

Relazione – SQL Injection con analisi tramite Wireshark

In questo esercizio ho voluto simulare un attacco di tipo SQL Injection, osservando nel dettaglio cosa succede "dietro le quinte" usando Wireshark, un software che permette di catturare e analizzare il traffico di rete.

L'obiettivo era capire come un'iniezione SQL venga trasmessa sulla rete, attraverso un pacchetto HTTP, e come analizzarla per imparare a riconoscere i segnali di una potenziale vulnerabilità.

Ho lavorato su una macchina virtuale Kali Linux, e ho utilizzato Wireshark per avviare la cattura del traffico di rete. Il file della cattura è stato salvato come

`sql_injection_test.pcapng`.

Mi sono collegata al sito testphp.vulnweb.com, un ambiente di test pensato proprio per simulazioni di sicurezza. Dopo aver aperto la pagina di login (come si vede negli screen), ho inserito una classica stringa di iniezione SQL:

```
username: ' or '1'='1  
password: qualsiasi_valore
```

In un'altra variante, ho usato:

```
username: ' UNION SELECT 1,2,3,4,5,6,7,8-- -
```

Queste stringhe servono a manipolare la query SQL che viene eseguita dal server per forzare un accesso non autorizzato o ottenere dati.

Analisi con Wireshark

Dopo l'attacco, ho filtrato i protocolli nel file pcap per facilitare l'analisi.

HTTP

Nel filtro HTTP ho trovato diverse richieste POST alla pagina [/userinfo.php](#). Tra i parametri trasmessi nel pacchetto in chiaro si vedono:

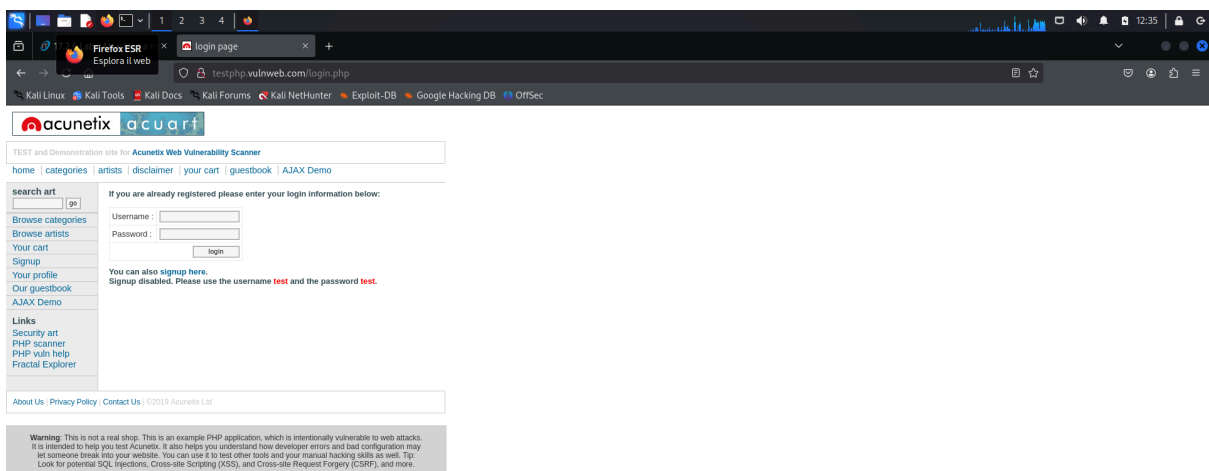
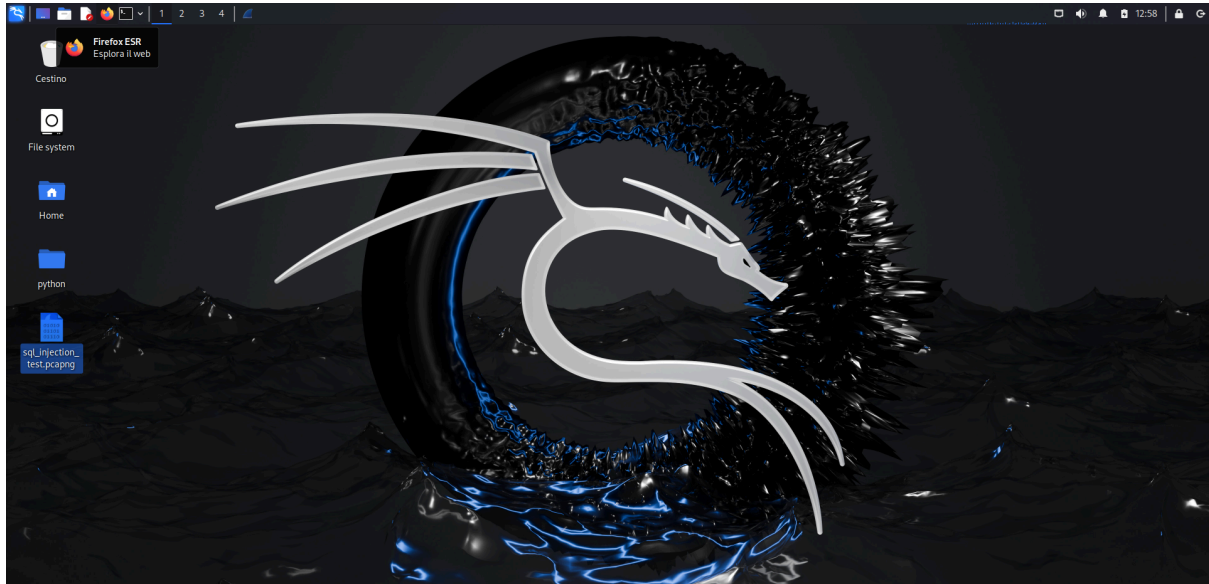
```
uname = ' UNION SELECT 1,2,3,4,5,6,7,8-- -  
pass = abc
```

Questo dimostra che l'iniezione SQL è stata inviata con successo, e che l'applicazione non cifra i dati, rendendo visibili tutte le credenziali e i tentativi di attacco. È un esempio chiaro di come una comunicazione non cifrata possa esporre dati sensibili.

TLS

In parallelo ho analizzato il traffico cifrato TLS. Qui, ovviamente, i contenuti non erano leggibili, ma si potevano comunque vedere le connessioni tra il client (192.168.50.100) e diversi IP esterni, indicativi di connessioni cifrate HTTPS.

Screenshot



No.	Time	Source	Destination	Protocol	Length	Info
8	0.612786646	192.168.50.100	44.228.249.3	HTTP	448	GET /login.php HTTP/1.1
10	0.827196905	44.228.249.3	192.168.50.100	HTTP	2802	HTTP/1.1 200 OK (text/html)
16	32.747293431	192.168.50.100	44.228.249.3	HTTP	630	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
78	32.860162699	44.228.249.3	192.168.50.100	HTTP	453	HTTP/1.1 200 OK (text/html)
103	66.139292938	192.168.50.100	44.228.249.3	HTTP	630	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
105	66.499748334	44.228.249.3	192.168.50.100	HTTP	453	HTTP/1.1 200 OK (text/html)
275	290.524288071	192.168.50.100	44.228.249.3	HTTP	640	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
277	290.742382675	44.228.249.3	192.168.50.100	HTTP	330	HTTP/1.1 302 Found (text/html)
279	290.745786750	192.168.50.100	44.228.249.3	HTTP	495	GET /login.php HTTP/1.1
281	290.963414548	44.228.249.3	192.168.50.100	HTTP	2802	HTTP/1.1 200 OK (text/html)
287	313.689751563	192.168.50.100	44.228.249.3	HTTP	661	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
289	313.831446964	44.228.249.3	192.168.50.100	HTTP	401	HTTP/1.1 200 OK (text/html)
303	357.375805378	192.168.50.100	44.228.249.3	HTTP	659	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
305	357.594130992	44.228.249.3	192.168.50.100	HTTP	401	HTTP/1.1 200 OK (text/html)
324	403.451001802	192.168.50.100	44.228.249.3	HTTP	637	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
326	403.668445873	44.228.249.3	192.168.50.100	HTTP	330	HTTP/1.1 302 Found (text/html)
328	403.673764978	192.168.50.100	44.228.249.3	HTTP	495	GET /login.php HTTP/1.1
330	403.890706322	44.228.249.3	192.168.50.100	HTTP	2802	HTTP/1.1 200 OK (text/html)
334	423.590392064	192.168.50.100	44.228.249.3	HTTP	634	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
336	423.710273912	44.228.249.3	192.168.50.100	HTTP	330	HTTP/1.1 302 Found (text/html)
337	423.724153737	192.168.50.100	44.228.249.3	HTTP	495	GET /login.php HTTP/1.1
339	423.941516173	44.228.249.3	192.168.50.100	HTTP	2802	HTTP/1.1 200 OK (text/html)
343	440.732193217	192.168.50.100	44.228.249.3	HTTP	637	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
345	440.950093259	44.228.249.3	192.168.50.100	HTTP	330	HTTP/1.1 302 Found (text/html)
346	440.955639718	192.168.50.100	44.228.249.3	HTTP	495	GET /login.php HTTP/1.1
349	441.172051383	44.228.249.3	192.168.50.100	HTTP	2802	HTTP/1.1 200 OK (text/html)
362	472.268841311	192.168.50.100	44.228.249.3	HTTP	637	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
364	472.486241021	44.228.249.3	192.168.50.100	HTTP	330	HTTP/1.1 302 Found (text/html)
365	472.490396559	192.168.50.100	44.228.249.3	HTTP	495	GET /login.php HTTP/1.1
367	472.706196807	44.228.249.3	192.168.50.100	HTTP	2802	HTTP/1.1 200 OK (text/html)
371	485.537372251	192.168.50.100	44.228.249.3	HTTP	637	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
373	485.754302039	44.228.249.3	192.168.50.100	HTTP	330	HTTP/1.1 302 Found (text/html)
374	485.757621108	192.168.50.100	44.228.249.3	HTTP	495	GET /login.php HTTP/1.1
376	485.983926809	44.228.249.3	192.168.50.100	HTTP	2802	HTTP/1.1 200 OK (text/html)
380	506.096574837	192.168.50.100	44.228.249.3	HTTP	653	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
382	506.313687151	44.228.249.3	192.168.50.100	HTTP	401	HTTP/1.1 200 OK (text/html)
404	518.164546428	192.168.50.100	44.228.249.3	HTTP	640	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
406	518.381415238	44.228.249.3	192.168.50.100	HTTP	450	HTTP/1.1 200 OK (text/html)
410	533.295027096	192.168.50.100	44.228.249.3	HTTP	645	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
412	533.512587669	44.228.249.3	192.168.50.100	HTTP	401	HTTP/1.1 200 OK (text/html)
418	546.139117113	192.168.50.100	44.228.249.3	HTTP	661	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)

No.	Time	Source	Destination	Protocol	Length	Info
14	1.447950336	192.168.50.100	108.157.194.113	TLSv1.2	93	Application Data
16	4.422532663	192.168.50.100	108.157.194.113	TLSv1.2	93	Application Data
17	4.422803264	192.168.50.100	108.157.194.113	TLSv1.2	93	Application Data
18	4.422923723	192.168.50.100	108.157.194.113	TLSv1.2	93	Application Data
19	4.423043422	192.168.50.100	108.157.194.113	TLSv1.2	93	Application Data
24	4.459190991	146.75.53.44	192.168.50.100	TLSv1.2	93	Application Data
26	4.461776053	108.139.240.239	192.168.50.100	TLSv1.2	93	Application Data
28	4.463657138	172.67.21.232	192.168.50.100	TLSv1.2	93	Application Data
30	4.495872482	18.203.104.239	192.168.50.100	TLSv1.2	93	Application Data
34	10.788973496	192.168.50.100	178.250.1.11	TLSv1.2	93	Application Data
35	10.789548219	192.168.50.100	178.250.1.11	TLSv1.2	93	Application Data
38	10.789838549	178.250.1.11	192.168.50.100	TLSv1.2	93	Application Data
40	10.789494367	178.250.1.11	192.168.50.100	TLSv1.2	93	Application Data
44	12.796658272	192.168.50.100	104.18.10.224	TLSv1.2	93	Application Data
46	12.840158143	104.18.10.224	192.168.50.100	TLSv1.2	93	Application Data
48	14.808043675	192.168.50.100	146.75.53.44	TLSv1.2	93	Application Data
50	14.839322407	146.75.53.44	192.168.50.100	TLSv1.2	93	Application Data
52	16.809403814	192.168.50.100	108.139.240.58	TLSv1.2	93	Application Data
53	16.810640318	192.168.50.100	108.139.240.58	TLSv1.2	78	Application Data
60	17.817361939	192.168.50.100	108.157.194.113	TLSv1.2	93	Application Data
61	17.818147999	192.168.50.100	108.157.194.113	TLSv1.2	78	Application Data
69	38.420160376	192.168.50.100	185.106.33.48	TLSv1.2	100	Application Data
81	38.750346315	192.168.50.100	52.72.220.143	TLSv1.2	93	Application Data
84	38.876838702	185.106.33.48	192.168.50.100	TLSv1.2	100	Application Data
86	38.905129432	52.72.220.143	192.168.50.100	TLSv1.2	93	Application Data
88	39.911327768	185.106.33.48	192.168.50.100	TLSv1.2	131	Application Data, Encrypted Alert
90	39.912063207	192.168.50.100	185.106.33.48	TLSv1.2	100	Application Data
91	39.912908451	192.168.50.100	185.106.33.48	TLSv1.2	85	Encrypted Alert
107	55.214913431	192.168.50.100	198.47.127.18	TLSv1.2	93	Application Data
108	55.215654553	192.168.50.100	198.47.127.18	TLSv1.2	78	Application Data
113	55.264806140	198.47.127.18	192.168.50.100	TLSv1.2	93	Application Data
118	58.217951858	192.168.50.100	108.138.200.231	TLSv1.2	93	Application Data
119	58.218230248	192.168.50.100	172.67.21.232	TLSv1.2	93	Application Data
120	58.218493414	192.168.50.100	18.203.104.239	TLSv1.2	93	Application Data
121	58.218761138	192.168.50.100	146.75.53.44	TLSv1.2	93	Application Data
122	58.219474053	192.168.50.100	108.138.200.231	TLSv1.2	78	Application Data
124	58.220167572	192.168.50.100	18.203.104.239	TLSv1.2	78	Application Data
126	58.221748134	192.168.50.100	146.75.53.44	TLSv1.2	78	Application Data
128	58.222817406	192.168.50.100	172.67.21.232	TLSv1.2	78	Application Data
142	58.236129000	146.75.53.44	192.168.50.100	TLSv1.2	78	Application Data
157	63.407277799	192.168.50.100	178.250.1.11	TLSv1.2	93	Application Data

Conclusioni

Questo esercizio è stato molto utile per capire come funziona un attacco SQL Injection a livello di rete, riconoscere i pacchetti HTTP vulnerabili, in cui le credenziali e i parametri sono visibili, vedere la differenza tra HTTP (in chiaro) e TLS (cifrato) e riflettere sull'importanza della cifratura delle comunicazioni nei siti web, soprattutto quando si usano form di login.

Wireshark permette di isolare e identificare facilmente i pacchetti sospetti con pochi click, il che lo rende uno strumento prezioso sia per la difesa che per l'analisi.