

【CTF-MISC-流量】WebShark 操作手册

WebShark 操作手册

1. 项目简介

WebShark 是一款基于 Web 的网络流量分析工具，类似于 Wireshark，但运行在浏览器中。它可以打开 PCAP 和 PCAPNG 格式的流量包文件，提供丰富的流量分析功能，包括概览统计、数据包列表、流分析、应用层请求分析等。

1.1 主要功能

- 支持 PCAP 和 PCAPNG 格式的流量包文件
- 提供直观的流量概览统计
- 支持数据包的搜索、筛选和排序
- 网络流分析与对话展示
- 应用层请求详情分析
- IP 端口使用统计
- 连接频率统计
- 关键字匹配功能
- 安全检测功能
- 表格列宽拖拽调整
- IP 归属地查询
- 端口描述查询
- 数据导出功能（Excel 格式）
- URL 解码功能
- 时间格式化功能
- 多种协议支持（HTTP、TCP、UDP、DNS、TLS 等）

2. 快速开始

2.1 启动应用

WebShark 是一个静态 Web 应用，可以通过以下方式启动：

本地 HTTP 服务器（推荐）：

```
# 进入代码目录
cd 代码
# 使用 Python 启动 HTTP 服务器
python -m http.server 8000
```

然后在浏览器中访问 `http://localhost:8000`

直接打开 HTML 文件：

直接双击 `代码/index.html` 文件在浏览器中打开

2.2 加载流量包

点击页面顶部的“选择 PCAP/PCAPNG 文件”按钮

在文件选择对话框中选择要分析的流量包文件

等待文件加载和分析完成

查看各个标签页的分析结果

3. 功能模块详解

3.1 概览

概览页面显示流量包的基本统计信息，包括：

- **数据包数量**：流量包中包含的数据包总数
- **文件大小**：流量包文件的大小
- **捕获时长**：流量捕获的总时长
- **平均包大小**：所有数据包的平均大小
- **总流量**：所有数据包的总字节数
- **发送流量**：发送方向的总字节数
- **接收流量**：接收方向的总字节数
- **平均速率**：平均数据传输速率
- **设备信息**：捕获设备的信息（如果可用）
- **源地址数量**：不同源 IP 地址的数量

此外，概览页面还显示**协议使用统计**，直观展示各种应用层协议的使用情况。

3.2 数据包列表

数据包列表页面显示所有数据包的详细信息，并提供搜索、筛选、排序和列宽调整等功能。

3.2.1 数据包字段说明

字段	说明
操作	包含操作按钮，用于查看数据包详情等
唯一 ID	数据包的唯一标识符，用于区分不同数据包
序号	数据包在流量包中的序号
时间	数据包的捕获时间，格式为 YYYY-MM-DD HH:MM:SS.SSS
源地址	数据包的源 IP 地址
源端口	数据包的源端口，显示实际端口号
目的地址	数据包的目的 IP 地址
目标端口	数据包的目标端口，显示实际端口号
协议	数据包使用的协议链，如 Ethernet → IPv4 → TCP → HTTP
流 ID	数据包所属的流 ID，用于标识同一连接的数据包
长度	数据包的长度，单位为字节
功能介绍	数据包的功能描述，如“TCP 握手请求”、“HTTP GET 请求”等
信息	数据包的详细信息，如 HTTP 请求的 URL、DNS 查询的域名等
关键字匹配	数据包是否匹配设定的关键字，显示匹配的关键字列表

3.2.2 搜索与筛选

简单搜索：

- 在搜索框中输入关键词
- 选择要搜索的字段（全部字段、唯一 ID、序号、时间、源地址等）
- 点击“搜索”按钮

高级筛选：

- 点击“高级筛选”区域
- 添加筛选条件：选择字段、操作符（包含、等于、开始于、结束于、不包含、不等于、大于、小于）、筛选值和逻辑关系（AND/OR）
- 可以添加多个筛选条件，构建复杂的筛选规则
- 点击“应用筛选”按钮执行筛选

表格列筛选：

- 点击表头右侧的“▼”筛选图标，打开筛选下拉菜单
- 选择要筛选的值（显示值及其出现次数）
- 点击“应用”按钮执行筛选
- 点击“清除”按钮清除该列的筛选条件

清除筛选：

- 点击“清除筛选”按钮清除所有筛选条件

3.2.3 排序

- 点击表头可以对对应字段进行排序
- 再次点击可以切换升序/降序
- 排序会实时应用到当前显示的数据上

3.2.4 表格列宽调整

- 将鼠标悬停在表头之间的分隔线上，鼠标指针会变为双向箭头
- 按住鼠标左键拖动分隔线，可以调整列宽
- 列宽调整会实时应用到表格上

3.2.5 导出数据

- 点击“导出 XLSX”按钮可以将数据包列表导出为 Excel 文件
- 导出的数据包含当前显示的所有数据包的详细信息

3.2.6 查看数据包详情

- 点击数据包行中的操作按钮，可以在“数据包详情”标签页查看该数据包的详细信息
- 数据包详情包括各个协议层的详细信息和十六进制数据

3.3 流列表

流列表页面显示网络流的信息，包括流列表和流对话，帮助用户分析网络连接的完整通信过程。

3.3.1 流列表

流列表显示所有网络流的基本信息，包括：

- **流 ID**：流的唯一标识符，用于区分不同的网络连接
- **源 IP:端口**：流的源地址和端口，格式为 IP:端口
- **目标 IP:端口**：流的目标地址和端口，格式为 IP:端口
- **数据包数量**：流中包含的数据包数量，反映连接的活跃度
- **长度**：流的总长度，单位为字节，反映数据传输量
- **协议**：流使用的主要协议，如 TCP、UDP、HTTP 等
- **协议统计**：流中各协议的使用统计，显示不同协议的分布情况

3.3.2 流对话

- 点击流列表中的任意一行，可以在右侧查看该流的对话内容
- 对话内容以消息气泡的形式展示，区分发送和接收方向
 - 发送方向：蓝色气泡，显示从源到目标的数据
 - 接收方向：绿色气泡，显示从目标到源的数据
- 每个消息气泡包含时间戳、发送/接收标识和数据内容
- 可以使用“上一条”和“下一条”按钮切换不同的流，方便浏览多个连接

3.3.3 流搜索与筛选

简单搜索：

- 在搜索框中输入关键词（流 ID、IP、端口、协议等）
- 选择要搜索的字段（全部字段、流 ID、源 IP、源端口、目标 IP、目标端口、数据包数量、协议、流对话）
- 点击“搜索”按钮执行搜索

高级筛选：

- 点击“高级筛选”区域
- 添加筛选条件：选择字段、操作符（包含、等于、开始于、结束于、不包含、不等于、大于、小于）、筛选值和逻辑关系（AND/OR）
- 可以添加多个筛选条件，构建复杂的筛选规则
- 点击“应用筛选”按钮执行筛选

表格列筛选：

- 点击流列表表头右侧的“▼”筛选图标，打开筛选下拉菜单
- 选择要筛选的值（显示值及其出现次数）
- 点击“应用”按钮执行筛选

清除筛选：

- 点击“清除筛选”按钮清除所有筛选条件

3.3.4 流排序

- 点击流列表表头可以对对应字段进行排序
- 可排序的字段包括：流 ID、源 IP:端口、目标 IP:端口、数据包数量、长度、协议
- 再次点击可以切换升序/降序

3.3.5 流协议识别

- 系统会自动识别流中使用的主要协议
- 对于包含多种协议的流，会显示出现次数最多的协议
- 协议统计功能会显示流中各协议的分布情况

3.4 应用层请求

应用层请求页面显示 HTTP 等应用层协议的请求信息，帮助用户分析应用层通信细节。

3.4.1 请求列表字段

字段	说明
序号	请求的序号
请求方法	HTTP 请求方法（GET、POST、PUT、DELETE 等）或其他协议名称
URL 路径	请求的 URL 路径，已自动 URL 解码
源 IP:端口	请求的源地址和端口
目标 IP:端口	请求的目标地址和端口
响应状态	HTTP 响应状态码，如 200 OK、404 Not Found 等
响应大小	响应的大小，单位为字节
Host	请求的 Host 头部，显示请求的域名
User-Agent	请求的 User-Agent 头部，显示客户端信息
Accept	请求的 Accept 头部，显示客户端可接受的内容类型
Accept-Language	请求的 Accept-Language 头部，显示客户端语言偏好
Cookie	请求的 Cookie 头部，显示客户端发送的 Cookie 信息
Content-Type	请求的 Content-Type 头部，显示请求体的内容类型
响应内容类型	响应的 Content-Type 头部，显示响应体的内容类型
服务器	响应的 Server 头部，显示服务器信息

字段	说明
响应时间	请求的响应时间，显示从请求到响应的延迟
请求体内容	请求的正文内容，只显示前 50 个字符
响应体内容	响应的正文内容，只显示前 50 个字符
安全状态	请求的安全检测结果，显示“安全”或“危险”
操作	包含操作按钮，用于查看请求详情等

3.4.2 搜索与筛选

简单搜索：

- 在搜索框中输入关键词
- 选择要搜索的字段（全部字段、请求方法、URL 路径、协议版本、源 IP:端口、目标 IP:端口、响应状态、响应大小等）
- 点击“搜索”按钮执行搜索

高级筛选：

- 点击“高级筛选”区域
- 添加筛选条件：选择字段、操作符（包含、等于、开始于、结束于、不包含、不等于、大于、小于）、筛选值和逻辑关系（AND/OR）
- 可以添加多个筛选条件，构建复杂的筛选规则
- 点击“应用筛选”按钮执行筛选

表格列筛选：

- 点击应用层请求列表表头右侧的“▼”筛选图标，打开筛选下拉菜单
- 选择要筛选的值（显示值及其出现次数）
- 点击“应用”按钮执行筛选

清除筛选：

- 点击“清除筛选”按钮清除所有筛选条件

3.4.3 排序

- 点击表头可以对对应字段进行排序
- 可排序的字段包括：序号、请求方法、URL 路径、源 IP:端口、目标 IP:端口、响应状态、响应大小等
- 再次点击可以切换升序/降序

3.4.4 安全检测

- 系统会自动对每个应用层请求进行安全检测
- 安全状态字段显示检测结果：
 - “安全”：请求未检测到安全风险
 - “危险”：请求检测到安全风险，如 XSS 攻击、SQL 注入等
- 安全检测基于多种规则，包括关键字匹配、请求特征分析等

3.4.5 URL 解码

- 系统会自动对 URL 路径进行 URL 解码，方便查看真实路径
- 解码后的 URL 路径显示在“URL 路径”列中

3.4.6 导出数据

- 点击“导出 XLSX”按钮可以将应用层请求列表导出为 Excel 文件
- 导出的数据包含当前显示的所有请求的详细信息

3.5 数据包详情

数据包详情页面显示单个数据包的详细信息，包括各协议层的解析结果和十六进制数据。

3.5.1 查看数据包详情

1. 在数据包列表中点击任意数据包的行
2. 切换到“数据包详情”标签页
3. 查看数据包的详细信息

3.5.2 详情内容

- **协议层信息：**按协议层级显示数据包的详细信息，包括：
 - 数据链路层：Ethernet 帧信息
 - 网络层：IP 头部信息（源 IP、目标 IP、TTL 等）
 - 传输层：TCP/UDP 头部信息（源端口、目标端口、序列号等）
 - 应用层：HTTP、DNS 等应用层协议的详细信息
- **十六进制数据：**显示数据包的原始十六进制数据，方便高级分析
- **协议字段：**显示各协议层的具体字段及其值
- **关系图：**显示数据包在流中的位置关系（如果适用）

3.5.3 详情特点

- **层次清晰：**按协议层级组织信息，方便理解数据包结构
- **详细全面：**包含从物理层到应用层的所有协议信息
- **直观易懂：**使用表格和结构化格式显示信息
- **原始数据：**提供十六进制原始数据，支持深度分析

3.6 IP 端口统计

IP 端口统计页面显示 IP 地址和端口的使用情况统计，帮助用户了解网络流量的来源和去向。

3.6.1 统计内容

字段	说明
IP 地址	网络流量中的源 IP 和目标 IP 地址
归属地	识别为内网或者外网
端口	网络流量中的源端口和目标端口
端口描述	端口的服务描述（如 80 端口显示 HTTP）
数据包数量	该 IP+端口组合的数据包数量
占比	该 IP+端口组合在总流量中的占比

3.6.2 统计特点

- **自动统计：**系统自动分析流量包，生成 IP 端口使用统计
- **双向统计：**同时统计源 IP+端口和目标 IP+端口
- **IP 归属地：**自动查询并显示 IP 地址的地理归属地
- **端口描述：**自动匹配并显示端口对应的服务描述
- **占比分析：**显示每个 IP+端口组合在总流量中的占比

3.6.3 查看方式

1. 加载流量包文件
2. 切换到“IP 端口统计”标签页
3. 查看 IP 端口使用统计信息

3.6.4 筛选和搜索

- 支持表格列筛选功能
- 点击表头右侧的“▼”筛选图标，选择要筛选的值
- 可以根据 IP 地址、归属地、端口、端口描述等进行筛选
- 筛选条件对应的数量为数据包的数量

3.7 连接频率统计

连接频率统计页面显示 IP+端口组合的连接频率统计，帮助用户识别频繁连接的主机和服务。

3.7.1 统计内容

- **IP+端口组合**：显示网络中的 IP+端口组合
- **连接频率**：该 IP+端口组合的连接次数
- **连接时间分布**：连接发生的时间分布情况

3.7.2 统计特点

- **频率分析**：分析连接的频繁程度
- **时间分布**：显示连接在时间上的分布
- **异常检测**：帮助识别异常的连接模式

3.7.3 查看方式

1. 加载流量包文件
2. 切换到“连接频率统计”标签页
3. 查看连接频率统计信息

3.8 设置

设置页面用于配置 WebShark 的各项功能，包括关键字管理、功能开关等。

3.8.1 关键字管理

关键字管理用于配置数据包关键字匹配功能，帮助用户快速识别包含特定关键字的数据包。

3.8.1.1 默认关键字

系统内置了以下默认关键字：

- `flag`、`fl`、`KEY` - 用于标识标志信息
- `pass`、`user`、`admin` - 用于标识认证信息
- `select`、`alter` - 用于标识 SQL 操作
- `ctf` - 用于 CTF 比赛场景
- `@eval`、`xss` - 用于标识安全漏洞
- `frpc` - 用于标识 FRP 客户端
- `linux` - 用于标识 Linux 系统命令
- `login`、`log`、`.log` - 用于标识日志相关信息
- `whoami`、`echo` - 用于标识命令执行

3.8.1.2 关键字匹配功能

启用/禁用关键字匹配：

- 使用开关按钮控制关键字匹配功能的开启和关闭
- 开启后，系统会自动扫描数据包，标记包含匹配关键字的数据包

添加关键字：

- 在输入框中输入要添加的关键字
- 点击“添加”按钮将关键字添加到列表中
- 支持添加多个关键字，每个关键字独立匹配

管理关键字：

- 在关键字列表中可以查看已添加的所有关键字
- 可以删除不需要的关键字（点击关键字旁边的删除按钮）
- 关键字列表实时更新，反映当前配置

还原默认关键字：

- 点击“还原默认关键字”按钮
- 系统会清除当前所有关键字，并恢复为默认关键字列表

保存设置：

- 点击“保存设置”按钮保存所有关键字配置
- 保存后，关键字配置会立即应用到数据包分析中

3.8.1.3 关键字匹配范围

关键字匹配会检查数据包的以下属性：

- 基本信息：唯一 ID、IP 地址、端口、协议等
- 应用层数据：HTTP 请求方法、URL、头部信息、请求体等
- 功能描述：数据包的功能介绍和信息字段
- 原始数据：应用层原始数据

3.8.2 设置保存

- 所有设置会保存在浏览器的本地存储中
- 刷新页面后，设置会自动恢复
- 更换浏览器或清除浏览器数据后，设置会丢失
- 建议定期备份重要设置

4. 项目结构

```
WebShark/
├── 代码/                                # 主程序代码
│   ├── app.js                          # 主应用逻辑
│   ├── chart.min.js                    # 图表库
│   ├── index.html                      # 主页面
│   ├── node_modules/                  # 依赖库
│   ├── package.json                   # 项目配置
│   ├── package-lock.json              # 依赖锁定文件
│   ├── pcapng-parser.js                # PCAPNG解析器
│   ├── security-detector.js            # 安全检测模块
│   └── xlsx.full.min.js                # Excel导出库
└── 操作手册.md                         # 操作手册
```

5. 技术栈

WebShark 采用纯前端技术栈开发，无需后端服务，可直接在浏览器中运行。

技术	版本	用途
HTML5	-	页面结构和布局
CSS3	-	页面样式和交互效果
JavaScript (ES6+)	-	核心逻辑和交互处理
PCAPNG 解析库	自定义	解析 PCAP 和 PCAPNG 格式的流量包
Excel 导出库	xlsx.full.min.js	将数据导出为 Excel 文件
jsdom	27.3.0	用于 Node.js 环境下的测试和开发

5.1 技术特点

- **纯前端实现**：所有功能在浏览器中完成，无需后端服务
- **高效解析**：优化的 PCAPNG 解析算法，支持大文件解析
- **响应式设计**：适配不同屏幕尺寸
- **模块化架构**：代码结构清晰，易于维护和扩展
- **丰富的交互**：表格排序、筛选、列宽调整等交互功能
- **实时分析**：流量包加载后实时进行分析和统计

5.2 浏览器兼容性

- Chrome 80+: 最佳支持
- Firefox 75+: 良好支持
- Safari 13+: 基本支持
- Edge 80+: 良好支持

6. 项目特点

6.1 易用性

- **直观的界面**: 清晰的标签页布局, 易于导航
- **简单的操作**: 拖拽文件即可加载, 点击即可查看详情
- **丰富的提示**: 友好的操作提示和状态反馈

6.2 功能性

- **全面的分析**: 从数据链路层到应用层的完整分析
- **强大的搜索**: 支持多种搜索和筛选方式
- **实时的统计**: 动态生成各种统计图表和数据
- **安全的检测**: 内置安全检测功能, 识别潜在威胁

6.3 扩展性

- **模块化设计**: 易于添加新的协议解析器
- **可定制的关键字**: 支持用户自定义关键字列表
- **开放的架构**: 支持扩展新的功能模块

6.4 性能

- **高效的解析**: 优化的解析算法, 支持大文件
- **流畅的交互**: 优化的渲染和交互性能
- **低内存占用**: 高效的内存管理, 支持长时间运行

7. 使用技巧

7.1 快速定位数据包

1. **使用关键字匹配**: 在设置中添加相关关键字, 系统会自动标记匹配的数据包
2. **使用搜索功能**: 利用搜索框快速查找特定 IP、端口或协议的数据包
3. **使用筛选功能**: 通过高级筛选条件精确查找数据包

7.2 分析网络流

1. 查看流列表, 了解网络连接情况
2. 点击流查看完整对话内容
3. 分析流的协议分布和数据传输情况

7.3 识别安全威胁

1. 查看应用层请求的安全状态字段
2. 关注标记为“危险”的请求
3. 分析危险请求的详细信息，确定威胁类型

7.4 优化大文件处理

1. 对于大型流量包，建议关闭关键字匹配功能
2. 调整每页显示数量，减少内存占用
3. 使用筛选功能，只查看感兴趣的数据

7.5 导出数据

1. 选择要导出的数据范围（使用筛选功能）
2. 点击相应的导出按钮
3. 保存导出的 Excel 文件，用于进一步分析

8. 技术细节

8.1 流量包解析

- **支持格式：**PCAP 和 PCAPNG 格式
- **解析方式：**基于 FileReader API 和 ArrayBuffer
- **解析流程：**
 1. 读取文件内容为 ArrayBuffer
 2. 解析文件头和块结构
 3. 解析每个数据包
 4. 提取协议信息
 5. 生成分析结果

8.2 流重组

- **流识别：**基于 5 元组（源 IP、源端口、目标 IP、目标端口、协议）
- **流重组：**将同一流的数据包组合在一起
- **对话生成：**根据数据包的方向生成对话内容

8.3 安全检测

- **检测方式：**基于规则匹配和特征分析
- **检测范围：**
 - HTTP 请求和响应
 - 应用层数据
 - 关键字匹配
- **检测规则：**
 - XSS 攻击检测
 - SQL 注入检测
 - 命令执行检测
 - 敏感信息泄露检测

8.4 数据存储

- **本地存储：**使用浏览器的 localStorage 存储设置和配置
- **临时存储：**使用内存存储解析结果和分析数据
- **无持久化存储：**刷新页面后，解析结果会丢失，需重新加载文件

9. 使用示例

9.1 分析 HTTP 请求

1. 加载包含 HTTP 流量的 PCAP/PCAPNG 文件
2. 切换到“应用层请求”标签页
3. 查看 HTTP 请求列表，包含请求方法、URL 路径、响应状态等信息
4. 使用搜索或筛选功能查找特定请求（如按 URL 路径搜索）
5. 点击请求查看详细信息，包括请求头、响应头和请求体
6. 查看安全状态字段，识别潜在的安全威胁

9.2 分析网络流

1. 加载流量包文件
2. 切换到“流列表”标签页
3. 查看流列表，了解所有网络连接的基本信息
4. 选择感兴趣的流，查看右侧的流对话内容
5. 观察对话的发送和接收方向，分析通信过程
6. 使用“上一条”和“下一条”按钮浏览不同流
7. 查看流的协议统计，了解流中使用的协议分布

9.3 查找匹配关键字的数据包

1. 切换到“设置”标签页
2. 启用关键字匹配功能（打开开关）
3. 添加感兴趣的关键词（如“password”、“login”、“flag”等）
4. 点击“保存设置”按钮
5. 切换到“数据包列表”标签页
6. 查看“关键字匹配”列，找到匹配的数据包
7. 点击匹配的数据包查看详细信息

9.4 分析 IP 端口使用情况

1. 加载流量包文件
2. 切换到“IP 端口统计”标签页
3. 查看 IP 地址和端口的使用统计
4. 查看 IP 地址的归属地信息
5. 查看端口的服务描述
6. 使用筛选功能，根据 IP 地址或端口进行筛选

9.5 导出分析结果

1. 完成流量包分析
2. 切换到要导出数据的标签页（如数据包列表、应用层请求）
3. 使用筛选功能选择要导出的数据范围
4. 点击“导出 XLSX”按钮
5. 在弹出的对话框中选择保存位置和文件名
6. 点击“保存”按钮，将数据导出为 Excel 文件

10. 常见问题

10.1 支持哪些文件格式？

- PCAP 格式
- PCAPNG 格式

10.2 为什么文件加载失败？

- 文件格式错误：请确保文件格式为 PCAP 或 PCAPNG
- 文件损坏：请确保文件没有损坏，尝试使用其他工具验证文件完整性
- 文件过大：对于大型文件，可能需要较长时间加载，请耐心等待
- 浏览器兼容性：请使用支持的浏览器版本（Chrome 80+、Firefox 75+、Safari 13+、Edge 80+）

10.3 如何提高大型文件的加载速度？

- 关闭不必要的功能（如关键字匹配）
- 优化浏览器性能：关闭其他标签页和扩展程序
- 使用较新版本的浏览器
- 考虑将大型文件分割为多个小型文件

10.4 如何保存分析结果？

- **导出为 Excel：**使用页面上的“导出 XLSX”按钮，将数据导出为 Excel 文件
- **截图保存：**使用浏览器的截图功能保存当前页面
- **复制数据：**直接从表格中复制数据到其他应用程序

10.5 为什么关键字匹配功能不生效？

- 请确保已启用关键字匹配功能（设置页面中的开关已打开）
- 请确保已保存设置
- 请检查关键字列表中是否包含要匹配的关键字
- 请确保数据包中确实包含要匹配的关键字

10.6 如何添加自定义关键字？

1. 切换到“设置”标签页
2. 在关键字输入框中输入要添加的关键字
3. 点击“添加”按钮
4. 点击“保存设置”按钮保存更改

11. 版本更新日志

最新版本

- 支持 PCAP 和 PCAPNG 格式的流量包文件
- 提供直观的流量概览统计
- 支持数据包的搜索、筛选和排序
- 网络流分析与对话展示
- 应用层请求详情分析
- IP 端口使用统计
- 连接频率统计
- 关键字匹配功能
- 安全检测功能
- 表格列宽拖拽调整
- IP 归属地查询
- 端口描述查询
- 数据导出功能（Excel 格式）
- URL 解码功能
- 时间格式化功能
- 多种协议支持

WebShark案例

案例一：分析SQL盲注问题

攻防世界：<https://adworld.xctf.org.cn/challenges/list>

流量分析

打开WebShark

选择流量包文件打开

概览界面出现了流量包的基本信息

打开HTTP请求URL模块

因为题目提示了sql注入，所以我们直接看HTTP请求就可以了
看到HTTP请求的URL路径

拖拉表头查看完整URL路径

一看就知道是SQL注入，还是盲注，那么看响应体内容

筛选响应体内容

把不一样的响应体筛选出来，就可以知道哪几次盲注成功了
一般都是数量少的是注入成功的，直接筛选，也可以点击响应详情仔细斟酌

分析其中一个注入成功的url

```
?id=1' and ascii(substring((select keyid from flag limit 0,1),18,1))=54#
```

“测试 flag 表中第一行的 keyid 字段值的第 18 个字符的 ASCII 码是否为 54（即是否为数字‘6’）。”

将筛选的HTTP请求导出为xlsx格式

用WPS的excel的高级分列，将盲注的信息分割出来

其他工具也可以，或者自己写个python代码分割也行，本人用WPS因为方便

使用=CHAR(E2)将ascii数值转换为字符串

再去word里面全部替换一下获取结果

得到最终答案

flag{c2bbf9cecdaf656cf524d014c5bf046c}

案例二：SMTP协议邮件分析

第二届全国网络安全行业职业技能大赛-电子数据取证分析师-初赛

其中15-19题和流量分析有关：

- 15.（检材3分析）收件人邮箱是什么？
- 16.（检材3分析）发件人使用的客户端软件以及版本是什么？（参考格式：abc 1.1.11.111[ab]）
- 17.（检材3分析）邮件的主题是什么？
- 18.（检材3分析）已知邮箱附件采用7位数字加密，请问该7位数字密码是什么？
- 19.（检材3分析）已知邮箱附件中有一个lvm文件，请填写里面的URL信息。（参考格式：http://a.com/）

15题：收件人邮箱是什么？

打开WebShark

选择要分析的流量包

进入数据包列表，搜索SMTP协议

查看SMTP协议的信息内容

发现RCPT TO: rihanaliyboy@163.com，表示邮箱发送至rihanaliyboy@163.com邮箱
所以，第15题答案为：rihanaliyboy@163.com

第16题：发件人使用的客户端软件以及版本是什么？

查看流对话

查看15题找到收件人信息的数据包，点击流对话

可以看到邮件客户端版本信息

答案：Foxmail 7.2.23.121[cn]

第17题：邮件的主题是什么？

从第16题的结果中可以看到主题

答案:info

第18题：已知邮箱附件采用7位数字加密，请问该7位数字密码是什么？

将流对话中的附件信息提取出来

进行base64解密，并下载为文件

Base64解密工具：<https://mate.tools/zh/base64-decoder>

下载发现有密码

使用破解工具破解密码Passware Kit Forensic

找到答案：7894123

第19题：已知邮箱附件中有一个lvm文件，请填写里面的URL信息。

用记事本打开上一道题的information.lvm文件

答案:<http://lovema.world3.com/>