



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 10.0.0, 规则: 0
扫描开始时间: 2021/4/9 19:29:43

目录

介绍

- 常规信息
- 登陆设置

摘要

- 问题类型
- 有漏洞的 URL
- 修订建议
- 安全风险
- 原因
- WASC 威胁分类

按问题类型分类的问题

- “Content-Security-Policy”头缺失或不安全 5
- “X-Content-Type-Options”头缺失或不安全 4
- “X-XSS-Protection”头缺失或不安全 4
- HTTP Strict-Transport-Security 头缺失或不安全 5
- 发现可高速缓存的 SSL 页面 1
- 发现信用卡号模式 (Diners Club) 1
- 检测到 SHA-1 密码套件 1
- 检测到隐藏目录 1
- 支持较老的 TLS 版本 1
- 发现可能的服务器路径泄露模式 1
- 客户端 (JavaScript) Cookie 引用 1
- 应用程序错误 1

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。

低严重性问题: 23
参考严重性问题: 3
报告中包含的严重性问题总数: 26
扫描中发现的严重性问题总数: 26

常规信息

扫描文件名称: scan.platon
扫描开始时间: 2021/4/9 19:29:43
测试策略: Default

主机 scan.platon.network
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:
跟踪或会话 ID cookie:
跟踪或会话 ID 参数:
登陆序列:

摘要









问题类型 12

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	4 
低 "X-XSS-Protection"头缺失或不安全	4 
低 HTTP Strict-Transport-Security 头缺失或不安全	5 
低 发现可高速缓存的 SSL 页面	1 
低 发现信用卡号模式 (Diners Club)	1 
低 检测到 SHA-1 密码套件	1 
低 检测到隐藏目录	1 
低 支持较老的 TLS 版本	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	1 

有漏洞的 URL 10

TOC

URL	问题的数量
低 https://scan.platon.network/browser-server/config.json	5 
低 https://scan.platon.network/browser-server/platon-websocket/352/inz5v2ts/xhr_streaming	4 
低 https://scan.platon.network/browser-server/platon-websocket/352/shbd u1fg/xhr	4 
低 https://scan.platon.network/browser-server/platon-websocket/352/shbd u1fg/xhr_send	2 
低 https://scan.platon.network/browser-server/platon-websocket/info	4 
低 https://scan.platon.network/browser-server/transaction/transactionList	1 
低 https://scan.platon.network/static/js/manifest.6edd6182dabf366e69af.js	2 
低 https://scan.platon.network/static/	1 

参	https://scan.platon.network/static/js/1.ce03bdd2a06c367a90b7.js	2	<div></div>
参	https://scan.platon.network/browser-server/platon-websocket/352/frczwvsvy/htmlfile	1	<div></div>

修订建议 12

TOC

修复任务	问题的数量
低 除去 Web 站点中的信用卡号	1 <div></div>
低 除去客户端中的业务逻辑和安全逻辑	1 <div></div>
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 <div></div>
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 <div></div>
低 更改服务器的受支持密码套件	1 <div></div>
低 将服务器配置为使用安全策略的“Content-Security-Policy”头	5 <div></div>
低 将服务器配置为使用值为“1”（已启用）的“X-XSS-Protection”头	4 <div></div>
低 将服务器配置为使用值为“nosniff”的“X-Content-Type-Options”头	4 <div></div>
低 实施具有长“max-age”的 HTTP Strict-Transport-Security 策略	5 <div></div>
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 <div></div>
低 为 Web 服务器或 Web 应用程序下载相关的安全补丁	1 <div></div>
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	1 <div></div>

安全风险 7

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、机器名和/或敏感文件位置	20 <div></div>
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 <div></div>
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	2 <div></div>
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 <div></div>
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 <div></div>
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 <div></div>
参 可能会收集敏感的调试信息	1 <div></div>

原因 7

TOC

原因		问题的数量
低	Web 应用程序编程或配置不安全	19
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	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	1
参	未执行验证以确保用户输入与预期的数据类型匹配	1

WASC 威胁分类

TOC

威胁	问题的数量
服务器配置错误	2
信息泄露	24

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:

<https://scan.platon.network/browser-server/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:

```
...
GET /browser-server/config.json?v=1617967809720 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://scan.platon.network/
Connection: keep-alive
Host: scan.platon.network
Accept: application/json, text/plain, */*
Accept-Language: en-US

HTTP/1.1 200
Last-Modified: Wed, 07 Apr 2021 07:14:52 GMT
Connection: keep-alive
Server: nginx/1.16.1
Accept-Ranges: bytes
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Content-Length: 3077
Date: Fri, 09 Apr 2021 12:02:30 GMT
Content-Type: application/json
```

```
{
  "context": "/browser-server",
  "siteName": "PlatScan",
  "headerChainName": "PlatON Mainnet",
  "chainName": "PlatON",
  ...
}
```

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: <https://scan.platon.network/browser-server/platon-websocket/info>

实体: info (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:

```
...
GET /browser-server/platon-websocket/info?t=1617967810672 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://scan.platon.network/
Connection: keep-alive
Host: scan.platon.network
Accept: */*
Accept-Language: en-US

HTTP/1.1 200
Connection: keep-alive
Server: nginx/1.16.1
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Content-Length: 79
Cache-Control: no-store, no-cache, must-revalidate, max-age=0
Date: Fri, 09 Apr 2021 12:02:31 GMT
Content-Type: application/json; charset=UTF-8

{
  "entropy": -1588330054,
  "origins": [
    "*"
  ],
}
```



```
"cookie_needed": true,  
"websocket": true  
}  
...
```

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: <https://scan.platon.network/browser-server/platon-websocket/352/shbdu1fg/xhr>

实体: xhr (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:

```
...  
  
Cookie: UM_distinctid=178b6658994d5-096920afeee20b-671b187c-fa000-178b66589969a;  
CNZZDATA1278248458=1496426898-1617967811-%7C1617967811  
Connection: keep-alive  
Host: scan.platon.network  
Content-Length: 0  
Origin: https://scan.platon.network  
Accept: /*/*  
Accept-Language: en-US  
  
HTTP/1.1 200  
Transfer-Encoding: chunked  
Connection: keep-alive  
Access-Control-Allow-Credentials: true  
Server: nginx/1.16.1  
Access-Control-Allow-Origin: https://scan.platon.network  
Vary: Origin  
Vary: Access-Control-Request-Method  
Vary: Access-Control-Request-Headers  
Cache-Control: no-store, no-cache, must-revalidate, max-age=0  
Date: Fri, 09 Apr 2021 12:02:31 GMT  
Content-Type: application/javascript; charset=UTF-8  
  
a["CONNECTED\nversion:1.1\nheart-beat:0,0\n\n\u0000"]  
  
...
```

“Content-Security-Policy”头缺失或不安全**严重性:** 低**CVSS 分数:** 5.0**URL:** https://scan.platon.network/browser-server/platon-websocket/352/shbdu1fg/xhr_send**实体:** xhr_send (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:**

```

HTTP/1.1 204
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.16.1
Access-Control-Allow-Origin: https://scan.platon.network
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Cache-Control: no-store, no-cache, must-revalidate, max-age=0
Date: Fri, 09 Apr 2021 12:02:31 GMT
Content-Type: text/plain; charset=UTF-8...

```

“Content-Security-Policy”头缺失或不安全**严重性:** 低**CVSS 分数:** 5.0**URL:** https://scan.platon.network/browser-server/platon-websocket/352/inz5v2ts/xhr_streaming**实体:** xhr_streaming (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:**

```
...

Cookie: UM_distinctid=178b6658994d5-096920afeee20b-671b187c-fa000-178b66589969a;
CNZZDATA1278248458=1496426898-1617967811-%7C1617967811
Connection: keep-alive
Host: scan.platon.network
Content-Length: 0
Origin: https://scan.platon.network
Accept: */*
Accept-Language: en-US

HTTP/1.1 200
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.16.1
Access-Control-Allow-Origin: https://scan.platon.network
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Content-Length: 40
Cache-Control: no-store, no-cache, must-revalidate, max-age=0
Date: Fri, 09 Apr 2021 12:02:31 GMT
Content-Type: application/javascript;charset=UTF-8

c[2010,"Another connection still open"]

...
```

低

“X-Content-Type-Options”头缺失或不安全 4

TOC

问题 1 / 4

TOC

“X-Content-Type-Options”头缺失或不安全

严重性: 低

CVSS 分数: 5.0

URL: <https://scan.platon.network/browser-server/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“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:

...

```
GET /browser-server/config.json?v=1617967809720 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://scan.platon.network/
Connection: keep-alive
Host: scan.platon.network
Accept: application/json, text/plain, */*
Accept-Language: en-US
```

```
HTTP/1.1 200
Last-Modified: Wed, 07 Apr 2021 07:14:52 GMT
Connection: keep-alive
Server: nginx/1.16.1
Accept-Ranges: bytes
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Content-Length: 3077
Date: Fri, 09 Apr 2021 12:02:30 GMT
Content-Type: application/json
```

```
{
  "context": "/browser-server",
  "siteName": "PlatScan",
  "headerChainName": "PlatON Mainnet",
  "chainName": "PlatON",
  ...
}
```

问题 2 / 4

TOC

“X-Content-Type-Options”头缺失或不安全

严重性: 低

CVSS 分数: 5.0

URL: <https://scan.platon.network/browser-server/platon-websocket/info>

实体: info (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:

```
...
GET /browser-server/platon-websocket/info?t=1617967810672 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://scan.platon.network/
Connection: keep-alive
Host: scan.platon.network
```

```

Accept: */*
Accept-Language: en-US

HTTP/1.1 200
Connection: keep-alive
Server: nginx/1.16.1
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Content-Length: 79
Cache-Control: no-store, no-cache, must-revalidate, max-age=0
Date: Fri, 09 Apr 2021 12:02:31 GMT
Content-Type: application/json;charset=UTF-8

{
  "entropy": -1588330054,
  "origins": [
    "*"
  ],
  "cookie_needed": true,
  "websocket": true
}
...

```

问题 3 / 4

TOC

“X-Content-Type-Options”头缺失或不安全

严重性: 低

CVSS 分数: 5.0

URL: <https://scan.platon.network/browser-server/platon-websocket/352/shbdu1fg/xhr>

实体: xhr (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:

```

...

Cookie: UM_distinctid=178b6658994d5-096920afeee20b-671b187c-fa000-178b66589969a;
CNZZDATA1278248458=1496426898-1617967811-%7C1617967811
Connection: keep-alive
Host: scan.platon.network
Content-Length: 0
Origin: https://scan.platon.network
Accept: */*
Accept-Language: en-US

HTTP/1.1 200
Transfer-Encoding: chunked
Connection: keep-alive

```

```
Access-Control-Allow-Credentials: true
Server: nginx/1.16.1
Access-Control-Allow-Origin: https://scan.platon.network
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Cache-Control: no-store, no-cache, must-revalidate, max-age=0
Date: Fri, 09 Apr 2021 12:02:31 GMT
Content-Type: application/javascript;charset=UTF-8

a["CONNECTED\nversion:1.1\nheart-beat:0,0\n\n\u0000"]

...
```

问题 4 / 4

TOC

“X-Content-Type-Options”头缺失或不安全

严重性: 低

CVSS 分数: 5.0

URL: https://scan.platon.network/browser-server/platon-websocket/352/inz5v2ts/xhr_streaming

实体: xhr_streaming (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:

```
...

Cookie: UM_distinctid=178b6658994d5-096920afeee20b-671b187c-fa000-178b66589969a;
CNZZDATA1278248458=1496426898-1617967811-%7C1617967811
Connection: keep-alive
Host: scan.platon.network
Content-Length: 0
Origin: https://scan.platon.network
Accept: */*
Accept-Language: en-US

HTTP/1.1 200
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.16.1
Access-Control-Allow-Origin: https://scan.platon.network
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Content-Length: 40
Cache-Control: no-store, no-cache, must-revalidate, max-age=0
Date: Fri, 09 Apr 2021 12:02:31 GMT
Content-Type: application/javascript;charset=UTF-8

c[2010,"Another connection still open"]
```

...

低

“X-XSS-Protection”头缺失或不安全 4

TOC

问题 1 / 4

TOC

“X-XSS-Protection”头缺失或不安全

严重性: 低

CVSS 分数: 5.0

URL: <https://scan.platon.network/browser-server/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:

```
...
GET /browser-server/config.json?v=1617967809720 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://scan.platon.network/
Connection: keep-alive
Host: scan.platon.network
Accept: application/json, text/plain, */*
Accept-Language: en-US

HTTP/1.1 200
Last-Modified: Wed, 07 Apr 2021 07:14:52 GMT
Connection: keep-alive
Server: nginx/1.16.1
Accept-Ranges: bytes
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Content-Length: 3077
Date: Fri, 09 Apr 2021 12:02:30 GMT
Content-Type: application/json

{
  "context": "/browser-server",
  "siteName": "PlatScan",
```

```
"headerChainName": "PlatON Mainnet",  
"chainName": "PlatON",  
...
```

“X-XSS-Protection”头缺失或不安全**严重性:** 低**CVSS 分数:** 5.0**URL:** <https://scan.platon.network/browser-server/platon-websocket/info>**实体:** info (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攻击

未经处理的测试响应:

```
...  
GET /browser-server/platon-websocket/info?t=1617967810672 HTTP/1.1  
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko  
Referer: https://scan.platon.network/  
Connection: keep-alive  
Host: scan.platon.network  
Accept: */*  
Accept-Language: en-US  
  
HTTP/1.1 200  
Connection: keep-alive  
Server: nginx/1.16.1  
Vary: Origin  
Vary: Access-Control-Request-Method  
Vary: Access-Control-Request-Headers  
Content-Length: 79  
Cache-Control: no-store, no-cache, must-revalidate, max-age=0  
Date: Fri, 09 Apr 2021 12:02:31 GMT  
Content-Type: application/json; charset=UTF-8  
  
{  
  "entropy": -1588330054,  
  "origins": [  
    "":*"  
  ],  
  "cookie_needed": true,  
  "websocket": true  
}  
...
```


“X-XSS-Protection”头缺失或不安全**严重性:** 低**CVSS 分数:** 5.0**URL:** <https://scan.platon.network/browser-server/platon-websocket/352/shbdu1fg/xhr>**实体:** xhr (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:

```
...  
  
Cookie: UM_distinctid=178b6658994d5-096920afeee20b-671b187c-fa000-178b66589969a;  
CNZZDATA1278248458=1496426898-1617967811-%7C1617967811  
Connection: keep-alive  
Host: scan.platon.network  
Content-Length: 0  
Origin: https://scan.platon.network  
Accept: */*  
Accept-Language: en-US  
  
HTTP/1.1 200  
Transfer-Encoding: chunked  
Connection: keep-alive  
Access-Control-Allow-Credentials: true  
Server: nginx/1.16.1  
Access-Control-Allow-Origin: https://scan.platon.network  
Vary: Origin  
Vary: Access-Control-Request-Method  
Vary: Access-Control-Request-Headers  
Cache-Control: no-store, no-cache, must-revalidate, max-age=0  
Date: Fri, 09 Apr 2021 12:02:31 GMT  
Content-Type: application/javascript;charset=UTF-8  
  
a["CONNECTED\nversion:1.1\nheart-beat:0,0\n\n\u0000"]  
  
...
```

“X-XSS-Protection”头缺失或不安全

严重性: 低

CVSS 分数: 5.0

URL: https://scan.platon.network/browser-server/platon-websocket/352/inz5v2ts/xhr_streaming

实体: xhr_streaming (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:

```
...

Cookie: UM_distinctid=178b6658994d5-096920afeee20b-671b187c-fa000-178b66589969a;
CNZZDATA1278248458=1496426898-1617967811-%7C1617967811
Connection: keep-alive
Host: scan.platon.network
Content-Length: 0
Origin: https://scan.platon.network
Accept: */*
Accept-Language: en-US

HTTP/1.1 200
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.16.1
Access-Control-Allow-Origin: https://scan.platon.network
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Content-Length: 40
Cache-Control: no-store, no-cache, must-revalidate, max-age=0
Date: Fri, 09 Apr 2021 12:02:31 GMT
Content-Type: application/javascript;charset=UTF-8

c[2010,"Another connection still open"]

...
```

低

HTTP Strict-Transport-Security 头缺失或不安全 5

TOC

问题 1 / 5

TOC

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

严重性: 低

CVSS 分数: 5.0

URL: https://scan.platon.network/browser-server/platon-websocket/352/shbdu1fg/xhr_send

实体: xhr_send (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/1.1 204
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.16.1
Access-Control-Allow-Origin: https://scan.platon.network
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Cache-Control: no-store, no-cache, must-revalidate, max-age=0
Date: Fri, 09 Apr 2021 12:02:31 GMT
Content-Type: text/plain; charset=UTF-8...
```

问题 2 / 5

TOC

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

严重性: 低

CVSS 分数: 5.0

URL: <https://scan.platon.network/browser-server/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: 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
Last-Modified: Wed, 07 Apr 2021 07:14:52 GMT
Connection: keep-alive
Server: nginx/1.16.1
Accept-Ranges: bytes
```

```
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Content-Length: 3077
Date: Fri, 09 Apr 2021 12:02:30 GMT
Content-Type: application/json

{
  "context": "/browser-server",
  "siteName": "PlatScan",
  "headerChainName": "PlatON Mainnet",
  ...
}
```

问题 3 / 5

TOC

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

严重性: 低

CVSS 分数: 5.0

URL: <https://scan.platon.network/browser-server/platon-websocket/info>

实体: info (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
Connection: keep-alive
Server: nginx/1.16.1
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Content-Length: 79
Cache-Control: no-store, no-cache, must-revalidate, max-age=0
Date: Fri, 09 Apr 2021 12:02:31 GMT
Content-Type: application/json; charset=UTF-8

{
  "entropy": -1588330054,
  "origins": [
    "*"
  ],
  "cookie_needed": true,
  "websocket": true
}...
```

HTTP Strict-Transport-Security 头缺失或不安全**严重性:** 低**CVSS 分数:** 5.0**URL:** <https://scan.platon.network/browser-server/platon-websocket/352/shbdu1fg/xhr>**实体:** xhr (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
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.16.1
Access-Control-Allow-Origin: https://scan.platon.network
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Cache-Control: no-store, no-cache, must-revalidate, max-age=0
Date: Fri, 09 Apr 2021 12:02:31 GMT
Content-Type: application/javascript;charset=UTF-8

a["CONNECTED\nversion:1.1\nheart-beat:0,0\n\n\u0000"]...
```

HTTP Strict-Transport-Security 头缺失或不安全**严重性:** 低**CVSS 分数:** 5.0**URL:** https://scan.platon.network/browser-server/platon-websocket/352/inz5v2ts/xhr_streaming**实体:** xhr_streaming (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
Connection: keep-alive
Access-Control-Allow-Credentials: true
Server: nginx/1.16.1
Access-Control-Allow-Origin: https://scan.platon.network
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Content-Length: 40
Cache-Control: no-store, no-cache, must-revalidate, max-age=0
Date: Fri, 09 Apr 2021 12:02:31 GMT
Content-Type: application/javascript;charset=UTF-8

c[2010,"Another connection still open"]...

```

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://scan.platon.network/browser-server/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

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
Last-Modified: Wed, 07 Apr 2021 07:14:52 GMT
Connection: keep-alive
Server: nginx/1.16.1
Accept-Ranges: bytes
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Content-Length: 3077
Date: Fri, 09 Apr 2021 12:02:30 GMT
Content-Type: application/json

{
  "context": "/browser-server",

```

```
"siteName": "PlatScan",  
"headerChainName": "PlatON Mainnet",  
...
```

低

发现信用卡号模式（Diners Club）

1

TOC

问题 1 / 1

TOC

发现信用卡号模式（Diners Club）

严重性: 低

CVSS 分数: 5.0

URL: <https://scan.platon.network/browser-server/transaction/transactionList>

实体: transactionList (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 Diners Club 信用卡号。

未经处理的测试响应:

```
...  
  
  "txType": "0",  
  "serverTime": 1617973732463,  
  "timestamp": 1617967469047,  
  "blockNumber": 191628,  
  "failReason": "",  
  "receiveType": "1",  
  "txReceiptStatus": 1  
},  
{  
  "txHash": "0x6d77026d096626776d8e368cbd2b3352f36814511359350f12220c132bdbd978",  
  "from": "lat1std0k68r8g27rqzekazkg34qrfp7th43cmvm7e",  
  "to": "lat1sh2u7xkhmycsj5d3ek17rw4pntyune2m5w9wew",  
  "seq": 19162800004,  
  "value": "10000000",  
  "actualTxCost": "0.000021",  
  "txType": "0",  
  "serverTime": 1617973732463,  
  "timestamp": 1617967469047,  
  "blockNumber": 191628,  
  ...  
}
```

问题 1 / 1

TOC

检测到 SHA-1 密码套件

严重性: 低

CVSS 分数: 4.2

URL: <https://scan.platon.network/static/js/manifest.6edd6182dabf366e69af.js>

实体: scan.platon.network (Page)

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 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
10	TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS 1.0
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
49170	TLS_ECDHE_RSA_WITH_3DES_EDE_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
10	TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS 1.1
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
49170	TLS_ECDHE_RSA_WITH_3DES_EDE_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
10	TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS 1.2
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
49170	TLS_ECDHE_RSA_WITH_3DES_EDE_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://scan.platon.network/static/>

实体:

static/ (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:

```
...
GET /static/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://scan.platon.network/
Connection: keep-alive
Host: scan.platon.network
Accept: */*
Accept-Language: en-US

HTTP/1.1 403 Forbidden
Connection: keep-alive
Server: nginx/1.16.1
```

```
Content-Length: 153
Date: Fri, 09 Apr 2021 12:37:21 GMT
Content-Type: text/html; charset=utf-8
```

...

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://scan.platon.network/static/js/manifest.6edd6182dabf366e69af.js>

实体: scan.platon.network (Page)

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 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
Last-Modified: Wed, 07 Apr 2021 01:40:58 GMT
Connection: keep-alive
Server: nginx/1.16.1
Accept-Ranges: bytes
Content-Length: 3733
ETag: "606d0daa-e95"
Date: Fri, 09 Apr 2021 11:30:04 GMT
Content-Type: application/javascript; charset=utf-8

!function(e){function t(t){for(var n,a,f=t[0],u=t[1],d=t[2],i=0,s=
[];i<f.length;i++)a=f[i],Object.prototype.hasOwnProperty.call(o,a)&&o[a]&&s.push(o[a]
[0]),o[a]=0;for(n in u)Object.prototype.hasOwnProperty.call(u,n)&&
(e[n]=u[n]);for(l&&l(t);s.length;)s.shift()();return c.push.apply(c,d||[]),r()}function r()
{for(var e,t=0;t<c.length;t++){for(var r=c[t],n=!0,a=1;a<r.length;a++){var u=r[a];0!==o[u]&&
(n=!1)}n&&(c.splice(t--,1),e=f(f.s=r[0]))}return e}var n={},a={5:0},o={5:0},c=[],function f(t)
{if(n[t])return n[t].exports;var r=n[t]={i:t,l:!1,exports:{}};return
e[t].call(r.exports,r,r.exports,f),r.l=!0,r.exports}f.e=function(e){var t=[];a[e]?
t.push(a[e]):0!==a[e]&&
{0:1,2:1,6:1,7:1,8:1,9:1,10:1,11:1,12:1,13:1,14:1,15:1,16:1,17:1,18:1,19:1,20:1,21:1,22:1}
[e]&&t.push(a[e]=new Promise(function(t,r){for(var n="static/css/"+({0:"common"
[e]||e)+"-bde601aeb8802c002332.css",o=f.p+n,c=document.getElementsByTagName("link"),u=0;u<c.lengt
h;u++){var d=(l=c[u]).getAttribute("data-href")||l.getAttribute("href");if("stylesheet"===l.rel&&
(d===n||d===o))return t()}var i=document.getElementsByTagName("style");for(u=0;u<i.length;u++)
{var l;if((d=(l=i[u]).getAttribute("data-href"))===n||d===o)return t()}var
```

```

s=document.createElement("link");s.rel="stylesheet",s.type="text/css",s.onload=t,s.onerror=function(t){var n=t&&t.target&&t.target.src||o,c=new Error("Loading CSS chunk "+e+" failed.\n("+n+")");c.code="CSS_CHUNK_LOAD_FAILED",c.request=n,delete a[e],s.parentNode.removeChild(s),r(c)},s.href=o,document.getElementsByTagName("head")[0].appendChild(s)).then(function(){a[e]=0}));var r=o[e];if(0!==r)if(r)t.push(r[2]);else{var n=new Promise(function(t,n){r=o[e]=[t,n]});t.push(r[2]=n);var c,u=document.createElement("script");u.charset="utf-8",u.timeout=120,f.nc&&u.setAttribute("nonce",f.nc),u.src=function(e){return f.p+"static/js/"+e+"."+{0:"c224ac8ce5eac44cdea0",2:"4dc19fb00b792aec4ffd",3:"5f5beefc786e761bd22a",6:"d5ccd65ef25223e7029b",7:"bc5496d4d15158072953",8:"51b382bcf0c3a4330b85",9:"04ec78c09f0a1bfef0...

```

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: <https://scan.platon.network/static/js/1.ce03bdd2a06c367a90b7.js>

实体: 1.ce03bdd2a06c367a90b7.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)?
a===e.replace(/\/*$/, ""):!!/^[\^\/]+\[/\^\/]+$/ .test(e)&&n===e)}}):this.Semit("file",...

...

...
... (? : 1? \d { 1, 2} | 2 [ 0-4] \d { 25 [ 0-5] }) { 2} (?: \. (?: [ 0-9] \d? | 1 \d \d { 2 [ 0-4] \d { 25 [ 0-4] }) | (?: (?: [ a-
z \u 00a1 - \u f f f 0 - 9] + - ?) * [ a-z \u 00a1 - \u f f f 0 - 9] +) (?: \. (?: [ a-z \u 00a1 - b...

...

...
...G[W]WWE", /\d { 4} W \d { 3} /], ["GGGG[W]WW", /\d { 4} W \d { 2} /, !1], ["YYYYDDD", /\d { 7} /]], wt=
[["HH:mm:ss.SSSS", /\d \d : \d \d : \d \d \. \d + /], ["HH:mm:ss.SSSS", /\d - - begin_highlight_ta...

...
```

客户端 (JavaScript) Cookie 引用

严重性: [参考](#)

CVSS 分数: 0.0

URL: <https://scan.platon.network/static/js/1.ce03bdd2a06c367a90b7.js>

实体: (window.webpackJsonp=window.webpackJsonp||[]).push([[1],{"+JPL":function(e,t,n){e.exports={default:n... (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

```
...
...isString(r)&&o.push("path="+r),i.isString(a)&&o.push("domain="+a),!0===s&&o.push("secure"),do
cument.cookie=g.join("; ");read:function(e){var t=document.cookie.match(new RegExp("(^|;\\s*)
(\\+e+)=([\\^;]*)"));re...
...
```

参

应用程序错误 1

TOC

应用程序错误

严重性: [参考](#)

CVSS 分数: 0.0

URL: <https://scan.platon.network/browser-server/platon-websocket/352/frczwvsv/htmlfile>

实体: c (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：

```
...

Referer: https://scan.platon.network/
Cookie: UM_distinctid=178b6658994d5-096920afeee20b-671b187c-fa000-178b66589969a;
CNZZDATA1278248458=1496426898-1617967811-%7C1617967811
Connection: keep-alive
Host: scan.platon.network
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-US

HTTP/1.1 500
Connection: keep-alive
Server: nginx/1.16.1
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Content-Length: 29
Cache-Control: no-store, no-cache, must-revalidate, max-age=0
Date: Fri, 09 Apr 2021 12:47:15 GMT
Content-Type: text/html; charset=UTF-8

...
```