换一种姿势挖掘任意用户密码重置漏洞

 上一篇文章我们提到了利用 Unicode 规范化来挖洞的思路以及方法，大家反响很热烈

一直在后台给我留言，苦苦哀求

让我憋 tm 写了，一直写烦不烦呀

现在的读者都已经这么体贴了吗？都已经开始关心我辛苦码字烦躁不烦躁了吗？

别担心，好歹我也是曾被称为阳光幼儿园四班劳动积极分子的男人，这点苦，不算啥！

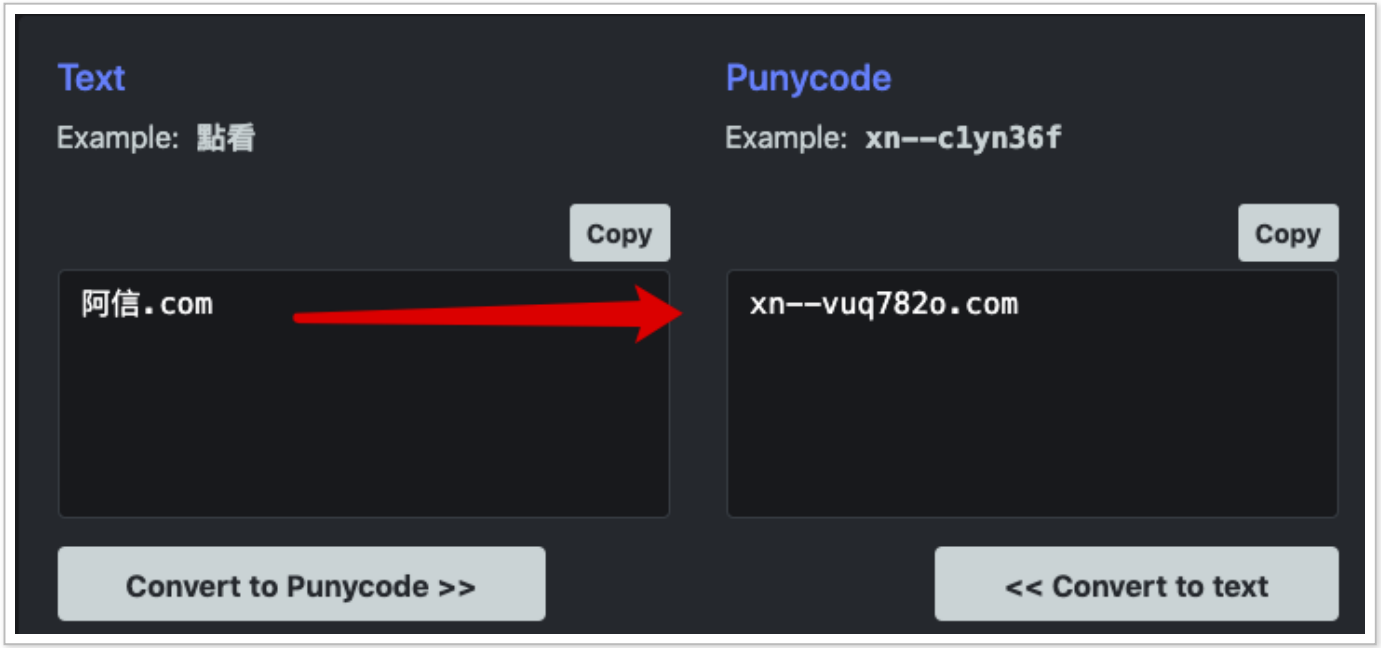
于是我打开电脑，给你们写了这篇。

国际化域名（IDN) 简介

上文已经提到过这个东西了，其实很简单，咱们通常使用的域名都是英文（ascii) 字符的，而 IDN 则允许我们注册 ascii 字符以外的字符为域名，比如我可以注册一个域名为 “阿信. com”，是不是挺拉风的😃

虽然我们是注册了这么一个域名奥，但是可能是为了方便存储？（我也不知道方便啥 🤔），国际化域名中提供了一种其他字符的域名到 ascii 字符域名的一个映射，这个映射就是 Punnycode，你可以到如下地址体验一下中文域名转换为 Punnycode 是啥样的：

https://www.punycoder.com/



漏洞场景

有了以上基础，我们来看一下大佬挖到的一个价值 $600 的任意用户密码重置漏洞。

我们假设目标网站地址为 `https://axin.com`

本次存在漏洞的接口为 `https://axin.com/forget-password?email=` ，可以看到，这是一个再普通不过的通过邮箱重置密码的功能点

但是这个接口没能正确的处理 Unicode 字符，也就是说，当我输入邮箱 `victim@gmáil.com` 会被规范化为 `victim@gmail.com`

然后目标站点 `axin.com` 就会把 `victim@gmail.com` 用户的重置密码链接发送到邮箱 `victim@xn--gmil-6na.com` 中，其中 `xn--gmil-6na.com` 是 `gmáil.com` 的 punnycode

所以，只要我去注册 `gmáil.com` 域名，并搭建一个邮件服务器就能够完成攻击

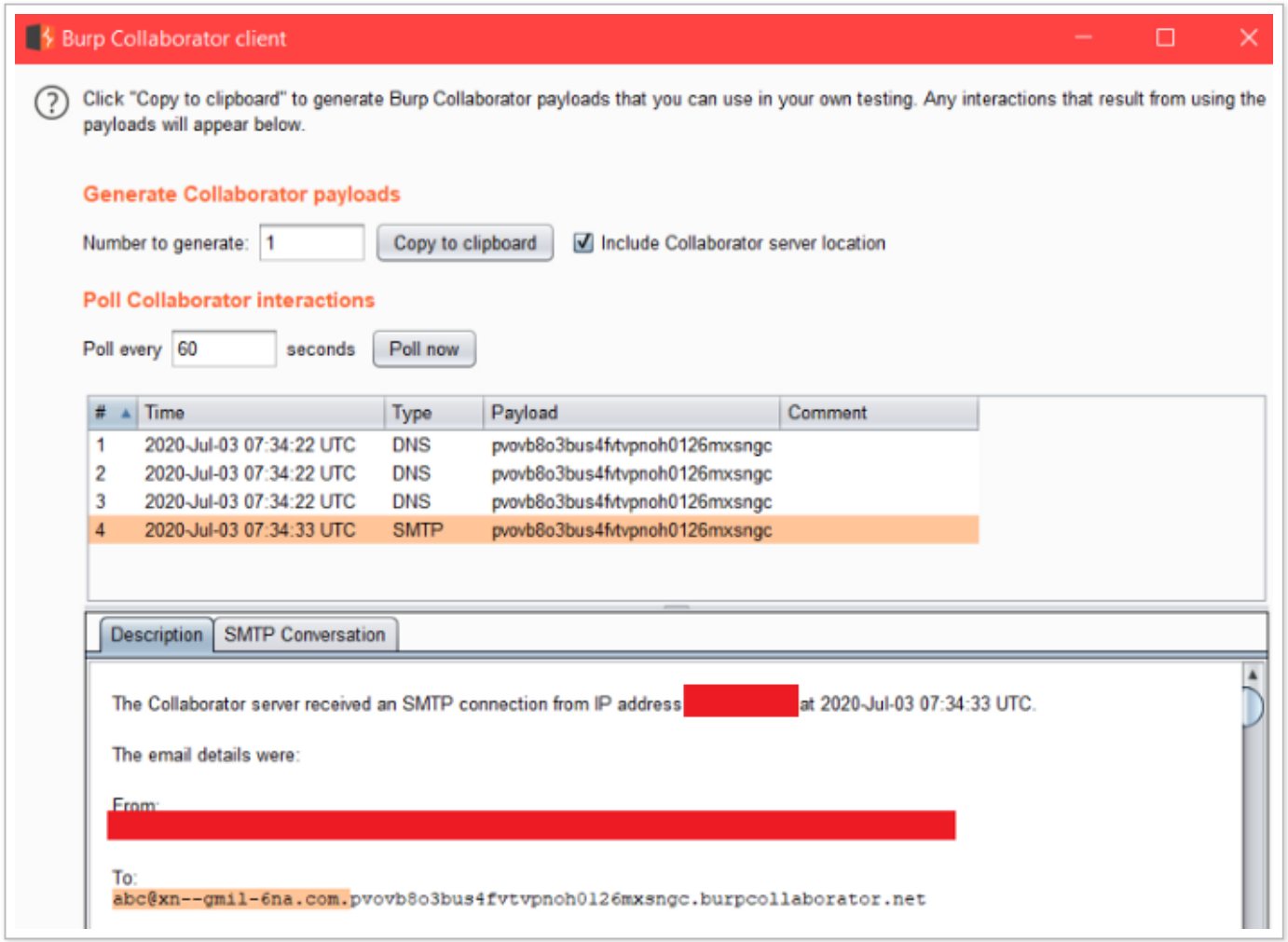
那有人又要说了，“这个漏洞的挖掘成本也太高了，还要去注册域名，太麻烦！”

其实，duck 不必自己去注册域名，我们只要确定这个点是存在 Unicode 规范化就行，借助 burp 插件 collabrator client 就可以实现

我们都知道 burp 为了方便我们测试一些没有回显的漏洞，提供了一个在公网能够访问到的域名 `burpcollaborator.net` ，并且在使用 collabrator 的时候会随机生成一个二级域名供我们使用，比如 `3bfqygorkwzimx55ppnmvkandej47t.burpcollaborator.net`

那我们怎么利用这个域名来挖掘这种漏洞呢？其实很简单，流程如下：

- 到目标站点用邮箱 `victim@gmail.com.3bfqygorkwzimx55ppnmvkandej47t.burpcollaborator.net` 注册一个测试账号
- 然后在重置密码的接口处输入含有 Unicode 字符的邮箱地址：`victim@gmáil.com.3bfqygorkwzimx55ppnmvkandej47t.burpcollaborator.net` ，发送
- 如果目标存在漏洞，我们就可以在 collobrator client 上看到目标站点发送给我们的 `victim@gmail.com` 用户的重置密码链接了


Burp Collaborator client
Click "Copy to clipboard" to generate Burp Collaborator payloads that you can use in your own testing. Any interactions that result from using the payloads will appear below.
Generate Collaborator payloads
Number to generate: 1
Copy to clipboard
Include Collaborator server location
Poll Collaborator interactions
Poll every 60 seconds
Poll now
Time Type Payload Comment
1 2020-Jul-03 07:34:22 UTC DNS pvovb8o3bus4fvtvpnoh0126mxsngc
2 2020-Jul-03 07:34:22 UTC DNS pvovb8o3bus4fvtvpnoh0126mxsngc
3 2020-Jul-03 07:34:22 UTC DNS pvovb8o3bus4fvtvpnoh0126mxsngc
4 2020-Jul-03 07:34:33 UTC SMTP pvovb8o3bus4fvtvpnoh0126mxsngc
Description
SMTP Conversation
The Collaborator server received an SMTP connection from IP address [redacted] at 2020-Jul-03 07:34:33 UTC.
The email details were:
From: [redacted]
To:
abc@xn--gmil-6na.com.pvovb8o3bus4fvtvpnoh0126mxsngc.burpcollaborator.net

/