

实验吧——WriteUp&&涨姿势（1）

原创

[浅零半泣](#) 于 2017-04-15 17:21:11 发布 1659 收藏 1

分类专栏: [CTF](#) 文章标签: [CTF wp web](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/sinat_34200786/article/details/70185661

版权



[CTF 专栏收录该内容](#)

19 篇文章 0 订阅

订阅专栏

WriteUp

- 1.NSCTF web200
- 2.Forbidden
- 3.猫抓老鼠

涨姿势

- 1.上传绕过
- 2.Guess Next Session
- 3.天下武功唯快不破
- 4.what a fuck!这是什么鬼东西?
- 5.头有点大

NSCTF web200

[原题](#)

tips:

这是一个php自定义加密函数。

key的密文:

a1zLbgQsCESEIqRLwuQAYmWLyq2L5VwBxqGA3RQAYumZ0tmMvSGM2ZwB4tws, 请解密!

[encode_API](#)

```
function encode($str) {
    $_o = strrev($str);
    for($_0=0;$_0<strlen($_o);$_0++){
        $_c = substr($_o,$_0,1);
        $__ = ord($_c)+1;
        $_c = chr($__);
        $_ = $_.$_c;
    }
    return str_rot13(strrev(base64_encode($_)));
}
```

http://blog.csdn.net/sinat_34200786

解题思路

就是一个很简单的逆向题，不多解释

WriteUp

```
<?php
$str = "a1zLbgQsCESEIqRLwuQAYmWLyq2L5VwBxqGA3RQAYumZ0tmMvSGM2ZwB4tws";
$str = base64_decode(strrev(str_rot13($str)));
$vstr = "";
for($i = 0;$i<strlen($str);$i++)
{
    $c = substr($str,$i,1);
    $k = ord($c)-1;
    $c = chr($k);
    $vstr = $vstr.$c;
}
$str = strrev($vstr);
echo $str;
?>
```

Forbidden

[原题](#)

Forbidden

You don't have permission to access / on this server.

Make sure you are in HongKong

http://blog.csdn.net/sinat_34200786

解题思路

抓包修改Accept-Language为zh-hk

WriteUp

```
user-agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:51.0) Gecko,
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*,
Accept-Language: zh-hk,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://www.hiyanbar.com/ctf/21
Cookie: Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1491999349,14920
Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*87165%2CnickName
Hm_lpv_34d6f7353ab0915a4c582e4516dffbc3=1492242581; PHPSESSID=
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

http://blog.csdn.net/sinat_34200786

猫抓老鼠

原题

Input your pass key:

http://blog.csdn.net/sinat_34200786

解题思路

查看返回头可发现Content-Row是一个base64加密的密文，此题有个小小的脑洞，就是密文不解密

WriteUp

Burp Suite抓包后将包发到Repeater

Intercept HTTP history WebSockets history Options

Request to http://ctf5.shiyanbar.com:80 [121.194.2.45]

Forward Drop Intercept is on Action

Raw Params Headers Hex

```

POST /basic/catch/ HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:51.0) Gecko/20100101 Firefox/51.0
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
Referer: http://ctf5.shiyanbar.com/basic/catch/
Cookie: Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=149174244,149174244,149174244,149174244,149174244
Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*vis
Hm_lpv_34d6f7353ab0915a4c582e4516dffbc3=149174244,149174244,149174244,149174244,149174244
Connection: close
Upgrade-Insecure-Request: 1
  
```

Send to Spider
Do an active scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools

查看Response可得密文

Response

Raw Headers Hex

```

HTTP/1.1 200 OK
Date: Sat, 15 Apr 2017 07:55:52 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.2.17
X-Powered-By: PHP/5.2.17
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Row: MTQ5MjIOMjgzMw==
Content-Length: 14
Connection: close
Content-Type: text/html
  
```

Check Failed!

将密文直接输入即可

上传绕过

原题

文件上传

Filename: 未选择文件。

http://blog.csdn.net/sinat_34200786

解题思路

- 4929482
- 5206298
- 4968406

[View the source code](#)

```
<?php
session_start();
if (isset ($_GET['password'])) {
    if ($_GET['password'] ==
$_SESSION['password'])
        die ('Flag: '.$flag);
    else
        print '<p>Wrong guess.</p>';
}

mt_srand((microtime() ^ rand(1, 10000)) %
rand(1, 10000) + rand(1, 10000));
?>
```

http://blog.csdn.net/sinat_34200786

解题思路

根据源码来看，如果想硬杠就得搞定那几个随机函数，这个可能性太低所以肯定另有妙计。仔细看可以发现只要 `$_GET['password']`：

WriteUp

抓包改数据如图

```
GET /web/Session.php?password=34553 HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
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
Referer: http://ctf5.shiyanbar.com/web/Session.php
Cookie: sample-hash=571580b26c65f306376d4f64e53cb5c7; source=0;
Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1491999349,1492088891,1492174244,1492241613;
Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*87165%2CnickName%3A%E5%BA%8F%E5%B9%95%E4%B8%83%E7%AB%AO;
Hm_lpvt_34d6f7353ab0915a4c582e4516dffbc3=1492244003; PHPSESSID=14eq4pm4eupohh17img2k6q764
Connection: close
Upgrade-Insecure-Requests: 1
```

http://blog.csdn.net/sinat_34200786

直接将后面的参数删除即可

```
GET /web/Session.php?password= HTTP/1.1
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
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
Referer: http://ctf5.shiyanbar.com/web/Session.php?password=34553
Cookie: sample-hash=571580b26c65f306376d4f64e53cb5c7; source=0;
Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1491999349,1492088891,1492174244,1492241613;
Hm_cv_34d6f7353ab0915a4c582e4516dffbc3=1*visitor*87165%2CnickName%3A%E5%BA%8F%E5%B9%95%E4%B8%83%E7%AB%AO;
Hm_lpvt_34d6f7353ab0915a4c582e4516dffbc3=1492244003; PHPSESSID=
Connection: close
Upgrade-Insecure-Requests: 1
```

http://blog.csdn.net/sinat_34200786

涨姿势点

抓包后将pass改为空则\$_GET['pass']为""，不输入直接提交也是""
由自己控制上传的session
确定是哪个session

天下武功唯快不破

原题

There is no martial art is indefectible, while the fastest speed is the only way for long success.
>>>>>----You must do it as fast as you can!----<<<<<<

http://blog.csdn.net/sinat_34200786

解题思路

很明显只有代码才够快

WriteUp

抓包查看Respond可以发现相应头有个FLAG

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Sat, 15 Apr 2017 08:42:11 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.2.17
X-Powered-By: PHP/5.2.17
FLAG: UDBTVF9USE1TX1QwXONINE5HRV9GTDROHjdVS3c3dHJ6eQ==
Content-Length: 216
Connection: close
Content-Type: text/html
```

```
There is no martial art is indefectible, while the
fastest speed is the only way for long
success.</br>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>----You must do it as fast as you
can!-----<<<<<<<</br>
<!-- please post what you find with parameter:key -->
```

解密得到: P0ST_THIS_T0_CH4NGE_FL4G:7UKw7trzy
于是知道冒号后面的参数是解题关键, 发送回去

Code(引用自[实验吧](#)@madman)

```
import urllib.request
import urllib.parse
import base64

opener = urllib.request.build_opener()
url = "http://ctf5.shiyanbar.com/web/10/10.php"

response = opener.open(url)
data = {"key": base64.b64decode(response.getheader("FLAG")).decode().split(":")[1]}
html = opener.open(url, urllib.parse.urlencode(data).encode()).read()

print(html)
```

涨姿势点

原来是发送回原来的网址, 一开始就迷惑到底发送到哪里去

what a fuck!这是什么鬼东西?

[原题](#)

Tips http header

Forbidden

You don't have permission to access / on this server.

Please make sure you have installed .net framework 9.9!

Make sure you are in the region of England and browsing this site with Internet Explorer

http://blog.csdn.net/sinat_34200786

解题思路

就按照题目的意思办，F12改请求头

WriteUp

事由	类型	已传输	消息头	Cookie	参数	响应	耗时	预览
JS document	html	1.32 KB	请求网址: http://ctf5.shiyanbar.com/sHeader/ 请求方法: GET 远程地址: 127.0.0.1:8080 状态码: 200 OK 版本: HTTP/1.1					
stylesheet	css	4.00 KB						
img	jpeg	—						
img	jpeg	—						

编辑和重发，User-Agent中添加 .NET CLR 9.9，修改Accept-Language为en-gb

```
Host: ctf5.shiyanbar.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:51.0; .NET CLR 9.9) Gecko/201
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-gb;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://www.shiyanbar.com/ctf/29
Cookie: Hm_lvt_34d6f7353ab0915a4c582e4516dffbc3=1491999349,1492088891,1492
Connection: keep-alive
```

发送后查看预览

5 个请求, 7.44 KB, 115.72 秒 过滤 URL

消息头	Cookie	参数	响应	耗时	预览
					The key is:HTTpH34der http://blog.csdn.net/sinat_34200786

涨姿势点

.NET framework 9.9 在请求头中的表示 — .NET CLR 9.9



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)