BWVS-命令执行漏洞

原创

baynk 于 2019-11-26 11:03:46 发布 475 收藏 1

文章标签： BWVS 命令执行漏洞

本文链接：https://blog.csdn.net/u014029795/article/details/103251194

BWVS 专栏收录该内容

14 篇文章 1 订阅

订阅专栏

0x00 RCE漏洞

有种回到了低配版`dvwa`的感觉。。。但是和`DoraBox`真的太像了，有一腿。。。

0x01 任意代码执行 `/bug/code_exec/code.php`

直接输入`phpinfo()`就出结果了，我猜是`assert()`

code: submit

PHP Version 5.5.38

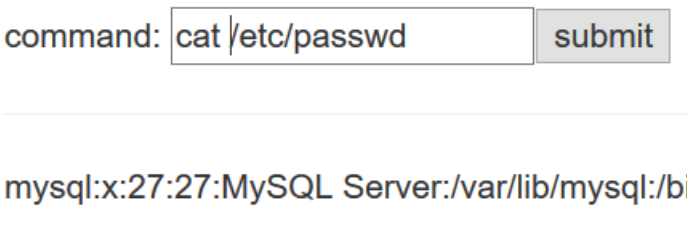
System	Linux baynk.QTJ.com 2.6.32-754.el6.x86_64 #1 SMP Tue Jun 19 21:26:04 UT
Build Date	Oct 22 2019 14:17:33

看源码去

```
<!DOCTYPE html>
<html>
<head>
        <meta charset="utf-8">
        <title>bugku - 代码执行</title>
</head>
<body>
<?php
        include_once('../../bwvs_config/sys_config.php');
        require_once('../header.php');
        include "../class/function.class.php";
        $p = new Func("GET","code");
        $p -> con_html();
        if (isset($_REQUEST['submit'])) {
                $code = $_REQUEST['code'];
                echo $p -> con_function('assert',$code);
        }
?>
</body>
</html>
<br>
<br>
<br>
<br>
<?php
require_once('../info.php');
?>
```

诚不欺我。。。

0x02 远程命令执行 `/bug/code_exec/exec.php`



mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash

这真的不是`DoraBox`里面的东西吗。。。我擦，刚刚去看了下，一模一样，这个`bug`目录里面的东西，感觉就是从`DoraBox`里面复制出来的，，？？？还是。。。
以后我也能搞一个靶场出来了，`读书人偷不叫做偷`？？？
我这感觉血亏。。。

0x03 PHP远程命令执行漏洞 `/ping.php`

这个。。。。好像是之前暴力破解那个题的坑吧，研究了下怎么伪造`session`让我直接登陆(这里不是用`cookie`检查的，是要通过`session`)，这里也简单去看了下`$_session`和`$_cookie`，真是细节满满，决定去补上用户名和密码看看到底是什么东西。

```
mysql> insert into dwvs_admin_message(DWVS_admin_id,DWVS_admin_name,DWVS_admin_passwd) values (1,"admin","admin"
);
Query OK, 1 row affected (0.02 sec)

mysql> select * from dwvs_admin_message;
+---------------+-----------------+-------------------+
| DWVS_admin_id | DWVS_admin_name | DWVS_admin_passwd |
+---------------+-----------------+-------------------+
|             1 | admin           | admin
```

结果发现不太行，然后去看了源码。。。

```php
<?php
include_once('../bwvs_config/sys_config.php');
if (isset($_POST['submit'])) {

        if(empty($_POST['admin_name']) || empty($_POST['admin_pass']))
        {
                $_SESSION['error_info'] = '温馨提示：用户名或密码错误1! ';
                header('Location: login.php');
        }else{
                $admin_name = $_POST['admin_name'];
                $admin_pass = $_POST['admin_pass'];

                $admin_name = clear_all($admin_name);
                $admin_pass = clear_all($admin_pass);

        $sql = "SELECT * FROM dwvs_admin_message WHERE DWVS_admin_name = '$admin_name' AND DWVS_admin_passwd = '
".md5($admin_pass,true)."'";

        $data = mysqli_query($connect, $sql) or die('MySQL Error!!');

    if (mysqli_num_rows($data) != 0){
                $_SESSION['admin'] = $admin_name;
                sleep(3);
        header('Location: manage.php');
        }else{
                $_SESSION['error_info'] = '温馨提示：用户名或密码错误2! ';
                header('Location: login.php');}
        }
}
else {
        not_find($_SERVER['PHP_SELF']);
}
?>
```

原来是做了`md5`的。。。再更新下数据库。

```
mysql> update  dwvs_admin_message set DWVS_admin_passwd=md5("admin") where DWVS_admin_id=1;
Query OK, 1 row affected (0.00 sec)
Rows matched: 1  Changed: 1  Warnings: 0

mysql> select * from dwvs_admin_message;
+---------------+-----------------+----------------------------------+
| DWVS_admin_id | DWVS_admin_name | DWVS_admin_passwd                |
+---------------+-----------------+----------------------------------+
|             1 | admin           | 21232f297a57a5a743894a0e4a801fc3 |
+---------------+-----------------+----------------------------------+
1 row in set (0.00 sec)
```

结果发现还是不行，对比了下`php`中写的是`md5(str,true)`。。。这，这，这，这不是我之前做的`ctf`题目吗。。
于是用户名`admin`，密码`ffifdyop`。。。

这也太套路了。。。我服了，没明白的看实验吧-后台登录 Writeup

感动的想哭。。。输入`127.0.0.1;/etc/passwd`出结果，这个就不多说了，简单。