 服务器类型、版本、操作系统等的敏感信息。
基本身份验证策略采用用户名和密码，Base64 对它们进行编码，并将结果值写入变量。结果值采用 Basic Base64EncodedString 形式，通常在 Authorization 头中发送。由于该策略使用易于解码的 Base64 编码技术，攻击者可以获取机密信息。

受影响产品：

此问题可能影响不同类型的产品。

修订建议：

常规

避免在响应中发送授权或身份验证相关信息。

CWE:

200

外部引用：

防止信息泄露
信息泄露

在应用程序中发现不必要的 Http 响应头

TOC

原因：

Web 应用程序编程或配置不安全

风险：

无法收集有关 Web 服务器类型、版本、操作系统等敏感信息。
AppScan 检测到不必要的 Http 响应头。
出于安全和隐私考虑，Web 页面中不应出现 Http 响应头，例如“Server”、“X-Powered-By”、“X-AspNetMvc-Version”和“X-AspNet-Version”。
“Server”头是通常在服务器每次将响应发送到客户端时缺省添加的头。
“X-Powered-By”头是在服务器每次将响应发送到客户端时可能缺省添加的头。
这些添加的头可能会泄露有关内部服务器软件版本和类型的敏感信息，从而使攻击者可以对其进行指纹识别并使用有针对性的漏洞进行攻击。
此外，在公布新的漏洞后，服务器很可能会受到该漏洞的攻击。

受影响产品：

该问题可能会影响各种类型的产品。

修订建议：

常规

配置服务器，从要发送给所有传出请求的内容中删除缺省“服务器”头。
对于 IIS，请参阅：
链接：设置 IIS 响应头
对于 nginx，请参阅：
链接：设置 nginx 响应头
对于 Weblogic，请参阅：
链接：设置 Weblogic 响应头
对于 Apache，请参阅：
链接：设置 Apache 响应头

CWE:

200

外部引用：

指纹
防止信息泄露

支持较老的 TLS 版本

TOC

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

风险：

可能会窃取或操纵客户会话和 cookie，它们可能用于假冒合法用户，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
服务器支持不提供加密或使用弱加密算法的 TLS 密码套件。因此攻击者可能能够
解密客户机与服务器之间的安全通信，或成功对客户机实施“man-in-the-middle”攻击，
使其能够查看敏感信息并代表客户机执行操作。

受影响产品：

此问题可能影响不同类型的产品。

修订建议：

常规

重新配置服务器以避免使用弱密码套件。此配置更改特定于服务器。
对于 Microsoft Windows XP 和 Microsoft Windows Server 2003，请按照以下说明操作：
http://support.microsoft.com/kb/245030
对于 Microsoft Windows Vista、Microsoft Windows 7 和 Microsoft Windows Server 2008，请按照以下说明操作，从受支持密码套件列表中移除标识为弱的密码套件：
http://msdn.microsoft.com/en-us/library/windows/desktop/bb870930(v=vs.85).aspx
对于 Apache TomCat 服务器，请按照以下说明操作：
https://www.owasp.org/index.php/Talk:Securing_tomcat#Disabling_weak_ciphers_in_Tomcat
对于 Apache 服务器，请按照以下说明操作：
https://httpd.apache.org/docs/trunk/ssl/ssl_howto.html

CWE:

327

外部引用：

正在弃用 TLS 1.0 和 1.1

"Referral Policy" Security 头缺失

TOC

原因：

不安全的 Web 应用程序编程或配置

风险：

可能会收集有关 Web 应用程序的敏感信息，例如用户名、密码、计算机名称和/或敏感文件位置
可能会诱使防备心不强的用户提供敏感信息，如用户名、密码、信用卡号、社会保险号等
缺少 Referrer Policy 或 Referrer Policy 的值不正确会导致 URL 本身泄露，甚至包含在 URL 中的敏感信息也会泄露到跨站点。
这是规则集的一部分，用于检查 Referrer Policy 是否存在，如果存在则测试其配置。“Referer Policy”头定义了在 Referer 头中可用的数据，用于目标位置 (document.referrer) 中的导航和 iframe。该头被设计用来修改浏览器呈现页面的方式，从而防止跨域 Referer 泄露。请务必要正确设置该头值，以免妨碍网站的正常运行。
Referer 头是一个请求报头，它指示流量来自哪个站点。如果没有适当的预防措施，URL 本身，甚至包含在 URL 中的敏感信息都会泄露到跨站点。
“no-referrer-when-downgrade”和“unsafe-url”是泄露第三方网站完整 URL 的策略。其余策略包括“no-referrer”、“origin”、“origin-when-cross-origin”、“same-origin”、“strict-origin”、“strict-origin-when-cross-origin”。
请参考以下链接获取更多信息。

受影响产品：

此问题可能会影响不同类型的产品

修订建议：

常规

配置您的服务器以发送“Referrer Policy”头。
建议使用其指令的安全值配置 Referrer Policy 头，如下所示：
“strict-origin-when-cross-origin”提供了更多的隐私。使用此策略，仅在跨源请求的 Referer 头中发送源。
对于 Google Chrome，请参见：
https://developers.google.com/web/updates/2020/07/referrer-policy-new-chrome-default
对于 Firefox，请参见：
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy.

CWE:

200

外部引用：

MDN Web 文档 - Referrer-Policy

JSON 中反映的未清理用户输入

TOC

原因：

- 当攻击者向受害者的浏览器发送恶意代码（大多数情况下使用 JavaScript）时，会出现跨站脚本攻击 (XSS) 漏洞。易受攻击的 Web 应用程序可能会在不进行过滤或编码的情况下将不受信任的数据嵌入到输出中。这样，攻击者便可以向该应用程序注入恶意脚本，并在响应中返回该脚本。然后，在受害者的浏览器上运行该脚本。
- 尤其是，未对用户输入或不受信任的数据正确执行危险字符的清理。
- 在反射型攻击中，攻击者诱骗最终用户将包含恶意代码的请求发送到易受攻击的 Web 服务器，然后该服务器将攻击反射回最终用户的浏览器。
- 服务器直接从 HTTP 请求接收恶意数据，并将其反射回 HTTP 响应。发送恶意内容的最常见方法是将其作为参数添加到公开发布或通过电子邮件直接发送给受害者的 URL 中。包含恶意脚本的 URL 构成了许多网络钓鱼方案的核心，被诱骗的受害者访问指向易受攻击站点的 URL。然后，该站点将恶意内容反射回受害者，接着受害者的浏览器会执行该内容。

风险：

XSS 攻击会暴露用户的会话 Cookie，从而使攻击者可以劫持用户的会话并获得对用户帐户的访问权限，以便假冒用户的身份。
攻击者可以修改和查看用户的记录，并以这些用户的身份执行交易。攻击者能够代表该用户执行特权操作，或者获得对属于该用户的任何敏感数据的访问权限。如果该用户具有管理员权限，那么将特别危险。
攻击者甚至可以在受害者的浏览器上运行恶意脚本，该脚本会将用户重定向到其他页面或站点，修改内容表示，甚至使运行恶意软件或加密矿工成为可能。

利用示例：

以下示例显示的脚本在响应中返回了一个参数值。
使用 GET 请求将该参数值发送至脚本，然后在嵌入 HTML 的响应中返回该参数值。

```
[REQUEST]
GET /index.aspx?name=JSmith HTTP/1.1
```

```
[RESPONSE]
HTTP/1.1 200 OK
Server: SomeServer
Date: Sun, 01 Jan 2002 00:31:19 GMT
```

```
Content-Type: text/html
Accept-Ranges: bytes
Content-Length: 27

<HTML>
Hello JSmith
</HTML>
```

攻击者可能会利用这种攻击。在这种情况下，浏览器将执行 JavaScript 代码。

```
[REQUEST]
GET /index.aspx?name=>"'><script>alert('XSS')</script> HTTP/1.1
```

```
[RESPONSE]
HTTP/1.1 200 OK
Server: SomeServer
Date: Sun, 01 Jan 2002 00:31:19 GMT
Content-Type: text/html
Accept-Ranges: bytes
Content-Length: 83

<HTML>
Hello >"'><script>alert('XSS')</script>
</HTML>
```

修订建议：

常规

对插入网页的不受信任的来源发送的所有动态数据进行完全编码，以确保将其作为文字文本处理，而不是作为可执行的脚本或可渲染的标记处理。
考虑将使用数据的上下文，并对数据进行上下文编码使其尽可能接近实际输出：例如用于 HTML 内容的 HTML 编码；用于属性值的数据输出的 HTML 属性编码；用于动态生成的 JavaScript 的 JavaScript 编码。例如，当 HTML 将非字母数字字符编码成 HTML 实体时，“<”和“>”将变为“<”和“>”。
作为额外的防御措施，无论来源如何，都需要对服务器上的所有外部输入进行验证。根据定义数据类型、大小、范围、格式和可接受值的严格规范（允许列表）认真检查每个输入参数。正则表达式或框架控件在某些情况下可能很有用，尽管它们不能替代输出编码。
必须对所有不受信任的数据进行输出编码和数据验证，无论这些数据来自哪里，例如表单字段、URL 参数、Web 服务参数、Cookie、来自网络的任何数据、环境变量、反向 DNS 查找、查询结果、请求标头、URL 组件、电子邮件、文件和文件名、数据库，以及向应用程序提供数据的任何外部系统。请谨记，可通过 API 调用间接获取此类输入。
对于服务器返回的每个网页，请明确设置“Content-Type”HTTP 响应标头。此标头值应定义特定的字符编码（字符集），例如“ISO-8859-1”或“UTF-8”。未指定编码时，Web 浏览器可以通过猜测网页实际使用的编码来选择另一个编码，这样，潜在攻击者便可以绕过 XSS 保护。
另外，在会话 Cookie 上设置“httpOnly”标志，以防止任何 XSS 漏洞窃取用户的 Cookie。
最好使用框架或标准库，它们通过根据上下文自动对所有动态输出进行编码来防止此漏洞，或者至少提供使其更容易避免的构造。
对于服务器返回的每个网页，明确设置“Content-Security-Policy”HTTP 响应标头，以使攻击者更加难以利用 XSS 攻击。

CWE:

79

外部引用：

跨站脚本攻击 (XSS)
OWASP XSS 速查表

发现电子邮件地址模式

TOC

原因：

Web 应用程序编程或配置不安全

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
Spambot 搜寻因特网站点，开始查找电子邮件地址来构建发送自发电子邮件（垃圾邮件）的邮件列表。
AppScan 检测到含有一或多个电子邮件地址的响应，可供利用以发送垃圾邮件。
而且，找到的电子邮件地址也可能是专用电子邮件地址，对于一般大众应是不可访问的。

受影响产品：

该问题可能会影响各种类型的产品。

修订建议：

常规

从 Web 站点中除去任何电子邮件地址，以便其不会被恶意用户利用。

CWE:

359

外部引用：

Spambot 的定义（维基百科）

发现可能的服务器路径泄露模式

TOC

原因：

未安装第三方产品的最新补丁或最新修补程序

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
AppScan 检测到包含文件绝对路径的响应（例如，Windows 中的 c:\dir\file，或 Unix 中的 /dir/file）。
攻击者可能能够利用这一信息访问服务器机器目录结构上的敏感信息，进而对站点发起进一步攻击。

受影响产品：

此问题可能影响不同类型的产品。

修订建议：

常规

有几种缓解技术：
[1] 如果漏洞存在于应用程序内，请修复服务器代码，以使得任何输出中都不包含文件位置。
[2] 否则，如果应用程序位于第三方产品中，请根据 Web 服务器或 Web 应用程序上使用的第三方产品下载相关的安全补丁。

CWE:

200

发现内部 IP 泄露模式

TOC

原因：

Web 应用程序编程或配置不安全

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
AppScan 检测到包含内部 IP 地址的响应。
内部 IP 定义为以下 IP 范围内的 IP：
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255
内部 IP 公开对于攻击者非常有价值，因为它揭示了内部网络的 IP 联网模式。获知内部网络的 IP 联网模式可能会帮助攻击者计划针对内部网络的进一步攻击。

受影响产品：

该问题可能会影响各种类型的产品。

修订建议：

常规

内部 IP 通常显现在 Web 应用程序/服务器所生成的错误消息中，或显现在 HTML/JavaScript 注释中。
[1] 关闭 Web 应用程序/服务器中有问题的详细错误消息。
[2] 确保已安装相关的补丁。
[3] 确保内部 IP 信息未留在 HTML/JavaScript 注释中。

CWE:

200

客户端（JavaScript）Cookie 引用

TOC

原因：

Cookie 是在客户端创建的

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
cookie 是一则信息，通常由 Web 服务器创建并存储在 Web 浏览器中。
web 应用程序主要（但不只是）使用 cookie 包含的信息来识别用户并维护用户的状态。
AppScan 检测到客户端上的 JavaScript 代码用于操控（创建或修改）站点的 cookie。
攻击者有可能查看此代码、了解其逻辑并根据所了解的知识将其用于组成其自己的 cookie，或修改现有 cookie。
攻击者可能导致的损坏取决于应用程序使用其 cookie 的方式或应用程序存储在这些 cookie 中的信息内容。
此外，cookie 操控还可能导致会话劫持或特权升级。
由 cookie 毒害导致的其他漏洞包含 SQL 注入和跨站点脚本编制。

受影响产品：

该问题可能会影响各种类型的产品。

修订建议：

常规

[1] 避免在客户端放置业务/安全逻辑。
[2] 查找并除去客户端不安全的 JavaScript 代码，该代码可能会对站点造成安全威胁。

CWE:

602

外部引用：

WASC 威胁分类：信息泄露