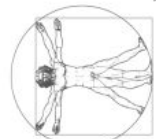




ITIS
LEONARDO DA VINCI

Via Toscana, 10 - 43122 PARMA - Tel 0521266511 - Fax 0521266550 - e-mail itis@itis.prit.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



The screenshot shows the Olicyber website interface. At the top, there is a navigation bar with the Olicyber logo (a white horse head on a blue background) and the text 'OLICYBER' and 'SISTEMI INFORMATICA E CYBERSECURITY'. To the right of the logo are buttons for 'REGISTRATI' and 'ACCEDI'. Below the navigation bar, the main content area features a red icon of a school building and the heading 'Materiale didattico'. Underneath, a paragraph states: 'In questa pagina trovi puntatori e riferimenti a tutto il materiale didattico disponibile dalle precedenti edizioni del progetto che puoi usare per prepararti alla nuova edizione.' There are two main columns of content. The left column is titled 'Lezioni teoriche' and contains a list of video lessons: 'Lezione di Network Security', 'Lezione di Web Security 1', 'Lezione di Web Security 2', 'Lezione di Cryptography 1', 'Lezione di Cryptography 2', 'Lezione di Software Security 1', 'Lezione di Software Security 2', and 'Lezioni dai Training Camp'. The right column is titled 'Selezione scolastica' and contains a list of selection years: 'Selezione scolastica 2021', 'Selezione scolastica 2022', and 'Selezione scolastica 2023'. Below this list, there is a section for 'Soluzioni commentate' with three entries: 'Soluzioni commentate selezione scolastica 2021', 'Soluzioni commentate selezione scolastica 2022', and 'Soluzioni commentate selezione scolastica 2023'. At the bottom of the page, there are two more sections: 'Selezione territoriale' and 'Competizione nazionale', each with a brief description of the respective activity.

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

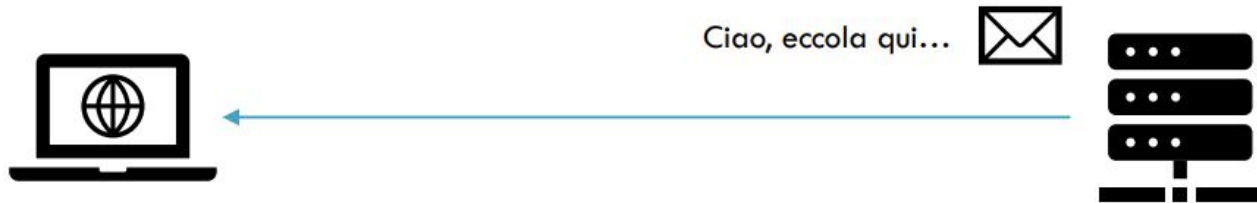
- Ogni risorsa nel web è identificata da un indirizzo, chiamato URL¹
- Un URL è composto da varie parti, ognuna delle quali ha un preciso scopo

`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



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...	0000 d0 50 99 40 5e 6a d4 5d 64 0c 25 40 08 00 45 00
276	11.671502	cs837.wac.edg...	192.168.1.4	TCP	66	http(80) → 24912 [SYN, ACK] Seq=0 Ack=1 Win=655...	0010 01 85 ec de 00 00 3b 06 89 25 c0 e5 85 dd c0 a8
277	11.672623	192.168.1.4	cs837.wac.edgecastc...	TCP	54	24912 → http(80) [ACK] Seq=1 Ack=1 Win=262656 L...	0020 01 04 00 50 61 50 83 16 3e 4e 1b 12 31 d0 50 18
278	11.674596	192.168.1.4	cs837.wac.edgecastc...	HTTP	470	GET /action_page.php?fname=prof&lname=ugo HTTP/1.1	0030 00 83 ad e5 00 00 48 54 54 50 2f 31 2e 31 20 33
281	11.786467	cs837.wac.edg...	192.168.1.4	TCP	60	http(80) → 24912 [ACK] Seq=1 Ack=417 Win=67072 ...	0040 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65
282	12.080241	cs837.wac.edg...	192.168.1.4	HTTP	403	HTTP/1.1 301 Moved Permanently (text/html)	0050 6e 74 6c 79 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79
283	12.125810	192.168.1.4	cs837.wac.edgecastc...	TCP	54	24912 → http(80) [ACK] Seq=417 Ack=350 Win=2624...	0060 70 65 3a 20 4d 6f 76 65 78 74 2f 68 74 6d 6c 0a 44
697	22.094786	192.168.1.4	cs837.wac.edgecastc...	TCP	55	[TCP Keep-Alive] 24912 → http(80) [ACK] Seq=416...	0070 61 74 65 3a 20 4d 6f 6e 2c 20 30 34 20 44 65 63
698	22.103716	cs837.wac.edg...	192.168.1.4	TCP	66	[TCP Keep-Alive ACK] http(80) → 24912 [ACK] Seq...	0080 20 32 30 32 33 20 32 30 3a 30 37 3a 31 30 20 47

> Frame 282: 403 bytes on wire (3224 bits), 403 bytes captured (3224 bits) on interface \Device\NPF_{D8AF3E44-12BE-4984-90...
> Ethernet II, Src: ASUSTek_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

Hypertext Transfer Protocol

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: awselsb/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 · 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: awselsb/2.0
Content-Length: 134

http response

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

Protocollo HTTP : METHODS

Web 10 - HTTP: il
metodo OPTIONS



SAFE METHODS	{	GET	HTTP/1.1 MUST IMPLEMENT THIS METHOD
NO ACTION ON SERVER		HEAD	INSPECT RESOURCE HEADERS
MESSAGE WITH	{	PUT	DEPOSIT DATA ON SERVER — INVERSE OF GET
BODY		POST	SEND INPUT DATA FOR PROCESSING
SEND DATA TO SERVER		PATCH	PARTIALLY MODIFY A RESOURCE
		TRACE	ECHO BACK RECEIVED MESSAGE
		OPTIONS	SERVER CAPABILITIES
		DELETE	DELETE A RESOURCE — NOT GUARANTEED

HTML

Pagine WEB includono:

- codice HTML
- codice CSS
- codice JS

Inoltre possono includere altre risorse, quali file:

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

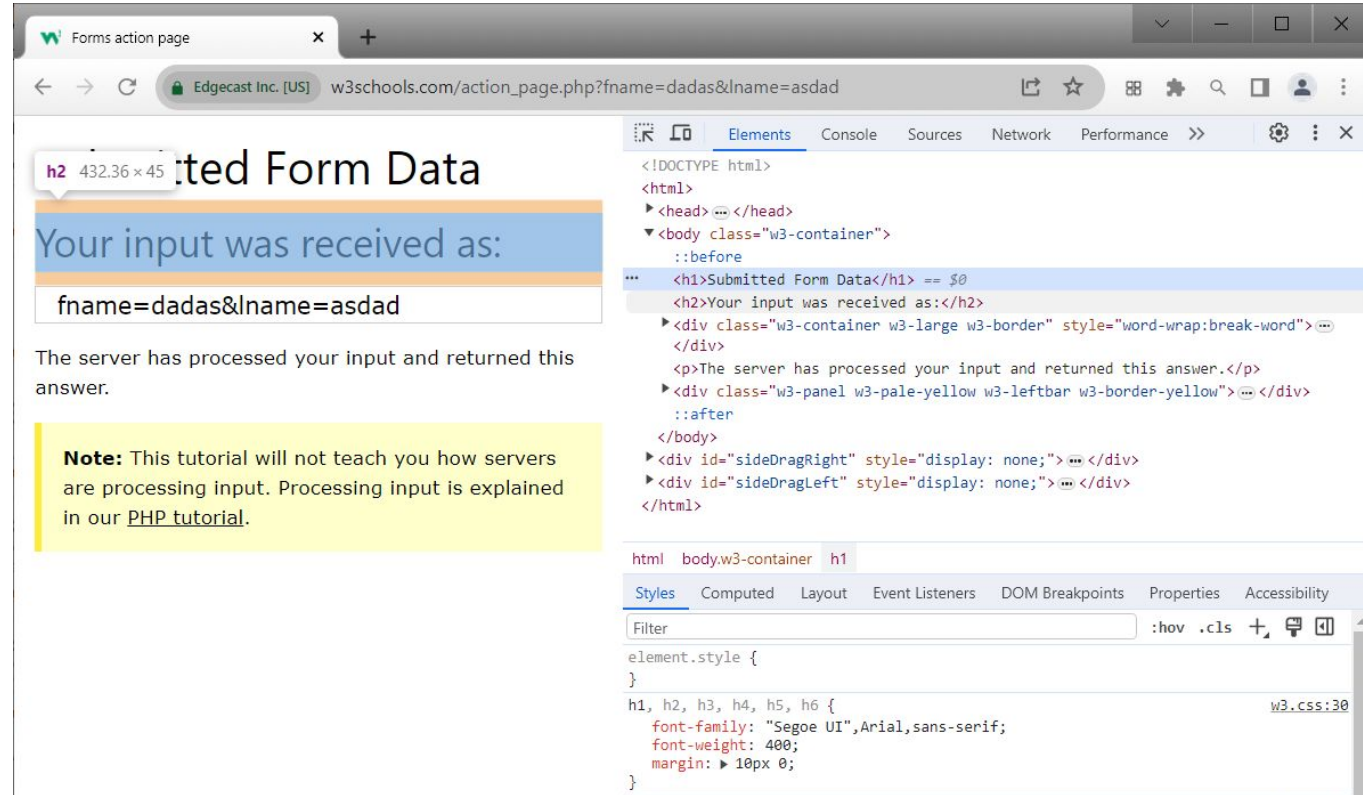
...tipicamente individuate e scaricate mediante richieste http concorrenti.

```
<!DOCTYPE html>
<html>
<!-- created 2010-01-01 -->
<head>
  <title>sample</title>
</head>
<body>
  <p>Voluptatem accusantium
  totam rem aperiam.</p>
</body>
</html>
```

HTML

Browser

Mette a disposizione gli strumenti per lo sviluppo (F12)



The screenshot shows a web browser window with the address bar displaying "w3schools.com/action_page.php?fname=dadas&lname=asadad". The page content includes a heading "Submitted Form Data", a message "Your input was received as:", and a form input containing "fname=dadas&lname=asadad". Below this, a note states: "Note: This tutorial will not teach you how servers are processing input. Processing input is explained in our [PHP tutorial](#)."

The browser's developer tools are open, showing the "Elements" panel with the following HTML structure:

```
<!DOCTYPE html>
<html>
  <head>
  </head>
  <body class="w3-container">
    ::before
    ...
    <h1>Submitted Form Data</h1> == $0
    <h2>Your input was received as:</h2>
    <div class="w3-container w3-large w3-border" style="word-wrap:break-word">
    </div>
    <p>The server has processed your input and returned this answer.</p>
    <div class="w3-panel w3-pale-yellow w3-leftbar w3-border-yellow"></div>
    ::after
  </body>
  <div id="sideDragRight" style="display: none;">
  <div id="sideDragLeft" style="display: none;">
  </html>
```

The "Styles" panel shows the default styles for h1, h2, h3, h4, h5, and h6:

```
h1, h2, h3, h4, h5, h6 {
  font-family: "Segoe UI",Arial,sans-serif;
  font-weight: 400;
  margin: 10px 0;
}
```

Browser

X Interagire con l'HTML

The screenshot shows the browser's developer tools interface. The 'Analisi pagina' button is highlighted with a red box, and a red arrow points from it to the text 'X Interagire con l'HTML'. The Network tab is active, displaying a list of requests. The first request is selected, and the 'Header' panel is open, showing the request headers for the selected request.

St...	M...	Dominio	File	Iniziatore	Ti...	Trasferito	I	Header	Cookie	Richiesta	Risposta	Tempi	Sicurezza
200	GET	training...	challenges	docume...	ht...	2.64 kB	...						
200	GET	ka-f.font...	free.min.css?token=8d4f83d...	8d4f83...	css	In cache	6						
200	GET	ka-f.font...	free-v4-shims.min.css?token:...	8d4f83...	css	In cache	2						
200	GET	ka-f.font...	free-v4-font-face.min.css?tok...	8d4f83...	css	In cache	2						

```
GET /challenges HTTP/3
Host: training.olicyber.it
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) (...)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br, zstd
Referer: https://training.olicyber.it/challenges
DNT: 1
Sec-GPC: 1
Alt-Used: training.olicyber.it
Connection: keep-alive
```

Browser

x Interagire con il JS

The screenshot shows the browser's developer tools. The 'Console' tab is highlighted with a red box, and a red arrow points from it to the text 'x Interagire con il JS'. The network tab is open, showing a list of requests. The first request is a GET to training.olicyber.it/challenges with a 200 status. The request headers are expanded, showing the following information:

```
GET /challenges HTTP/3
Host: training.olicyber.it
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br, zstd
Referer: https://training.olicyber.it/challenges
DNT: 1
Sec-GPC: 1
Alt-Used: training.olicyber.it
```


Browser

x analisi passo passo del JS

The image shows a browser's developer tools interface. The 'Debugger' tab is highlighted with a red box and a red arrow pointing to the text 'x analisi passo passo del JS'. The 'Header' panel is open, showing the request headers for a GET request to /challenges. The headers include Host, User-Agent, Accept, Accept-Language, Accept-Encoding, Referer, DNT, Sec-GPC, and Alt-Used.

St...	M...	Dominio	File	Iniziatore	Ti...	Trasferito	I	Header	Cookie	Richiesta	Risposta	Tempi	Sicurezza	
200	GET	training...	challenges	docume...	ht...	2.64 kB	...	2						
200	GET	ka-f.font...	free.min.css?token=8d4f83d6	8d4f83...	css	In cache	6							
200	GET	ka-f.font...	free-v4-shims.min.css?token=	8d4f83...	css	In cache	2							
200	GET	ka-f.font...	free-v4-font-face.min.css?tok	8d4f83...	css	In cache	2							

```
GET /challenges HTTP/3
Host: training.olicyber.it
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) (...)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br, zstd
Referer: https://training.olicyber.it/challenges
DNT: 1
Sec-GPC: 1
Alt-Used: training.olicyber.it
Connection: keep-alive
```

Browser

x analisi dei pacchetti HTTP

Analisi pagina Console Debugger **Rete** Editor stili Prestazioni Memoria Archiviazione

Filtra URL

Tutti **HTML** CSS JS XHR Caratteri Immagini Media WS Altro

St...	M...	Dominio	File	Inziatore	Ti...	Trasferito	I	Header	Cookie	Richiesta	Risposta	Tempi	Sicurezza
200	GET	training...	challenges	docume...	ht...	2,64 kB ...	2						
200	GET	ka-f.font...	free.min.css?token=8d4f83df...	8d4f83...	css	In cache	6						
200	GET	ka-f.font...	free-v4-shims.min.css?token=...	8d4f83...	css	In cache	2						
200	GET	ka-f.font...	free-v4-font-face.min.css?tok...	8d4f83...	css	In cache	2						

Header

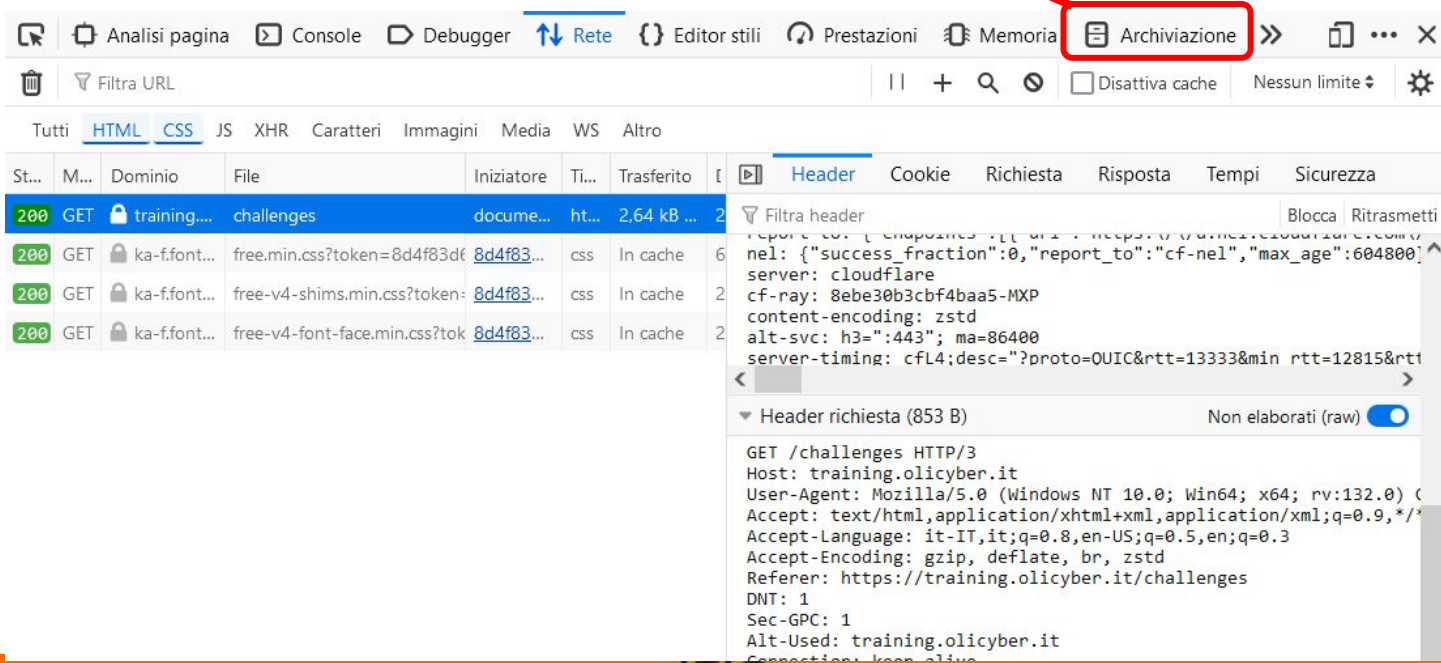
Filtra header

Header richiesta (853 B) Non elaborati (raw)

```
GET /challenges HTTP/3
Host: training.olicyber.it
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br, zstd
Referer: https://training.olicyber.it/challenges
DNT: 1
Sec-GPC: 1
Alt-Used: training.olicyber.it
```

Browser

x analisi dei dati che la pagina
salva nella nostra Memoria



The screenshot shows the browser's developer tools interface. The 'Rete' (Network) tab is active, displaying a list of requests. The first request, 'challenges', is selected. The 'Header' sub-tab is open, showing the request headers for the selected request. A red box highlights the 'Archiviazione' (Cache) icon in the top toolbar, and a red arrow points from the text above to it.

St...	M...	Domínio	File	Iniziatore	Ti...	Trasferito	I	Header	Cookie	Richiesta	Risposta	Tempi	Sicurezza
200	GET	training...	challenges	docume...	ht...	2.64 kB	...	Filter header					
200	GET	ka-f.font...	free.min.css?token=8d4f83d6	8d4f83...	css	In cache	6						
200	GET	ka-f.font...	free-v4-shims.min.css?token=	8d4f83...	css	In cache	2						
200	GET	ka-f.font...	free-v4-font-face.min.css?tok	8d4f83...	css	In cache	2						

```
GET /challenges HTTP/3
Host: training.olicyber.it
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br, zstd
Referer: https://training.olicyber.it/challenges
DNT: 1
Sec-GPC: 1
Alt-Used: training.olicyber.it
Connection: keep-alive
```

LEONARDO DA VINCI



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

Challenge: Web 02

Web 02 - HTTP: richiesta GET con query string

2348 50

web

@ Aquilalreale

Status: **up**, last checked: 15 minutes ago

La richiesta di alcune risorse può essere parametrizzata, per ottenere particolari versioni della risorsa in questione. Ad esempio, un blog potrebbe utilizzare un'unica risorsa per rappresentare tutti i post pubblicati (che sono strutturalmente tutti uguali, differendo solo per il contenuto) identificando il contenuto specifico desiderato tramite un parametro numerico *id*.

L'obiettivo di questa challenge è ottenere la risorsa <http://web-02.challs.olicyber.it/server-records> specificando il parametro *id* con il valore *flag*. Si consiglia di utilizzare la parola chiave *params* della funzione *get* illustrata nella challenge precedente.

Attachments

```
C:\> Prompt dei comandi
C:\> curl "http://web-02.challs.olicyber.it/server-records?id=flag"
flag{[REDACTED]}
C:\>
```


ITIS

LEONARDO DA VINCI