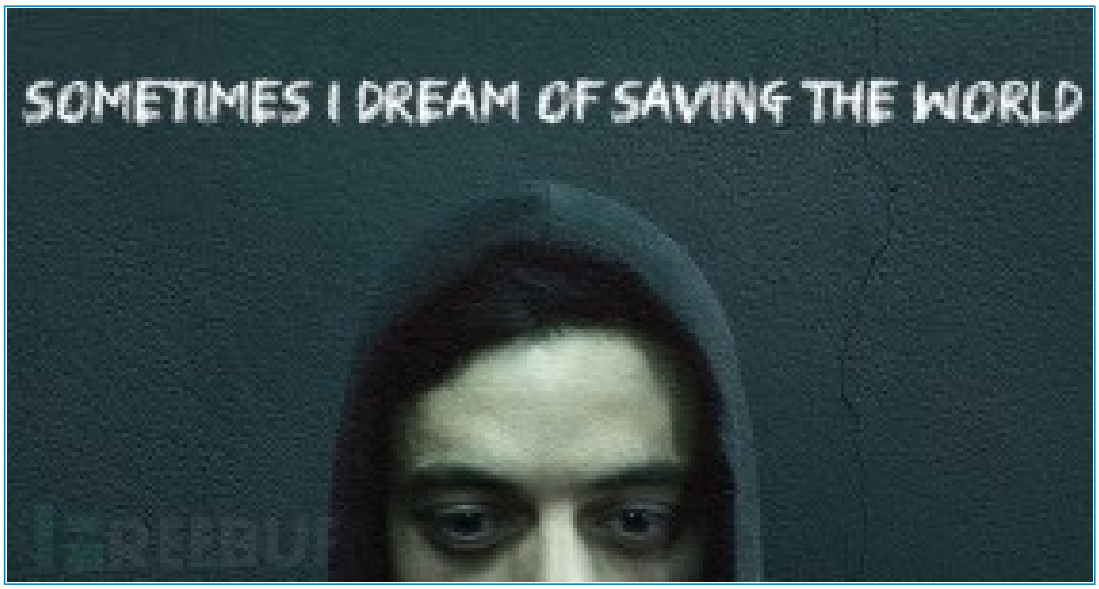
挖洞经验丨敏感信息泄露+IDOR+密码确认绕过=账户劫持

转载

systemino 于 2019-07-29 13:38:18 发布

本文中涉及到的相关漏洞已报送厂商并得到修复，本文仅限技术研究与讨论，严禁用于非法用途，否则产生的一切后果自行承担。

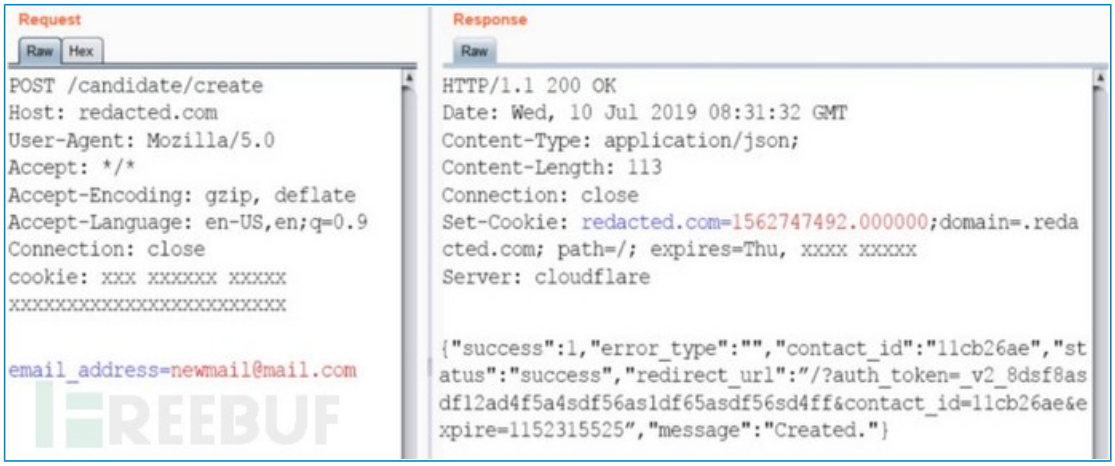


今天分享的这篇Writeup是作者在HackerOne上某个邀请测试项目的发现，目标网站存在不安全的访问控制措施，可以利用其导致的敏感信息泄露(auth_token) +密码重置限制绕过，以越权（IDOR）方式，实现网站任意账户劫持（Takeover）。整个测试过程是一次最基本的IDOR和密码限制绕过操作，一起来看看。 PHP大马

获得账户auth_token

目标网站是一个工作招聘门户网站，测试保密原因暂且称其为redacted.com。一开始，我登录以应聘者身份去测试CSRF或某些存储型XSS，但没什么发现。接下来，我就想到了越权测试（IDOR），为此，我又创建了另外一个账号，两个账号一起可以测试如注册、登录、忘记密码等功能点的越权可能。

创建账号前我开启了流量抓包想看看具体服务端的响应，注册开始时，网站会跳出一个提示，输入注册邮箱检查是否是注册用户。在这里，我随便输入了一个未注册过的邮箱，服务端竟然有了异常响应，如下：



其中包含了auth_token的信息：

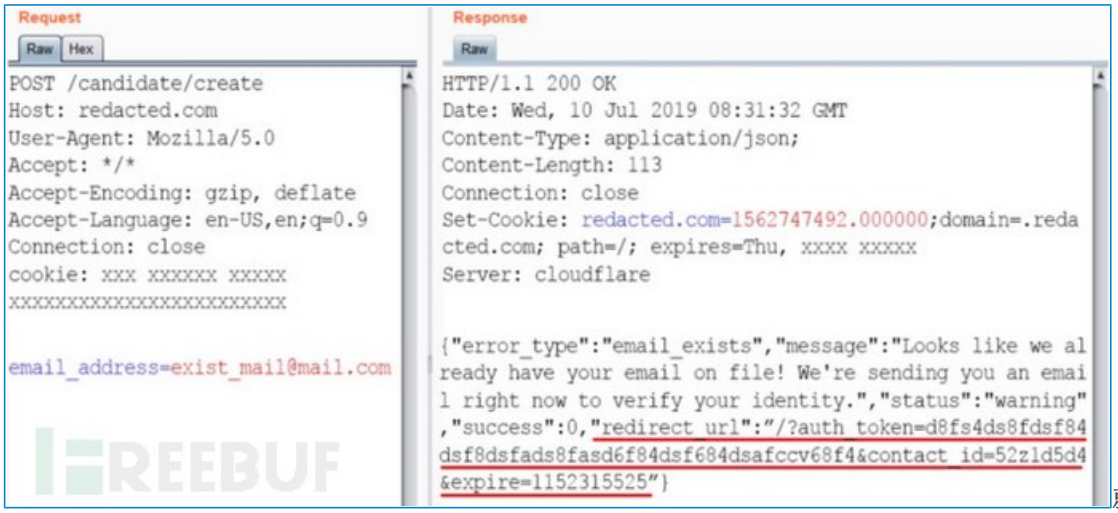
```
“redirect_url”:“/?auth_token=_v2_8dsf8as

df12ad4f5a4sdf56as1df65asdf56sd4ff&contact_id=11cb26ae&e

xpire=1152315525”
```

账户劫持（Account Takeover）

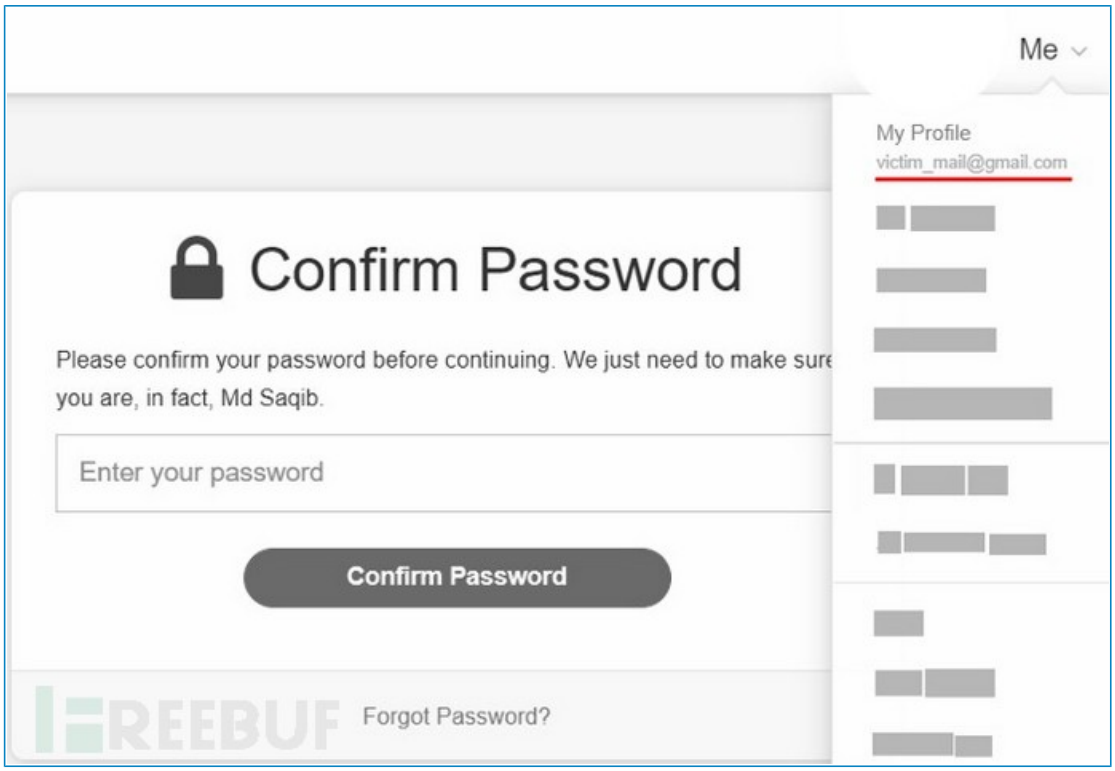
哦，这就有点意思了，于是，我把这个邮箱更改为我另一个与注册账号对应的邮箱：



就这样！也就是说，通过“/candidate/create”这个路径我就能获取网站注册用户的auth_token信息了。现在我只需要一个利用它的点就行，接着，我在 burpsuite的代理历史中查看有哪些请求用到了auth_token，哦，很简单，就是这个：

> https://redacted.com/?auth_token=d8fs4ds8fdsf84dsf8dsfads8fasd6f84dsf684dsafccv68f4&contact_id=52z1d5d4&expire=1152315525

我开启了浏览器隐身模式访问了上述链接，BOOM，就这么简单地登录到了受害者账户（另一测试账户）中去了，完美的账户劫持。但当我查看受害者账户中的个人资料想更改密码或注册邮箱时，却无法看到个人资料信息，而且跳出来一个密码确认输入框（仔细观察，其中包含Forgot Password忘记密码功能）：



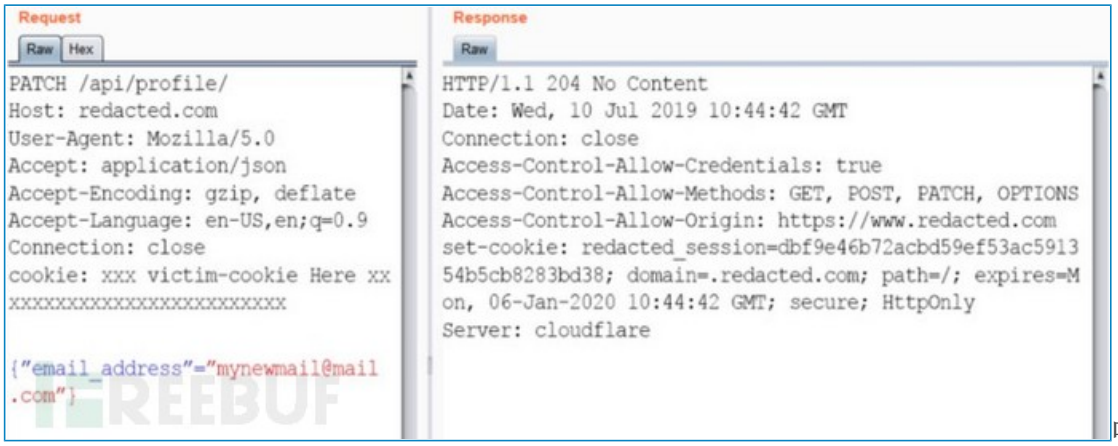
该死，如何来绕过它呢？

绕过密码确认限制

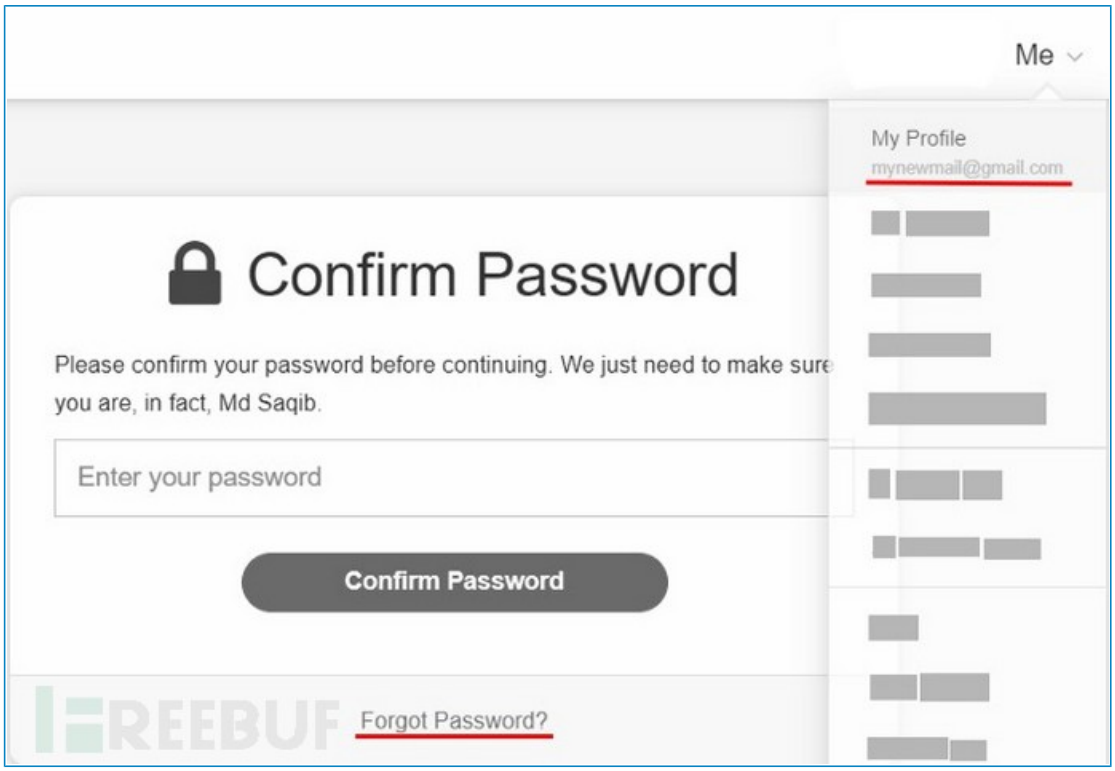
先来一种猜想：要是我把受害都注册邮箱更改为我自己的邮箱，然后利用忘记密码功能发送密码更改请求，那我的邮箱会不会收到密码重置链接呢？来试试看。

于是，我在我自己的测试账户中找到了注册邮箱更改路径为 '/api/profile'，该路径下，通过类似{"email_address":"attackers@gmail.com"}`的JSON格式PATCH请求，就能实现注册邮箱更改。天天好彩

接下来，我在受害者账户登录cookie下，以这种方式在"https://redacted.com/api/profile"下，发送了JSON格式的PATCH请求-'{"email_address":"mynewmail@gmail.com"}' ：



响应成功显示请求有效，那么之后，我只需登录受害者账户环境，点击个人资料查看，在跳出的密码确认框那点击忘记密码（Forgot Password），那么我自己的邮箱就能收到服务端发来的一封密码重置链接邮件了。



漏洞上报后，厂商在四天之内做了修复，最终我也获得了$2,500美金的奖励。但后来，我又发现目标网站还存在一个类似上述可通过更改邮箱绕过密码确认的路径“/contact/api/update/v1”，上报之后，我又获得了厂商$150美金奖励。