3. URL安全

授课教师：游伟 副教授
授课时间：周一16:00 – 17:30（立德0412），周二14:00 – 15:30（教二2402）
课程主页：https://rucsesec.github.io/cybersecurity

引子1

游戏作弊：挤上“魂斗罗”的游戏排行榜

http://www.4399.com/flash/225668_4.htm

引子2

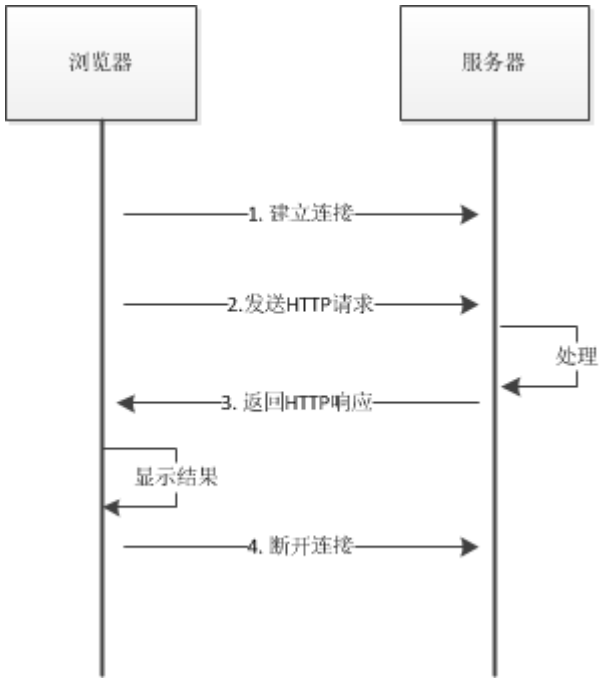
获取“UV的匿名测试墙”管理员密码

http://weixiao.nickboy.cc/go_to_wall/gh_77aef1d9cf29

目录

3.1 HTTP协议与消息

- HTTP：超文本传输协议（HyperText Transfer Protocol），基于TCP/IP之上的应用协议



HTTP协议通讯过程

1. 客户机与服务器建立连接。只要单击某个超级链接，HTTP 的工作开始。
2. 客户机发送一个请求给服务器，请求方式的格式为：统一资源标识符（URL）、协议版本号，后边是MIME信息包括请求修饰符、客户机信息和可能的内容。
3. 服务器接到请求后，处理并返回响应信息，其格式为一个状态行，包括信息的协议版本号、一个成功或错误的代码，后边是MIME 信息包括服务器信息、实体信息和可能的内容。
4. 客户端接收服务器所返回的信息通过浏览器显示在用户的显示屏上，然后客户机与服务器断开连接。

3.1.1 HTTP协议

- 无连接
  - 每次连接只处理一个请求
  - 服务器处理完客户的请求，并收到客户的应答后，即断开连接
- 无状态
  - 协议对于事务处理没有记忆能力
  - 如果后续处理需要前面的信息，则它必须重传
- 媒体独立的
  - 只要客户端和服务器知道如何处理的数据内容，任何类型的数据都可以通过HTTP发送
  - 客户端以及服务器指定使用适合的内容类型

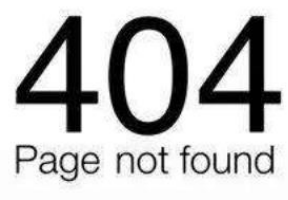
3.1.2 HTTP消息

- 消息类型：
  - 请求：客户端->服务器端
  - 响应：服务器端->客户端
- 消息构成：
  - 请求/响应行
  - 消息头
  - 消息体

HTTP请求

① 是请求方法，HTTP/1.1 定义的请求方法有8种。一般常用的是GET和POST。
② 为请求对应的URL地址，它和报文头的Host属性组成完整的请求URL
③ 是协议名称及版本号。
④ 是HTTP的报文头，包含若干个属性，格式为"属性名:属性值"，服务端据此获取客户端信息。
⑤ 是报文体，承载请求参数的数据等内容

HTTP响应



① 报文协议及版本；
② 状态码及状态描述；
③ 响应报文头，也是由多个属性组成；
④ 响应报文体，即我们真正要的“干货”。

HTTP的响应状态码由5段组成：

```
1xx 消息，一般是告诉客户端，请求已经收到了，正在处理，别急...
2xx 处理成功，一般表示：请求收悉、我明白你要的、请求已受理、已经处理完成等信息.
3xx 重定向到其它地方。它让客户端再发起一个请求以完成整个处理。
4xx 处理发生错误，责任在客户端，如客户端的请求一个不存在的资源，客户端未被授权，禁止访问等。
5xx 处理发生错误，责任在服务端，如服务端抛出异常，路由出错，HTTP版本不支持等。
```

3.2 URL概述

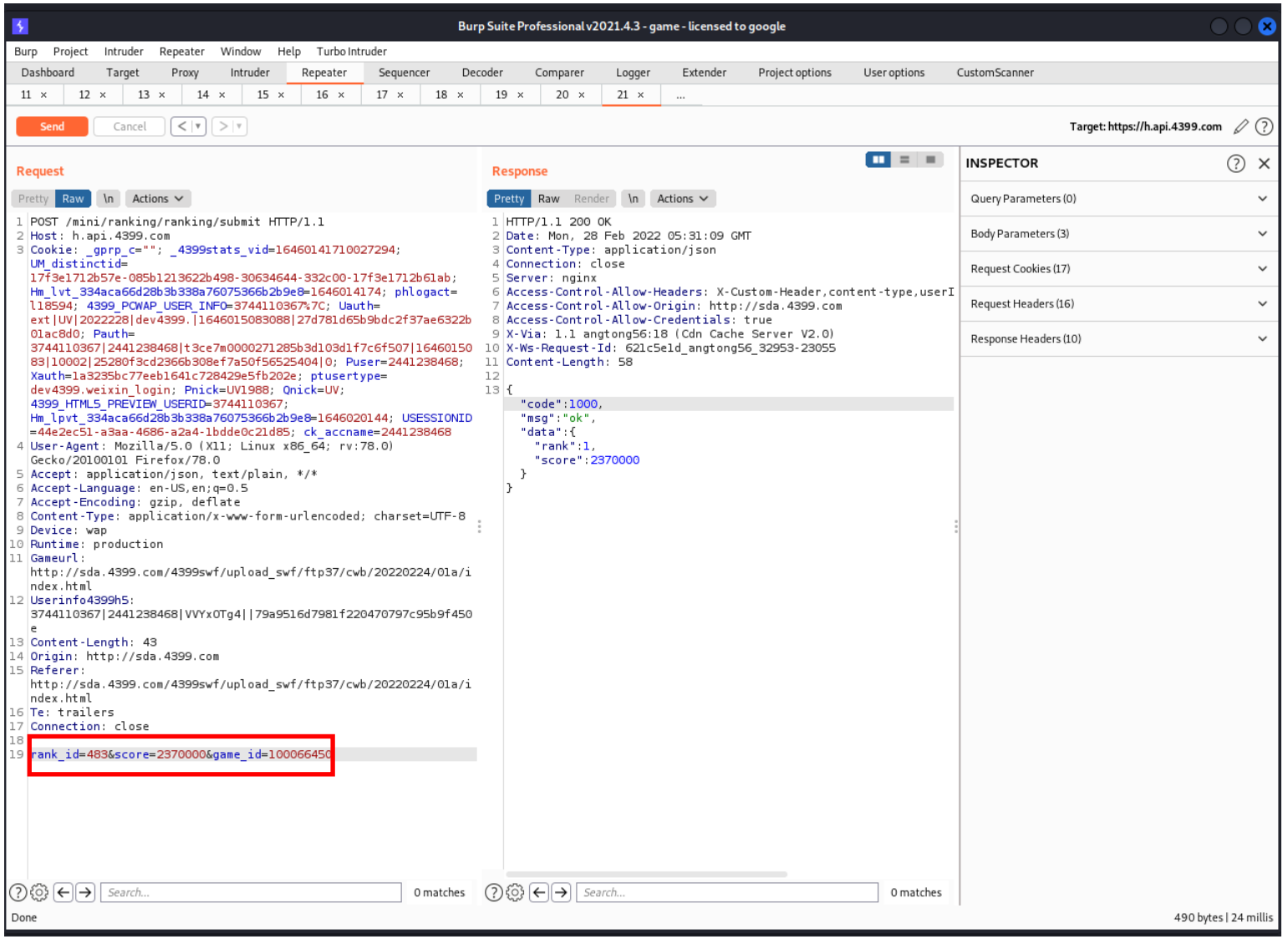
- Web资源（如HTML文档、图像、视频等）的访问通过**URL（Uniform Resoure Locator）**统一资源定位器来进行
- URL一般由多个部分组成：
  - 资源的访问机制（协议），如http、ftp等等
  - 存放资源的主机名及端口号：localhost:8080
  - 资源自身的名称：/abc/index.jsp
  - 查询参数：?username=anybody
  - ……

http://localhost:8080/abc/index.jsp?username=anybody

3.3 URL攻击

- 方式1：利用服务器端参数检测的不完备
  - 原理：当服务器端认证存在漏洞时，通过URL来猜测某些资源的存放地址，从而非法访问应受保护的资源或执行非法操作
  - 本质：服务端代码对客户端请求参数缺乏完备的检查
  - 实例：
    - 例1：若某网站的找回密码链接URL为：
      http://example.org/private.php?user=abc&email=abc@d.org
      可尝试替换user域为其他用户，将找回密码邮件发至指定邮箱
    - 例2：若某教学系统网站学生查看成绩链接的URL为：
      http://a.edu.cn/score.jsp?stuno=2021200XXX
      可尝试替换stuno域为其他同学的学号，查看其他同学的成绩
  - 缓解方法：对于每一个受保护的访问目标，都需要进行用户认证的检查

演示：挤上“魂斗罗”的游戏排行榜



3.3 URL攻击

- 方式2：嗅探关键的参数信息
  - 原理：关键的参数信息以“明文”形式通过URL中进行传播，可以被相同网络接入点内的其它主机截获；若关键信息具有某种简单的特征，即便不在同一个网络环境中，也可以通过暴力破解的方式获得
  - 实例：

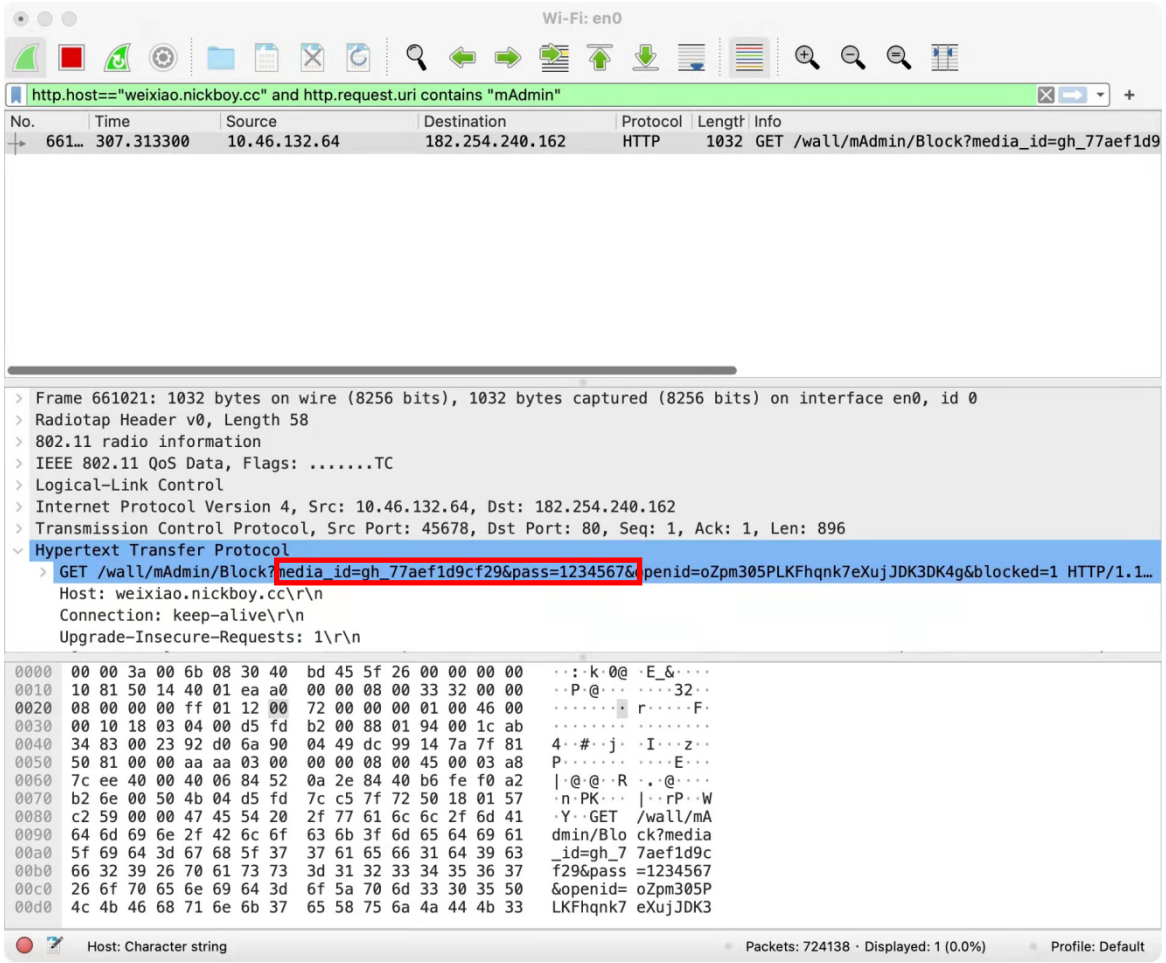
在“UV的匿名测试墙”上禁言用户oZpm305PLKFhqnk7eXujJDK3DK4g：

https://weixiao.nickboy.cc/wall/mAdmin/Block?media_id=gh_77aef1d9cf29&pass=*******&openid=oZpm305PLKFhqnk7eXujJDK3DK4g&blocked=1

  - 缓解：在作为URL参数发送前，对关键信息进行加密，或者引入校验和

演示：获取“UV的匿名测试墙”管理员密码

- 方式1：使用Wireshark监听WiFi网络



演示：获取“UV的匿名测试墙”管理员密码

- 方式2：使用BurpSuite进行密码爆破