ITIS
LEONARDO DA VINCI
Via Toscana, 10 - 43122 PARMA - Tel 0521266511 - Fax 0521266550 - e-mail itis@itis.pr.it - cf.80007330345 - PRTF010006

CORSO DI CYBER SECURITY

Incontro #06 - Mar 3 Dic 24

Prof. Ugolotti 2024-2025

Obiettivi del corso:

OLIMPIADI ITALIANE DI CYBERSICUREZZA

CYBER CHALLENGE.IT

Selezione scolastica
18/01/2025

Preselezione
? Febbraio 2024

Non dimenticate il primo obiettivo....

https://olicyber.it/materiale

La Selezione scolastica (18 Gen 2025)

- networking
- Indirizzamento IPv4
- Funzioni ricorsive
- Operatori bitwise
- Calcolo combinatorio
- Probabilità
- Logica

World Wide Web

- Il web è basato su una architettura client-server
- Ogni utente usa un client per accedere a una *risorsa* su un server attraverso la rete
  - Il client web è chiamato browser web
  - Il server è chiamato server web

URLs

- Ogni risorsa nel web è identificata da un indirizzo, chiamato URL[1]
- Un URL è composto da varie parti, ognuna delle quali ha un preciso scopo

`https://www.example.com/index.html`

1: Uniform Resource Locator

Protocollo HTTP

- Client e server scambiano informazioni usando un protocollo, chiamato HTTP
- La comunicazione viene sempre avviata dal client, che manderà richieste a un server
- Il server interpreta queste richieste e risponde al client

Protocollo HTTP

Web 09 - HTTP: una richiesta POST con body JSON

Web 02 - HTTP: richiesta GET con query string

CAPTURE THE FLAG

No.	Time	Source	Destination	Protocol	Length	Info
273	11.662539	192.168.1.4	cs837.wac.edgecastc…	TCP	66	24912 → http(80) [SYN] Seq=0 Win=64240 Len=0 MS…
276	11.671502	cs837.wac.edg…	192.168.1.4	TCP	66	http(80) → 24912 [SYN, ACK] Seq=0 Ack=1 Win=655…
277	11.672623	192.168.1.4	cs837.wac.edgecastc…	TCP	54	24912 → http(80) [ACK] Seq=1 Ack=1 Win=262656 L…
278	11.674596	192.168.1.4	cs837.wac.edgecastc…	HTTP	470	GET /action_page.php?fname=prof&lname=ugo HTTP/1…
281	11.786467	cs837.wac.edg…	192.168.1.4	TCP	60	http(80) → 24912 [ACK] Seq=1 Ack=417 Win=67072 …
282	12.080241	cs837.wac.edg…	192.168.1.4	HTTP	403	HTTP/1.1 301 Moved Permanently (text/html)
283	12.125810	192.168.1.4	cs837.wac.edgecastc…	TCP	54	24912 → http(80) [ACK] Seq=417 Ack=350 Win=2624…
697	22.094786	192.168.1.4	cs837.wac.edgecastc…	TCP	55	[TCP Keep-Alive] 24912 → http(80) [ACK] Seq=416…
698	22.103716	cs837.wac.edg…	192.168.1.4	TCP	66	[TCP Keep-Alive ACK] http(80) → 24912 [ACK] Seq…

```
0000  d0 50 99 40 5e 6a d4 5d  64 0c 25 40 08 00 45 00   ·P·@^j·] d·%@··E·
0010  01 85 ec de 00 00 3b 06  89 25 c0 e5 85 dd c0 a8   ·····;·· ·%····
0020  01 04 00 50 61 50 83 16  3e 4e be 12 31 d0 50 18   ···PaP·· >N··1·P·
0030  00 83 ad e5 00 00 48 54  54 50 2f 31 2e 31 20 33   ·····HT TP/1.1 3
0040  30 31 20 4d 6f 76 65 64  20 50 65 72 6d 61 6e 65   01 Moved  Permane
0050  6e 74 6c 79 0d 0a 43 6f  6e 74 65 6e 74 2d 54 79   ntly··Co ntent-Ty
0060  70 65 3a 20 74 65 78 74  2f 68 74 6d 6c 0d 0a 44   pe: text /html··D
0070  61 74 65 3a 20 4d 6f 6e  2c 20 30 34 20 44 65 63   ate: Mon , 04 Dec
0080  20 32 30 32 33 20 32 30  3a 30 37 3a 31 30 20 47    2023 20 :07:10 G
0090  4d 54 0d 0a 4c 6f 63 61  74 69 6f 6e 3a 20 68 74   MT··Loca tion: ht
00a0  74 70 73 3a 2f 2f 77 77  77 2e 77 33 73 63 68 6f   tps://ww w.w3scho
00b0  6f 6c 73 2e 63 6f 6d 3a  34 34 33 2f 61 63 74 69   ols.com: 443/acti
00c0  6f 6e 5f 70 61 67 65 2e  70 68 70 3f 66 6e 61 6d   on_page. php?fnam
00d0  65 3d 70 72 6f 66 26 6c  6e 61 6d 65 3d 75 67 6f   e=prof&l name=ugo
00e0  0d 0a 53 65 72 76 65 72  3a 20 61 77 73 65 6c 62   ··Server : awselb
00f0  2f 32 2e 30 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   /2.0··Co ntent-Le
0100  6e 67 74 68 3a 20 31 33  34 0d 0a 0d 0a 3c 68 74   ngth: 13 4····<ht
0110  6d 6c 3e 0d 0a 3c 68 65  61 64 3e 3c 74 69 74 6c   ml>··<he ad><titl
```

```
> Frame 282: 403 bytes on wire (3224 bits), 403 bytes captured (3224 bits) on interface \Device\NPF_{D8AF3E44-12BE-49B4-90
> Ethernet II, Src: ASUSTekC_0c:25:40 (d4:5d:64:0c:25:40), Dst: ASRockIn_40:5e:6a (d0:50:99:40:5e:6a)
> Internet Protocol Version 4, Src: cs837.wac.edgecastcdn.net (192.229.133.221), Dst: 192.168.1.4 (192.168.1.4)
> Transmission Control Protocol, Src Port: http (80), Dst Port: 24912 (24912), Seq: 1, Ack: 417, Len: 349
v Hypertext Transfer Protocol
  v HTTP/1.1 301 Moved Permanently\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 301 Moved Permanently\r\n]
      Response Version: HTTP/1.1
      Status Code: 301
      [Status Code Description: Moved Permanently]
      Response Phrase: Moved Permanently
    Content-Type: text/html\r\n
    Date: Mon, 04 Dec 2023 20:07:10 GMT\r\n
    Location: https://www.w3schools.com:443/action_page.php?fname=prof&lname=ugo\r\n
    Server: awselb/2.0\r\n
  > Content-Length: 134\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.405645000 seconds]
    [Request in frame: 278]
    [Request URI: http://www.w3schools.com/action_page.php?fname=prof&lname=ugo]
    File Data: 134 bytes
> Line-based text data: text/html (6 lines)
```

wireshark_Ethernet_20231204210658_a12080.pcapng

Wireshark · Segui flusso HTTP (tcp.stream eq 13) · Ethernet

```
GET /action_page.php?fname=prof&lname=ugo HTTP/1.1
Host: www.w3schools.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/
*;q=0.8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

http request

```
HTTP/1.1 301 Moved Permanently
Content-Type: text/html
Date: Mon, 04 Dec 2023 20:07:10 GMT
Location: https://www.w3schools.com:443/action_page.php?fname=prof&lname=ugo
Server: awselb/2.0
Content-Length: 134

<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
</body>
</html>
```

http response

Protocollo HTTP : METHODS

HTML

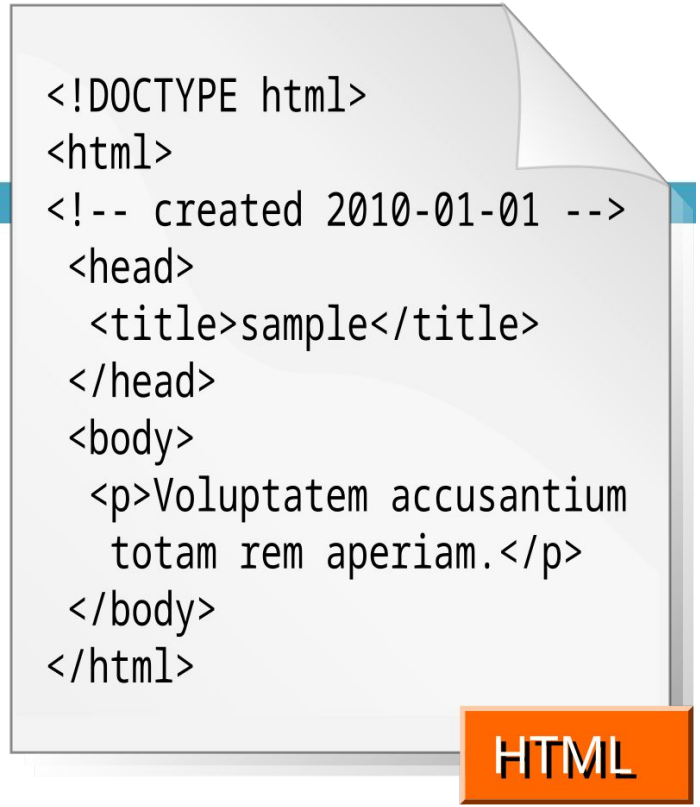
Pagine WEB includono:

- codice HTML
- codice CSS
- codice JS

Inoltre possono includere altre risorse, quali file:

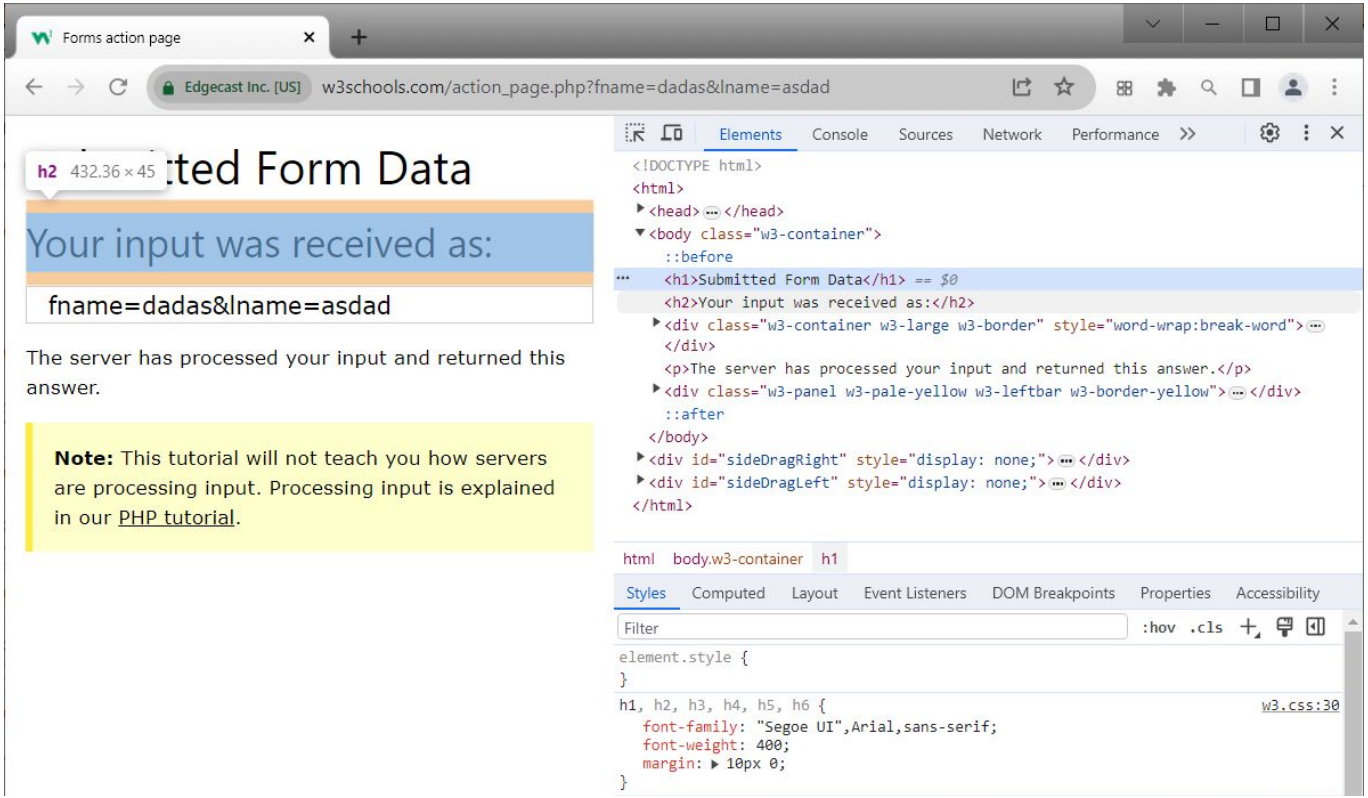
- Immagini / Video / Audio
- Fogli di stile
- Script

...tipicamente individuate e scaricate mediante richieste http concorrenti.



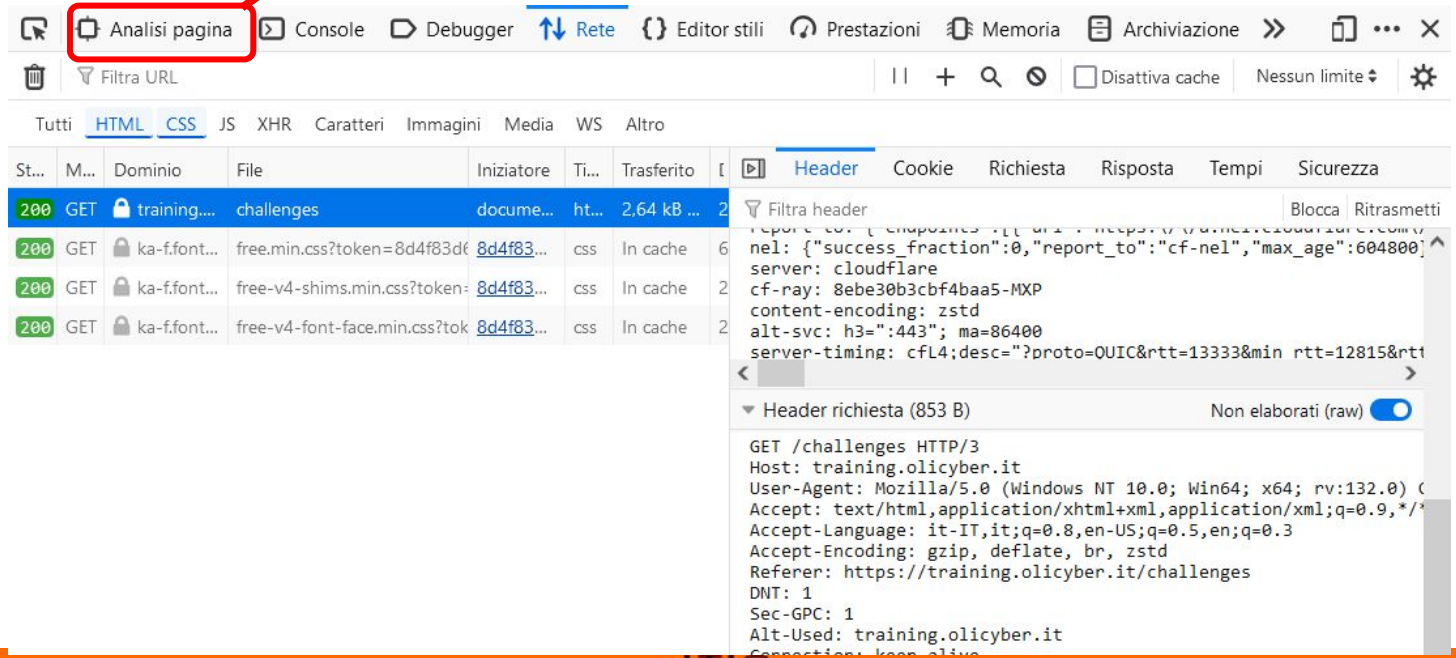
Browser

Mette a disposizioni gli strumenti per lo sviluppo (**F12**)



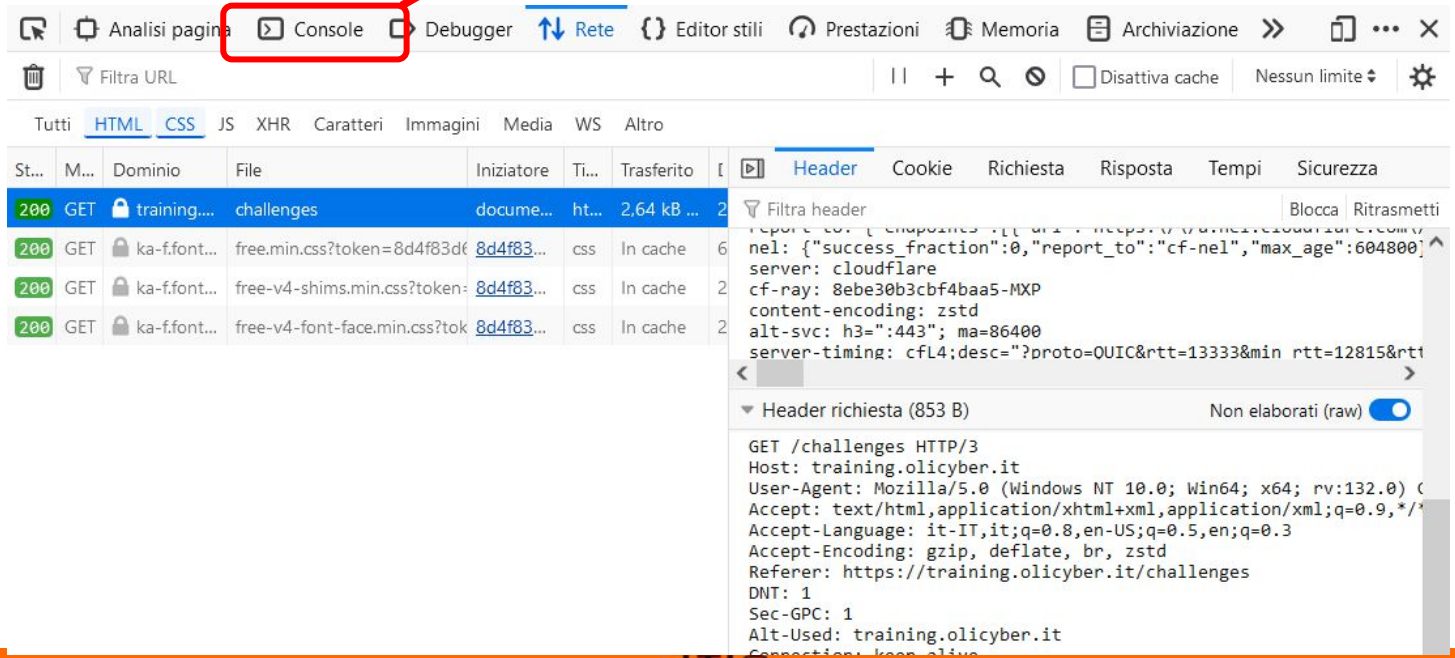
Browser

X Interagire con l'HTML



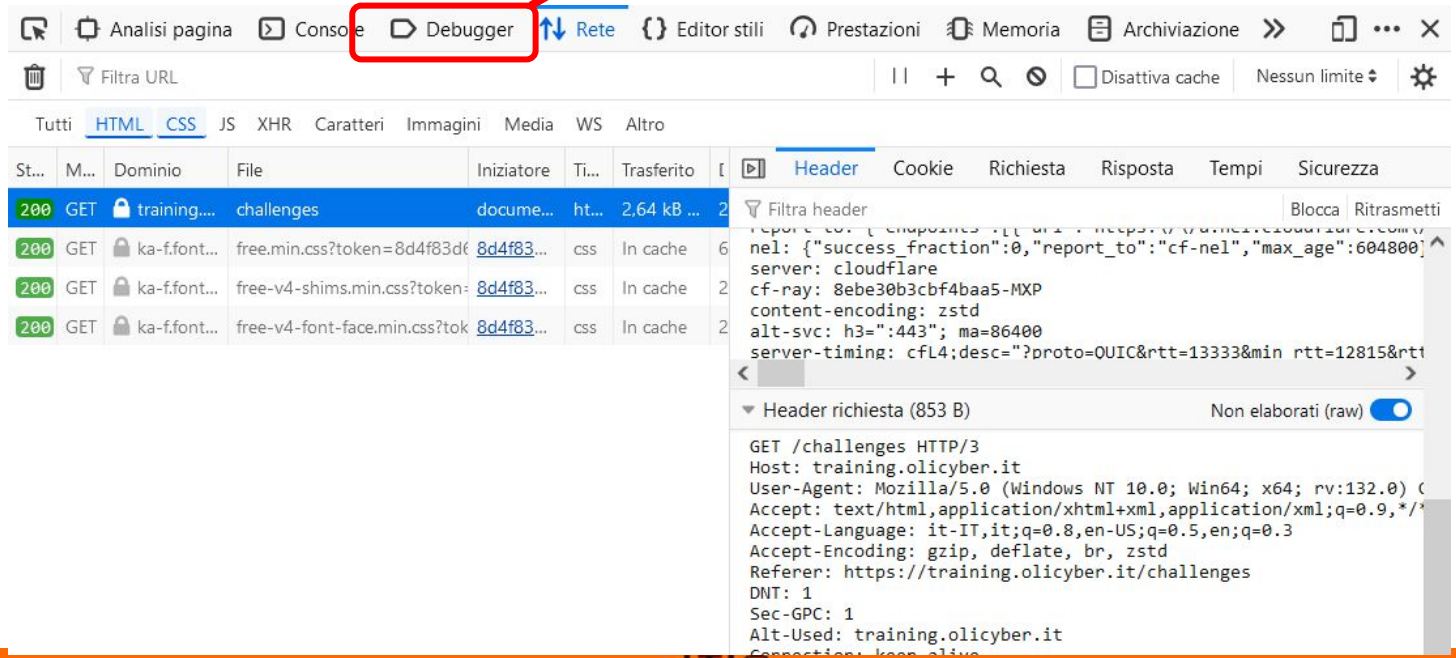
Browser

x Interagire con il JS



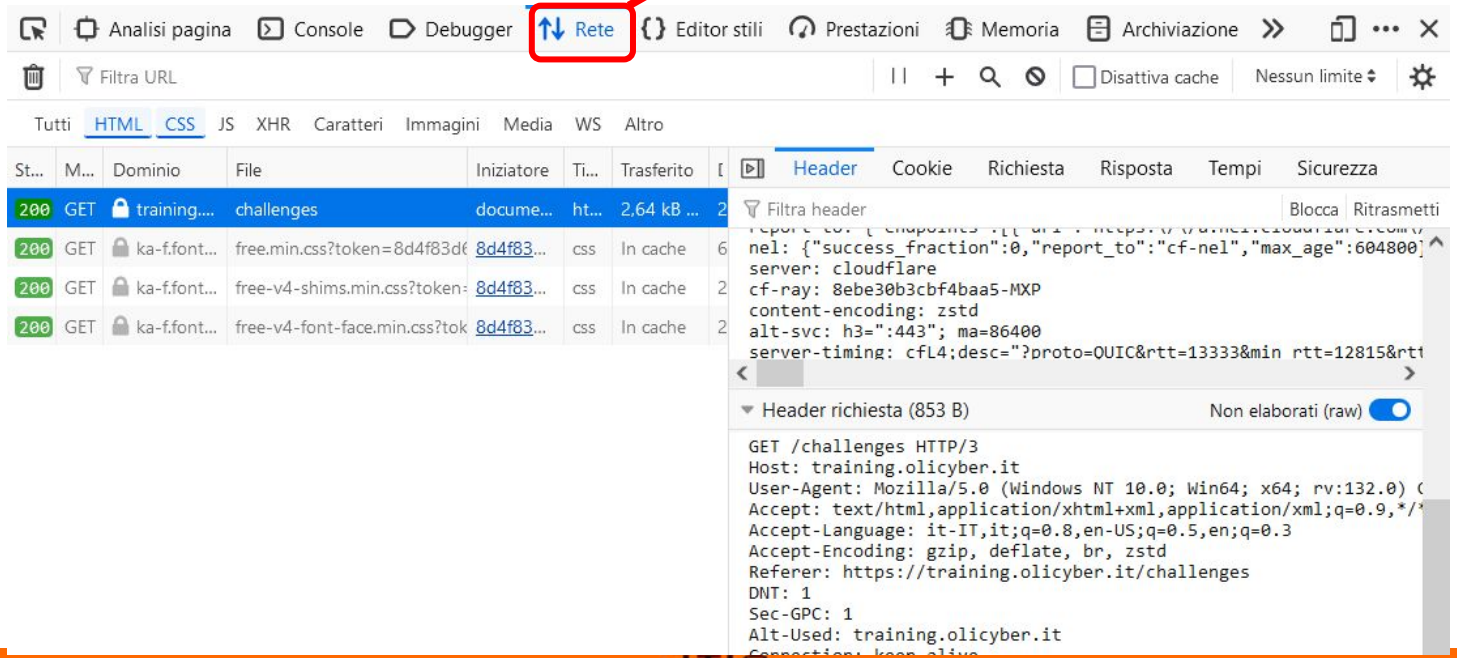
Browser

x analisi passo passo del JS



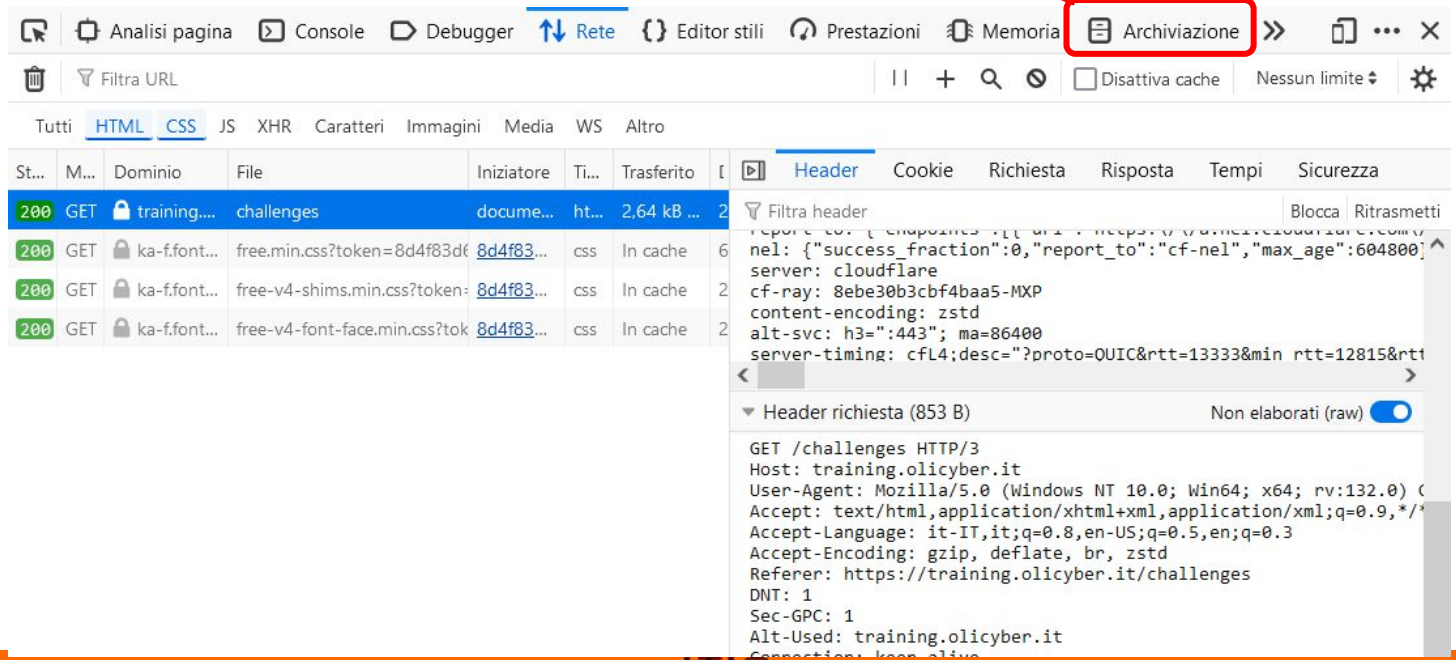
Browser

x analisi dei pacchetti HTTP



Browser

x analisi dei dati che la pagina salva nella nostra Memoria



curl://

Curl by example: Interactive guide

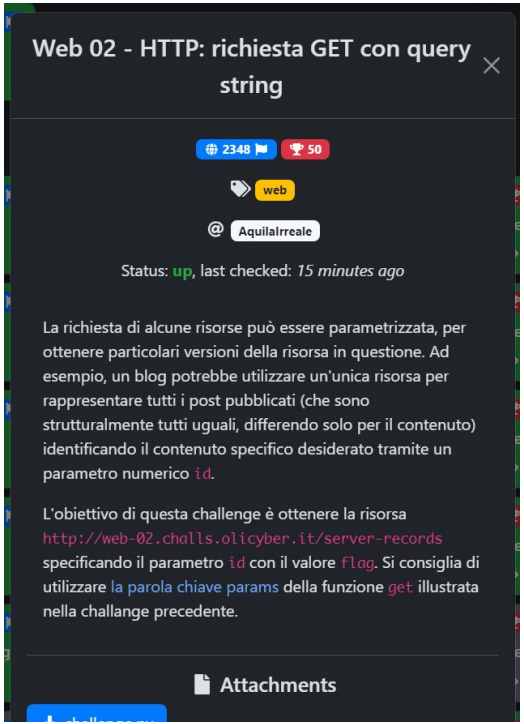
All one command line

```
curl -X POST
-d "Body=Hi there, this is a test message from cURL"
-d "From=$TWILIO_NUMBER"
-d "To=$TO_NUMBER"
"https://api.twilio.com/2010-04-01/Accounts/$TWILIO_ACCOUNT_SID/Messages"
-u "$TWILIO_ACCOUNT_SID:$TWILIO_AUTH_TOKEN"
```

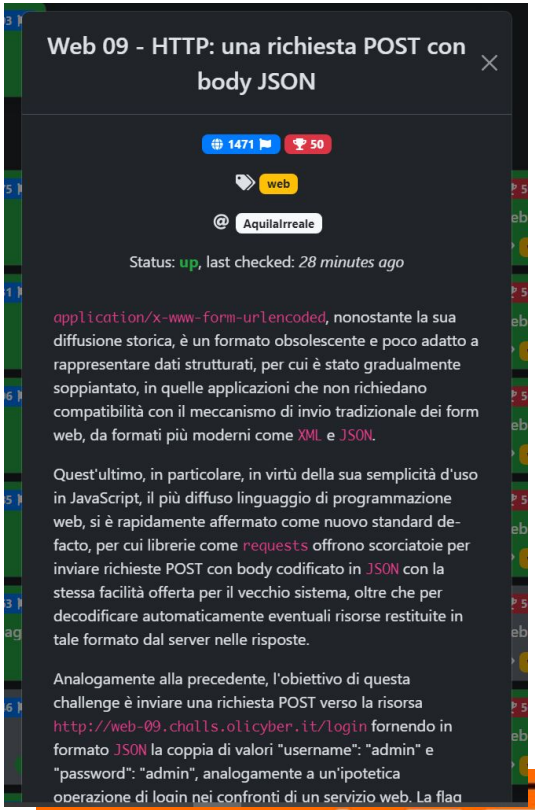
- The first section in the line is the method
- The second section is the data required for a request to the endpoint
- The third section is the url
- The fourth section is for authentication, like a username and password

CAPTURE THE FLAG

Challenge: Web 02



Challenge: Web 09 - HTTP: POST con body JSON



Web 09 - HTTP: una richiesta POST con body JSON

1471 50

web

AquilaIrreale

Status: up, last checked: *28 minutes ago*

application/x-www-form-urlencoded, nonostante la sua diffusione storica, è un formato obsolescente e poco adatto a rappresentare dati strutturati, per cui è stato gradualmente soppiantato, in quelle applicazioni che non richiedano compatibilità con il meccanismo di invio tradizionale dei form web, da formati più moderni come XML e JSON.

Quest'ultimo, in particolare, in virtù della sua semplicità d'uso in JavaScript, il più diffuso linguaggio di programmazione web, si è rapidamente affermato come nuovo standard de-facto, per cui librerie come requests offrono scorciatoie per inviare richieste POST con body codificato in JSON con la stessa facilità offerta per il vecchio sistema, oltre che per decodificare automaticamente eventuali risorse restituite in tale formato dal server nelle risposte.

Analogamente alla precedente, l'obiettivo di questa challenge è inviare una richiesta POST verso la risorsa http://web-09.challs.olicyber.it/login fornendo in formato JSON la coppia di valori "username": "admin" e "password": "admin", analogamente a un'ipotetica operazione di login nei confronti di un servizio web. La flag

```
user@ubuntu:~$ curl -H 'Content-Type: application/json' -d '{"username":"admin", "password":"admin"}' -X POST http://web-09.challs.olicyber.it/login
{
  "token": "flag{[redacted]}"
}user@ubuntu:~$
```

curl -H 'Content-Type: application/json' -d '{"username":"admin", "password":"admin"}' -X POST http://web-09.challs.olicyber.it/login