



ITIS  
**LEONARDO DA VINCI**

Via Toscana, 10 - 43122 PARMA - Tel 0521266511 - Fax 0521266550 - e-mail [itis@itis.prit.it](mailto:itis@itis.prit.it) - cf.80007330345 - PRIF010006



# CORSO DI **CYBER SECURITY**

Incontro #07 - Mer 17 DIC 24

Prof. Ugolotti 2024-2025

# Obiettivi del corso:



OLIMPIADI  
ITALIANE DI  
CYBERSICUREZZA



CYBER  
CHALLENGE.IT

**Selezione scolastica**  
**18/01/2025**



**Preselezione**  
**25/28 Gennaio 2025**

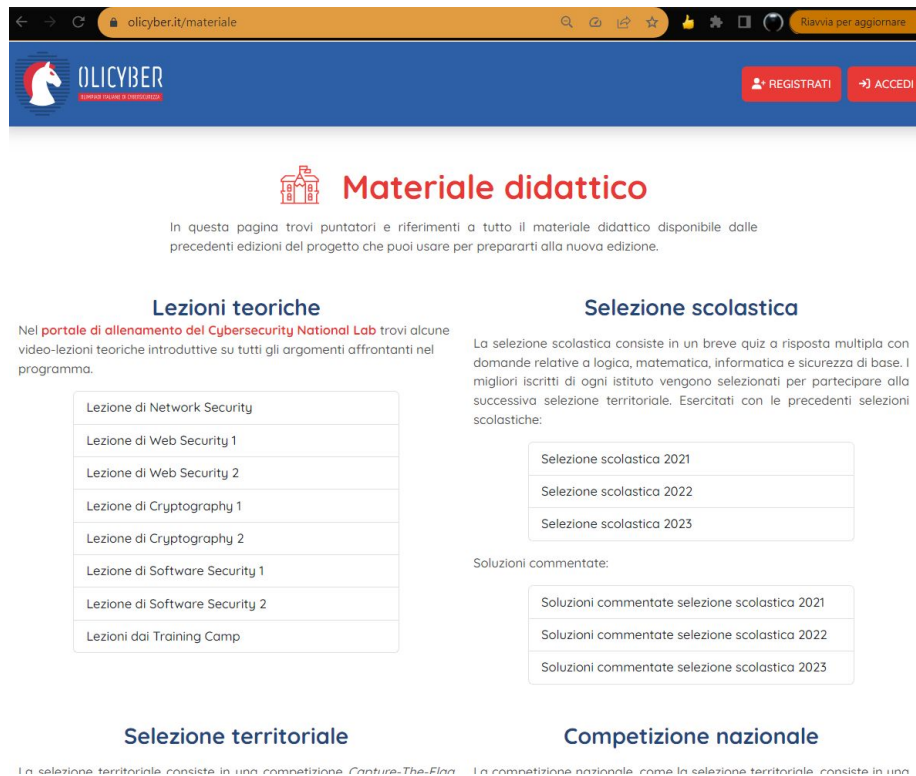


# Non dimenticate il primo obiettivo...

<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 includes a sub-heading 'Nel portale di allenamento del Cybersecurity National Lab trovi alcune video-lezioni teoriche introduttive su tutti gli argomenti affrontanti nel programma.' Below this is a table listing various 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 includes a sub-heading 'La selezione scolastica consiste in un breve quiz a risposta multipla con domande relative a logica, matematica, informatica e sicurezza di base. I migliori iscritti di ogni istituto vengono selezionati per partecipare alla successiva selezione territoriale. Esercitati con le precedenti selezioni scolastiche:'. Below this is a table listing 'Selezione scolastica 2021', 'Selezione scolastica 2022', and 'Selezione scolastica 2023'. Underneath that table is the text 'Soluzioni commentate:' followed by a table listing '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'. The 'Selezione territoriale' section has a sub-heading 'La selezione territoriale consiste in una competizione Capture-The-Flag' and the 'Competizione nazionale' section has a sub-heading 'La competizione nazionale, come la selezione territoriale, consiste in una'.

# Cosa faremo Oggi: Web Security

1. Cookies
2. Sessione Utente / la libreria request in python e l'oggetto Session
3. Database
4. SQLi



# Sessione utente

- Eseguita l'autenticazione, il server affida all'utente una **identità**
- L'applicazione web è poi incaricata di *ricordarsi* l'identità dell'utente
- Come il login, anche questa operazione **deve essere eseguita in un ambiente trusted**, altrimenti un utente malevolo potrebbe spacciarsi per un altro utente

# Cookies

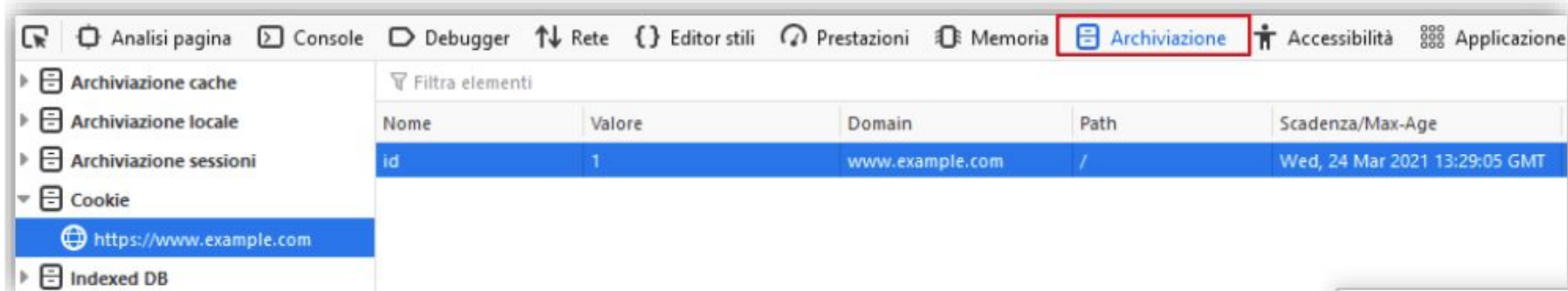
---

- HTTP mette a disposizione i **cookies** per questa operazione
- I cookies sono una informazione che il browser salva **localmente** e che invia in ogni richiesta HTTP

↑  
I cookies non sono affidabili!

# Cookies

- Cliccando sul nome-valore sarà poi possibile modificare il cookie



The screenshot shows the browser's developer tools with the 'Archiviazione' (Storage) tab selected. The left sidebar shows the 'Cookie' section expanded for the URL 'https://www.example.com'. The main area displays a table of cookies:

Nome	Valore	Domain	Path	Scadenza/Max-Age
id	1	www.example.com	/	Wed, 24 Mar 2021 13:29:05 GMT

# Cookies

Impostazioni di Sicurezza:

1. I cookie settati da un dominio sono accessibili solo a quel dominio
2. Ogni dominio **non** può settare o leggere i cookie degli altri domini visitati (non direttamente)

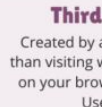
## TYPES OF INTERNET COOKIES

Internet cookie is a text file with small pieces of data that a web server generates when you visit a website.



### First-Party Cookies

Created by the website you are visiting to track your browsing activity in that site and remember them over multiple visits.



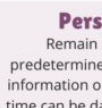
### Third-Party Cookies

Created by a third-party website other than visiting website to track your activity on your browser on different websites. Used by advertisers.



### Session Cookies

Tracks a user's session on a website and exists only for that session after which they are automatically deleted.



### Persistent Cookies

Remain in user's browser for a predetermined length of time and collect information on the websites you visit. The time can be days, weeks, months or years.



### Secure Cookies

Any cookie made secure by adding "Secure" flag to transmit sensitive information. Can be sent over only secure and encrypted connections like HTTPS.



### Zombie Cookies

Regenerated cookies after original ones are deleted. They create backup versions of themselves and store outside your browser only to reappear after original cookies are deleted from browser. Used by unethical ad networks and hackers.





# Cookies

- Da browser, i due modi più semplici per creare/modificare/cancellare cookie sono:
  - Usare la console di sviluppo
  - Usare Javascript

`document.cookie="nome=valore"`

# Cookies

---

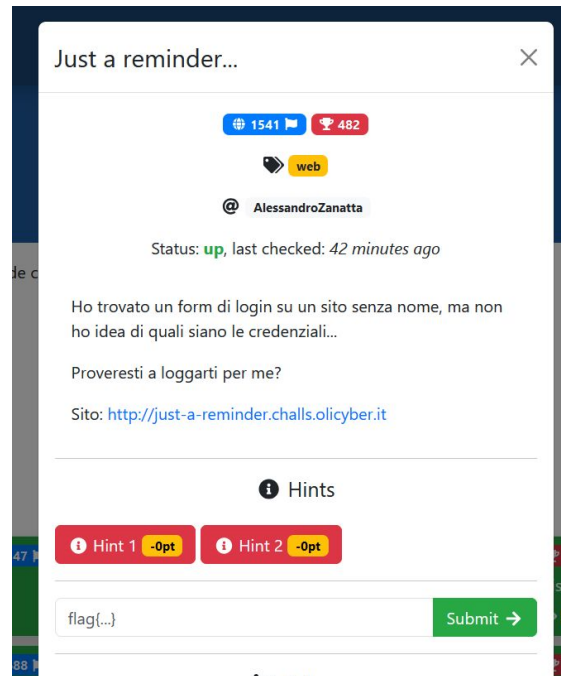
- Come detto prima, tutta la parte di autenticazione deve essere eseguita in un ambiente trusted
- Come è possibile osservare, **i cookies non sono affidabili**, in quanto è possibile cambiarli a piacimento

# Autenticazione sicura

Considera un sito web con meccanismo di autenticazione. Quale tra le seguenti operazioni sono necessarie per avere un processo di login sicuro?

Risposte

- (A) Verifica username e password lato client
- (B) Verifica username e password lato server
- (C) Verifica username e password lato client e server
- (D) Nessuna delle altre risposte



 "Just a reminder..." 

# Compiti per casa!

Gestione dati lato client:

<https://training.olicyber.it/challenges#challenge-43>



# Sessione Utente

Per rendere sicuro il cookie di sessione:

1. Firmare digitalmente il cookie
2. Generare una “password” temporanea (session-id) al login, che viene verificata ad ogni richiesta successiva

```
3 import requests
4
5 # URL delle risorse
6 BASE_URL = "http://web-11.challs.olicyber.it"
7 LOGIN_URL = f"{BASE_URL}/login"
8 FLAG_URL = f"{BASE_URL}/flag_piece"
9
10 # Credenziali di login
11 credentials = {
12     "username": "admin",
13     "password": "admin"
14 }
15
16 # Creazione della sessione
17 session = requests.Session()
18
19 # Login per ottenere il cookie di sessione e il token CSRF iniziale
20 login_response = session.post(LOGIN_URL, json=credentials)
21 if login_response.status_code != 200:
22     print(f"Errore durante il login: {login_response.status_code}")
23     exit()
24 print(login_response.json())
25
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

```
[Running] python -u "c:\Users\rugol\WorkSpace\CSFR.py"
{'status': 'ok', 'csrf': '4feefa60708a81ac'}
```

# Challenge: Web 11 - HTTP: i token CSRF

## Web 11 - HTTP: i token CSRF

932 50

web

@ Aquilareale

Status: **up**, last checked: *an hour ago*

Il *token CSRF* è un sistema impiegato per impedire l'esecuzione di attacchi di tipo *Cross-Site Request Forgery*. L'attacco consisterebbe nell'ingannare un utente di un servizio web a cliccare su un link o sul tasto di invio di un form inclusi in un'email o su un sito controllato dall'attaccante, che abbiano come target una risorsa "pericolosa" del servizio bersaglio (p.e. una risorsa la cui richiesta rappresenti un comando di cancellazione dell'account). Il meccanismo del cookie di sessione, ottenibile solo con username e password sconosciuti all'attaccante, impedisce a quest'ultimo di eseguire personalmente l'operazione "pericolosa" spacciandosi per l'utente, ma se l'utente viene indotto con l'inganno a cliccare il link malevolo su una macchina su cui abbia precedentemente eseguito l'accesso al servizio bersaglio, il cookie contenente il token di sessione verrà allegato automaticamente alla richiesta effettuata, validandola, senza che l'attaccante abbia bisogno di rubarlo o di riprodurre un contraffatto.

```
26 # Parsing del token CSRF iniziale
27 csrf_token = login_response.json().get("csrf")
28 if not csrf_token:
29     print("Token CSRF non trovato nella risposta del login.")
30     exit()
31
32 # Recupero dei pezzi della flag
33 flag = ""
34 for i in range(4):
35     # Aggiunta del token CSRF nell'header
36     # headers = {"X-CSRF-Token": csrf_token}
37     # Richiesta del pezzo di flag
38     response = session.get(FLAG_URL, params={"index": i, "csrf": csrf_token})
39     if response.status_code != 200:
40         print(f"Errore nel recupero del pezzo {i}: {response.status_code}")
41         exit()
42     # Aggiornamento del token CSRF
43     csrf_token = response.json().get("csrf")
44     if not csrf_token:
45         print(f"Token CSRF non trovato nella risposta per il pezzo {i}.")
46         exit()
47     # Aggiunta del pezzo alla flag
48     flag += response.json().get("flag_piece")
49
50 # Output della flag completa
51 print(f"\nFlag completa: {flag}")
```

# Signed Cookie

In pratica il server genere

- Un ID univoco per l'utente loggato
- Un certificato digitale (*sign*) che garantisce l'autenticità del cookie

# Session-id ..vulnerabili

Chiaramente

- Session-ID devono avere entropia adeguata
- Altrimenti sono facilmente “GUESS-ABILI”

```
HTTP/1.1 302 FOUND
Date: Wed, 24 Mar 2021 16:36:04 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 223
Connection: close
Server: gunicorn/19.9.0
Location: /cookies
Set-Cookie: session=32; Path=/
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
```





Challenge: Web??? - ???

ITIS

LEONARDO DA VINCI

# Cookie di Sessione

Strumenti di sviluppo – Modifica quiz: Esercitazione Assembly 1 (Gio 7/12) - Recupero 14/12 – https://moodle.itis.pr.it/n

Analisi pagina Console Debugger Rete Editor stili Prestazioni Memo

- Archiviazione cache
- Archiviazione locale
- Archiviazione sessioni
- Cookie
  - https://moodle.itis.pr.it
- Indexed DB

Filtra elementi

Nome	Valore	Domain	Path	Scadenza/Ma
ext_pgvwcount	-0.1	moodle.itis...	/	Mon, 18 Dec
MoodleSession	6a95mohvcqei9er...	moodle.itis....	/moodle/	Sessione



Durante la lezione il prof. mostra (incautamente) il proprio session\_id del login moodle... e a fine lezione si trova il profilo hackerato

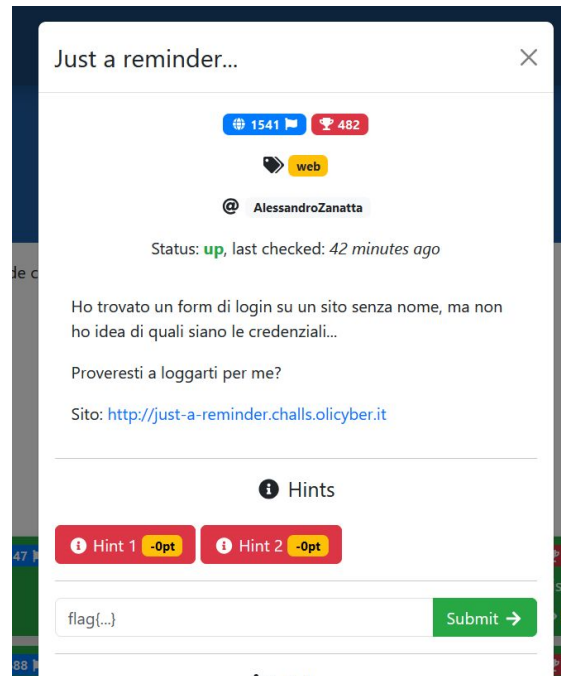


# Autenticazione sicura

Considera un sito web con meccanismo di autenticazione. Quale tra le seguenti operazioni sono necessarie per avere un processo di login sicuro?

Risposte

- (A) Verifica username e password lato client
- (B) Verifica username e password lato server
- (C) Verifica username e password lato client e server
- (D) Nessuna delle altre risposte

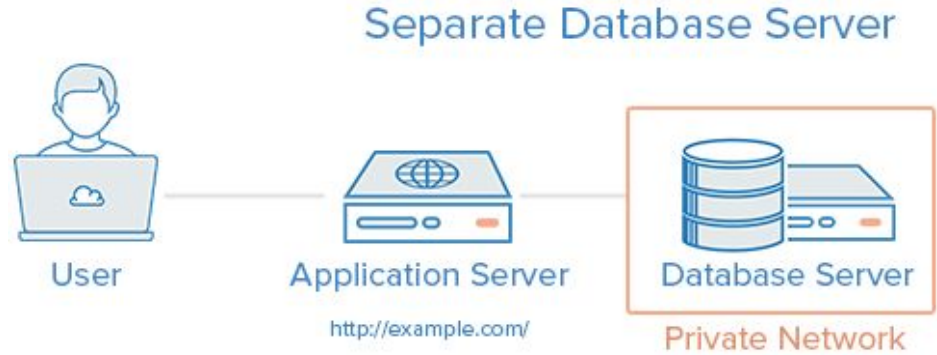


 "Just a reminder..." 



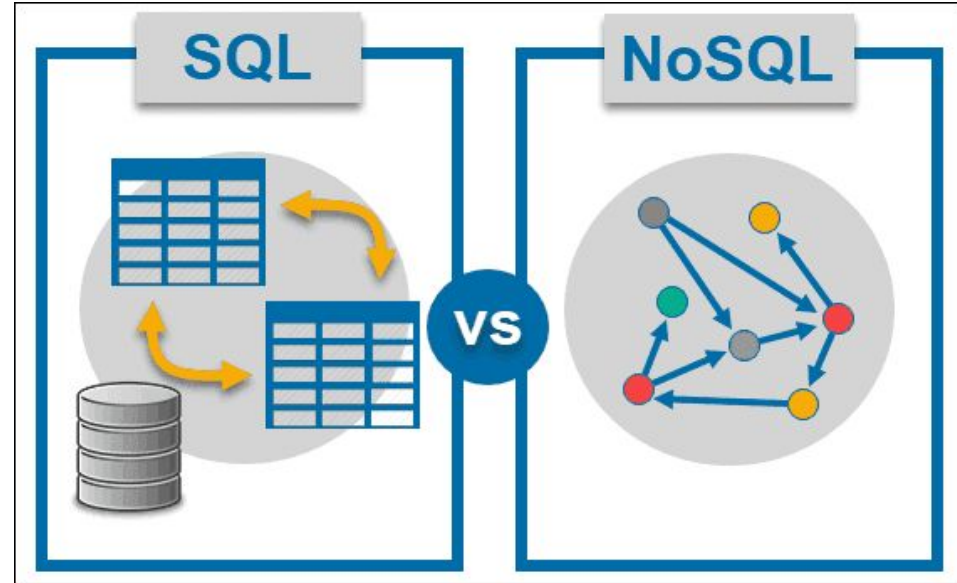
# Database

- Il server WEB è *stateless*
  - Ha bisogno di un server scripting per la gestione delle pagine dinamiche (php, python, node.js, ecc)
  - Ha bisogno di un DBMS per memorizzare (input utente, scelte, ecc) e per recuperare informazioni



# Database ...più tipi

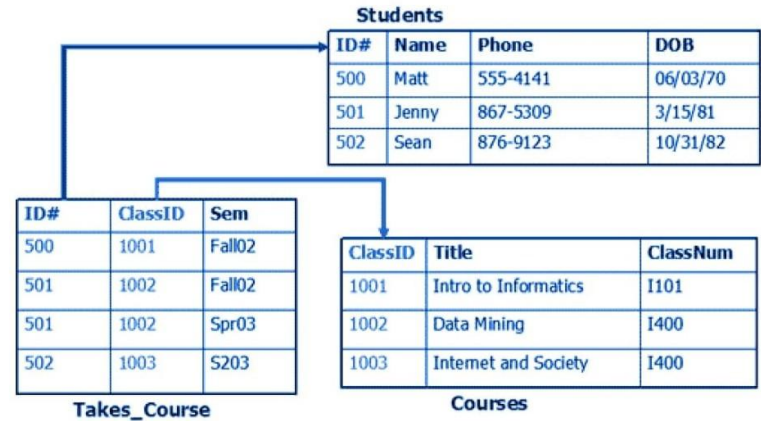
- RELAZIONALI (SQL)
- NoSQL
- BigData
- ...



# Database Relazionali

- E' un insieme di tabelle
- Talvolta collegate tra loro mediantei “Chiavi”
- Il DBMS fornisce:
  - meccanismi di autenticazione
  - gestione permessi (cosa possiamo fare e su quali tabelle)

## Relational Database Management System



# Database Relazionale.. Un Esempio

- Vediamo la struttura del DB di una diffusissimo CMS: Wordpress
- Esempi di Query
-

# SQL Injection



- Tecnica per sfruttare vulnerabilità in applicazioni mal programmate

Users			
	UserName	Passwd	UserID
1	A-JayBibbins637	uslwfpua	10000
2	A-JayTorain976	iyvqxzrq	10001
3	AadamDobbin507	aufvxyuy	10002
4	AadamHaws649	vonolnrv	10003
5	AadamThiengtham0	ydypixak	10004
6	AadhishAyon371	fbecsnda	10005
7	AadiAccardi419	imkboytx	10006
8	AadiGnau621	12345	10007
9	AadiMarinko33	juhktina	10008
10	AadishivLathon60	ohhiumw	10009
11	AadishivPioletti873	dragon	10010
12	AadityaTerre708	123456	10011
13	AadmClary990	uqqbmdr	10012
14	AadvikAllman584	qwerty	10013
15	AadvikMannheimer804	aforkuf	10014
16	AadvaRogan194	drann	10015



Normal User

```
SELECT * FROM Users  
WHERE UserID = "941938"  
AND password = "XFNEifQwKH08";
```

Expected Input



Attacker

```
SELECT * FROM Users  
WHERE UserID = "" OR 1=1 --  
" AND password = "";
```

Injected SQL Statement



SQL Database  
Statement  
Parser



Expected Output



Data Breach

© TechTerms.com

ITIS

LEONARDO DA VINCI