可选漏洞复现列表（包括但不限于，可自行寻找项目代码查找漏洞，也可自行选择别的漏洞进行复现）要求自己完全弄懂每一个步骤，并能进行解释

https://vulhub.org/#/environments/

ActiveMQ 反序列化漏洞
ActiveMQ 任意文件写入漏洞
Apache Airflow 示例 dag 中的命令注入
Apache Airflow Celery 消息中间件命令执行
Apache Airflow 默认密钥导致的权限绕过
Apereo CAS 4.1 反序列化命令执行漏洞
Apache APISIX 默认密钥漏洞
AppWeb 认证绕过漏洞
Aria2 任意文件写入漏洞
Bash Shellshock 破壳漏洞
Celery <4.0 Redis 未授权访问+Pickle 反序列化利用
CGI HTTPoxy 漏洞
Adobe ColdFusion 文件读取漏洞
Adobe ColdFusion 反序列化漏洞
Atlassian Confluence 路径穿越与命令执行漏洞
Atlassian Confluence OGNL 表达式注入代码执行漏洞
Couchdb 垂直权限绕过漏洞
Couchdb 任意命令执行漏洞
Discuz 7.x/6.x 全局变量防御绕过导致代码执行
Discuz!X ≤3.4 任意文件删除漏洞
Django debug page XSS 漏洞
Django < 2.0.8 任意 URL 跳转漏洞
Django JSONField/HStoreField SQL 注入漏洞
Django GIS SQL 注入漏洞
Django QuerySet.order_by() SQL 注入漏洞
DNS 域传送漏洞
docker daemon api 未授权访问漏洞
Drupal < 7.32 “Drupalgeddon” SQL 注入漏洞
Drupal Core 8 PECL YAML 反序列化任意代码执行漏洞
Drupal Drupalgeddon 2 远程代码执行漏洞
Drupal 远程代码执行漏洞
Drupal 远程代码执行漏洞
Drupal XSS 漏洞
Aapche Dubbo Java 反序列化漏洞
ECShop 4.x collection_list SQL 注入
ECShop 2.x/3.x SQL 注入/任意代码执行漏洞
ElasticSearch 命令执行漏洞
ElasticSearch Groovy 沙盒绕过 && 代码执行漏洞
ElasticSearch 插件目录穿越漏洞
ElasticSearch 目录穿越漏洞
Elasticsearch 写入 webshell 漏洞

electron 远程命令执行漏洞
Electron WebPreferences 远程命令执行漏洞
elFinder ZIP 参数与任意命令注入
fastjson 反序列化导致任意命令执行漏洞
Fastjson 1.2.47 远程命令执行漏洞
ffmpeg 任意文件读取漏洞/SSRF 漏洞
ffmpeg 任意文件读取漏洞
Jinja2 SSTI 模板注入
Apache Flink 文件上传漏洞
Apache Flink jobmanager/logs 目录穿越漏洞
GhostScript 沙箱绕过（命令执行）漏洞
GhostScript 沙箱绕过（命令执行）漏洞
GhostScript 沙箱绕过（命令执行）漏洞
GIT-SHELL 沙盒绕过
Gitea 1.4.0 目录穿越导致命令执行漏洞
GitLab 任意文件读取漏洞
GitLab 远程命令执行漏洞
gitlist 0.6.0 远程命令执行漏洞
GlassFish 任意文件读取漏洞
GoAhead 远程命令执行漏洞
GoAhead Server 环境变量注入
Gogs 任意用户登录漏洞
Grafana 8.x 插件模块目录穿越漏洞
H2 Database Console 未授权访问
Hadoop YARN ResourceManager 未授权访问漏洞
Apache HTTPD 换行解析漏洞
Apache HTTP Server 2.4.48 mod_proxy SSRF 漏洞
Apache HTTP Server 2.4.49 路径穿越漏洞
Apache HTTP Server 2.4.50 路径穿越漏洞
Apache HTTPD 未知后缀解析漏洞
Apache SSI 远程命令执行漏洞
Imagemagick PDF 密码位置命令注入漏洞
Imagetragick 命令执行漏洞
Influxdb 未授权访问漏洞
Jackson-databind 反序列化漏洞
Java RMI codebase 远程代码执行漏洞
Java RMI Registry 反序列化漏洞(<=jdk8u111)
Java RMI Registry 反序列化漏洞(<jdk8u232_b09)
JBoss 5.x/6.x 反序列化漏洞
JBoss 4.x JBossMQ JMS 反序列化漏洞
JBoss JMXInvokerServlet 反序列化漏洞
Jenkins-CI 远程代码执行漏洞
Jenkins 远程命令执行漏洞
Jetty WEB-INF 敏感信息泄露漏洞

Jetty 通用 Servlets 组件 ConcatServlet 信息泄露漏洞
Jetty WEB-INF 敏感信息泄露漏洞
Atlassian Jira 模板注入漏洞
Jmeter RMI 反序列化命令执行漏洞（CVE-2018-1297）
Joomla 3.4.5 反序列化漏洞
Joomla 3.7.0 SQL 注入漏洞
Jupyter Notebook 未授权访问漏洞
Kibana 本地文件包含漏洞
Kibana 原型链污染导致任意代码执行漏洞
Laravel Ignition 2.5.1 代码执行漏洞
libssh 服务端权限认证绕过漏洞
Liferay Portal CE 反序列化命令执行漏洞
Apache Log4j Server 反序列化命令执行漏洞
Apache Log4j2 lookup JNDI 注入漏洞
Magento 2.2 SQL 注入漏洞
mini_httpd 任意文件读取漏洞
Mojarra JSF ViewState 反序列化漏洞
mongo-express 远程代码执行漏洞
Mysql 身份认证绕过漏洞
Nacos 认证绕过漏洞
Neo4j Shell Server 反序列化漏洞
Nexus Repository Manager 3 远程命令执行漏洞
Nexus Repository Manager 3 远程命令执行漏洞
Nexus Repository Manager 3 远程命令执行漏洞
Nginx 文件名逻辑漏洞
Nginx 越界读取缓存漏洞
Nginx 配置错误三例
Nginx 解析漏洞
Node.js 目录穿越漏洞
node-postgres 代码执行漏洞分析
ntopng 权限绕过漏洞
Apache OfBiz 反序列化命令执行漏洞
OpenSMTPD 远程命令执行漏洞 (CVE-2020-7247)
OpenSSH 用户名枚举漏洞
OpenSSL 心脏出血漏洞
OpenSSL 无限循环 DOS 漏洞
PHP 8.1.0-dev 开发版本后门事件
PHP-CGI 远程代码执行漏洞
PHP imap 远程命令执行漏洞
PHP-FPM 远程代码执行漏洞
PHP-FPM Fastcgi 未授权访问漏洞
PHP 文件包含漏洞（利用 phpinfo）
PHP XML 实体注入
XDebug 远程调试漏洞（代码执行）

PHPMailer 任意文件读取漏洞
phpMyAdmin 4.0.x—4.6.2 远程代码执行漏洞
phpmyadmin 4.8.1 远程文件包含漏洞
phpmyadmin scripts/setup.php 反序列化漏洞
phpunit 远程代码执行漏洞
Polkit pkexec 权限提升漏洞
PostgreSQL 提权漏洞
PostgreSQL 高权限命令执行漏洞（CVE-2019-9193）
Python PIL 远程命令执行漏洞（GhostButt）
Python PIL 远程命令执行漏洞（via Ghostscript）
Python unpickle 反序列化漏洞
Ruby On Rails 路径穿越漏洞
Ruby on Rails 路径穿越与任意文件读取漏洞
Redis 4.x/5.x 主从复制导致的命令执行
Redis Lua 沙盒绕过命令执行
Rocket Chat MongoDB 注入漏洞
rsync 未授权访问漏洞
Ruby Net::FTP 模块命令注入漏洞
SaltStack 水平权限绕过漏洞
SaltStack 任意文件读写漏洞
SaltStack 命令注入漏洞
Samba 远程命令执行漏洞
scrapyd 未授权访问漏洞
Apache Shiro 1.2.4 反序列化漏洞
Apache Shiro 认证绕过漏洞
Apache Skywalking 8.3.0 SQL 注入漏洞
Apache Solr 远程命令执行漏洞
Apache Solr XML 实体注入漏洞
Apache Solr 远程命令执行漏洞
Apache Solr Velocity 注入远程命令执行漏洞
Apache Solr RemoteStreaming 文件读取与 SSRF 漏洞
Apache Spark 未授权访问漏
Spring Security Oauth2 远程命令执行漏洞
Spring WebFlow 远程代码执行漏洞
Spring Data Rest 远程命令执行漏洞
Spring Messaging 远程命令执行漏洞
Spring Data Commons 远程命令执行漏洞
Spring Cloud Gateway Actuator API SpEL 表达式注入命令执行
Spring Cloud Function SpEL 表达式命令注入
Spring 框架 Data Binding 与 JDK 9+导致的远程代码执行漏洞
S2-001 远程代码执行漏洞
S2-005 远程代码执行漏洞
S2-007 远程代码执行漏洞
S2-008 远程代码执行漏洞

S2-009 远程代码执行漏洞
S2-012 远程代码执行漏洞
S2-013 远程代码执行漏洞
S2-015 远程代码执行漏洞
S2-016 远程代码执行漏洞
S2-032 远程代码执行漏洞
S2-045 远程代码执行漏洞
S2-046 远程代码执行漏洞
S2-048 远程代码执行漏洞
S2-052 远程代码执行漏洞
S2-053 远程代码执行漏洞
Struts2 S2-057 远程命令执行漏洞
Struts2 S2-059 远程命令执行漏洞
Struts2 S2-061 远程命令执行漏洞
Supervisord 远程命令执行漏洞
ThinkPHP 2.x 任意代码执行漏洞
ThinkPHP5 5.0.22/5.1.29 远程代码执行漏洞
ThinkPHP5 5.0.23 远程代码执行漏洞
ThinkPHP5 SQL 注入漏洞/信息泄露
Tiki Wiki CMS Groupware 认证绕过漏洞
Tomcat PUT 方法任意写文件漏洞
Aapache Tomcat AJP 文件包含漏洞
Tomcat 弱口令
Apache Unomi 远程表达式代码执行漏洞
uWSGI PHP 目录穿越漏洞
uWSGI 未授权访问漏洞
Weblogic < 10.3.6 'wls-wsat' XMLDecoder 反序列化漏洞
Weblogic WLS Core Components 反序列化命令执行漏洞
Weblogic 任意文件上传漏洞
Weblogic 管理控制台未授权远程命令执行漏洞
Weblogic SSRF 漏洞
Weblogic 文件读取漏洞
Webmin 远程命令执行漏洞
Wordpress 4.6 任意命令执行漏洞（PwnScriptum）
XStream 反序列化命令执行漏洞
XStream 反序列化命令执行漏洞
XXL-JOB executor 未授权访问漏洞
YApi 开放注册导致 RCE
zabbix latest.php SQL 注入漏洞
Zabbix Server trapper 命令注入漏洞