【译】要么保证你的JENKINS绝对安全，要么就受黑客威胁

□ / 2017-08-29 12:09:00 / 浏览数 4110 安全技术 漏洞分析 顶(0) 踩(0)

之前在LevelUP会议上演讲了《Doing Recon Like a Boss》，之后在HackerOne上发布了一篇同样主题的博文。所以我决定开始在公开应用上寻找漏洞来验证那个方法论是否同样适用。作为整个实践过程序的一部分，我决定

第一步-子域名爆破

对于大型的赏金程序来说，子域名爆破是个经典的切入口，但不幸的是我所发现的域名没有什么意思，我就是想找到一些看起来有意思的事。

那接着开始第二阶段吧。

第二步-亚马逊的web服务

亚马逊算不上一个好的切入点，但从snapchat的外观来看可得知它是高度依赖google的，除此之外他们在HackOne的赏金程序说明中提到他们的app是托管在google的。

所以不要在s3 buckets上浪费时间了，去看看其他的地方还有些什么。

第三步-查阅Snapchat在HackerOne的公开报告

作为侦察的一部分，我通常是去寻找已知或公开的漏洞。我快速浏览了他们的活动踪迹，有了下面这些发现

- render.bitstrips.com
- blog.snapchat.com
- accounts.snapchat.com
- fastly.sc-cdn.net
- sc-corp.net (Thanks, Shubs)

“sc-cdn.net” and “sc-corp.net” 引起了我的注意。

我的第一反应是子域名爆破，但这不是在开玩笑么。这些都是corp和cdn域名，更有可能的是大多数有趣的子域名更可能是独立的形式。

现在的问题是如何找到它们？

第四步-使用Censys和Shodan

通常好的开始是从Censys.io上寻找网站证书入手。在censys上，我通常去查询看起来像这样的东西：

```
443.https.tls.certificate.parsed.extensions.subject_alt_name.dns_names:domain.com
```

这足够我找到一些有意思的子域名了，这些域名通过暴力破解是无法找到的。现在来看下找到的结果，有这么一个子域名：REDACTED-jenkins-Environment.sc-corp.net其
alpha, stage, prod, beta, local,
test”配合脚本来寻找不同组合的REDACTED-jenkins-$env.sc-corp.net域名.正如预期的那样，其中一些返回的是302作为其响应代码，这意味它们可能在登录请求的背后。

第五步-从这开始该做什么？

我最初的想法是去尝试访问生产环境然后尝试登陆，接着我去实践了这个想法，才发现这并没有作用。所以，让我们跳到清单上的下一个项，在其他实例上同样进行一样的尝

第六步-利用Jenkins

我写这篇文章不是来谈论提交给Snapchat团队的报告，因为通过阅读在HackerOne上仅有的公开报告和一些基本调查就能猜测到大部分的信息。我写这篇文章的目的是想深

为了演示这些，我使用自己的Jenkins实例来演示不同的攻击场景（截图与提交给Snapchat的报告无关系）

例子1：公开漏洞

CVE-2016-9299 – Jenkins ‘Java Deserialization’ Remote Code Execution Vulnerability.

CVE-2015-8103 – Jenkins CLI – RMI Java Deserialization (Exploit)

例子2：访问构建信息

通常拥有了访问Jenkins内容权限，就相当于拥有访问凭证、API_KEYS，密钥甚至是源码的权限。

例子3：插件

Jenkins允许设置不同的插件，比如Github的OAuth凭证，你可以用来控制用户登录你的组织，这可能导致你的Github token泄漏。

接着可以通过Github的API来获取更多的数据。

比如: https://api.github.com/orgs/ORG_NAME/repos?access_token=XXXXX

例子4：诱人的脚本

正如前面所提到的，脚本控制台允许使用一行代码读取文件：

你可以通过执行下面的操作在服务器上执行命令：

```
def sout = new StringBuilder(), serr = new StringBuilder()
def proc = 'ls /etc/'.execute()
proc.consumeProcessOutput(sout, serr)
proc.waitForOrKill(1000)
println "out> $sout err> $serr"
```

关键点：

1. Jenkins允许你拥有不同用户权限。这意味着你已经被授权了，但不能保证你能够进行远程代码执行。
2. 如果需要通过Github或者Google OAuth进行认证，请不要慌张.
3. 你的权限可能是有限的（不能执行脚本、访问构建信息等等），或许你能访问到人员下的名单用户。这可能赋予你访问Jenkins实例的权限，当然前提是通过暴力破解来获
4. 通常情况，JenKins是用来部署的，所以思路就是寻找IP、主机名等等。如果你控制了Jenkins并想深入的话（在赏金程序中请不要这样做，一是没必要，二是大多程序规
5. 不要向赏金程序提交公开可访问的Jenkins报告，除非你能利用其中一个或者上面例子中的一个。
6. 在提交报告后不久，Snapchat立马删除了实例并给予了我奖励。

他们人也很好，同意我写了这篇文章。

感谢阅读，享受hacking吧。

上一篇：TLS握手协议分析与理解——某HT... 下一篇：先知Xss挑战赛 - L3m0n ...

1. 0 条回复
   - 动动手指，沙发就是你的了！