信息安全引论

实验五

实验环境

- https://www.cloudrange.cn/
- 账号名：a24XXX（XXX对应各组编号001~051）
- 初始密码：P@ssW0rd，在首次登录后需要修改，各人需要记住自己的密码，选择密码的原则：易记难猜
- 每个账号同时只能有一个位置登录，如果在第二个位置登录，会把第一个位置登录的同学踢出
- 2位同学一组，可以共同讨论一起完成实验
- 也可以独立完成，2个人协商好不同时间就可以

实验分组

帐号	组长	帐号	组长	帐号	组长
a24001	张子苏	a24010	温非凡	a24019	智旭生
a24002	袁傲慕飞	a24011	丁宏骏	a24020	朱俊霖
a24003	李玖熹	a24012	谢佳璇	a24021	任科同
a24004	毛嘉楷	a24013	张弛	a24022	石尚
a24005	许仕熠	a24014	马啸宇	a24023	兰晰程
a24006	黄学郅	a24015	连烨	a24024	胡建波
a24007	黄高翔	a24016	曹原	a24025	冯子康
a24008	张浩卓	a24017	陈冠霖	a24026	李兆彬
a24009	李致城	a24018	蒋轩林	a24027	孟德松

实验分组

帐号	组长	帐号	组长	帐号	组长
a24028	桑钰超	a24037	尹秋衡	a24046	李秀燕
a24029	潘馨仪	a24038	袁晓坤	a24047	邢政
a24030	徐培尧	a24039	张龄心	a24048	孙沐岩
a24031	庞湫凡	a24040	黄净栩	a24049	戴傅聪
a24032	刘鲁阳	a24041	淦林川	a24050	王子琪
a24033	尹骄洋	a24042	屈振华	a24051	王振宇
a24034	吕宗蔚	a24043	徐天艺		
a24035	罗珑赞	a24044	张金涛		
a24036	王昱博	a24045	杨嘉文		

实验五 内容

- 实验内容：

① 探索-OWASP ZAP扫描工具

② 探索-OWASP 敏感数据暴露

③ 认知-Burp Suite - Proxy模块概述

④ 探索-Burp Suite 探索Proxy模块

⑤ 认知-Burp Suite - Repeater与Decoder模块概述

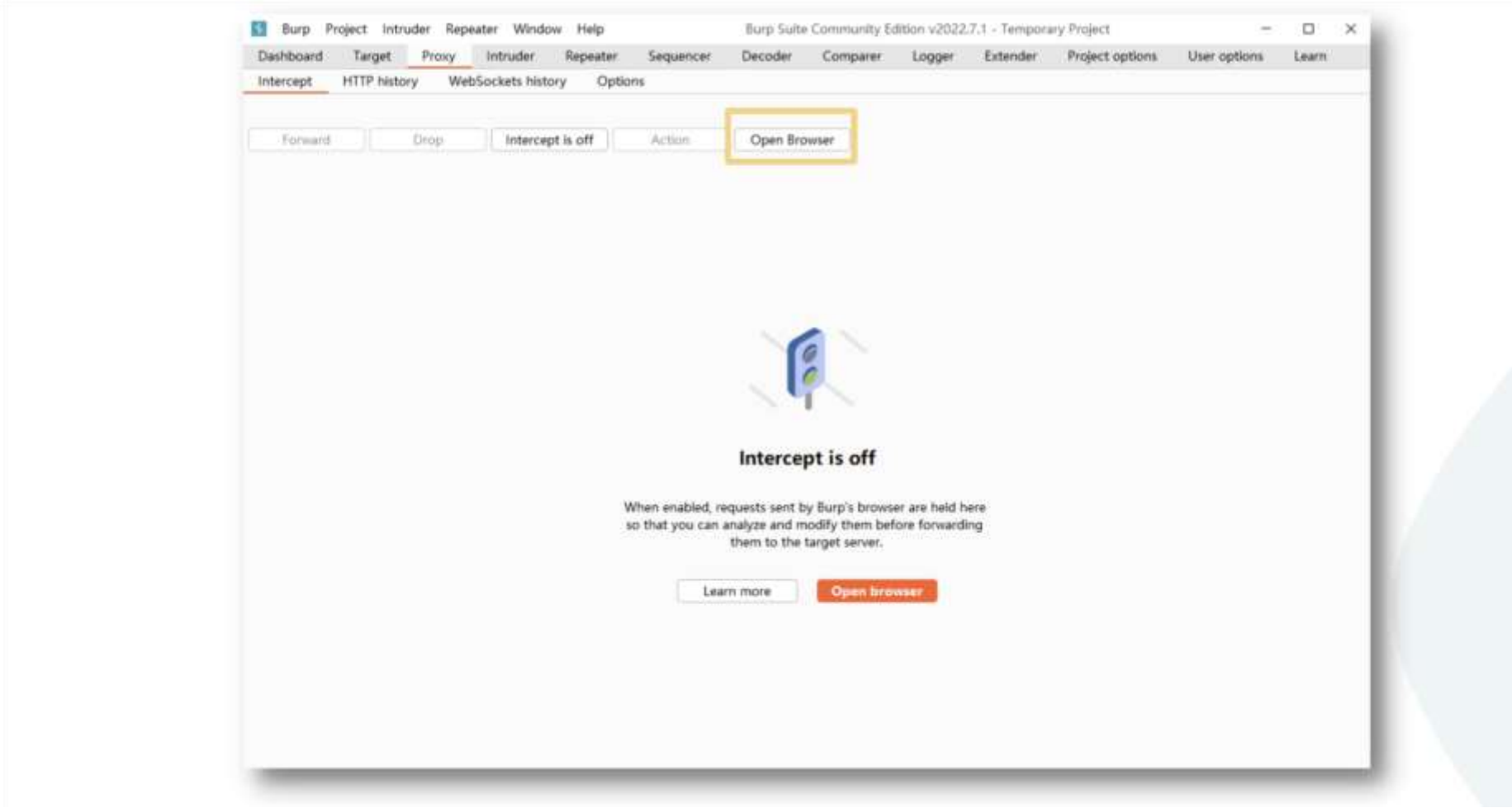
⑥ 探索-OWASP 失效的访问控制

Burp Suite

- Burp Suite 是最著名的用于测试 Web 应用程序安全性的工具。
- 它里面集成了大多数安全测试中常用的功能，而且它还支持通过插件进行扩展，足以帮助安全工程师完成整个安全测试流程。

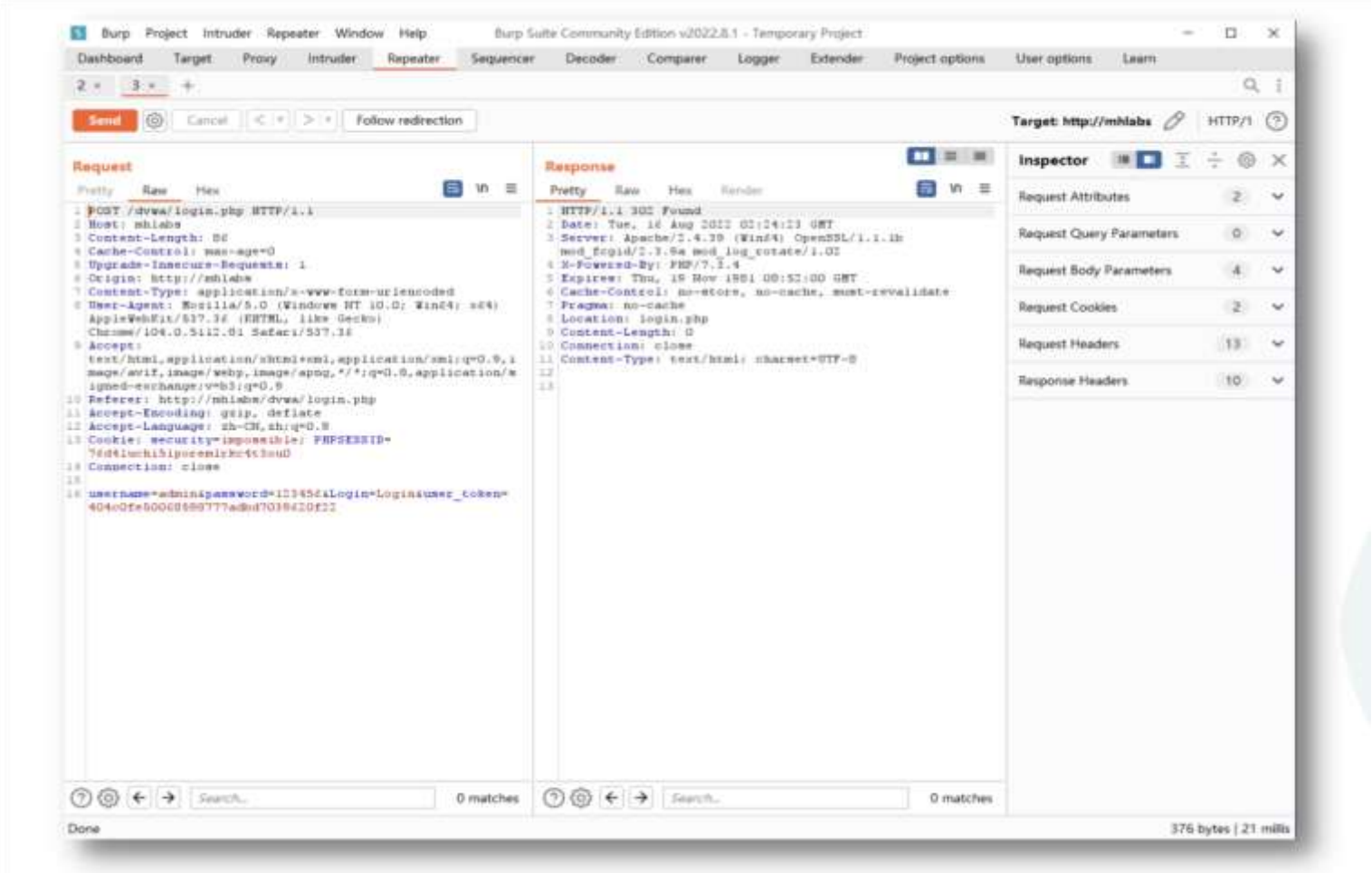
Proxy模块

- Burp Proxy 是Burp Suite以用户驱动测试流程功能的核心，作为 Web 代理服务器，它位于您的浏览器和目标 Web 服务器之间，过代理模式，可以让我们拦截、查看、修改所有在客户端和服务端之间传输的数据。



Repeater模块

- Repeater是一款手工验证HTTP消息的测试工具，通常用于多次重放请求、响应和手工修改请求消息修改后对服务器端响应的消息分析



ICMP

- 支持性协议
- OSI模型中的第三层，网络层
- ICMP依靠IP协议来完成其功能，报文封装在IP报文中
- 虽然是名称是Internet协议，但与TCP/UDP等四层协议无关
- 无连接，不可靠的协议
- 核心功能：
  - 反馈网络中的错误信息，诊断网络故障
  - 判断数据是否能正常抵达目的地
- ICMP的工作机制是一种差错报告的机制，由于封装在IP包中（其中只记录了传输的源目地址），当出现差错时，ICMP消息会被发送给数据传输的源地址，并不会通知中间路径上的设备
- Ping和Traceroute是比较特殊的两个直接使用ICMP来完成功能的应用，其余情况ICMP协议都是被更高层的应用调用。

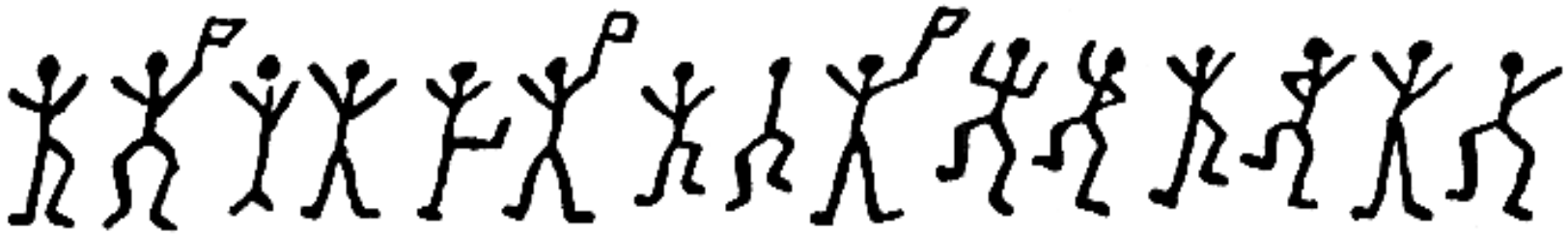
知行实验室版权所有© 2022

实验说明

① 认知实验为视频讲解，熟悉相关知识的可以不用看。

② 探索实验是多个选择题，每个实验指定最长多少时间（比如45分钟）结束。

- 实验成绩只记录探索实验的完成得分




Q&A?