****

网络安全理论与技术课程设（乙）

Web攻击实验

实 验 报 告

|  |  |  |  |
| --- | --- | --- | --- |
| **学 院** | 网络空间安全学院 | | |
| **专 业** |  | | |
| **班 级** |  | | |
| **学 号** |  | | |
| **学生姓名** |  | | |
| **教师姓名** | 陈黎丽 | | |
| **完成日期** |  | | |
| **成 绩** |  | | |
| **组长/组员姓名** | | **学号** | **报告分工** | |
|  | |  |  | |
|  | |  |  | |
|  | |  |  | |
|  | |  |  | |
| **目录（自动生成，引用可生成）** | | | | |
| **Web攻击实验** | | | | |
| **实验目的**  1、深入理解SQL注入原理、实现和验证SQL注入流程  2、通过不同的代码测试，学习XSS（Cross Site Script）攻击和CSRF（Cross-site request forgery）攻击  3、学习典型web攻击的过程中，提升发现问题解决问题的能力。 | | | | |
| **实验任务**   1. 能够通过把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。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。 2. 通过不同的代码测试反馈的结果的差异，能解释说明XSS（Cross Site Script）攻击和CSRF（Cross-site request forgery）攻击   **扩展功能：**实现基于二分法的盲注、Apache Log4J2漏洞复现、真实环境下自己收集网站信息，实现一个web网站的渗透。（任选一种也可以） | | | | |
| 一、必做题实验任务1（SQL注入攻击）（学生1，学生2）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](https://blog.csdn.net/qq_41420747/article/details/81836327" \l "Less-1 GET - Error based - Single quotes - String(%E5%9F%BA%E4%BA%8E%E9%94%99%E8%AF%AF%E7%9A%84GET%E5%8D%95%E5%BC%95%E5%8F%B7%E5%AD%97%E7%AC%A6%E5%9E%8B%E6%B3%A8%E5%85%A5)" \t "https://blog.csdn.net/qq_41420747/article/details/_self)，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。 * 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  实验原理 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。 实验环境  * 在虚拟机上下载Win10操作系统，并下载相应软件。 * phpstudy是一个PHP调试环境的程序集成包，包含"PHP+Mysql+Apache"。 * Php版本选择php5.5.9。 * 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。 * 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。  实验过程及结果分析实验问题及解决1.1.6 实验总结实验任务2（XSS攻击和CSRF攻击）（学生3） XSS攻击和CSRF攻击 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:   * 学习存储型xSs攻击   输入low级别测试代码:<script>alert(/xss/)<lscript>  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)>   * 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lmpossible 级别测试代码:<script>alert('hack')</script>   * 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 实验原理  * XSS攻击：通常指的是通过利用网页开发时留下的漏洞，通过巧妙的方法注入恶意指令代码到网页，使用户加载并执行攻击者恶意制造的网页程序。这些恶意网页程序通常是JavaScript，但实际上也可以包括Java、 VBScript、ActiveX、 Flash 或者甚至是普通的HTML。攻击成功后，攻击者可能得到包括但不限于更高的权限（如执行一些操作）、私密网页内容、会话和cookie等各种内容。 * CSRF攻击：CSRF漏洞是因为web应用程序在用户进行敏感操作时，如修改账号密码、添加账号、转账等，没有校验表单token或者http请求头中的referer值，从而导致恶意攻击者利用普通用户的身份（cookie）完成攻击行为。  实验环境实验过程及结果分析实验问题及解决实验总结二、选做题（学生4） **2.1.1 实验任务** 2.1.2实验原理2.1.3 实验环境2.1.4 实验过程及结果分析2.1.5实验问题及解决2.1.6 实验总结 | | | | |