山东大学 软件 学院

网络攻防 课堂报告

|  |  |  |
| --- | --- | --- |
| 学号：202200201095 | 姓名： 杨伟康 | 班级： 22网安 |
| 硬件环境：  处理器 11th Gen Intel(R) Core(TM) i5-11400H @ 2.70GHz 2.69 GHz  机带 RAM 16.0 GB (15.9 GB 可用)  设备 ID 9DCDB7C5-EBBA-4C1F-845F-94B127DFAE09  产品 ID 00342-30515-76480-AAOEM  系统类型 64 位操作系统, 基于 x64 的处理器  笔和触控 没有可用于此显示器的笔或触控输入 | | |
| 软件环境：  Window+burpsuite | | |
| Blog记录：   1. Burp Suite简介   Burp Suite（简称BP）是一个面向Web的安全工具，它基于Java开发，集成了多种用于攻击Web应用程序的工具和接口。Burp Suite的主要功能包括拦截HTTP会话、修改数据包、自动化攻击等，是渗透测试中不可或缺的工具之   1. 核心功能—Proxy   数据是一切的基础  Proxy代理模块主要用于拦截浏览器的http会话内容，给其他模块功能提供数据，Proxy模块如下图所示    Proxy模块由四个部分组成，分别是Intercept、HTTP history、Websockets history、options，接下来分别演示使用  第一个功能拦截intercept，内置了浏览器方便渗透测试    拦截开启后所有符合条件的数据包都会被留下  当拦截到新的数据包后，对应的标题会高亮显示，此时我们就可以对数据包进行修改了    修改完成后可以点击放送或丢弃    在操作(Action)一栏中存在很多选项，可以将proxy中的数据包发送至其他模块中    HTTP历史记录  这里记录了每一个HTTP数据包，可以通过此功能查看历史数据包    点击过滤器可以设置过滤选项    最后就是拦截的设置，这里详细说明    1.代理监听器，即数据来源，ip和端口  2. 拦截客户端请求  该部分用于配置请求数据包的拦截条件，支持多条规则同时匹配  现在增加一条规则：拦截所有目标IP为123.123.123.123的数据包    服务器响应拦截和修改  该部分主要配置响应数据包的拦截条件及自动修改    响应规则的自动修改    自动替换，响应和请求中的属性     1. 个人试用   针对软件的支付/充值/兑换功能，对整个操作流程进行抓包，判断有无敏感信息可修改。  1、访问待测的支付界面（以下仅为演示示例），填入订单数据，先不购买    在拦截到的网站请求中下面是网站内容但经过了url加密，  解码后可得feesItemdeforms=1708==&ords==202409&sysid=01060&billamts=1200.00==&feeTotal=1200==&type==&counts=0==&feeamts=1200.00==&unpaid=1200.00==&feeyear==202409,202409==&feesItemordall==1707,1708&userid=202200201095&sign==z1d804059a9c87054596c4e182671288==  指代我们的缴费金额是1200    第九项是unpaid，修改为5元    可以看到学校的付款系统还是比较完善的  支付数据发生变动会拒绝我们访问  想要少交学费的愿望失败了……   1. 其他功能   仪表盘可以看到我们访问的网站可能存在的漏洞    等等 | | |
| 结论分析与体会：  在使用Burp Suite的过程中，我深刻体会到了其Proxy模块的核心价值。作为拦截HTTP/HTTPS数据包的代理服务器，它允许我们在浏览器和目标应用程序之间充当中间人，拦截、查看并修改两个方向上的原始数据流。这种能力对于发现和探索应用程序的漏洞至关重要，通过恶意修改浏览器请求，我们可以进行如SQL注入、cookie欺骗、提升权限、会话劫持等多种攻击测试。  此外，Burp Suite的Scanner模块也给我留下了深刻印象。这个高级工具能够自动地发现Web应用程序的安全漏洞，尽管存在误报的可能，但它仍然为快速识别潜在威胁提供了有力支持。而Intruder模块则以其高度可配置的特性，允许我们对Web应用程序进行定制化的自动化攻击，如枚举标识符、收集有用数据以及使用fuzzing技术探测常规漏洞。  学习过程中，我也遇到了一些挑战。例如，在配置和使用HTTPS证书时，需要确保Burp Suite伪造的公钥证书得到客户端的验证并信任，这需要我们仔细操作并理解证书的工作原理。同时，对于Intruder模块的四种攻击类型（Sniper、Battering ram、Pitchfork、Cluster bomb）的选择和应用，也需要根据具体的测试目标和场景进行灵活调整。 | | |