root@hacklab:~/parte-01/lezione-04

ETHICAL HACKING POTENZIATO DALL'IA // PARTE I

LEZIONE 04

Web Application Security

Test delle applicazioni web secondo OWASP.

docente **Vincenzo Calabro** fase Fase mirata: test delle applicazioni web (OWASP)

root@hacklab:~/lezione-04/agenda $

LEZIONE 04 / AGENDA

In questa lezione

// PERCORSO

> Superficie d'attacco e OWASP Top 10
> Injection e Cross-Site Scripting
> SSRF, IDOR e logic flaws
> Discovery e fuzzing
> Sicurezza di API e token

metodo obiettivi -> teoria -> strumenti -> laboratorio -> caso di studio -> etica -> verifica

LEZIONE 04 / OBIETTIVI

Obiettivi di apprendimento

// AL TERMINE SAPRAI (TASSONOMIA DI BLOOM)

> Comprendere — OWASP Top 10 e superficie d'attacco
> Applicare — proxy di intercettazione e test automatici
> Analizzare — injection, XSS, SSRF, access control
> Valutare — l'efficacia delle contromisure
> Creare — un report di web penetration test

LEZIONE 04 / INQUADRAMENTO

Inquadramento

// DI COSA PARLIAMO

Le applicazioni web sono la superficie d'attacco piu esposta: qui concentriamo OWASP Top 10 e il metodo WSTG. La lezione collega ogni classe di vulnerabilita alla sua causa radice e alla relativa contromisura.

// PERCHE CONTA

Test delle applicazioni web secondo OWASP.

LEZIONE 04 / MAPPA // INSIEME

Mappa d'insieme del modulo

Attacco/tecnica · Difesa · Norme & metodo · IA

FONDAMENTI

- 01 Fondamenti HTTP e OWASP Top 10
- 02 Injection e XSS/CSRF
- 03 SSRF, traversal, IDOR e logic flaw
- 04 Discovery e fuzzing
- 05 Sicurezza di API, JWT e CORS

APPROFONDIMENTI

- 06 CSRF, clickjacking e header
- 07 Upload e path traversal
- 08 Access control e logica di business
- 09 JWT, CORS e sessioni
- 10 Fuzzing guidato dall'IA

LEZIONE 04 / MAPPA // FONDAMENTI

Mappa dei concetti — Fondamenti

Attacco/tecnica · Difesa · Norme & metodo · IA

LEZIONE 04 / CONCETTO 1/10

[Attacco/tecnica]

Fondamenti HTTP e OWASP Top 10

// SPIEGAZIONE

Le applicazioni web poggiano su HTTP, cookie di sessione e meccanismi di autenticazione: capirne il funzionamento e il prerequisito per trovarne i difetti. L'OWASP Top 10 raccoglie le dieci classi di rischio piu diffuse come mappa di partenza.

// ESEMPIO

> Un cookie di sessione senza flag HttpOnly e Secure e esposto a furto via XSS.

LEZIONE 04 / CONCETTO 2/10

[Attacco/tecnica]

Injection e XSS/CSRF

// SPIEGAZIONE

Le injection nascono quando input non validato finisce in una query o in un comando (SQL, NoSQL, OS). L'XSS inietta script nel browser della vittima; il CSRF le fa compiere azioni non volute sfruttando la sua sessione attiva.

// ESEMPIO

```
$ ' OR '1'='1 -- in un campo login rivela una SQL injection classica
```

LEZIONE 04 / CONCETTO 3/10

[Attacco/tecnica]

SSRF, traversal, IDOR e logic flaw

// SPIEGAZIONE

Oltre alle injection, le app soffrono di SSRF, con il server indotto a contattare risorse interne, upload non controllati, path traversal, IDOR (accesso a oggetti altrui cambiando un id) e difetti di logica che eludono le regole di business.

// ESEMPIO

> Cambiare /fattura?id=1001 in id=1002 mostra la fattura di un altro cliente (IDOR).

LEZIONE 04 / CONCETTO 4/10

[Attacco/tecnica]

Discovery e fuzzing

// SPIEGAZIONE

Si parte mappando endpoint, parametri e contenuti nascosti; il fuzzing invia poi molti input anomali per far emergere errori e comportamenti inattesi. L'IA puo suggerire payload e parametri plausibili, accelerando la scoperta.

// ESEMPIO

```
$ ffuf -u https://esempio.it/FUZZ -w wordlist.txt
```

LEZIONE 04 / CONCETTO 5/10

[Norme & metodo]

Sicurezza di API, JWT e CORS

// SPIEGAZIONE

Le API REST e GraphQL ampliano la superficie d'attacco: vanno verificate autenticazione, autorizzazione per oggetto e rate limiting. I JWT mal validati e le policy CORS troppo permissive sono errori ricorrenti che espongono dati e sessioni.

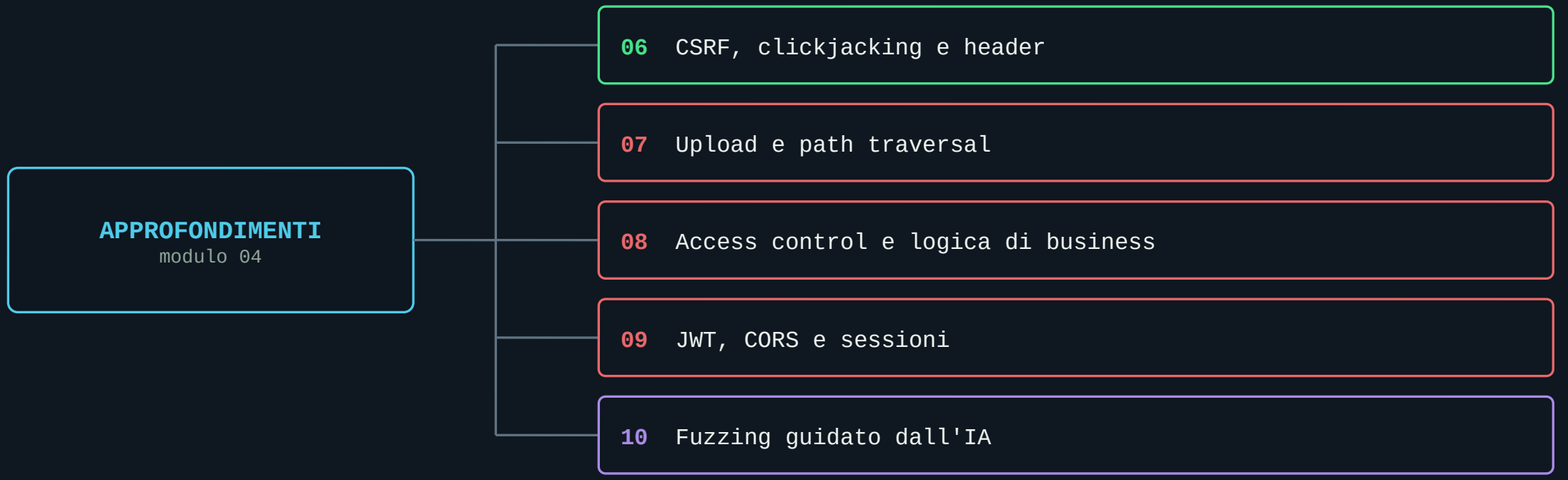
// ESEMPIO

> Un JWT accettato con alg=none bypassa completamente la verifica della firma.

LEZIONE 04 / MAPPA // APPROFONDIMENTI

Mappa dei concetti — Approfondimenti

Attacco/tecnica · Difesa · Norme & metodo · IA



LEZIONE 04 / CONCETTO 6/10

[Difesa]

CSRF, clickjacking e header

// SPIEGAZIONE

CSRF e clickjacking sfruttano la fiducia del browser nella sessione dell'utente; si mitigano con token anti-CSRF, cookie SameSite e header come X-Frame-Options e Content-Security-Policy, che istruiscono il browser su cosa e lecito.

// ESEMPIO

```
> Header X-Frame-Options: DENY impedisce di incorniciare la pagina per il clickjacking.
```

LEZIONE 04 / CONCETTO 7/10

[Attacco/tecnica]

Upload e path traversal

// SPIEGAZIONE

Un upload senza controlli su tipo, contenuto e destinazione puo portare all'esecuzione di codice; il path traversal usa sequenze come ../ per uscire dalla cartella prevista e leggere o scrivere file arbitrari sul server.

// ESEMPIO

```
$ GET /download?f=../../etc/passwd
```

LEZIONE 04 / CONCETTO 8/10

[Attacco/tecnica]

Access control e logica di business

// SPIEGAZIONE

Molti attacchi non rompono la crittografia ma la logica: funzioni accessibili senza i giusti privilegi, passaggi saltabili, limiti aggirabili. Il broken access control e in cima all'OWASP Top 10 proprio perche spesso invisibile agli scanner.

// ESEMPIO

> Chiamare un endpoint /admin non linkato ma non protetto lato server.

LEZIONE 04 / CONCETTO 9/10

[Attacco/tecnica]

JWT, CORS e sessioni

// SPIEGAZIONE

Un token di sessione sicuro deve essere firmato correttamente, avere scadenza e poter essere revocato. CORS mal configurato, con Access-Control-Allow-Origin riflesso e credenziali, espone i dati a siti terzi: va limitato alle origini fidate.

// ESEMPIO

> Un ACAO che riflette qualunque Origin consente a un sito malevolo di leggere risposte autenticate.

LEZIONE 04 / CONCETTO 10/10 [IA]

Fuzzing guidato dall'IA

// SPIEGAZIONE

L'IA puo generare payload e varianti contestuali per un parametro, un formato o un framework, rendendo il fuzzing piu mirato ed efficiente. Resta da validare manualmente ogni anomalia, perche il modello non comprende l'impatto reale.

// ESEMPIO

> Un LLM propone payload di injection specifici per GraphQL a partire dallo schema.

LEZIONE 04 / STRUMENTI

Strumenti della lezione

// TOOLKIT

Burp Suite | OWASP ZAP | SQLMap | Nuclei | ffuf | Gobuster | WPScan | Commix | XSStrike

// NOTA OPERATIVA

> Ogni strumento si usa in ambiente virtualizzato e isolato, solo su bersagli di proprieta o autorizzati. Output e artefatti vanno protetti e, a fine ingaggio, gestiti o distrutti.

root@hacklab:~/lezione-04/lab-1 $

LEZIONE 04 / LABORATORIO 1

Laboratorio 1

$ Injection e XSS (Burp, SQLMap su DVWA/Juice Shop)

// PROCEDURA

[1] Intercetta e manipola richieste (Burp)

[2] sfrutta una SQL injection (SQLMap)

[3] trova un XSS stored

[!] Verifica: Perche la validazione lato server e imprescindibile?

root@hacklab:~/lezione-04/lab-2 $

LEZIONE 04 / LABORATORIO 2

Laboratorio 2

$ Discovery, SSRF e access control (ffuf, Nuclei)

// PROCEDURA

[1] Esegui fuzzing (ffuf)

[2] sfrutta SSRF e IDOR

[3] scansiona con Nuclei

[!] Verifica: Come nasce una SSRF?

LEZIONE 04 / CASO DI STUDIO

Caso di studio

// SCENARIO

> Breccia via SSRF verso il metadata service in cloud (anticipo del caso Capital One).

// ANALISI RICHIESTA

> Ricostruisci la dinamica dei fatti con metodo e tracciabilita
> Individua errori, cause radice e punti di decisione critici
> Proponi contromisure, controlli e lezioni apprese

LEZIONE 04 / ETICA & DIRITTO

Nota etico-legale

// PRINCIPI INDEROGABILI

> autorizzazione scritta scope definito ambiente isolato dati protetti responsible disclosure

// SPECIFICO DELLA LEZIONE

[!] I test possono corrompere dati o causare indisponibilita: ambiente isolato o finestre autorizzate.

LEZIONE 04 / RICAPITOLAZIONE

Ricapitolazione

// PUNTI CHIAVE

> OWASP Top 10 e superficie d'attacco
> Proxy di intercettazione e test automatici
> Injection, XSS, SSRF, access control
> L'efficacia delle contromisure
> Un report di web penetration test

LEZIONE 04 / AUTOVALUTAZIONE

Autovalutazione

// DOMANDE DI VERIFICA

? Perche la validazione lato server e imprescindibile?

? Reflected, stored o DOM: che differenza c'e?

? Come si testa un controllo di accesso (IDOR)?

// VALUTAZIONE

Report di web application penetration test.

// LETTURE

OWASP WSTG e Top 10; Web App Hacker's Handbook.

lezione 04 completata

$ next

Web Application Security

[!] Le competenze di questa lezione si impiegano esclusivamente in contesti legali, autorizzati e deontologicamente corretti, entro lo scope e con autorizzazione scritta.

root@hacklab:~# _

root@hacklab:~/contatti $

CONTATTI / RISORSE

Restiamo in contatto

Vincenzo Calabro

cyber security / digital forensics /
docenza e divulgazione

// SCANSIONA O VISITA

> vincenzocalabro.it

Inquadra il QR con la fotocamera per aprire il sito.