

Web Security 1

Autenticazione e sessione

**Riccardo
BONAFEDE**

Università degli Studi di
Padova



<https://cybersecnatlab.it>

Obiettivi

3

- Comprendere il concetto di sessione
- Comprendere il concetto di ambiente trusted

Prerequisiti

4

- Modulo [NS_1.1](#) - Fondamenti di reti di calcolatori
- Modulo [WS_1.1](#) - Il browser web e HTTP

Argomenti

5

- Autenticazione
- Sessione utente
 - Cookies
 - Server-Side Session vs Client-Side Session

Argomenti

6

- Autenticazione
- Sessione utente
 - Cookies
 - Server-Side Session vs Client-Side Session

Introduzione

7

- I siti web devono proteggere alcune risorse e funzionalità da utenti non autorizzati
- Il problema principale per una applicazione web è verificare se un utente è effettivamente chi dice di essere

Introduzione

8

- Dal momento in cui un utente naviga su un sito web, si dice che inizia una **sessione**
- La vita di una sessione è composta da tre momenti principali:
 1. **Autenticazione**: quando l'utente si identifica (facendo login ad esempio)
 2. **Sessione Utente**: Il momento in cui l'utente è identificato
 3. **Logout**: quando l'utente finisce la sua sessione

Autenticazione

9

- Il modo più diffuso per verificare l'identità di un utente è mediante l'uso di un username e di una password
- A livello teorico, l'username indica qual è l'identità dell'utente, mentre la password è un segreto che garantisce per l'identità

Autenticazione

10

- È importante notare come ogni metodo di autenticazione fa uso di un qualche tipo di segreto che solo l'utente vero dovrebbe conoscere
 - Ad esempio le impronte digitali sfruttano il fatto che solo l'utente legittimo ha accesso alle sue impronte digitali

Autenticazione

11

- L'autenticazione, e tutta la sessione utente, deve essere eseguita in un ambiente *trusted*
- In un ambiente trusted le informazioni sono protette da utenti malevoli, i quali non possono violarne né la confidenzialità né l'integrità

Autenticazione

12

- Un esempio di login in ambiente non trusted è dato da un sito web in cui è implementato un login client side
- L'identità dell'utente è verificata all'interno del browser, quindi in un ambiente che potenzialmente è sotto controllo di un utente malevolo
- Questo permette all'attaccante di scoprire il segreto (la password) su cui si basa il login
 - O volendo di autenticarsi senza neanche fare login

Sessione utente

14

- 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

15

- 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

Cookies

16

- 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

17

- I cookies sono delle coppie chiave-valore. La chiave è il nome del cookie, il valore i dati che contiene

The screenshot shows the 'Archiviazione' (Cookies) tab in a browser's developer tools. The left sidebar shows the 'Cookie' section selected for the URL 'https://www.example.com'. The main area displays a table of cookies with the following columns: Nome, Valore, Domain, Path, and Scadenza/Max-Age. A single cookie is listed and highlighted with a red border:

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

Cookies

18

```
HTTP/1.1 302 FOUND
Date: Wed, 24 Mar 2021 16:29:10 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 223
Connection: close
Server: gunicorn/19.9.0
Location: /cookies
Set-Cookie: nome=valore; Path=/
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
```

```
GET /cookies HTTP/1.1
Host: httpbin.org
accept: text/plain
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
Chrome/89.0.4389.90 Safari/537.36
Referer: http://httpbin.org/
Accept-Encoding: gzip, deflate
Accept-Language: it-IT, it;q=0.9, en-US;q=0.8, en;q=0.7
Cookie: nome=valore
Connection: close
```

Cookies

19

- È da notare che i cookie sono soggetti ad alcune regole di sicurezza:
 1. I cookie settati su un determinato dominio sono inviati **solo** a quel dominio

Altrimenti www.delfino.com avrebbe accesso a tutti i cookies di www.instagram.com

Cookies

20

- È da notare che i cookie sono soggetti ad alcune regole di sicurezza:
 1. I cookie settati su un determinato dominio sono inviati **solo** a quel dominio
 2. Un dominio **non può** settare cookie per altri domini

Altrimenti www.delfino.com avrebbe accesso a tutti i cookies di www.instagram.com

1: Diverse vulnerabilità sfruttano iniezioni di questo tipo. Ad esempio Session Fixation

Cookies

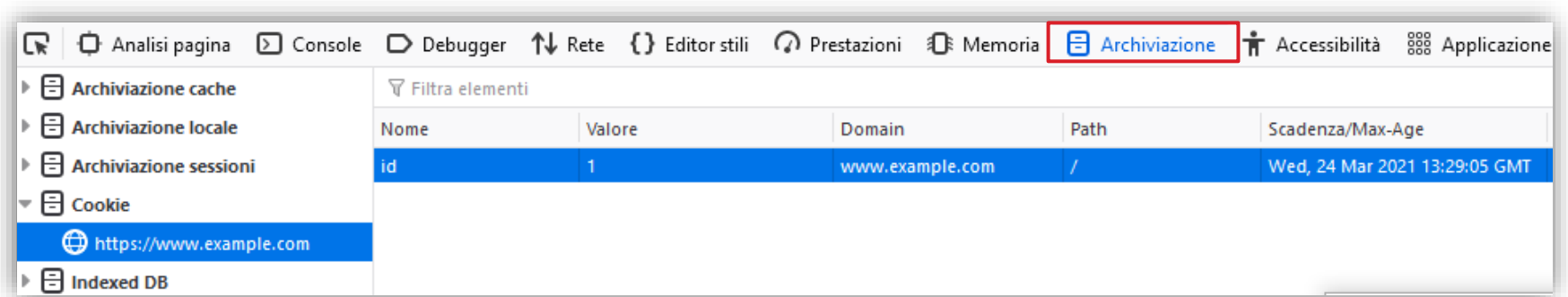
21

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

Cookies

22

- Per settare/cambiare cookie dalla console, andare su archiviazione



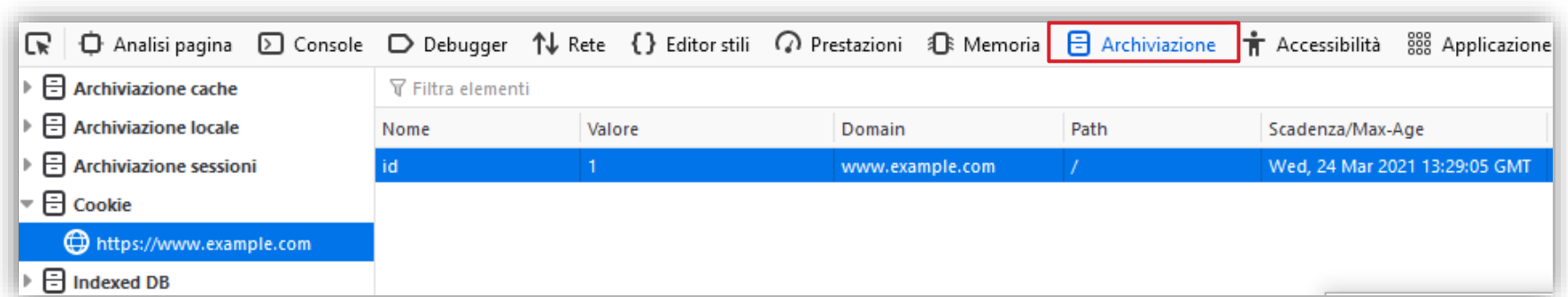
The screenshot shows the Chrome DevTools interface with the 'Archiviazione' (Storage) tab selected in the top navigation bar. The left sidebar shows the 'Cookie' folder expanded, with the URL 'https://www.example.com' selected. The main panel displays a table of cookies for this domain.

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

Cookies

23

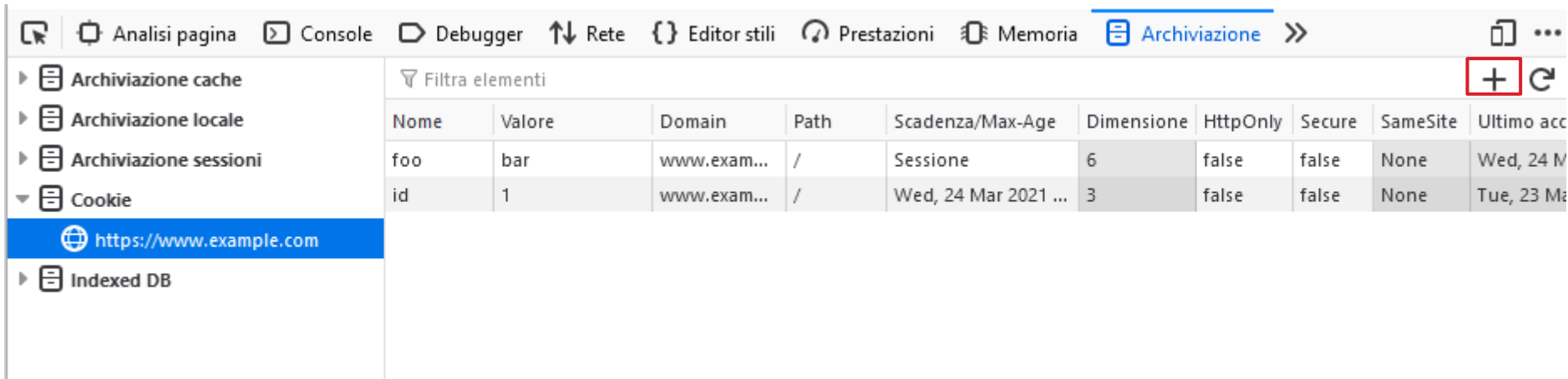
- Cliccando sul nome-valore sarà poi possibile modificare il cookie



Cookies

24

- Per crearne uno nuovo basta cliccare il +



Analisi pagina Console Debugger Rete Editor stili Prestazioni Memoria Archiviazione

Filtra elementi

Nome	Valore	Domain	Path	Scadenza/Max-Age	Dimensione	HttpOnly	Secure	SameSite	Ultimo acc
foo	bar	www.exam...	/	Sessione	6	false	false	None	Wed, 24 M
id	1	www.exam...	/	Wed, 24 Mar 2021 ...	3	false	false	None	Tue, 23 M

https://www.example.com

Indexed DB

Cookies

25

- Usando Javascript invece, dal sito in cui si vuole settare un cookie:
 - Aprire la console Javascript
 - Inserire:

```
document.cookie="nome=valore"
```

Cookies

26

- 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

Cookies

27

- Un utente, con o senza credenziali valide, potrebbe affermare di essere un altro utente o avere un privilegio più alto
- ...se ti fidi del cookie, ti fidi di quello che dice l'utente

Sessioni Utente

28

- Vi sono due modi per ovviare a questo problema:
 - Firmare digitalmente le informazioni contenute sui cookies
 - Fornire una "password" temporanea, detta *session-id*, che verrà verificata ad ogni richiesta e che può essere conosciuta solo a chi ha effettuato correttamente il login

Sessioni Utente

29

- I meccanismi di firma digitale garantiscono che una informazione derivi direttamente dal server
- Poiché un utente maligno non è in grado di firmare queste informazioni, il server può considerarle come affidabili

```
id=1;  
sign=651797b2026d502f76cb2ad0111293ae;
```

- **id**: l'id associato all'utente
- **sign**: una firma che garantisce l'autenticità del cookie

Sessioni Utente

30

- Le sessioni fanno invece uso di una password temporanea che viene associata server-side all'identità dell'utente
- PHP ad esempio, utilizza un token a 128 bit, generato casualmente e univoco per ogni utente che visita il sito

Sessioni Utente

31

- Le session-id devono avere una entropia adeguata
- Sessioni con poca entropia sono indovinabili da un attaccante

```
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
```

Web Security 1

Autenticazione e sessione

**Riccardo
BONAFEDE**

Università degli Studi di
Padova



<https://cybersecnatlab.it>