



中國人民大學

RENMIN UNIVERSITY OF CHINA

信息学院

SCHOOL OF INFORMATION

新生研讨课
(网络空间的安全攻防)

3. URL安全

授课教师：游伟 副教授

授课时间：周五10:00 – 11:30（立德楼909）

课程主页：<https://www.youwei.site/course/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



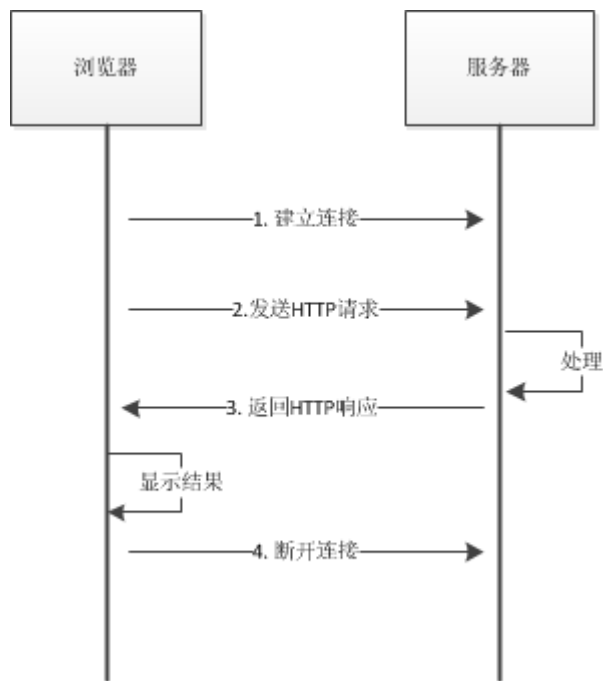


目录

1. HTTP协议与消息
2. URL概述
3. URL攻击

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

- 只要客户端和服务端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



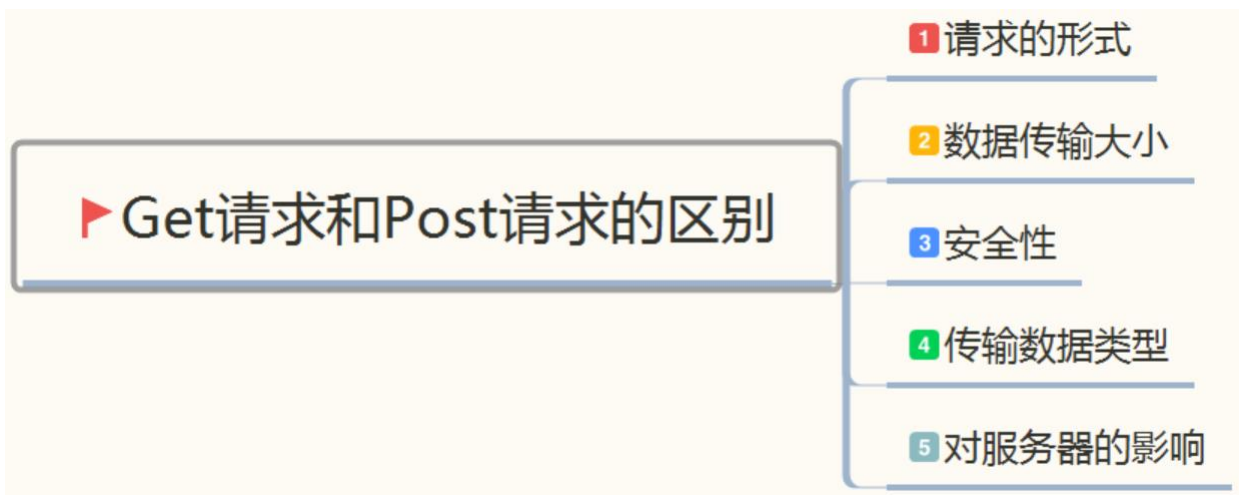
- ① 是请求方法，HTTP/1.1 定义的请求方法有8种。一般常用的是GET和POST。
- ② 为请求对应的URL地址，它和报文头的Host属性组成完整的请求URL
- ③ 是协议名称及版本号。
- ④ 是HTTP的报文头，包含若干个属性，格式为“属性名:属性值”，服务端据此获取客户端信息。
- ⑤ 是报文体，承载请求参数的数据等内容

GET请求与POST请求

■ 概念

- GET：从指定的资源请求数据
- POST：向指定的资源提交要被处理的数据

■ 对比



	GET	POST
后退按钮/刷新	无害	数据会被重新提交（浏览器应该告知用户数据会被重新提交）。
书签	可收藏为书签	不可收藏为书签
缓存	能被缓存	不能缓存
编码类型	application/x-www-form-urlencoded	application/x-www-form-urlencoded or multipart/form-data。为二进制数据使用多重编码。
历史	参数保留在浏览器历史中。	参数不会保存在浏览器历史中。
对数据长度的限制	是的。当发送数据时，GET 方法向 URL 添加数据；URL 的长度是受限制的（URL 的最大长度是 2048 个字符）。	无限制。
对数据类型的限制	只允许 ASCII 字符。	没有限制。也允许二进制数据。
安全性	与 POST 相比，GET 的安全性较差，因为所发送的数据是 URL 的一部分。 在发送密码或其他敏感信息时绝不要使用 GET ！	POST 比 GET 更安全，因为参数不会被保存在浏览器历史或 web 服务器日志中。
可见性	数据在 URL 中对所有人都是可见的。	数据不会显示在 URL 中。
传输效率	在连接建立后会将请求头和请求数据一起发送。	会先将请求头发送给服务器进行确认，然后才真正发送数据。

HTTP响应



404
Page not found

HTTP的响应状态码由5段组成：

- 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”。

- | | |
|---|--|
| 1 | 1xx 消息，一般是告诉客户端，请求已经收到了，正在处理，别急... |
| 2 | 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。 |
| 3 | 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。 |
| 4 | 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。 |
| 5 | 5xx 处理发生错误，责任在服务器端，如服务器端抛出异常，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 Resource 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

Burp Suite Professional v2021.4.3 - game - licensed to google

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options CustomScanner

11 x 12 x 13 x 14 x 15 x 16 x 17 x 18 x 19 x 20 x 21 x ...

Send Cancel < >

Target: https://h.api.4399.com

Request

Pretty Raw In Actions

```
1 POST /mini/ranking/ranking/submit HTTP/1.1
2 Host: h.api.4399.com
3 Cookie: _gprp_c=""; _4399stats_vid=16460141710027294;
  UM_distinctid=
  17f9e1712b57e-085b1213622b498-30634644-332c00-17f9e1712b61ab;
  Hm_lvt_334aca66d28b3b338a76075366b2b9e8=1646014174; phlogact=
  118594; 4399_PCWAP_USER_INFO=37441103677C; Uauth=
  ext|UV|2022228|dev4399.|1646015083088|27d781d65b9bdc2f37ae6322b
  01ac8d0; Pauth=
  3744110367|2441238468|t3ce7m0000271285b3d103d1f7c6f507|16460150
  83|10002|25280f3cd2366b308ef7a50f56525404|0; Puser=2441238468;
  Xauth=1a3235bc77eeb1641c728429e5fb202e; ptusertype=
  dev4399.weixin_login; Prick=UV1988; Qnick=UV;
  4399_HTML5_PREVIEW_USERID=3744110367;
  Hm_lpv1_334aca66d28b3b338a76075366b2b9e8=1646020144; USESSIONID
  =44e2ec51-a3aa-4686-a2a4-1bdde0c21d85; ck_accname=2441238468
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
  Gecko/20100101 Firefox/78.0
5 Accept: application/json, text/plain, */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
9 Device: wap
10 Runtime: production
11 Gameurl:
  http://sda.4399.com/4399swf/upload_swf/ftp37/cwb/20220224/01a/i
  ndex.html
12 Userinfo4399h5:
  3744110367|2441238468|VVYxOTg4||79a9516d7981f220470797c95b9f450
  e
13 Content-Length: 43
14 Origin: http://sda.4399.com
15 Referer:
  http://sda.4399.com/4399swf/upload_swf/ftp37/cwb/20220224/01a/i
  ndex.html
16 Te: trailers
17 Connection: close
18
19 rank_id=483&score=2370000&game_id=100066450
```

Response

Pretty Raw Render In Actions

```
1 HTTP/1.1 200 OK
2 Date: Mon, 28 Feb 2022 05:31:09 GMT
3 Content-Type: application/json
4 Connection: close
5 Server: nginx
6 Access-Control-Allow-Headers: X-Custom-Header,content-type,userI
7 Access-Control-Allow-Origin: http://sda.4399.com
8 Access-Control-Allow-Credentials: true
9 X-Via: 1.1 angton56:18 (Cdn Cache Server V2.0)
10 X-Request-Id: 621c5eld_angton56_32953-23055
11 Content-Length: 58
12
13 {
  "code":1000,
  "msg":"ok",
  "data":{
    "rank":1,
    "score":2370000
  }
}
```

INSPECTOR

Query Parameters (0)

Body Parameters (3)

Request Cookies (17)

Request Headers (16)

Response Headers (10)

Done

490 bytes | 24 millis

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：

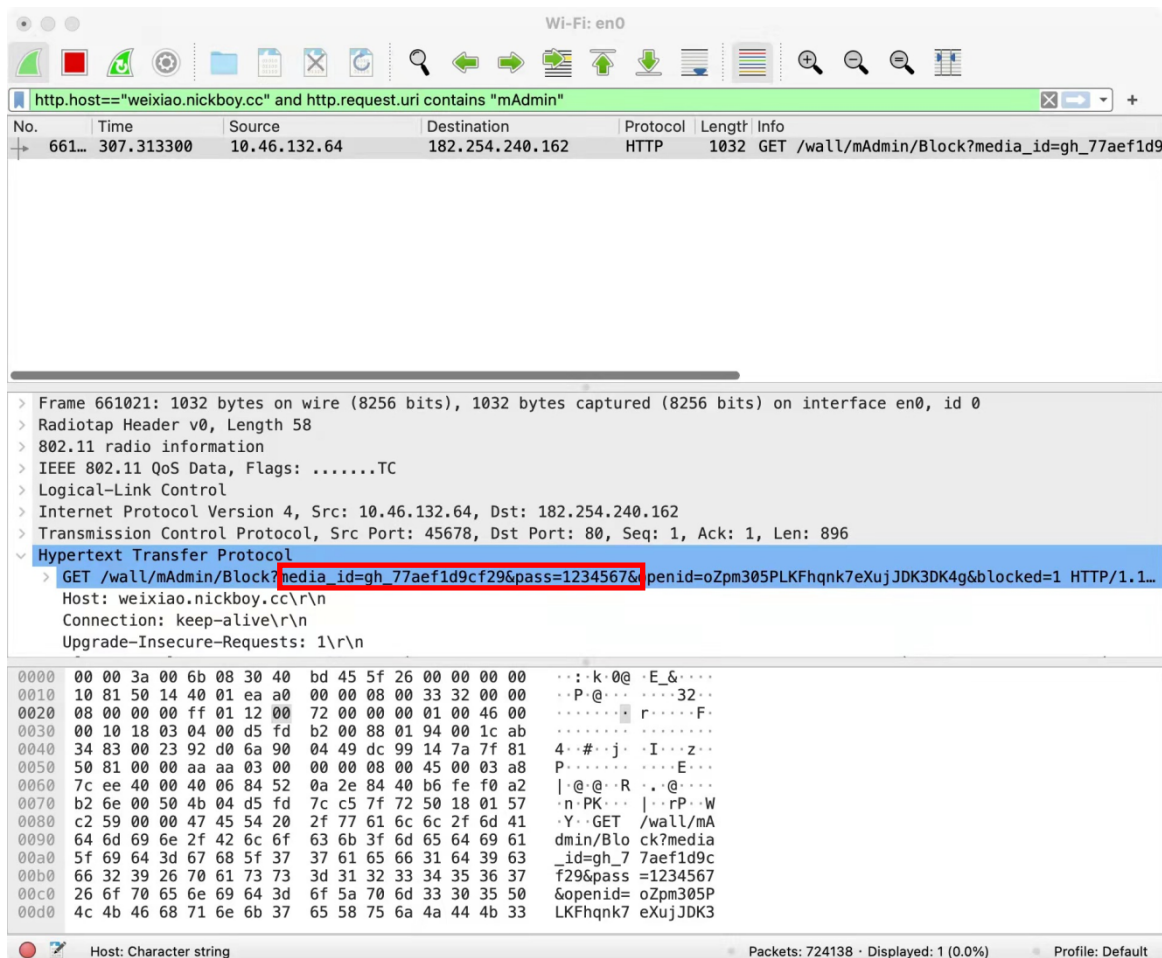
在“UV的匿名测试墙”上禁言用户oZpm[REDACTED]DK3DK4g：

[https://weixiao.nickboy.cc/wall/mAdmin/Block?media_id=gh_77aef1d9cf29
&pass=*****&openid=oZpm\[REDACTED\]DK3DK4g&blocked=1](https://weixiao.nickboy.cc/wall/mAdmin/Block?media_id=gh_77aef1d9cf29&pass=*****&openid=oZpm[REDACTED]DK3DK4g&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

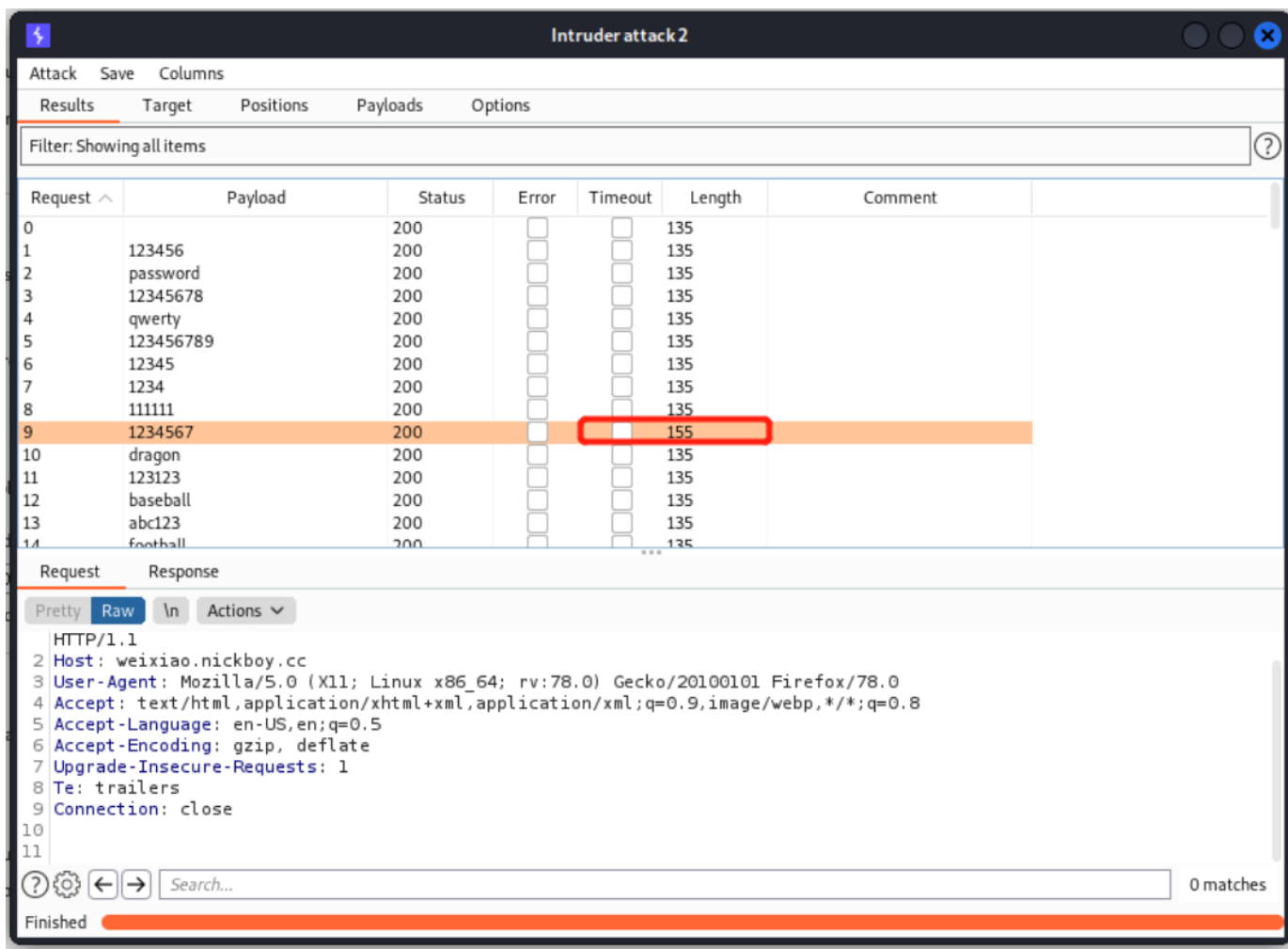
演示：获取 “UV的匿名测试墙” 管理员密码

■ 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



Intruder attack 2

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request ^	Payload	Status	Error	Timeout	Length	Comment
0		200	☐	☐	135	
1	123456	200	☐	☐	135	
2	password	200	☐	☐	135	
3	12345678	200	☐	☐	135	
4	qwerty	200	☐	☐	135	
5	123456789	200	☐	☐	135	
6	12345	200	☐	☐	135	
7	1234	200	☐	☐	135	
8	111111	200	☐	☐	135	
9	1234567	200	☐	☐	155	
10	dragon	200	☐	☐	135	
11	123123	200	☐	☐	135	
12	baseball	200	☐	☐	135	
13	abc123	200	☐	☐	135	
14	football	200	☐	☐	135	

Request Response

Pretty Raw In Actions

```
HTTP/1.1
2 Host: weixiao.nickboy.cc
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Upgrade-Insecure-Requests: 1
8 Te: trailers
9 Connection: close
10
11
```

Search... 0 matches

Finished