登录

Host-header-injection

bywalks / 2018-03-28 12:18:39 / 浏览数 1688 技术文章 技术文章 顶(0) 踩(0)

前言：

遇到个Host-header-injection，简单的查查资料，总结一下这方面的知识。

目录：

漏洞原理

在互联网上，大部分情况下一个web服务器，有着一个IP和多个网站。那么当我们向web服务器做出请求时，web服务器是如何识别到底是访问其中的哪个网站呢？这就是H
而当服务器获取HOST的方式不当时，就会产生很多问题。
例如下面的代码。

```
<a href="http://<?php echo _SERVER['HOST'] ?>">Redirect</a>
```

SERVER['HOST']是可以通过抓包修改的。一切用户的输入都是不可相信的。

正常
Request：

```
GET / HTTP/1.1
Host: example.com
```

Response:

```
HTTP/1.1 302 Object moved
Location: http://www.example.com

<a href="http://www.example.com">Redirecting...</a>
```

黑盒测试

三种修改方式

- 直接修改
  Host: bywalks.com
- 参数污染
  Host: google.com
  Host: bywalks.com
- 伪造请求头
  X-Forwarded-For: bywalks.com

漏洞危害

- 缓存投毒
  1：用浏览器访问example.com
  2：服务器返回302跳转到https://www.example.com/login
  3：当我们访问example.com的时候，修改请求头，为bywalks.com
  4：服务器返回302跳转到https://www.bywalks.com/login
  5：当我们再一次访问example.com时，或许服务器没有经过验证，直接跳转到http://www.bywalks.com/login
- Open Redirection
  302跳转
  CRLF
  POC：

  ```
  %0d%0aset-cookie%20%3atest%3dtrue;
  ```

- 密码重置
  网站一般都存在这密码修改功能，直接输入email即可。账号绑定的email就会接收到邮件。
  类似于这样。http://www.example.com/Token/
  HOST可以修改，我们就可以修改HOST，email接受的邮件就变成了这样:http://www.bywalks.com/Token/
  当用户点击这个URL之后，我们就可以从网站日记看到这个TOKEN，从而达到密码重置的目的。

如何修复
1：HOST白名单
2：获取真实HOST。

个人博客：www.bywalks.com

上一篇：Apache JMeter rmi... 下一篇：Jolokia JNDI Inje...
1. 1 条回复


停云落月 2018-03-28 13:07:30

CRLF

0 回复Ta
