实验：学习 Web 攻击

评分标准：

（1）必做题做完，根据实验结果，小组每人获得基本分 70-75 分，做第 1 题的同学个人加 5-8 分，做第 2 题的同学个人加 8-15 分。
（2）对于选做题，每个同学每做 1 题，个人加 10-15 分。
（3）满分不超过 100 分。

【关于本次实验的配置环境，有点复杂，建议大家在一个相对干净的操作系统上部署实验，比如在虚拟机上安装 win10，win10 上之前没有部署 mysql】

为了保证主机环境的安全，请在虚拟机上部署实验环境。本次实验建议在 windows 的系统上做。

本实验过程中会碰到的各种可能的问题，及解决办法：

1. 针对任务 1.1 和 1.2，之前已经安装了 mysql，本次实验又安装 mysql，可能本次安装不成功或者安装成功了但是不能用，可能是因为本次安装 mysql 时默认端口被占用，建议如果已经有 mysql 了，就不要再安装了。
2. 针对任务 1.1 和 1.2，之前已经安装了 mysql，如果卸载了，有可能没下载干净，导致实验的时候读取到之前版本 mysql 的配置文件，如果版本不兼容，也可能存在问题。

任务 1：利用现有工具实施 web 攻击【必做题】

任务 1.1： SQL 注入攻击

（1）实验原理

所谓 SQL 注入，就是通过把 SQL 命令插入到 Web 表单提交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的 SQL 命令。

它是利用现有应用程序，可以通过在 Web 表单中输入（恶意）SQL 语句得到一个存在安全漏洞的网站上的数据库。

比如先前的很多影视网站泄露 VIP 会员密码大多就是通过 WEB 表单递交查询字符暴出的，这类表单特别容易受到 SQL 注入式攻击。例：12306.cn 和 csdn 等网站帐号和密码的泄露，都有可能是 sql 注入导致的。

（2）实验环境

下载软件：

1. phpStudy 是一个 PHP 调试环境的程序集成包，包含"PHP+Mysql+Apache"。
   Phpstudy 下载地址 https://www.xp.cn；
   安装参考 https://www.jianshu.com/p/aef111e0ce5d
   安装到 Kali 或者 win10
   注意：PHP 的版本，7.X 版本不行
   注意：安装 python 5.3-7 之间的 python 环境，否则本实验会不符合理论。

2. SQLmap 是一个自动化的 SQL 注入工具，其主要功能是扫描，发现并利用给定的 URL 的 SQL 注入漏洞，目前支持的数据库是 MySQL，Oracle，PostgreSQL，Microsoft SQL Server，Microsoft Acess，IBM DB2，SQLLite，Firebird，Sybase 和 SAP MaxDB……SQLmap 采用几种独特的 SQL 注入技术，分别是盲推理 SQL 注入，UNION 查询 SQL 注入，对查询和盲注。其广泛的功能和选项包括数据库指纹，枚举，数据库提取，访问目标文件系统，并在获取完全操作权限时实行任意命令。

2. Sqli-labs：SQLI-LABS 是集成了多种 SQL 注入类型的漏洞测试环境，可以用来学习不同类型的 SQL 注入。

下载地址：https://github.com/Audi-1/sqli-labs

安装参考：https://www.fujieace.com/penetration-test/sqli-labs-ec.html

Sqli-labs 应用学习视频：

https://blog.csdn.net/qq_41420747/article/details/81836327

https://blog.csdn.net/he_and/article/details/79979616

（3）实验任务

- 对 Phpstudy、SQLmap 和 Sqli-labs 的安装过程和配置进行截图以及文字说明
- 练习 Less-1 GET - Error based - Single quotes - String，完成以下任务：（1）找到注入点；（2）获得数据库名字；（3）获得数据表的名称；（4）获得每个数据表的字段数量和名称；（5）获得某一个数据表（自己指定）id=2 的记录的值；（6）获得某一个数据库中全部的数据。
- 练习 Less-2、Less-3、Less-4，找到注入点，学习 SQL 语句的闭合；
- 练习 Less-8 GET - Blind - Boolian Based - Single Quotes ，完成以下任务：（1）找到注入点；（2）获得数据库名字；（3）获得数据表的名称；（4）获得每个数据表的字段数量和名称；（5）获得某一个数据表（自己指定）id=2 的记录的值；（6）获得某一个数据库中全部的数据。【不要用工具，要自己写语句实现】
- 做更多练习；
- 对实验过程的每个步骤进行截图以及文字说明

任务 1.2： XSS 攻击和 CSRF 攻击

（1）实验原理

XSS（Cross Site Script）攻击，从本质上来说就是将恶意的 HTML 或者 Javascript 等注入到了静态脚本代码中，当浏览器渲染整个 HTML 文档的过程中触发了注入的脚本，导致了 XSS 攻击的发生。XSS 是一种在 web 应用中的计算机安全漏洞，它允许恶意 web 用户将代码植入到提供给其它用户使用的页面中。从而达到攻击的目的。如，盗取用户 Cookie、破坏页面结构、重定向到其它网站等。

CSRF（Cross-site request forgery），中文名称：跨站请求伪造。可以这么理解 CSRF 攻击：攻击者盗用了你的身份，以你的名义发送恶意请求。CSRF 能够做的事情包括：以你名义发送邮件，发消息，盗取你的账号，甚至于购买商品，虚拟货币转账.....造成的问题包括：个人隐私泄露以及财产安全。

（2）实验环境

1. phpStudy 是一个 PHP 调试环境的程序集成包，包含"PHP+Mysql+Apache"。（如果之前的环境安装了 PHP+Mysql+Apache，可以不用安装 phpStudy）

Phpstudy 下载地址 https://www.xp.cn/，

安装参考 https://www.jianshu.com/p/aef111e0ce5d

安装到 win10

2. DVWA 是一款基于 PHP 和 mysql 开发的 web 靶场练习平台，集成了常见的 web 漏洞如 sql 注入，密码破解等常见漏洞。

下载地址：https://github.com/ethicalhack3r/DVWA

配置：放在 phpstudy 的 www 目录下，然后修改 config.inc.php.dist 中的连接数据库的用户名和密码。然后进入 http://localhost/DVWA/setup.php 点击 Create Database，进入 http://localhost/DVWA/login.php，用 username 是 admin，和 password 为 password 账户登录。

参考资料：https://www.freebuf.com/sectool/102661.html

3. Burp Suite 是用于攻击 web 应用程序的集成平台。它包含了许多 Burp 工具，这些不同的 burp 工具通过协同工作，有效的分享信息，支持以某种工具中的信息为基础供另一种工具使用的方式发起攻击。它主要用来做安全性渗透测试，可以实现拦截请求、Burp Spider 爬虫、漏洞扫描（付费）等类似 Fiddler 和 Postman 但比其更强大的功能。

下载地址 https://portswigger.net/burp/

（3）实验任务

- 对 Phpstudy、DVWA 和 Burp Suite 的安装过程和配置进行截图以及文字说明
- 具体实验任务包括以下三点：

1) 学习存储型 XSS 攻击

输入 low 级别测试代码： <script>alert(/xss/)</script>

输入 Medium 级别测试代码：<sc<script>ript>alert(/xss/)</script>

输入 High 级别测试代码： <img src=1 onerror=alert(1)>

参考资料：https://www.cnblogs.com/hzk001/p/12261728.html

2) 学习反射性 XSS 攻击

输入 low 级别测试代码： <script>alert('hack')</script>

输入 Medium 级别测试代码：<SCRIPT>alert('hack')</SCRIPT>

输入 High 级别测试代码： <img src=1 onerror=alert(/hack/)>

输入 Impossible 级别测试代码： <script>alert('hack')</script>

参考资料：https://zhuanlan.zhihu.com/p/88013741

3) 学习 CSRF 攻击

修改用户密码

实现 low 级别测试

实现 Medium 级别测试

实现 High 级别测试代码

参考资料：

https://blog.csdn.net/qq_42785117/article/details/97008858?utm_medium=distribute.pc_relevant.none-task-blog-BlogCommendFromMachineLearnPai2-1.channel_param&depth_1-u

tm_source=distribute.pc_relevant.none-task-blog-BlogCommendFromMachineLearnPai2-1.channel_param

https://blog.csdn.net/yaofeiNO1/article/details/54667698

- 学习使用 Burp Suite 对注入过程的流量进行抓包

  参考资料：https://blog.csdn.net/LUOBIKUN/article/details/87457545
- 对 DVWA 的安装过程进行截图以及文字说明
- 对实验过程的每个步骤进行截图以及文字说明
- 对攻击前后代码的变化进行截图比较及文字说明

任务 2：选做题

任务 2.1 基于二分法的盲注，完成以下内容：

学习任务 1.1 中实验环境配置，练习 less-15 POST - Blind- Boolian/time Based - Single quotes，编写脚本，构造 http post 请求，基于二分法，实现基于 bool 型/时间延迟单引号 POST 型盲注。

任务 2.2 Apache Log4J2 漏洞复现

1、根据参考资料（1）学习 Log4J2 漏洞利用的原理

2、根据参考资料（1）和（2）配置安装 CentOS 和 vulfocus 靶场

3、根据参考资料（3）配置环境，复现 Log4J2 漏洞

4、学习 Log4J2 漏洞修复方案

参考资料：

（1）https://www.cnblogs.com/hhhhhxian/p/16214263.html

（2）https://cloud.tencent.com/developer/article/1987103

（3）https://blog.csdn.net/qq_46162550/article/details/124720947

任务 2.3 真实环境下自己收集网站信息，实现一个 web 网站的渗透