实验10 WebGoat8.0 HTTP Basic攻击实验

1 实验简介

本实验属于网络攻防技术课程-Web攻防技术-Web技术基础章节。

本实验用于加深学生对web应用与浏览器之间数据传输的基本概念和细节，使学生掌握如何通过代理（proxy）抓取请求/响应。

2 预备知识

学生应对Web应用程序有基本的认知，理解HTTP的基本工作过程。

3 实验目的

- 使学生熟悉WebGoat特性
- 能够使用代理工具拦截HTTP 请求与响应
- 能够查看 http request cookies
- 能够查看 java source code
- 加深学生对web应用与浏览器之间数据传输的基本概念和细节

4 实验环境

- ubuntu 虚拟机，内含docker镜像：webgoat/webgoat-8.0；
- kali 2019 虚拟机，内含burpsuite pro等工具。
- 以上虚拟机需要在vm的同一虚拟网络下，例如同在nat连接模式，ip段：10.10.10.0/24

5 实验难度

一般

6 实验内容

所有HTTP传输遵循一致的格式，每个 client request 和 server response都有3个部分：

- request or response 行，例如：

```
GET /index.html?param=value HTTP/1.0
```

- header部分，例如：

```
User-Agent: Mozilla/4.06 Accept: image/gif,image/jpeg, /
```

- body部分

7 实验时长

1课时（45分钟/课时，n为正整数）

8 实验选题背景

介绍与本实验直接相关的现实生产环境、知识背景，实验与现实世界场景、本课程中相关知识、课程外的其他知识或领域的联系。

9 实验步骤

1.启动内含webgoat8.0 docker 镜像的 ubuntu server 虚拟机。启动后，使用ifconfig命令查看虚拟机ip地址。下面以 10.10.10.129 为例。

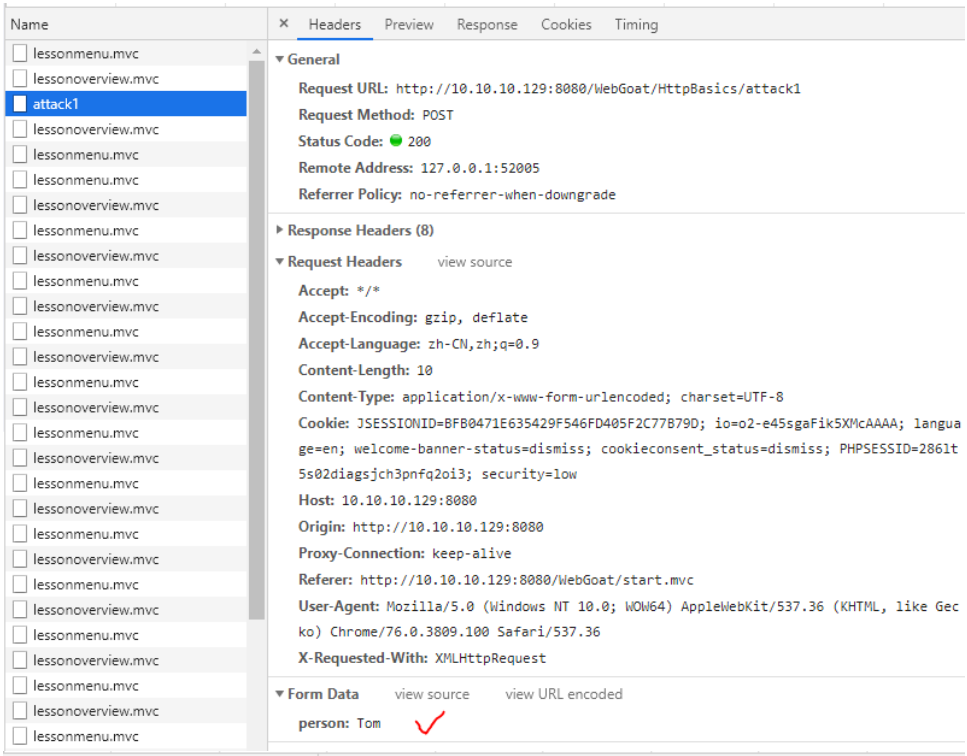
2.运行下列命令启动webgoat/webgoat-8.0 docker 容器。

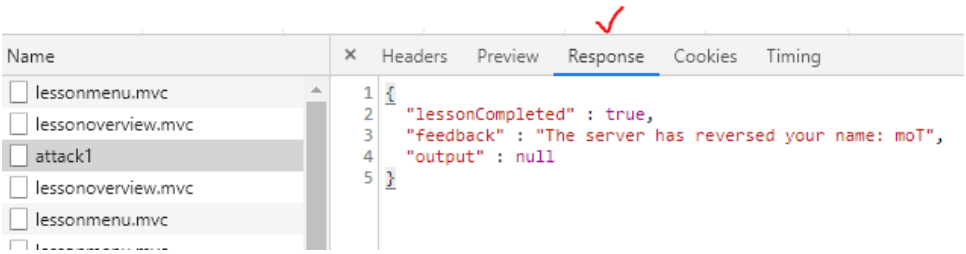
```
sudo docker run --rm -it -p 8080:8080 webgoat/webgoat-8.0
```

之后在某个浏览器上打开这个应用： http://10.10.10.129:8080/WebGoat/login, 然后进行注册用户密码。

3.使用 Google Chrome 浏览器浏览链接：
http://10.10.10.129:8080/WebGoat/start.mvc#lesson/HttpBasics.lesson/1

4.打开chrome浏览器的开发者工具，点击“network”，然后在上图页面中键入“Tom”，然后点击“network”中的“attack1”页面请求。





10 实验总结

> 总结本实验涉及的关键知识、技能、应用方法，对学生的现实实践进行指引。

11 参考资料

> 列举本实验的相关参考资料，保证本实验指导书的严谨性的同时，为学生提供拓展学习资源索引。