

云演CTF——这里有几首歌

原创

长街395 于 2022-01-16 19:37:44 发布 2718 收藏

文章标签: [安全](#) [web安全](#)

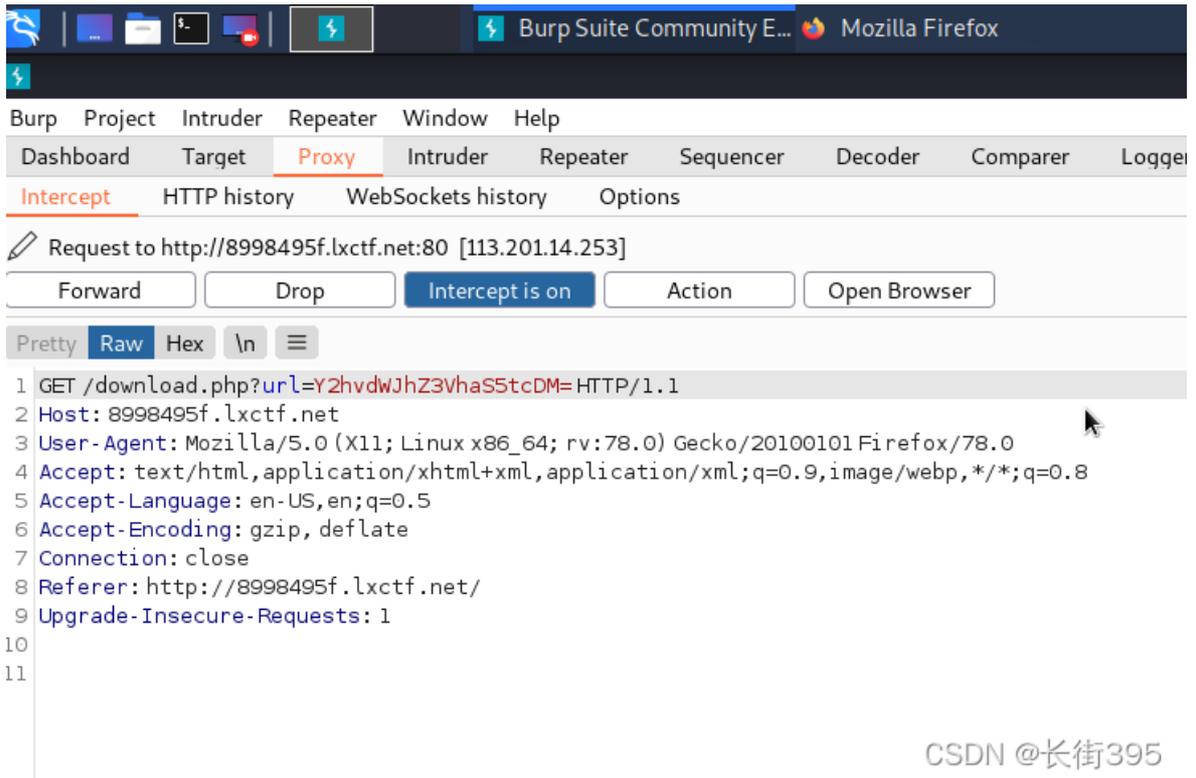
版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_56301399/article/details/122527350

版权

通过这道题可以掌握一些抓包的技巧, 做法如下:

首先点击下载用bp抓包, 可以发现url=的漏洞



利用base64加密, 将download.php加密(可采用网上的在线加密工具加密)

download.php

清空 加密 解密 解密为UTF-8字节流

ZG93bmxvYWQucGhw

复制

CSDN @长街395

然后对download.php文件进行审计，可以发现还有一个hereiskey.php

```
download.php
文件(F) 编辑(E) 搜索(S) 选项(O) 帮助(H)
<?php
error_reporting(0);
include("hereiskey.php");
$url=base64_decode($_GET[url]);
if( $url=="hereiskey.php" || $url=="choubaguai.mp3" || $ur
    $file_size = filesize($url);
    header ( "Pragma: public" );
    header ( "Cache-Control: must-revalidate, post-check=0,
    header ( "Cache-Control: private", false );
    header ( "Content-Transfer-Encoding: binary" );
    header ( "Content-Type:audio/mpeg MP3");
    header ( "Content-Length: " . $file_size);
    header ( "Content-Disposition: attachment; filename=".$
    echo(file_get_contents($url));
    exit;
}
else {
    echo "Access Forbidden!";
}
```

CSDN @长街395

以同样的方式对hereiskey.php进行下载和审计，最后得到flag

```
hereiskey.php
文件(F) 编辑(E) 搜索(S) 选项(O) 帮助(H)
<?php
// key is d0wnload_0k
?>
```

CSDN @长街395