第5章

重放攻击

CHAPTER 5

通过本章学习，可以达到以下目标：

- 掌握重放攻击概念。
- 掌握 DVWA 网络靶场的安装和常用使用方法。
- 掌握 Web 攻击集成平台 Burp Suite 的常用使用方法。
- 掌握典型重放攻击——DVWA 暴力破解模块低、中两种难度级别攻防案例。

5.1　重放攻击概述

5.1.1　重放攻击的原理

重放攻击(replay attack)又称重播攻击或回放攻击,其基本原理是将以前发送过的报文进行截获,原封不动地或稍加修改后,再重新发送给接收方。重放攻击的发送方既可以是原来的发送方,也可以是利用网络监听的第三方。

重放攻击具有欺骗接收方的目的,最常使用的场景是用于身份认证过程,破坏认证的安全性。攻击者可以使用暴力破解的方式对认证系统进行攻击,当认证系统的服务端未做请求来源验证和错误次数限制时,就可以根据字典来暴力破解。例如,实验七远程暴力破解 Windows 远程桌面用户登录密码就是典型案例,以及本章将介绍的 DVWA 网站登录口令的暴力破解案例。

另外,攻击者也可利用网络监听或其他方式盗取合法用户的认证凭据,包括口令、验证码、Token、Cookies 等,在进行一定的处理后,再将其重新发给认证服务器。网络上传输的数据很多是经过加密的,但是攻击者如果截获到关键加密数据就有可能用来做重放攻击。例如,攻击者在传输线路上截获到一个合法用户发送的加密登录口令,虽然无法解密,但如果攻击者再次发送这些加密口令给接收方,就有可能认证成功,并以此达到欺骗接收方的目的。又如,在一个没有识别重放攻击机制的加密电子交易过程中,合法用户发送一段加密报文表示该用户支取了一笔存款,攻击者可以截获该报文并多次发送给系统,从而可能反复偷窃存款。从这个意义上讲,加密可以有效防止明文信息被监听后破坏信息机密性,但是一般无法防止重放攻击。

5.1.2　重放攻击的防御方法

1. 错误登录锁定机制

当重放攻击用于身份认证时,攻击者一般通过暴力破解方式尝试破解登录口令,如果登录口令不是弱口令,意味着攻击者的错误登录次数将会是一个较大值。认证系统设置错误登录次数阈值(如 3～5 次),只要超过这个阈值就对该账户或该攻击者 IP 地址进行锁定,下次允许尝试登录的时间向后延迟一段时间(如数小时甚至数天),以降低口令破解成功的概率。更严格的手段是直接禁止该账户或该 IP 地址再次尝试登录系统,除非管理员手动解除锁定。

2. 添加浏览器指纹

添加浏览器指纹方法主要实施在 Web 应用中。浏览器指纹是 JavaScript 语言实现的技术,仅通过浏览器的各种信息,如系统字体、屏幕分辨率及色深、浏览器插件等,无须 Cookie 等技术,就能近乎绝对定位一个用户(浏览器)。浏览器指纹本身可用于网站对客户的广告投放和精准推送,但除此之外,由于网站身份认证口令的暴力攻击一般使用软件工具进行重复发送数据包攻击,这些工具很难使用 JavaScript 生成或修改浏览器指纹。因此,服

务器通过验证客户端发来的浏览器指纹,可以防御客户端通过程序自动发数据包实施的暴力攻击。

3. 添加随机数

通信双方在每次通信交互时更新一个随机数,双方验证此随机数是否一致。例如,在身份认证时,通常随机数的更新由服务器端完成并发送给客户端,客户端收到后向服务器端发送下一次数据时附带此随机数,若服务器端发现此随机数并非最近一个随机数,则认为客户端可能存在重放攻击。服务器端向客户端发送的随机数最好不是字符串形式,因为这样会通过抓包抓取该字符串,并快速重放给服务器端;随机数可以是以随机数图片(如验证码图片)形式发送给客户端,客户端需要人工识别该图片对应的随机数。客户端将口令和随机数合并后,使用单向 Hash 函数生成一个摘要,将其发给服务器端提交身份认证。

4. 添加时间戳

时间戳是能够表示一份数据在一个特定时间点已经存在的完整的可验证数据。加时间戳策略是指设置大小适当的时间窗口(间隔),合法的通信双方会在这个时间窗口内完成通信,即保持时间同步。当双方通信时差突破时间窗口(不能保持同步)时,认为有网络重放攻击的存在。

在成熟的网络应用中,防范重放攻击的更佳手段往往是采用包括但不限于以上多重措施的共同使用。此外,使用 SSL/TLS 等加密传输手段可以更好地防御重放攻击。

5.2 DVWA 靶场简介

DVWA(Damn Vulnerable Web App,极易受攻击的 Web 应用程序)是一个 PHP/MySQL 的 Web 应用程序,也是一个基于 Web 的网络靶场,其主要目标是帮助安全专业人员在安全的环境中测试相关技能和工具,从而帮助 Web 开发人员更好地理解保护 Web 应用程序的过程。DVWA 可在本地安装部署,因此非常利于学习者在课堂环境中学习 Web 应用程序安全。DVWA 是 PHP 开源系统,可以通过阅读源码甚至修改源码学习对于各种漏洞的安全防护编码。

DVWA 中可以练习的模块如下。

- Brute Force:暴力破解。
- Command Injection:命令注入。
- CSRF:跨站点请求伪造。
- File Inclusion:文件包含。
- File Upload:文件上传。
- Insecure CAPTCHA:不安全的验证。
- SQL Injection:SQL 注入(显注)。
- SQL Injection(Blind):SQL 注入(盲注)。
- Weak Session IDS:弱会话 IDS。
- XSS(DOM):跨站脚本(文档对象模型)。

- XSS(Reflected)：跨站脚本(反射型)。
- XSS(Stored)：跨站脚本(存储型)。
- Content Security Policy (CSP) Bypass：内容安全策略。
- JavaScript Attacks：JavaScript 攻击。

DVWA 可手动调整靶场所有模块源码的安全级别，分别为 Low、Medium、High 和 Impossible 4 个级别。级别越高，安全防护越严格，渗透难度越大。Low 级别为最低安全防护级别，基本上没有实施防护，很容易就能够渗透成功；Medium 级别会使用到一些比较简单的防护，需要使用者懂得如何去绕过防护措施；High 级别的防护则会大大提高防护级别，一般 High 级别的防护需要非常丰富的经验才能成功渗透；Impossible 级别基本上不可能渗透成功，Impossible 级别的源码一般可被参考作为生产环境 Web 防护的最优手段。DVWA 网络靶场的主界面如图 5-1 所示。

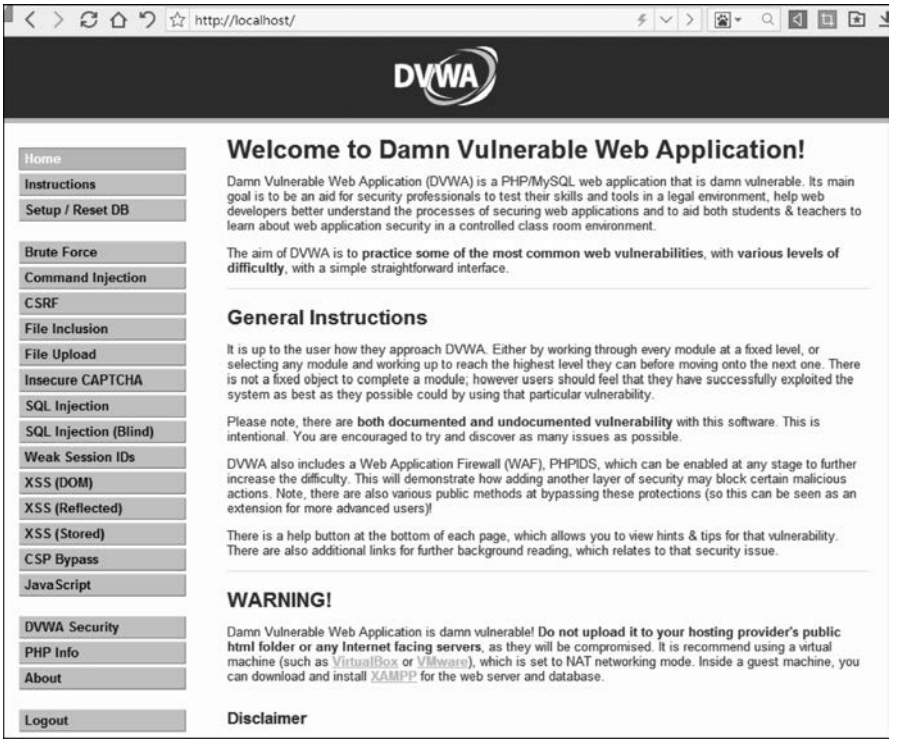


图 5-1　DVWA 网络靶场主界面

5.3　Web 应用测试工具 Burp Suite 简介

Burp Suite 是 Web 应用程序测试的最佳工具之一，也是用于自定义攻击 Web 应用程序的强大工具。Burp Suite 可执行各种 Web 相关的测试和攻击任务，包括请求的拦截和修改、枚举标识符、获取有用数据、漏洞模糊测试、SQL 注入、跨站脚本、缓冲区溢出、路径遍历、暴力攻击认证系统、操纵参数、识别隐藏的内容和功能、会话令牌测序和会话劫持、数据挖掘、并发攻击、应用层的拒绝服务式攻击等。

Burp Suite 的所有工具都共享一个请求,并能处理对应的 HTTP 消息、持久性、认证、代理、日志、警报。Burp Suite 的基本运行模式是开启默认的 8080 端口作为本地代理接口,即监听 8080 端口。Burp Suite 可使用内置的浏览器,该浏览器默认设置本地 8080 端口作为代理服务器,也可以设置第三方浏览器的本地 8080 端口作为代理服务器,所有的 HTTP 网站流量都可以被拦截、查看和修改,在导入 Burp Suite 自身数字证书后也可以拦截 HTTPS 网站流量。在默认情况下,对非图片资源的请求将被拦截并显示,可以通过 Burp Proxy 选项里的 Options 选项修改默认值。

Burp Suite 的主要功能模块如下。

- Proxy(代理):拦截 HTTP/HTTPS 的代理服务器,作为在浏览器和目标 Web 应用程序之间的"中间人",可拦截、查看、修改双向的原始数据流。
- Spider(爬虫):智能感应的网络爬虫,能完整地枚举应用程序的内容和功能。
- Scanner(扫描器):该功能仅限于专业版,能自动发现 Web 应用程序的安全漏洞。
- Intruder(攻击器):Burp Suite 最重要的模块之一,可对 Web 应用程序进行自动化暴力攻击,枚举标识符,收集有用的数据,以及使用模糊技术探测常规漏洞。该模块主要有 4 个子模块:Target(配置攻击目标)、Positions(设置 Payload 的插入点及 4 种攻击类型)、Payloads(设置数据包中的载荷,配置攻击字典)、Options(包括请求头,请求引擎,攻击结果,全文检索匹配、提取、载荷填充和重定向)。
- Repeater(重放器):可手动操作发送单独的 HTTP 请求,并分析应用程序响应。
- Sequencer(定序器):用于检测数据样本随机性质量的工具,通常用于检测访问令牌是否可预测、密码重置令牌是否可预测等场景,通过定序器的数据样本分析,能很好地降低这些关键数据被伪造的风险。
- Decoder(解码器):通过手动执行或对应用程序进行智能解码和编码。
- Comparer(对比器):对一些相关请求和响应得到的数据进行差异比对,并将结果进行可视化展示。

Burp Suite 主界面如图 5-2 所示。

图 5-2 Burp Suite 主界面

5.4　实验九：Burp Suite 重放攻击 DVWA 靶场登录用户名和密码


视频讲解

1. 实验目的

(1) 掌握 DVWA 靶场和 Burp Suite 的安装配置方法。

(2) 掌握 Burp Suite 重放攻击 DVWA 靶场登录用户名和密码的方法。

(3) 理解对 Web 网站登录口令使用重放攻击的原理。

2. 实验任务与要求

(1) 安装 phpStudy 集成工具和 MySQL 数据库，搭建 DVWA 网络靶场。

(2) 安装 Burp Suite 工具。

(3) 在 DVWA 网络靶场中使用 Brute Force 模块，设置安全级别为 Low，使用 Burp Suite 对 DVWA 的用户登录报文进行网络重放攻击，结合字典文件的使用，分别对密码单独进行暴力破解、对用户名和密码同时进行暴力破解。

3. 实验原理(技术)

(1) Burp Suite 工具。

Burp Suite 是用于自定义攻击 Web 应用程序的强大工具。Burp Suite 可执行各种 Web 相关的测试和攻击任务，包括请求的拦截和修改，枚举标识符，获取有用数据，漏洞模糊测试，SQL 注入，跨站脚本，缓冲区溢出，路径遍历，暴力攻击认证系统，操纵参数，识别隐藏的内容和功能，会话令牌测序和会话劫持，数据挖掘，并发攻击，应用层的拒绝服务式攻击等。

(2) DVWA 网络靶场 Brute Force 模块。

DVWA 是一个基于 PHP/MySQL 搭建的 Web 应用程序，其中包含 Brute Force 模块。Brute Force 可以通过用户名和密码登录网站，并进行暴力破解测试。DVWA 部署在本地。

(3) Burp Suite 对 Web 网站登录口令进行重放攻击的原理。

重放攻击是指攻击者将曾经发送给目标的数据报文再重复发送。Burp Suite 启动后监听本地 8080 端口，浏览器使用 8080 端口代理上网，此时 Burp Suite 充当了浏览器与 Web 服务器之间的中间人。Burp Suite 使用 Proxy 模块拦截用户提交登录口令(用户名和密码)给服务器的报文，使用 Intruder 模块定位到口令字符串并将其设置为变量，加载口令字典，再程序化反复发送登录报文给服务器，以此进行暴力攻击。在每次尝试登录口令时，服务器返回验证通过报文的 Length 值是否不同，以此筛选出正确的口令，完成重放攻击并破解正确登录口令。

4. 实验仪器设备(环境条件)

虚拟机 VMware Workstation 15.5＋Windows 7，其中应包括 phpStudy 8.1、DVWA 1.10 和 Burp Suite 社区版 2021。

5. 实验过程

(1) 攻击前的软件安装。

在 Windows 7 上安装 phpStudy(包括 Apache、Nginx、MySQL),在 phpStudy 中部署 DVWA 靶场,安装 Burp Suite,详细过程见本书配套视频。

(2) 攻击前的软件环境设置。

启动 phpStudy,单击 WNMP"一键启动"后,确保 MySQL 数据库、Nginx(Web 服务器)都已启动,其中 Nginx 也可用 Apache 替代,如图 5-3 所示。

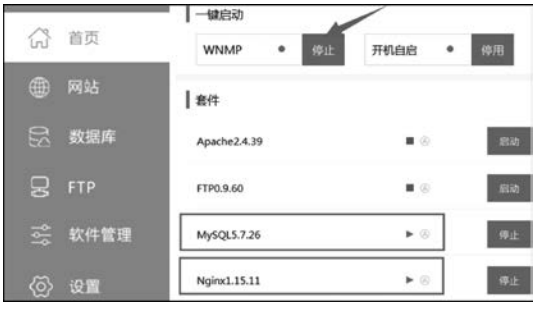


图 5-3 启动 MySQL 数据库和 Nginx 服务

启动 Burp Suite,单击 Proxy 模块,单击 Open Browser 按钮,即可打开内置浏览器,如图 5-4 所示。

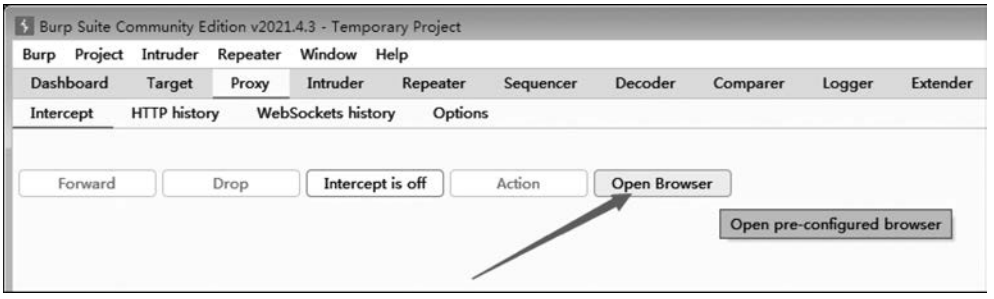


图 5-4 启动 Burp Suite 的内置浏览器

在 Proxy 模块中的 Options 选项卡中,可以看到内置浏览器使用了 Web 代理服务器,接口是 127.0.0.1:8080,如图 5-5 所示。

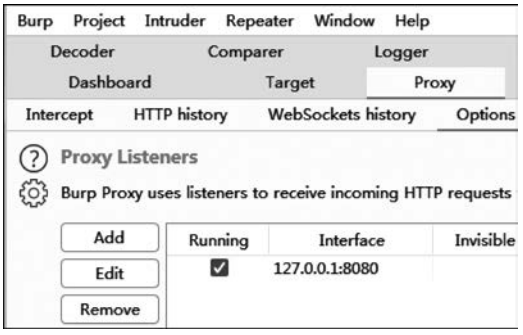


图 5-5 Burp Suite 查看 Proxy 模块

Web 代理服务器的作用是将浏览器与 Web 服务器的请求和接收响应都通过代理服务器进行中间转发。由于使用 Burp Suite 作为代理转发，因此用户名、密码等数据都能被 Burp Suite 截获并进行重放攻击处理。此时可以使用 netstat -ano 命令查看 8080 端口处于本地监听状态，如图 5-6 所示。

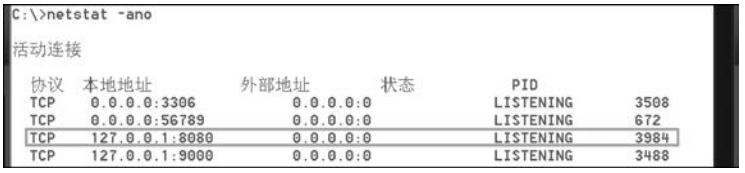


图 5-6　查看 8080 端口处于本地监听状态

使用 Burp Suite 内置浏览器访问本地 DVWA 网址 http://localhost 或 http://127.0.0.1，以 admin 为用户名、password 为密码登录，如图 5-7 所示。

注意，如果不使用 Burp Suite 自带浏览器而使用第三方浏览器，需要在对应浏览器的 Internet 属性中单击局域网设置，在代理服务器中选中“为 LAN 使用代理服务器”复选框，设置 IP 地址为 127.0.0.1、端口为 8080，如图 5-8 所示。

图 5-7　访问本地 DVWA 网址

图 5-8　第三方浏览器设置代理服务器

在浏览器中单击 DVWA 左侧菜单中的 DVWA Security 页面，将 DVWA 的安全级别设置为最低级 Low，如图 5-9 所示。

查看 DVWA 的 PHP 脚本，分析该级别的安全设置。在 DVWA 网站根目录下访问子目录 vulnerabilities，可查看所有的 14 个攻击模块。本实验中涉及的 Brute Force 模块对应 brute 目录，如图 5-10 所示。

继续访问 brute 下的 source 目录，其中有 low.php、medium.php、high.php 和 impossible.php 4 个文件，对应 Brute Force 模块低、中、高、不可能 4 个安全级别的源码，如图 5-11 所示。当然，DVWA 其他所有模块的安全级别源码也都在其模块各自目录下的 4 个同名文件中。

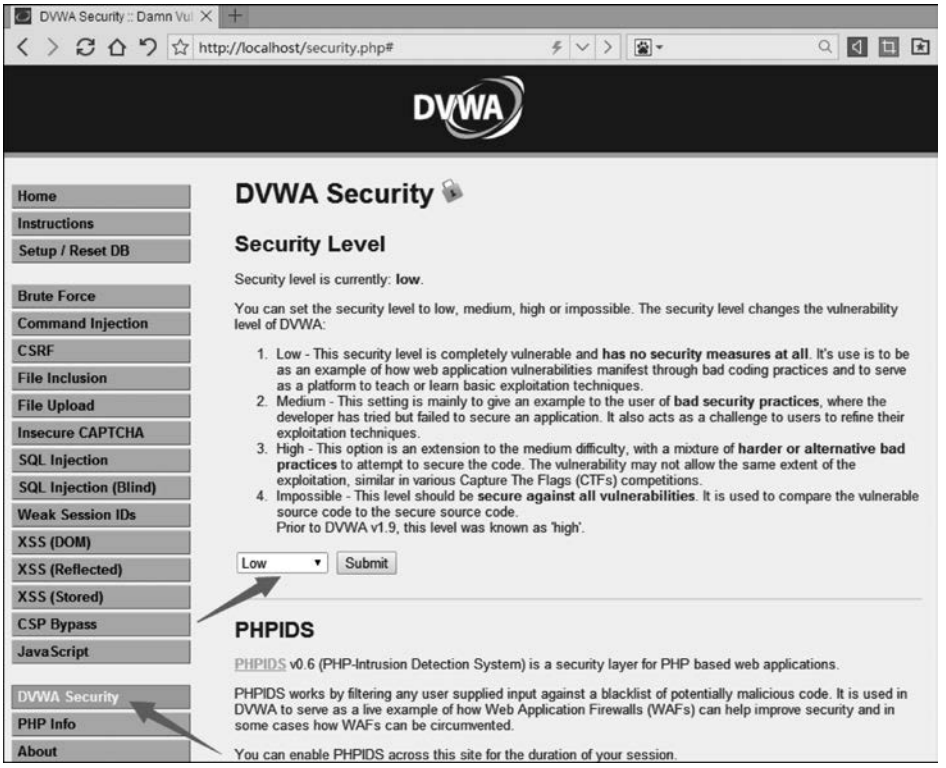


图 5-9　DVWA 的安全级别设置为最低级 Low

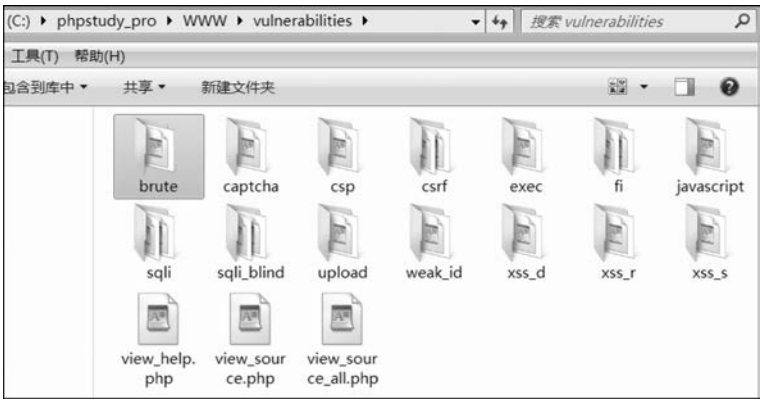


图 5-10　查看 DVWA 网站各个模块的目录

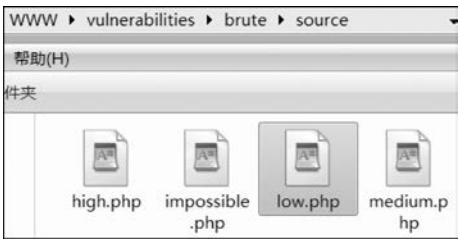


图 5-11　查看 DVWA 的 Brute Force 模块下的 4 个安全级别文件

使用文本编辑器(如记事本)打开 low.php 文件,其内容如下,其中//所在的行为注释。

```
<?php
if( isset( $_GET[ 'Login' ] ) ) {
    // Get username【获取用户名】
    $user = $_GET[ 'username' ];

    // Get password【获取密码】
    $pass = $_GET[ 'password' ];
    $pass = md5( $pass );

    // Check the database【检索数据库】
    $query = "SELECT * FROM 'users' WHERE user = '$user' AND password = '$pass';";
    $result = mysqli_query( $GLOBALS["___mysqli_ston"], $query ) or die( '<pre>' . ((is_
object( $GLOBALS["___mysqli_ston"])) ? mysqli_error( $GLOBALS["___mysqli_ston"]) : (( $___
mysqli_res = mysqli_connect_error()) ? $___mysqli_res : false)) . '</pre>' );

    if( $result && mysqli_num_rows( $result ) == 1 ) {
        // Get users details【得到用户详情】
        $row = mysqli_fetch_assoc( $result );
        $avatar = $row["avatar"];

        // Login successful【登录成功】
        $html .= "<p>Welcome to the password protected area {$user}</p>";
        $html .= "<img src=\"{$avatar}\" />";
    }
    else {
        // Login failed【登录失败】
        $html .= "<pre><br />Username and/or password incorrect.</pre>";
    }

    ((is_null( $___mysqli_res = mysqli_close( $GLOBALS["___mysqli_ston"]))) ? false : $___
mysqli_res);
}
?>
```

分析可知,该文件中的 Low 级别仅将用户名和密码提交到服务器查询数据库并进行用户身份验证,并未进行其他安全控制(如随机数校验、时间戳、错误登录锁定等安全防范措施),很容易进行重放攻击。

(3) 重放攻击测试。

单击 DVWA 菜单中的 Brute Force 链接,在页面中输入正确的用户名 admin 和密码 password,暂时不单击 Login 按钮,如图 5-12 所示。

回到 Burp Suite,单击 Proxy 模块中的 Intercept is off 按钮,使其变为 Intercept is on,此时已启动拦截器,如图 5-13 所示。

回到 DVWA 的 Brute Force 模块,单击 Login 按钮登录,此时网站暂无响应。回到 Burp Suite 的 Proxy 模块,可见网页登录时提交到服务器的报文数据已被拦截,其中第一行解析为 GET /vulnerabilities/brute/?username=admin&password=password&Login=Login HTTP/1.1。可见提交方式为 GET,而 username=admin&password=password 代表客户端向服务器提交的两个字段名 username 和 password 的赋值分别为 admin 和 password,如图 5-14 所示。

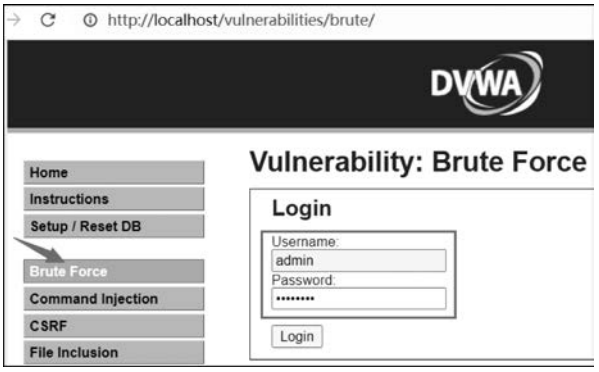


图 5-12　DVWA 在 Brute Force 模块中输入正确的用户名和密码

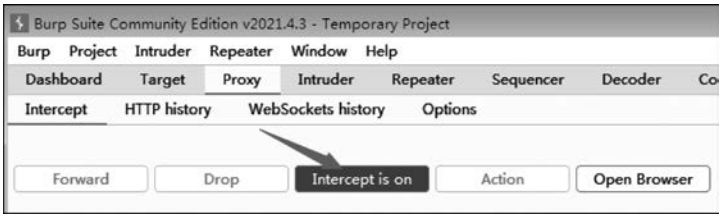


图 5-13　在 Burp Suite 中启动拦截器

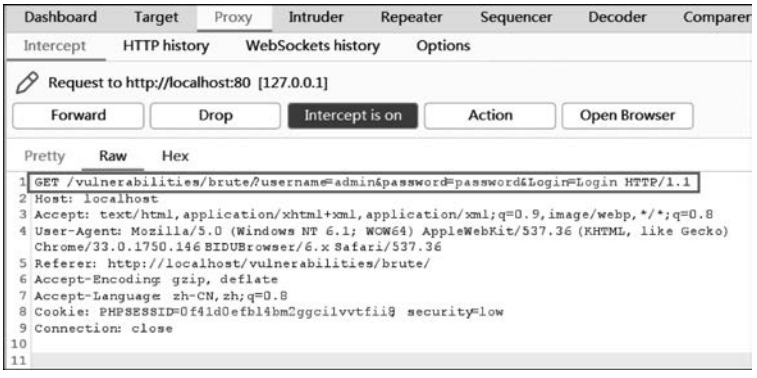


图 5-14　登录提交时被拦截的报文

在 Proxy 模块中被拦截报文的任意区域右击选择 Send to Repeater 选项，如图 5-15 所示。

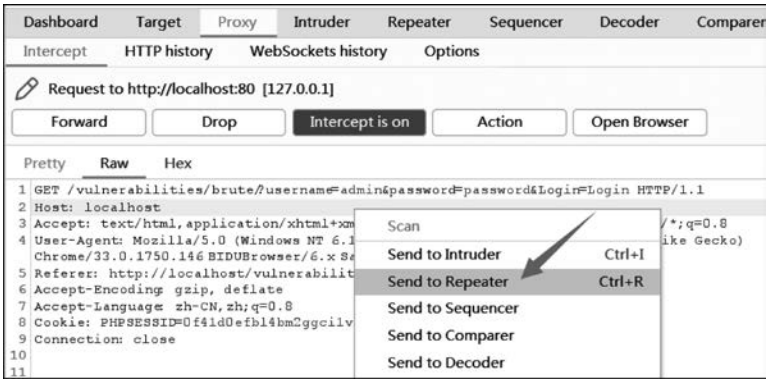


图 5-15　把被拦截报文发送到 Repeater 模块

此时该报文会被复制到 Repeater 模块中。由于网页提交数据被截获并阻塞，可单击 Forward 按钮放行，如图 5-16 所示。

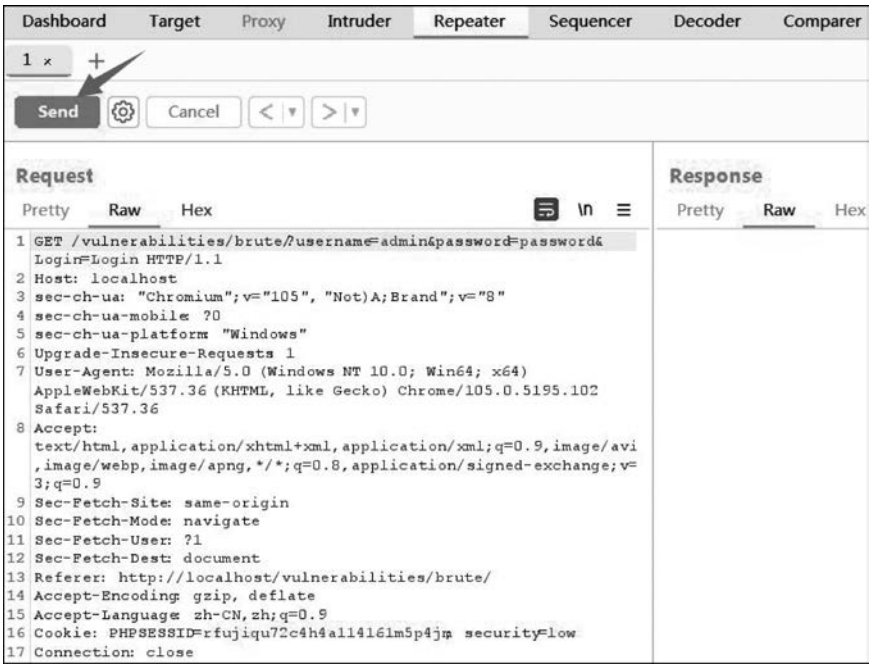


图 5-16　在 Repeater 模块发送登录报文

此时服务器收到提交的报文，查询数据库后响应并返回登录结果。在 Repeater 模块右边有一个 Response 区域，这是一个嵌入 Burp Suite 内部的浏览器引擎，可以将服务器返回的原始报文进行显示、解析和渲染。单击其中的 Render 按钮即可渲染页面，显示“Welcome to the password protected area admin”表示用户登录成功，如图 5-17 所示。

图 5-17　服务器响应后渲染页面显示登录成功

需要注意的是,此时外部浏览器的报文始终保持被拦截状态,单击 Proxy 模块中的 Intercept 选项卡中的 Forward 按钮,以步进方式放行报文,浏览器会正常响应,如图 5-18 所示。

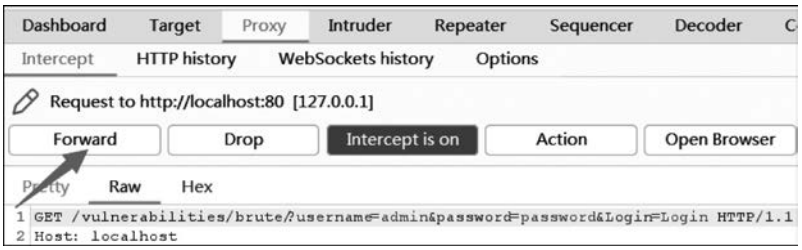


图 5-18 在 Proxy 模块中放行报文

如何实现重放攻击呢?如果反复在 Repeater 模块中单击 Send 按钮,右边 Response 区域会重复渲染页面并显示登录成功,这便是不修改原始报文类型的重放攻击。而修改原始报文的重放攻击如何实现呢?在左边 Request 区域修改原始报文即可,例如,修改 password 字段的值为 123456,再单击 Send 按钮,右边 Response 区域会重新渲染页面并显示"Username and/or password incorrect.",即登录失败,如图 5-19 所示。

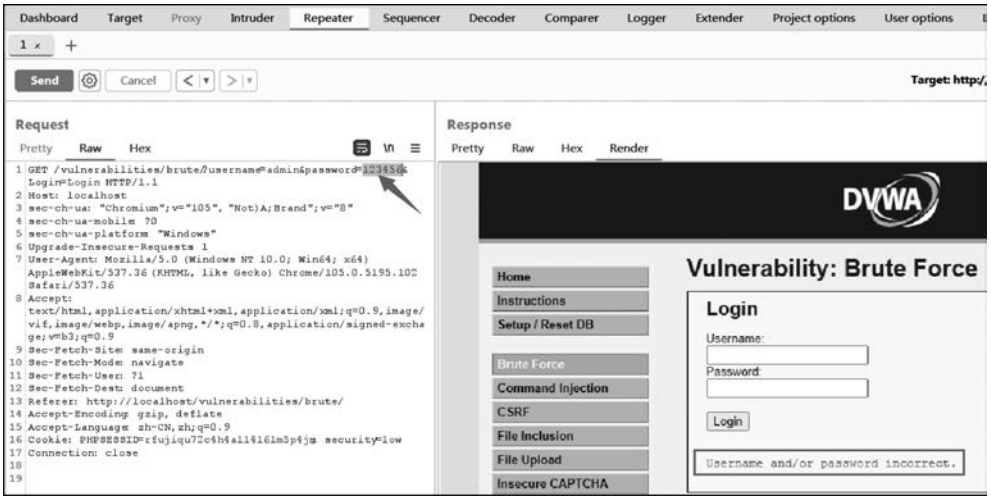


图 5-19 修改原始报文中的 password 变量值后,渲染页面显示登录失败

(4) 利用重放攻击对登录密码进行暴力破解。

假设已知用户名 admin,密码未知但取值存在于自定义的字典文件中,攻击原理是对需要重复尝试登录的密码值设定为变量,从字典逐一读取候选密码,利用 Intruder 模块程序化地反复攻击。

继续在 Repeater 模块左侧 Request 区域任意报文位置右击选择 Send to Intruder 选项,如图 5-20 所示。

当然,如果是重新打开网页,开始以错误密码如 123456 登录,也可以在 Proxy 模块中被拦截报文的任意区域右击选择 Send to Intruder 选项,如图 5-21 所示。

在 Intruder 模块的 Positions 选项卡中,默认部分值前后被自动添加了 $ 符号,这代表变量。在暴力攻击中,变量是非常重要的参数,代表每个重复报文中的可变值,该值常常来自于自定义的字典。

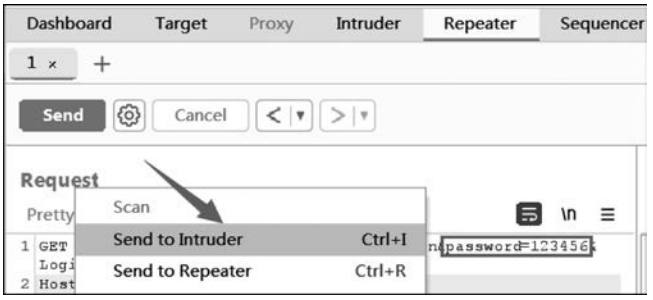


图 5-20　以错误密码登录时从 Repeater 模块将报文发送到 Intruder 模块

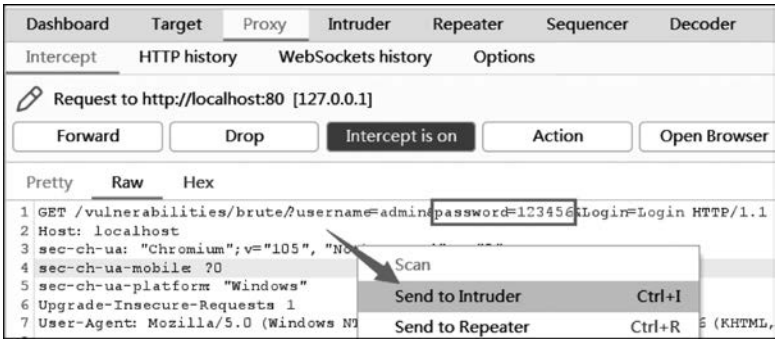


图 5-21　以错误密码登录时从 Proxy 模块将报文发送到 Intruder 模块

由于只对密码值进行暴力破解，因此先单击右边的 Clear $ 按钮，将清除所有默认被设置的变量。再双击选中被拦截报文中第一行中的 password 字段值即 123456，并单击右边的 Add $ 按钮，将此作为变量。此外，Choose an attack type 保持默认 Sniper，如图 5-22 所示。

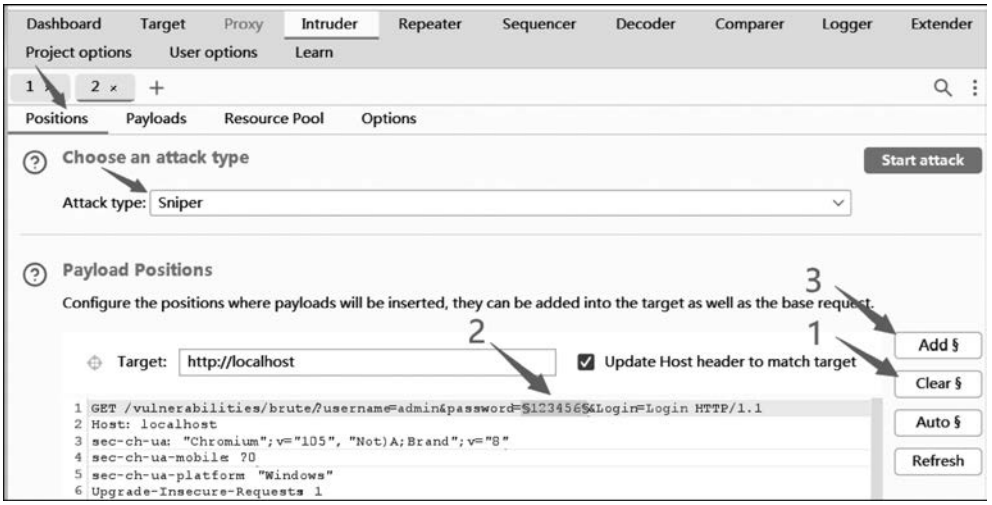


图 5-22　将密码值设置为攻击变量

接着创建一个密码字典并命名为 dictest.txt，其中候选值为 123456、12345678、admin、admin123、burpsuite、password、dvwa 等 7 个，每行一个值。单击 Payloads 选项卡，再在下

面单击 Load 按钮加载 dictest.txt 字典文件。Payload Sets 中的设置保持默认,由于候选值有 7 个,要爆破的变量只有 1 个,因此爆破次数为 7。最后单击右边的 Start attack 按钮开始重复攻击,如图 5-23 所示。

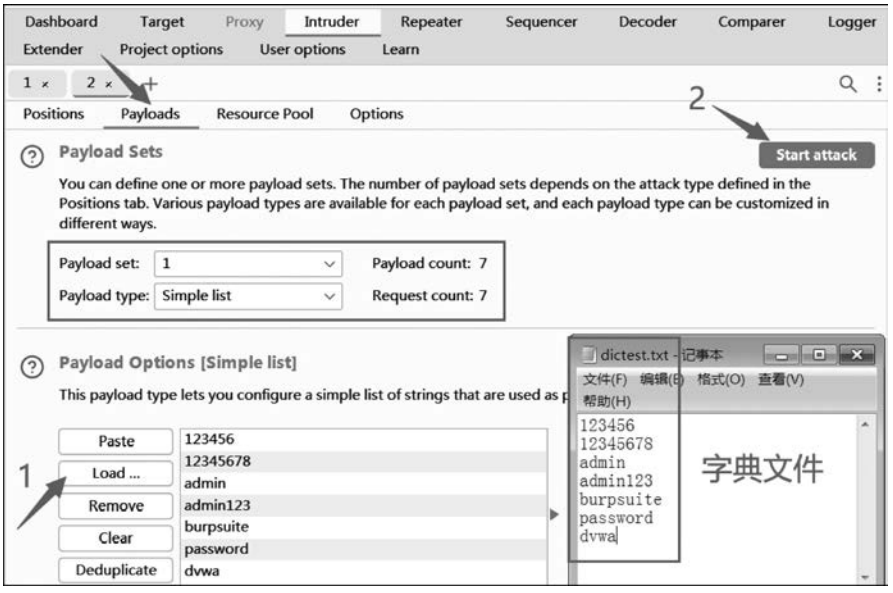


图 5-23 对密码变量加载字典文件并开始暴力攻击

攻击完成后,观察 Results 选项卡,其中有 0～7 共 8 条记录,序号 0 的 Payload 为空值,序号 1～7 的 Payload 值均为字典中的候选值。最右边的 Length 代表返回值的长度,其中 Payload 为 password 的所在行 Length 列值为 4559,与其余所有行 Length 列值均为 4521 不同。选中 password 的所在行,依次单击下方 Response 选项卡、Render 按钮即可渲染响应的页面,显示“Welcome to the password protected area admin”,即用户登录成功,如图 5-24 所示。

如果单击其余 Length 值均为 4521 的行,则渲染页面均显示“Username and/or password incorrect.”,即登录失败。因此,正确密码值 password 通过重放攻击成功暴力破解。

(5) 利用重放攻击对登录用户名和密码同时暴力破解。

在 Intruder 模块的 Positions 选项卡中,除了将 password 字段后的值添加为变量外,还需要将 username 字段后的值也添加为变量。先单击右边的 Clear $ 按钮,将 admin 值和 password 值都先后选中并添加为变量,再单击 Attack type 下拉菜单并选中 Cluster bomb(集束炸弹),如图 5-25 所示。

下一步进入 Payload 选项卡,首先需要选择 Payload set(载荷集合)下拉菜单,选择 1 表示对 username 字段加载字典文件,选择 2 表示对 password 字段加载字典文件。由于 dictest.txt 文件中同时包含了正确的用户名和密码两个值,因此都可加载该字典文件。当 Payload set 下拉菜单对两个变量都分别选择好字典文件后,可见右边提示“Payload count: 7”,即用户名和密码候选值均为 7 个 ,而提示“Request count: 49”表示会进行 7×7=49 次遍历,如图 5-26 所示。假设用户名和密码是两个不同的字典文件,则要分别选取各自的字典文件。例如,用户名字典中的候选值有 3 个,密码字典中的候选值有 7 个,则会进行 3×7=21 次遍历。

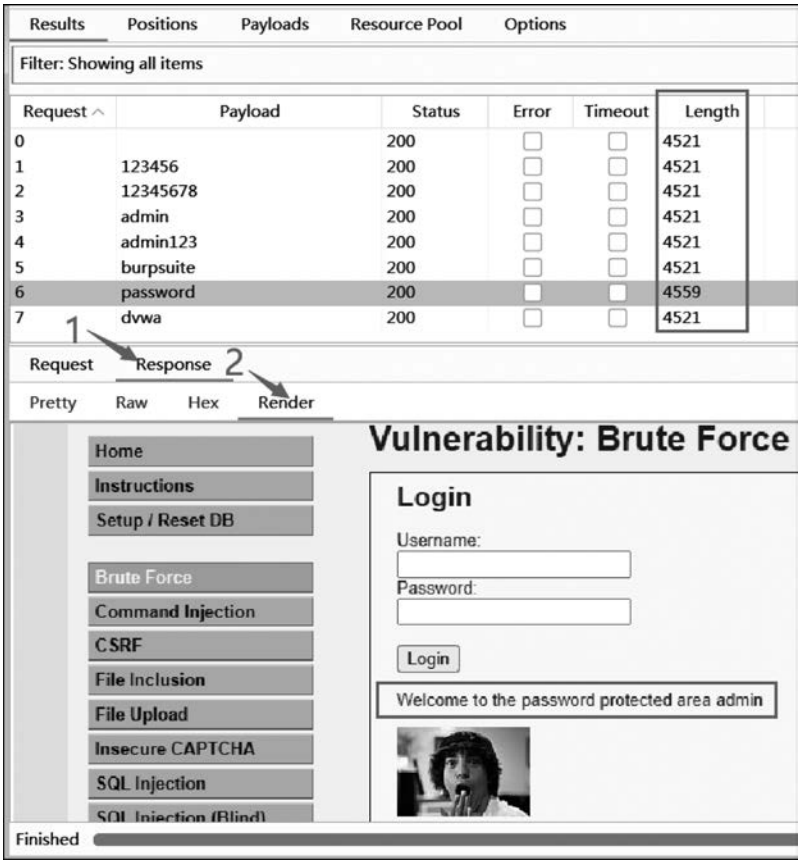


图 5-24　正确密码值渲染页面显示登录成功

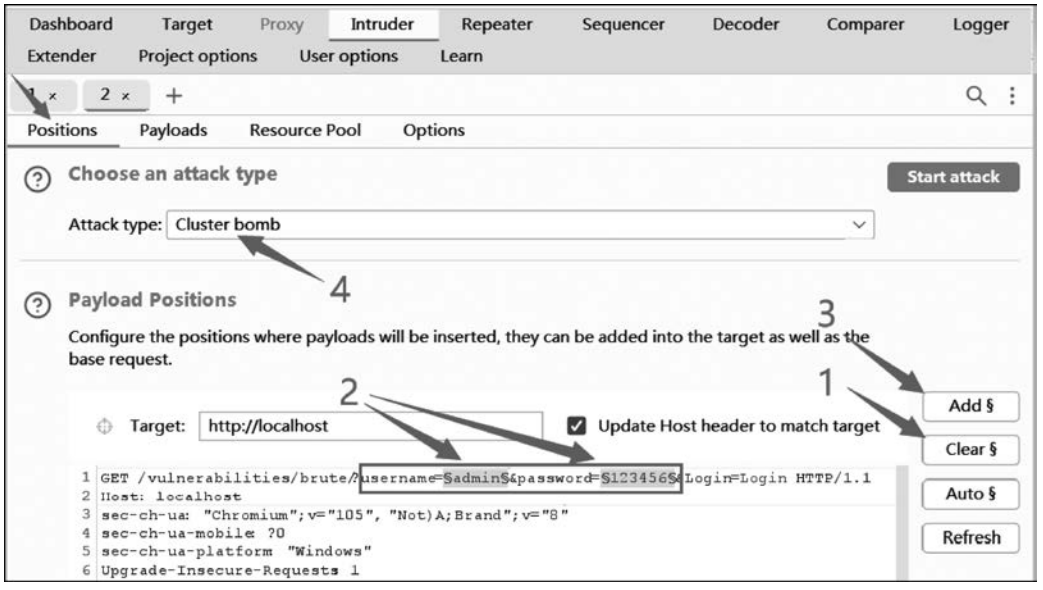


图 5-25　将用户名值和密码值均设置为攻击变量

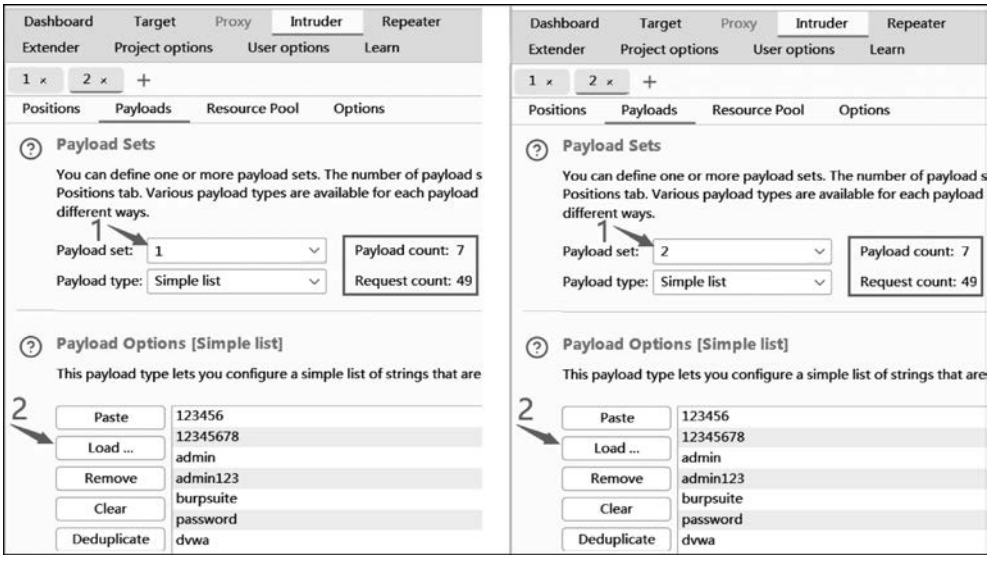


图 5-26 对用户名和密码变量加载同一个字典文件并开始暴力攻击

开始攻击后,会有 49 次 Payload 带非空值攻击(序号 1～49),1 次 Payload 带空值攻击(序号 0)。由于攻击结果条目较多,可单击右边的 Length 标题进行排序,快速定位不同值 4559,以此猜解出正确的用户名值 admin、密码值 password,如图 5-27 所示。

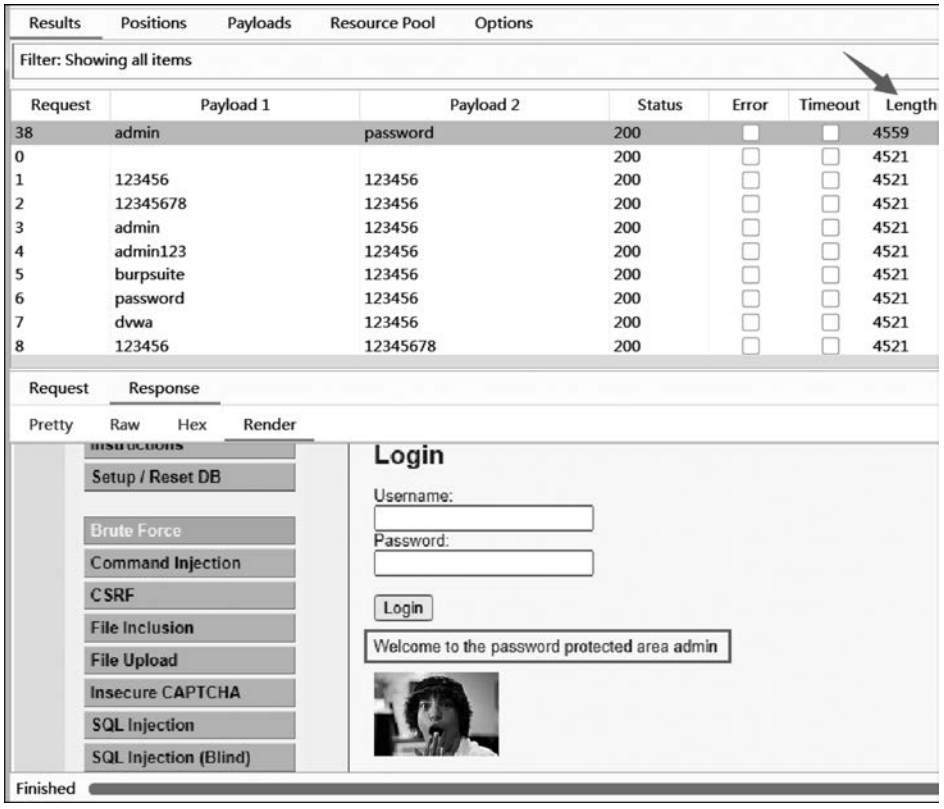


图 5-27 正确用户名值和密码值渲染页面显示登录成功

(6) 有关 HTTP 状态码。

在图 5-22 和图 5-25 的攻击结果中，显示 Status 列值均为 200，代表请求成功。Status 列为 HTTP 状态码，当浏览器向服务器发出请求时，服务器会返回一个包含 HTTP 状态码的信息头(server header)用以响应浏览器的请求。常见的 HTTP 状态码如下。

- 200：请求成功。
- 301：资源(如网页等)被永久转移到其他 URL(如页面跳转等)。
- 302：资源(如网页等)被临时转移到其他 URL(如页面跳转等)。
- 404：请求的资源(如网页等)不存在。
- 500：内部服务器错误。

如果此处状态码值不是 200 而是其他，则说明网页没有正常返回响应。无论字典中是否包含了正确的用户名和密码，重放攻击都可能不会成功。

5.5　实验十：Burp Suite 重放攻击 DVWA 靶场带 Token 认证的登录密码


视频讲解

1. 实验目的

(1) 理解和分析 DVWA 靶场登录时带 Token 认证的原理。

(2) 掌握 Burp Suite 重放攻击 DVWA 靶场带 Token 认证的登录密码的方法。

2. 实验任务与要求

(1) DVWA 靶场安全级别设置为 High。

(2) 参照实验九的方法进行重放攻击。

(3) 分析 DVWA 靶场登录时带 Token 认证的原理。

(4) Burp Suite 重放攻击 DVWA 靶场带 Token 认证的登录密码。

3. 实验原理(技术)

(1) DVWA 靶场登录时带 Token 认证原理。

Token 又称为令牌，每一个 Token 只代表一次认证交互行为。当 DVWA 靶场安全级别设置为 High 时，浏览器提交给服务器的数据除了用户名和密码之外还有 Token 值，而且每次刷新页面登录时，Token 值都在变化。该值每次先由服务器端产生并返回给浏览器，每次用户登录时，浏览器将用户名、密码连同最新的 Token 值提交给服务器，服务器要先判断当前 Token 值是否匹配最新的 Token 值，如果是则继续判断用户名和密码是否正确，否则就终止登录尝试。

(2) Burp Suite 重放攻击 DVWA 靶场带 Token 认证的登录密码原理。

在 Intruder 模块中需要设置 Token 值与密码值两个变量，如果还需要破解用户名则需要设置 3 个变量。在重放攻击过程中需要保持单线程方式，保持获取 Token 值与暴力攻击交替依序进行。Intruder 模块要跟踪并抓取服务器返回的最新 Token 值，再将该 Token 值与密码两个变量作为 Payload 一起暴力攻击。

4. 实验仪器设备(环境条件)

虚拟机 VMware Workstation 15.5+Windows 7,其中应包括 phpStudy 8.1、DVWA 1.10 和 Burp Suite 社区版 2021。

5. 实验过程

(1) DVWA 靶场安全级别设置为 High 及其源码分析。

5.4 节介绍了当 DVWA 靶场安全级别设置为 Low 时,如何进行重放攻击破解登录用户名和密码。在这一节中,将 DVWA 靶场安全级别设置为 High,如图 5-28 所示。

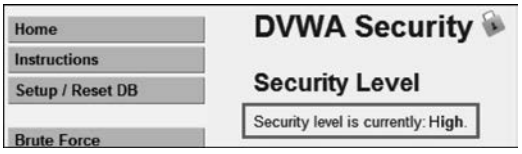


图 5-28 DVWA 靶场安全级别设置为 High

在 DVWA 的 Brute Force 模块下查看 4 个安全级别文件,使用文本编辑器(如记事本)打开 high.php 文件,其内容如下,其中//所在的行为注释。

```
<?php
if( isset( $_GET[ 'Login' ] ) ) {
    // Check Anti-CSRF token【检查提交的 user_token 值是否匹配】
    checkToken( $_REQUEST[ 'user_token' ], $_SESSION[ 'session_token' ], 'index.php' );

    // Sanitise username input【对输入用户名进行过滤处理】
    $user = $_GET[ 'username' ];
    $user = stripslashes( $user );
    $user = ((isset( $GLOBALS[ "___mysqli_ston"]) && is_object( $GLOBALS[ "___mysqli_
ston"])) ? mysqli_real_escape_string( $GLOBALS["___mysqli_ston"], $user ) : ((trigger_error
("[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.", E_USER_
ERROR)) ? "" : ""));

    // Sanitise password input【对输入密码进行过滤处理】
    $pass = $_GET[ 'password' ];
    $pass = stripslashes( $pass );
    $pass = ((isset( $GLOBALS[ "___mysqli_ston"]) && is_object( $GLOBALS[ "___mysqli_
ston"])) ? mysqli_real_escape_string( $GLOBALS["___mysqli_ston"], $pass ) : ((trigger_error
("[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.", E_USER_
ERROR)) ? "" : ""));
    $pass = md5( $pass );

    // Check database【检索数据库】
    $query = "SELECT * FROM 'users' WHERE user = '$user' AND password = '$pass';";
    $result = mysqli_query( $GLOBALS["___mysqli_ston"], $query ) or die( '<pre>' . ((is_
object( $GLOBALS["___mysqli_ston"])) ? mysqli_error( $GLOBALS["___mysqli_ston"]) : (( $___
mysqli_res = mysqli_connect_error()) ? $___mysqli_res : false)) . '</pre>' );

    if( $result && mysqli_num_rows( $result ) == 1 ) {
        // Get users details【得到用户详情】
```

```
            $row = mysqli_fetch_assoc( $result );
            $avatar = $row["avatar"];

            // Login successful【登录成功】
            $html .= "<p>Welcome to the password protected area {$user}</p>";
            $html .= "<img src=\"{$avatar}\" />";
        }
        else {
            // Login failed【登录失败】
            sleep( rand( 0, 3 ) );
            $html .= "<pre><br />Username and/or password incorrect.</pre>";
        }

        ((is_null($___mysqli_res = mysqli_close($GLOBALS["___mysqli_ston"]))) ? false : $___
    mysqli_res);
    }

    // Generate Anti-CSRF token【生成防跨站请求伪造的 Token】
    generateSessionToken();
    ?>
```

相比 5.4 节将安全级别设置为 Low，High 级别最重要的特点是增加了 Token 值校验。

(2) 使用实验九的方法对登录密码进行重放攻击。

以用户名 admin、密码 123456 登录，使用拦截器抓取登录报文并发送到 Intruder 模块，只将密码值设置为变量。在第 1 行报文中，GET 参数后除了 username、password 字段外，还增加了一个 user_token 字段，其值为 32 位十六进制数，会一并发送给服务器。此外，在第 16 行报文中，Cookie 参数后的 security 字段值为 high，如图 5-29 所示。

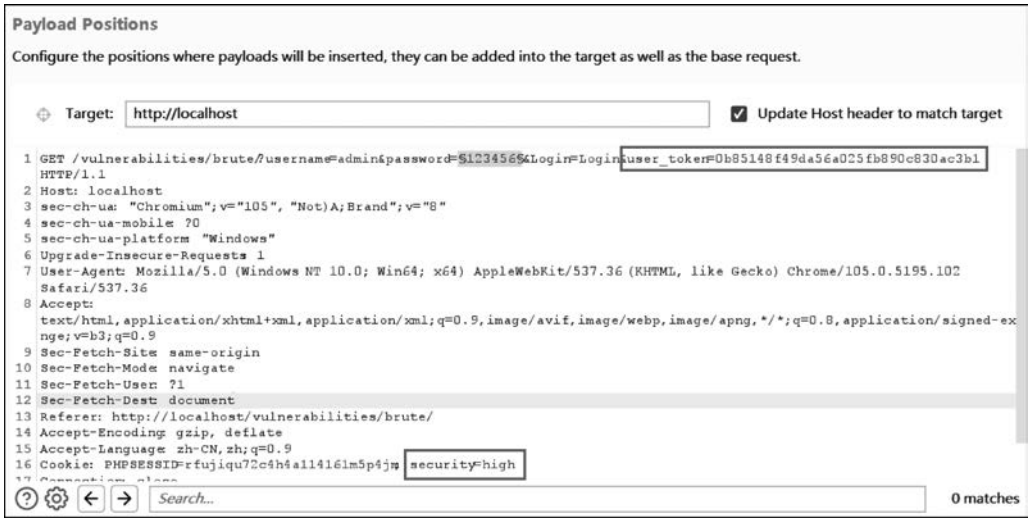


图 5-29　Intruder 模块 Positions 选项卡中的报文

继续加载密码字典，其中包括正确密码值 password，并开始攻击。由于字典中的候选密码值有 7 个，因此攻击 7 次。在攻击结束后，包括正确密码值 password 在内的每个候选密码的返回结果状态都是 302，代表要请求的网页被跳转到其他页面，而且 Response 选项

卡中的 Render 按钮为灰色即单击无效。另外,所有的 Length 长度都是相同的(如本例为 316)。由于正确密码与错误密码尝试后的返回值没有任何差异,无法区分,因此攻击未成功,如图 5-30 所示。

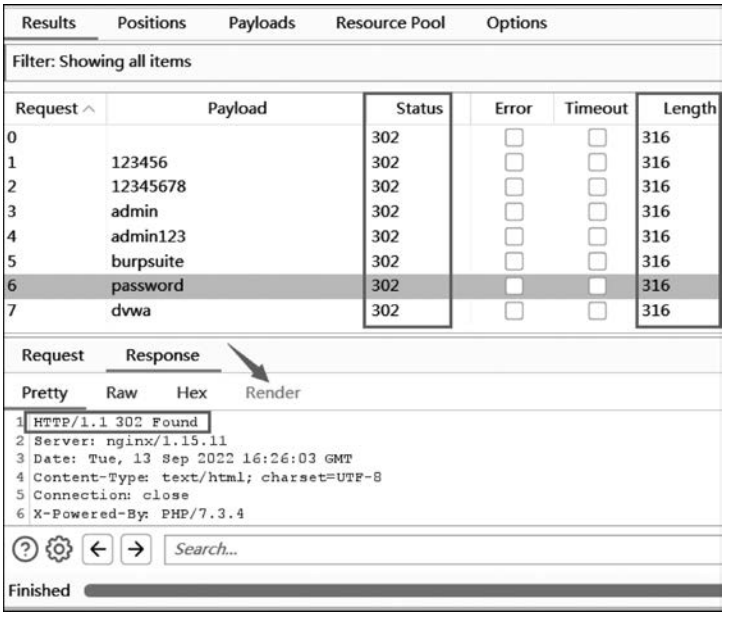


图 5-30 重放攻击结果显示未成功

(3) 从网络流量角度分析 DVWA 靶场带 Token 认证的实现原理。

启动 Wireshark,由于访问 DVWA 的网址是 http://localhost 或 http://127.0.0.1,因此需要对本地回环(chiasmus)接口捕获流量,如图 5-31 所示。

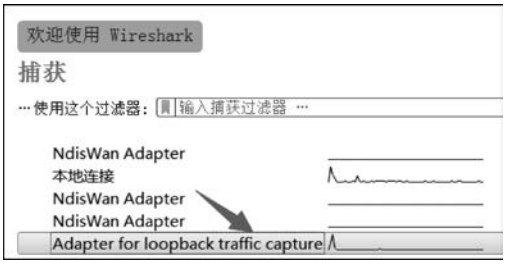


图 5-31 Wireshark 选择本地回环接口捕获流量

在浏览器中访问 Brute Force 模块的页面,先后输入 3 次用户名和密码登录,分别为 admin、12345,admin、67890,admin、password。Wireshark 对已捕获的报文用参数值 tcp.port == 80 and http 进行过滤,捕获的报文如图 5-32 所示。

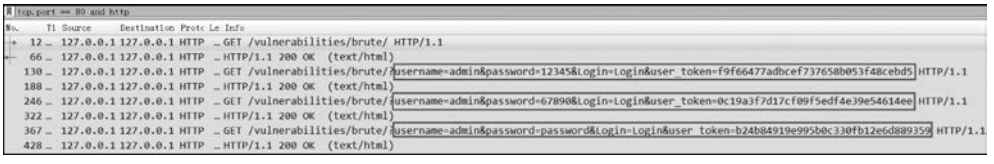


图 5-32 Wireshark 捕获 3 次用户名密码登录的相关分组

经分析，序号 130、246、367 分组为浏览器向服务器请求的分组，也对应提交 3 次用户名和密码的分组，每个分组中都包含 username、password、login 和 user_token 等 4 个参数。其中，user_token 值为 32 位十六进制数，且每个 user_token 值都不相同。接着需要继续分析 user_token 值的来源。

将序号为 66、130 的两个分组进行组合分析，对应第一次用户名和密码登录。66 号分组的 Info 为 HTTP/1.1 200 OK，代表服务器响应的状态码，因此该分组由服务器发给浏览器。选中该分组，在分组解析中，包含的脚本< form action＝"＃" method＝"GET">代表表单，表单中的脚本< input type＝'hidden' name＝'user_token' value＝'f9f66477adbcef737658b053f48cebd5' />代表 hidden 类型的 name 为 user_token 的 input 标签，其值为 f9f66477adbcef737658b053f48cebd5。130 号分组的 Info 以 GET /vulnerabilities/brute/? username＝admin&password＝12345 开始，可判断为浏览器向服务器的请求，后面包含参数 user_token，其值为 f9f66477adbcef737658b053f48cebd5，该值与上一个分组中的 value 参数值完全一致，如图 5-33 所示。

图 5-33　Wireshark 捕获第一次用户名密码登录的相关分组

因此，对这两个分组分析可知，在浏览器上打开登录页面后，服务器就已经向浏览器下发了 Token，该值隐藏于页面中不会显示。接着，在浏览器上输入用户名和密码并提交后，浏览器会将用户名、密码和该 Token 值一起向服务器提交。

用同样的方法对序号 188 和 246 分组进行分析，对应第二次用户名和密码登录。188 号分组为服务器发送给浏览器，其中隐藏的 user_token 值为 0c19a3f7d17cf09f5edf4e39e54614ee。246 分组为浏览器向服务器提交的分组，其中包含的 user_token 值也为 0c19a3f7d17cf09f5edf4e39e54614ee，两者完全相同，如图 5-34 所示。

图 5-34　Wireshark 捕获第二次用户名密码登录的相关分组

对第三次用户名和密码登录对应分组的分析参考相同方法，具有相同规律。DVWA 靶场带 Token 认证的实现原理如下。

第一次访问登录页，服务器下发第一个 user_token 值，在浏览器登录单击提交时，携带第一个 user_token；

第二次访问登录页，服务器下发第二个 user_token 值，在浏览器登录单击提交时，携带

第二个 user_token;

……

以此类推。

使用实验九的方法对带有 Token 认证的登录密码进行重放攻击失败的原因是,Burp Suite 的 Intruder 模块中只设定了密码作为变量,而将 user_token 值作为恒定的常量提交给服务器,服务器校验该值不通过,因而出现 http302 状态码。增加动态 Token 机制,类似于网页中每次刷新网页会动态变化的图片验证码,对浏览器端的合法身份增强了校验,也增加了重放攻击的难度。

(4) Burp Suite 重放攻击 DVWA 靶场带 Token 认证的登录密码的原理和方法。

Burp Suite 支持通过编写正则表达式对报文进行文本查找和模式匹配功能,对 Payload 变量可递归式(交替式)查找和攻击,在攻击中可重定向报文,并且可设置攻击线程数量。因此,Burp Suite 重放攻击 DVWA 靶场带 Token 认证的登录用户名和密码的原理是,设置 3 个 Payload 变量,分别是用户名、密码、Token,其中用户名、密码使用如上方法加载字典,而 Token 需要在每次攻击前先抓取上一次服务器返回报文,用正则表达式查找 Token 值,在下一次攻击前将此 Token 值以及候选用户名和密码填充到向服务器发送的攻击报文中。攻击采用单线程方式,接收和处理响应、攻击,下一个接收和处理响应、攻击,以此往返重复。

本案例演示只攻击密码的情形,只需设置两个 Payload 变量,分别是密码和 Token。

重新抓取登录报文并放入 Intruder 模块,给 password 与 user_token 字段的值都加上变量符,并将 Attack type 改为 Pitchfork(权子),如图 5-35 所示。

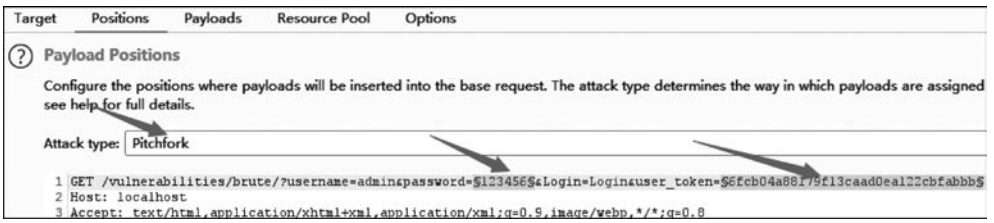


图 5-35 设置 Attack type 为 Pitchfork

在 Payloads 选项卡中选择 Payload set,先选 Payload set 值为 1,对应 password 变量,Payload type 为 simple list,并加载 txt 字典文件,如图 5-36 所示。再选 Payload set 值为 2,对应 user_token 变量,Payload type 为 Recursive grep,此值从服务器端返回报文中查找,因此不再选择爆破字典,如图 5-37 所示。

在 Options 选项卡中,在栏目 Grep - Extract 中勾选 Extract the following items from responses:复选框,即通过正则表达式从服务器响应中匹配以下的内容,然后单击 Add 按钮,如图 5-38 所示。

在 Define extract grep item 窗口中进行如下 4 步操作:①单击右边的 Refetch response 按钮;②在底部查找框中输入关键字 token 或 user_token,即可在服务器响应报文中定位当前的 user_token 值,该字符串为 32 位十六进制;③用鼠标全选该 user_token 值并复制,留待后面步骤中作为第一个要填充的 user_token 值。此时,左上窗口中自动设置了对 user_token 值的正则表达式,其中 Start after expression 选项值自动变为"value='",即字符串从

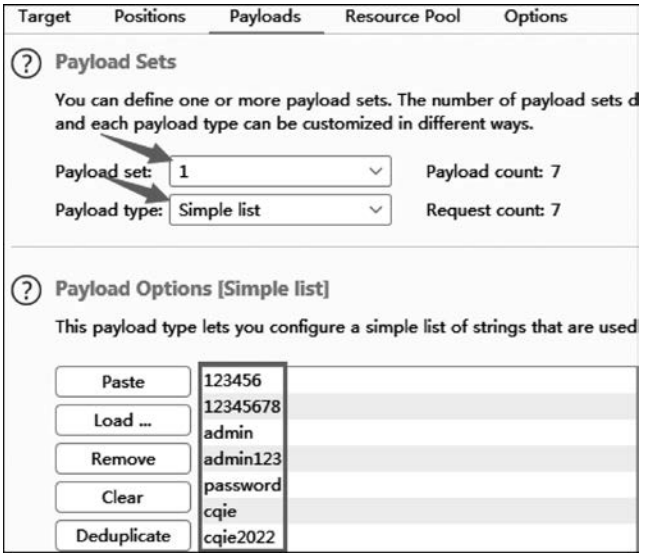


图 5-36　密码变量加载字典

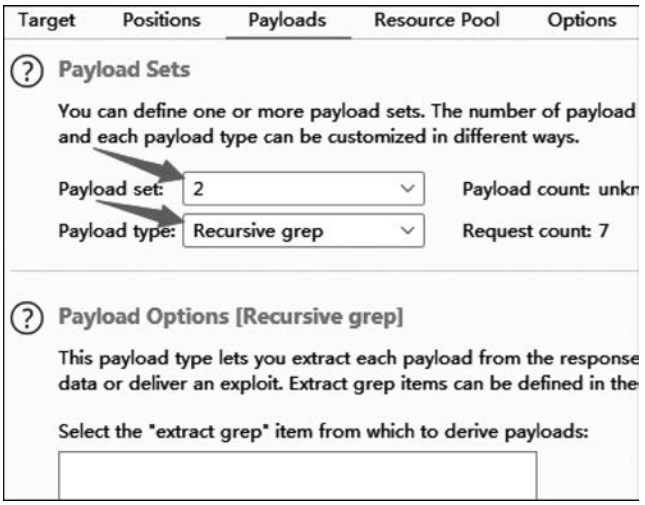


图 5-37　user_token 变量设置递归查找

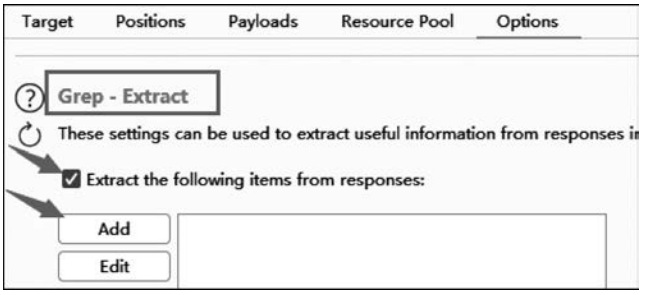


图 5-38　user_token 变量设置递归查找

value='后开始,End at delimiter 选项值自动变为"/>\r\n </form>",即定位结束位置;④单击 OK 按钮。整个操作过程如图 5-39 所示。

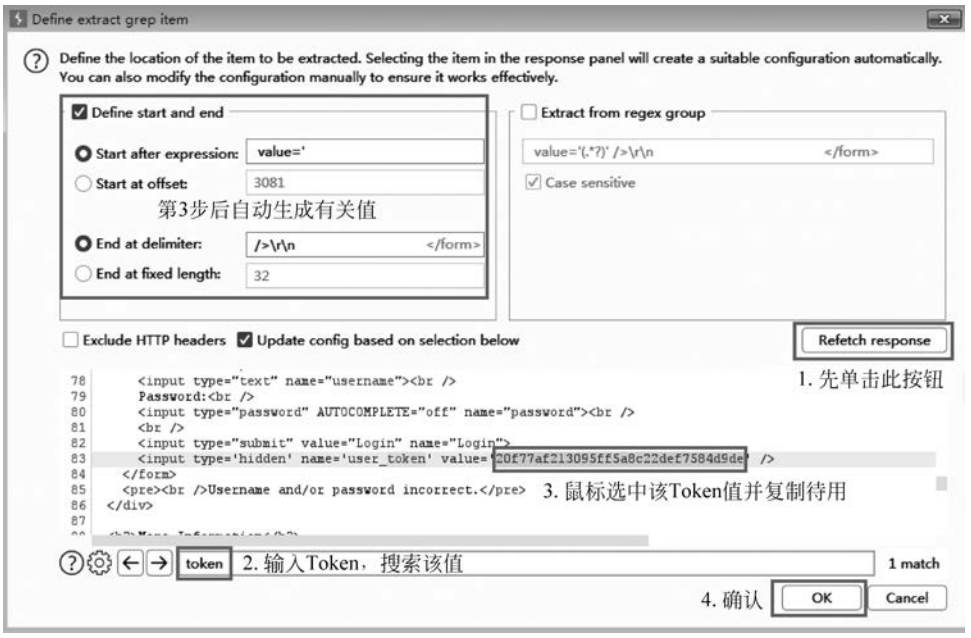


图 5-39 通过正则表达式提取服务器响应报文中的 user_token 值

在 Options 选项卡中的 Redirections 栏目中选择选项值 Always,代表总是遵循重定向到 URL,如图 5-40 所示。

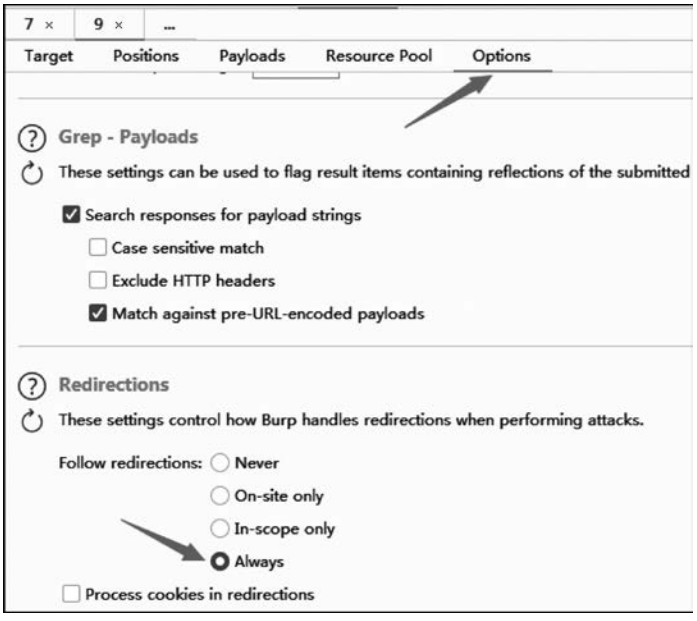


图 5-40 设置总是遵循重定向到 URL

回到 Payloads 选项卡中的 Payloads Options[Recursive grep]栏目,将刚才复制过的 user_token 值粘贴到 Initial payload for first request 后的输入框中,代表在第一个攻击报文

中填充 Payload 的初始 user_token 值，如图 5-41 所示。

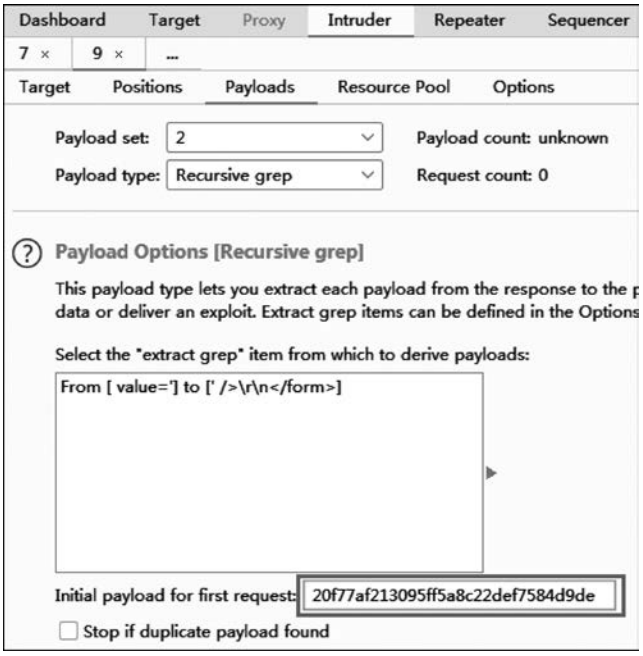
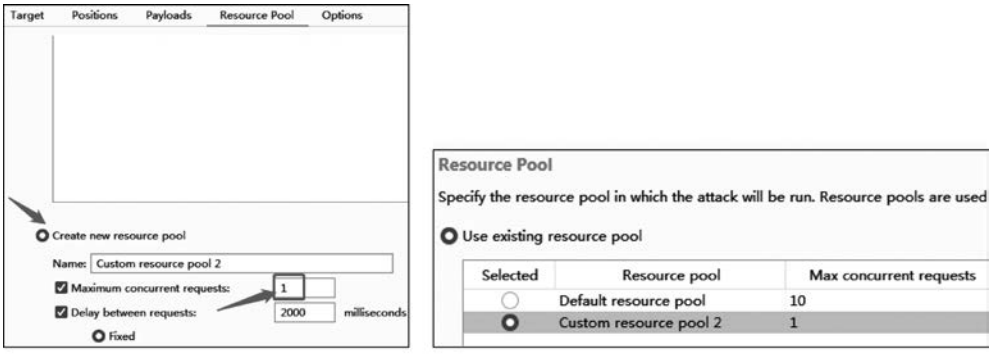


图 5-41　填充初始的 user_token 值

在 Resource Pool 选项卡中，将攻击线程数目设置为 1。由于是 Recursive grep 递归匹配，将上一个响应的 user_token 值作为下一个请求中的 user_token 值，因此就不能多线程并发攻击，而只能是单线程。设置单线程攻击方式如图 5-42 所示。



(a) 设置攻击线程数目为1　　(b) 使用已有资源池

图 5-42　设置单线程攻击方式

最后开始攻击，当攻击结束后，所有攻击报文对应的 HTTP 状态码都为正常值 200，表明对 user_token 值的递归查找、填充和 URL 重定向均正常。正确密码值 password 所在行的报文长度为 4647，服务器端响应报文的渲染结果也是“Welcome to the password protected area admin”，代表密码正确，攻击完成。攻击结果如图 5-43 所示。

(5) 思考。

带 Token 的用户名和密码登录认证过程，与带图片验证码的网站登录过程非常相似。两者的共同点是，本次登录时需要向服务器端提交上一次下发的 Token 或验证码。但是正

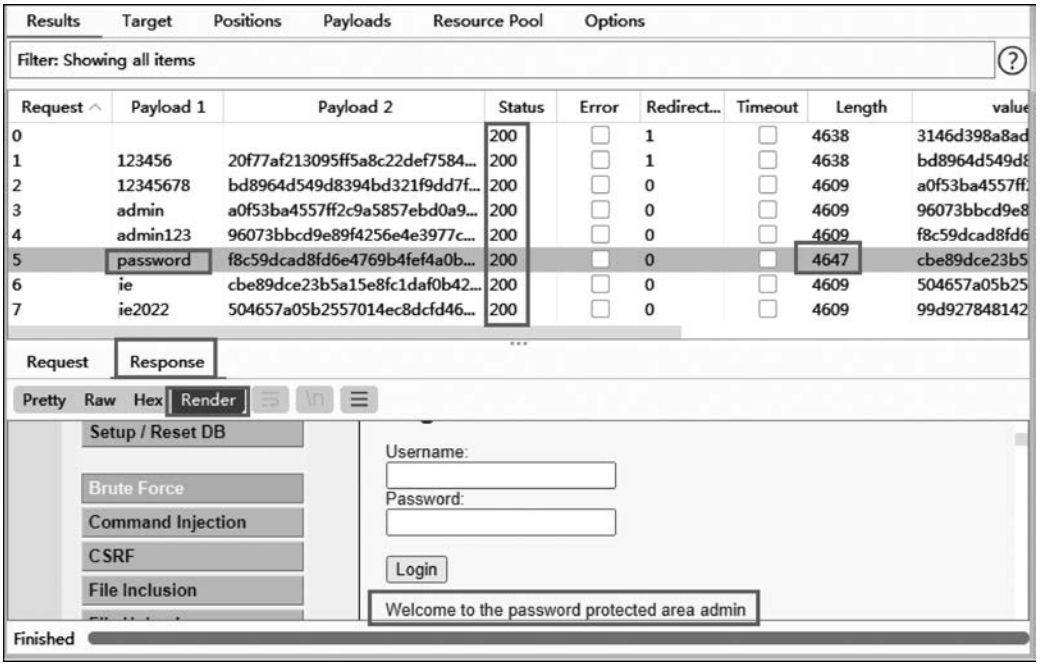


图 5-43 攻击结果

如本案例所示,带 Token 的用户名和密码登录也可以用字典来重放攻击,那么在图片验证码从服务器端下发到浏览器的过程中,如何进行保护处理以避免被类似 Burp Suite 这样的工具截获和自动查找识别呢?

5.6 本章小结

本章介绍了重放攻击的概念、原理和防御措施。引入了基于 Web 的网络靶场 DVWA,以及 Web 应用测试工具 Burp Suite。通过实验九的案例,展示了 Burp Suite 基本使用方法,以及重放攻击 DVWA 靶场登录用户名和密码的方法。

在实验十中,通过配置 DVWA 网络靶场的安全级别为 High,增加了 Token 认证,可防止 CSRF(跨站点请求伪造)攻击,提高了网站的认证安全级别,但是并未做频次限制或账号锁定机制。由于服务器向浏览器下发 Token 值是字符串传输方式,而且该字符串在 form 表单的隐藏域中,Burp Suite 可以通过正则表达式快速定位和抽取 Token 字符串,也可以通过单线程攻击方式,交互式地提取最新 Token 字符串,并填充到下一个攻击报文中,并连同用户名和密码一起进行重放攻击。因此,即便 DVWA 网络靶场的安全级别为 High,也是可以重放攻击的。当 DVWA 网络靶场的安全级别更改为最高级 Impossible 后,除了有 Token 认证外,还增加了登录失败次数的计数,当超过阈值(默认设置为 3 次)时,该用户名会被锁定(默认设置锁定时间为 15min)。此外,DVWA 的源码可自定义修改前述的两个值。在这种情况下只要不是弱口令,重放攻击都可能会快速失败。有兴趣的读者可自行通过实验进行验证。

5.7　习题


在线测试

一、选择题

1. 将以前发送过的报文进行截获，原封不动地或稍加修改后，重新再发送给接收方称为(　　)。

A. 重放攻击　　B. 扫描　　C. 监听　　D. 流量分析

2. 在使用浏览器访问 http://127.0.0.1 时，访问的是(　　)。

A. 网关

B. 本机

C. 网络上 IP 地址为 127.0.0.1 的其他主机

D. 交换机

3. 身份认证系统对错误登录次数超过阈值的账户或攻击者 IP 地址进行锁定并限制随后的登录，主要是为了防止(　　)。

A. 暴力破解登录口令　　B. 重放攻击

C. 对身份认证系统的攻击　　D. 以上类型都是

4. 重放攻击的防御方法主要有错误登录锁定机制、(　　)。

A. 添加浏览器指纹　　B. 添加随机数

C. 添加时间戳　　D. 以上方法都是

5. DVWA 靶场可手动调整靶场所有模块源码的安全级别，共有(　　)个级别。

A. 1　　B. 2　　C. 3　　D. 4

6. Burp Suite 默认开启 TCP (　　)端口作为本地代理接口，以监听 HTTP/HTTPS 通信。

A. 80　　B. 443　　C. 445　　D. 8080

7. (　　)是请求资源(如网页等)不存在的 HTTP 状态码。

A. 200　　B. 301　　C. 302　　D. 404

8. (　　)是请求资源成功的 HTTP 状态码。

A. 200　　B. 301　　C. 302　　D. 404

9. (　　)是内部服务器错误的 HTTP 状态码。

A. 200　　B. 301　　C. 404　　D. 500

10. 以下有关 Burp Suite 暴力破解 DVWA 靶场带 Token 的登录口令，说法错误的是(　　)。

A. 可使用正则表达式从网页上的隐藏区域查找动态变化的 Token 值

B. 攻击线程数目可设置为多线程

C. 正确口令与错误口令返回的报文长度一般是不同的

D. 候选口令既可来自字典，也可手工逐一添加

二、判断题

1. 使用浏览器访问 http://127.0.0.1 时并不需要物理网卡连接外网。 ( )

2. 加密可以有效防止明文数据被监听,也一定能防止重放攻击。 ( )

3. 为防御重放攻击添加随机数时,随机数是由客户端产生的。 ( )

4. 为防御重放攻击添加浏览器指纹,目的是甄别发送报文的来源是浏览器而不是程序化发送报文的工具。 ( )

5. DVWA 靶场登录口令添加 Token,就是添加随机数的方法。 ( )

6. 使用 Burp Suite 暴力破解网站登录口令的原理是模拟键盘、鼠标在登录窗口重复输入口令以重复尝试登录。 ( )

7. 使用 Burp Suite 暴力破解网站登录口令的原理是将初次登录的报文拦截、修改后重复发送报文尝试登录。 ( )

8. 使用 Burp Suite 要拦截 Web 浏览器发送的 HTTP 报文,Web 浏览器可以不设置 Burp Suite 作为代理服务器。 ( )

9. Burp Suite 内置浏览器默认设置了本地代理接口,以监听 HTTP/HTTPS 通信。 ( )

10. DVWA 靶场带 Token 的登录口令可以被 Burp Suite 通过重放攻击来暴力测试。 ( )