Institute of Computer Technology

B. Tech Computer Science and Engineering

Sub: Identity and Access Management (2CSE507)

Name - Nisarg Prajapati

Branch - Cyber Security

Enrollment no. – 23162171019

Semester - 5

Class - A

Batch – 52

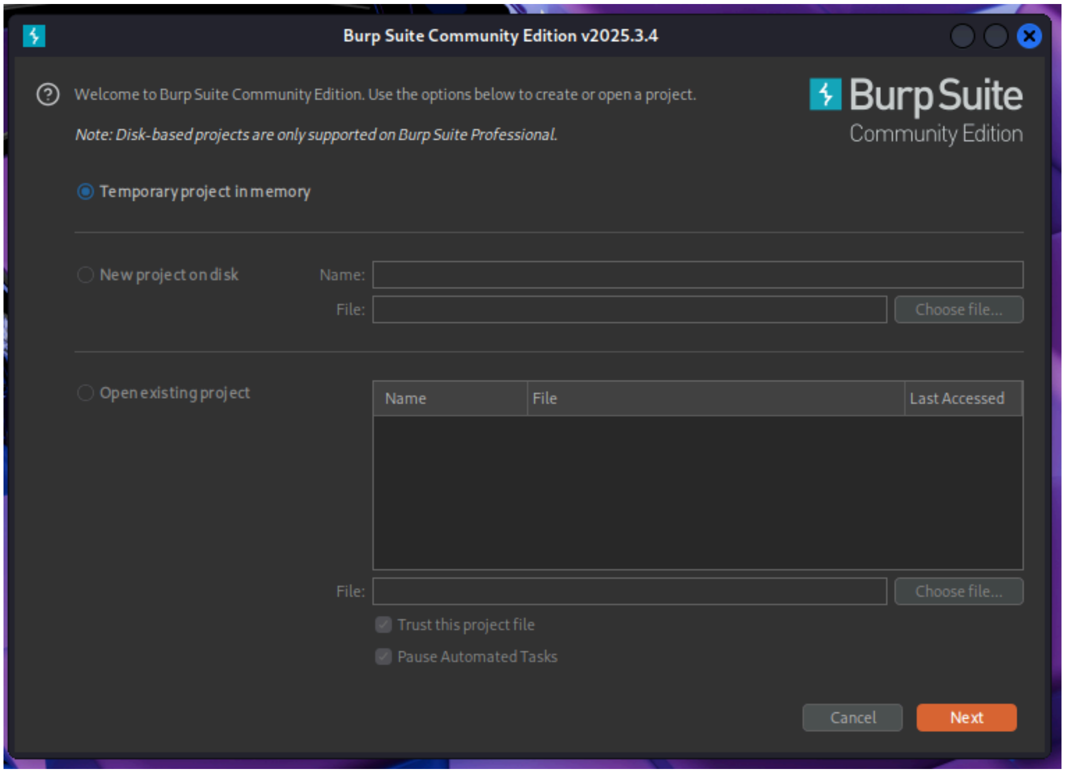
PRACTICAL NO:- 3

Aim:

Performing Bruteforcing using BurpSuite

Process:

1. Open Burpsuite and open a temporary project.



Burp Suite Community Edition v2025.3.4

Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

Note: Disk-based projects are only supported on Burp Suite Professional.

● Temporary project in memory

○ New project on disk Name: File:

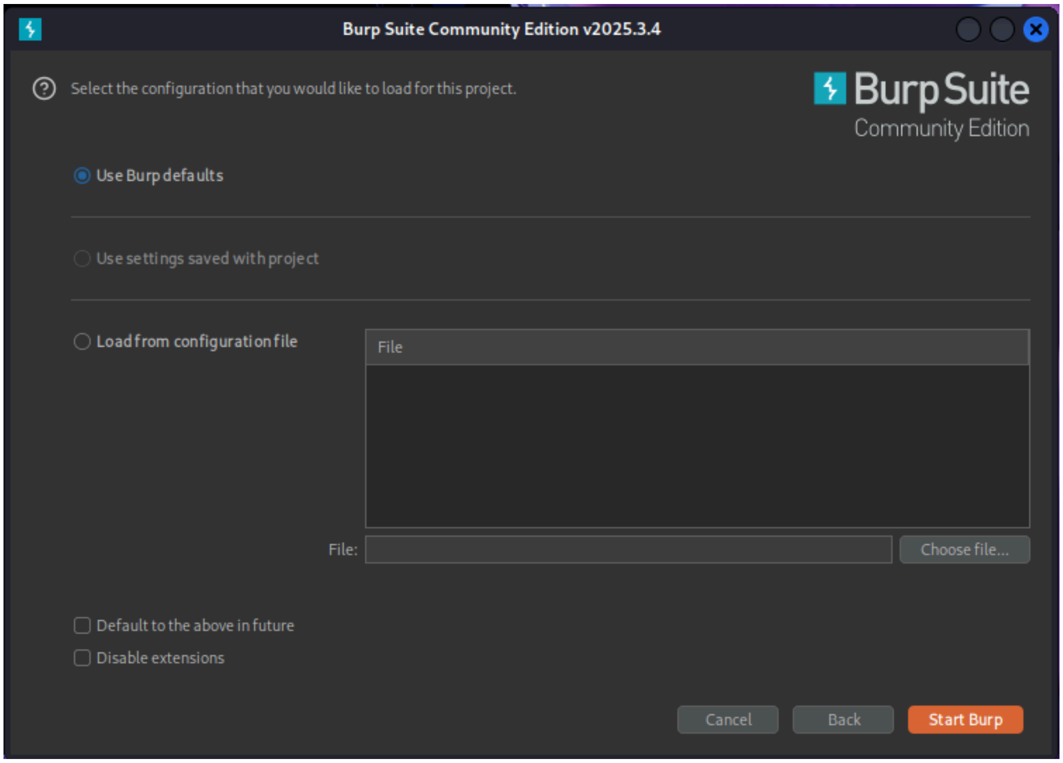
○ Open existing project

Name	File	Last Accessed

File:

☑ Trust this project file

☑ Pause Automated Tasks



Burp Suite Community Edition v2025.3.4

Select the configuration that you would like to load for this project.

● Use Burp defaults

○ Use settings saved with project

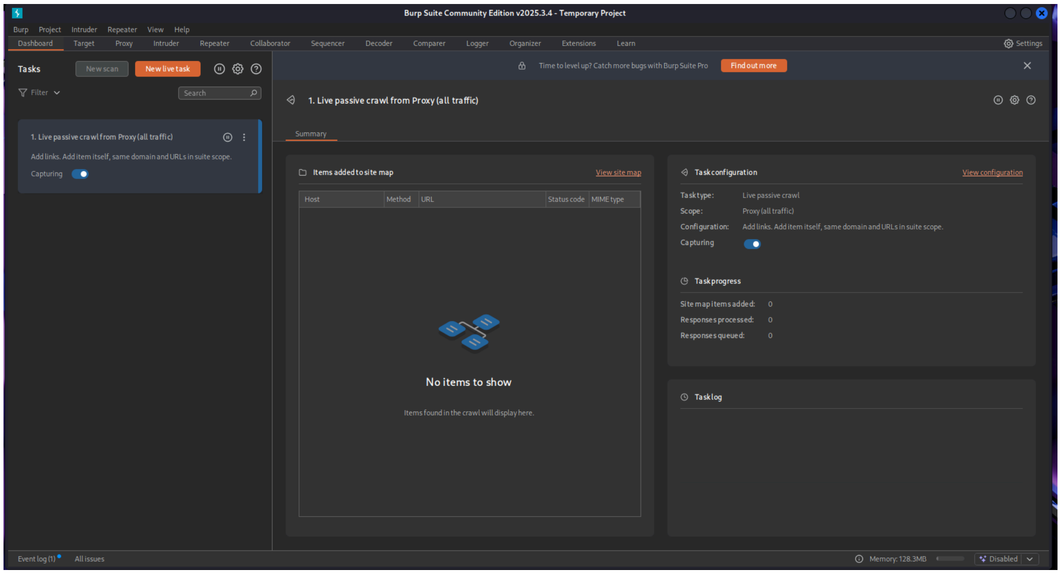
○ Load from configuration file

File

File:

☐ Default to the above in future

☐ Disable extensions



Time to level up? Catch more bugs with Burp Suite Pro

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite scope.

Capturing

No items to show

Items found in the crawl will display here.

Task type: Live passive crawl

Scope: Proxy (all traffic)

Configuration: Add links. Add item itself, same domain and URLs in suite scope.

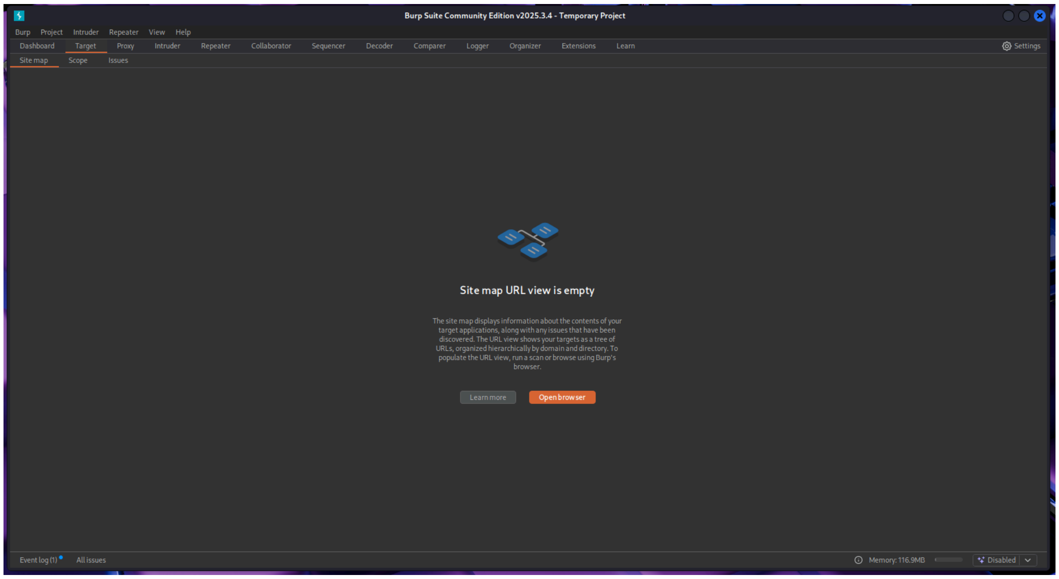
Capturing

Site map items added: 0

Responses processed: 0

Responses queued: 0

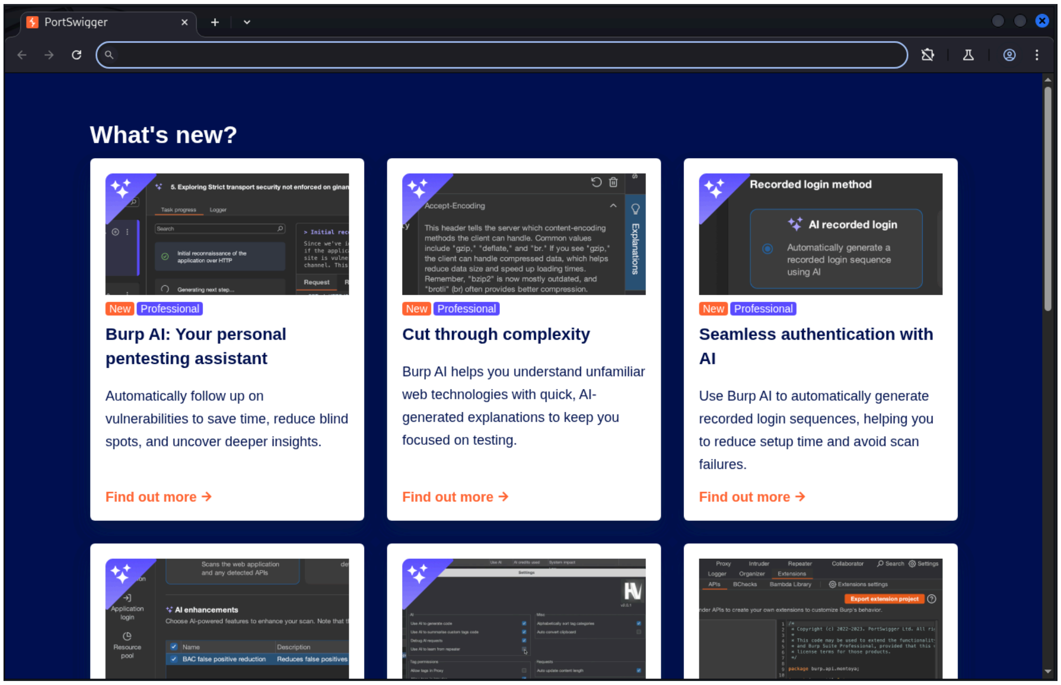
2. Now, open the chromium browser from the burpsuite and search for the site you want to perform brute force on.


Burp Suite Community Edition v2025.3.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Site map Scope Issues
Learn more
Open browser
Event log (1)
All issues
Memory: 116.9MB
Disabled

Site map URL view is empty

The site map displays information about the contents of your target applications, along with any issues that have been discovered. The URL view shows your targets as a tree of URLs, organized hierarchically by domain and directory. To populate the URL view, run a scan or browse using Burp's browser.

23162171019



What's new?

New Professional

Burp AI: Your personal pentesting assistant

Automatically follow up on vulnerabilities to save time, reduce blind spots, and uncover deeper insights.

Find out more →

New Professional

Cut through complexity

Burp AI helps you understand unfamiliar web technologies with quick, AI-generated explanations to keep you focused on testing.

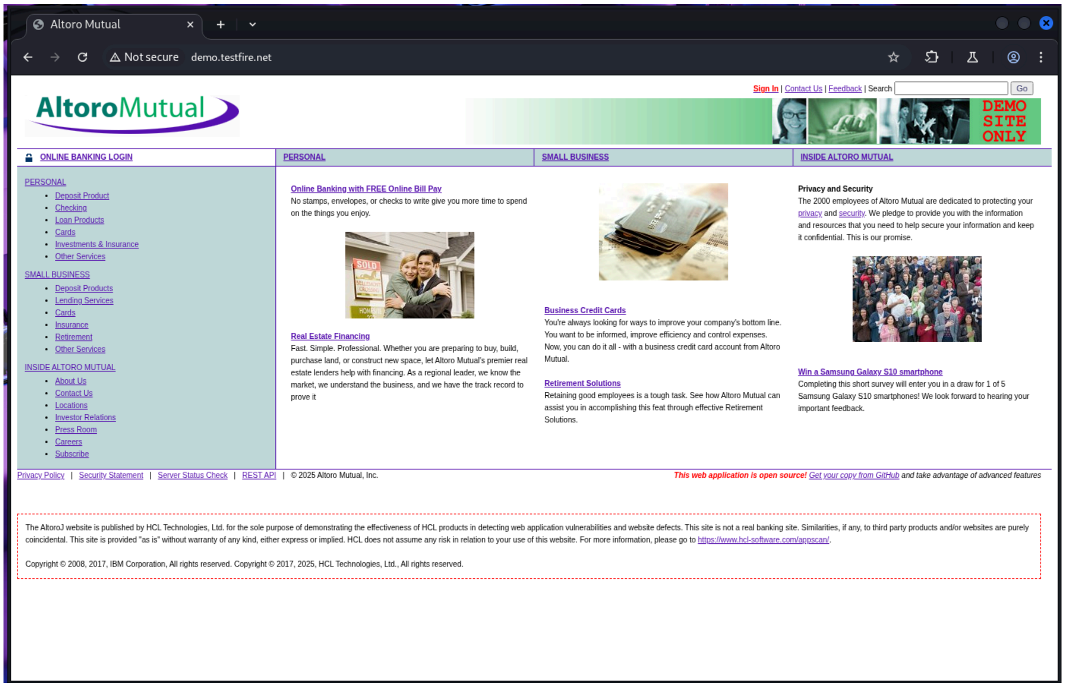
Find out more →

New Professional

Seamless authentication with AI

Use Burp AI to automatically generate recorded login sequences, helping you to reduce setup time and avoid scan failures.

Find out more →



Sign In | Contact Us | Feedback | Search

ONLINE BANKING LOGIN | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

PERSONAL
- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS
- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL
- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Online Banking with FREE Online Bill Pay
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.

Real Estate Financing
Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it

Business Credit Cards
You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.

Retirement Solutions
Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.

Privacy and Security
The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.

Win a Samsung Galaxy S10 smartphone
Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.

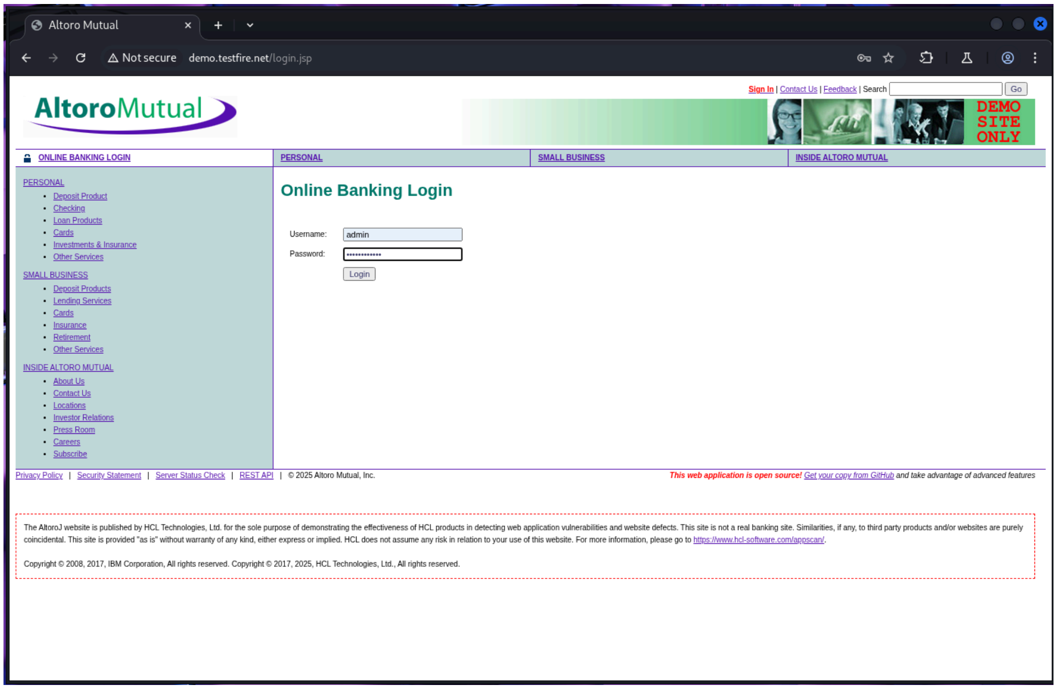
Privacy Policy | Security Statement | Server Status Check | REST API | © 2025 Altoro Mutual, Inc.

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, 2025, HCL Technologies, Ltd., All rights reserved.

3. Go to the login page, enter the correct username and any random password.



Online Banking Login

Username: admin

Password: ••••••••••••

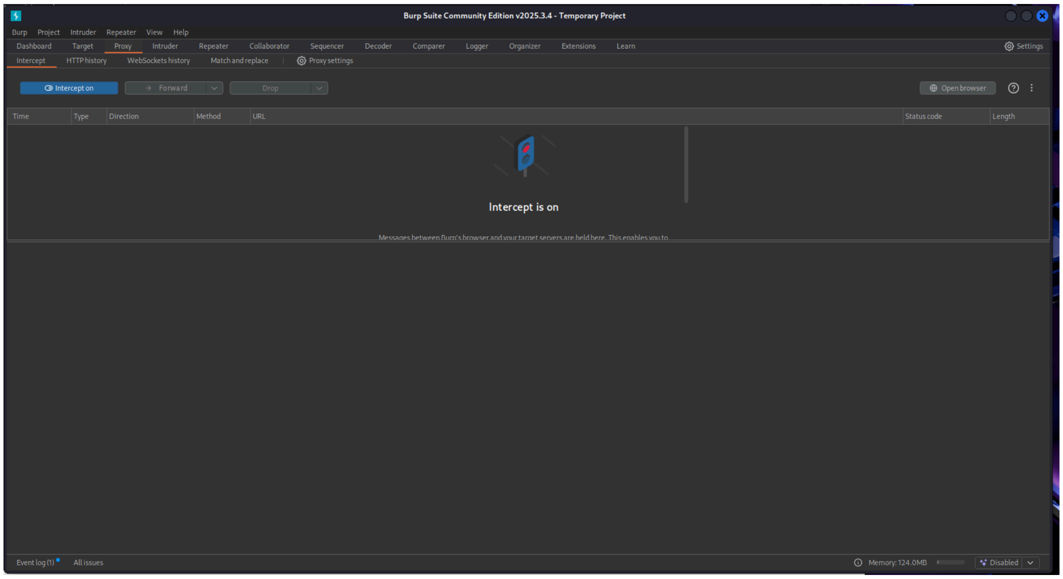
© 2025 Altoro Mutual, Inc.

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, 2025, HCL Technologies, Ltd., All rights reserved.

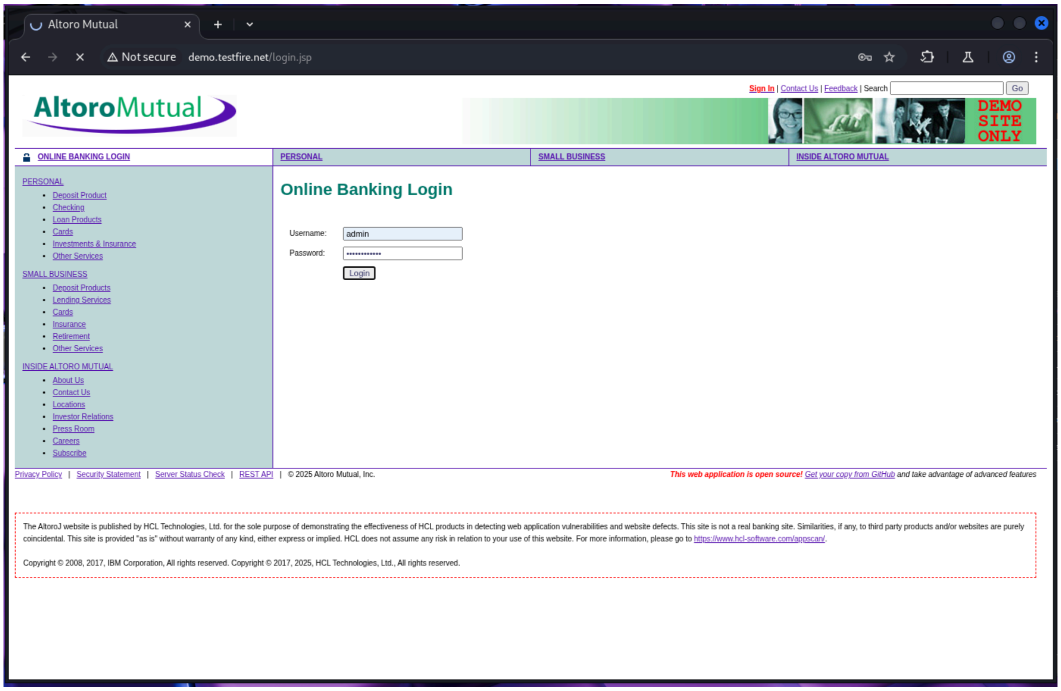
4. Before submitting, switch to burpsuite, go to the proxy tab and turn on the intercept.



Intercept is on

Messages between Burp's browser and your target servers are held here. This enables you to

5. Now, go back to the browser and submit the login form.



Online Banking Login

Username: admin

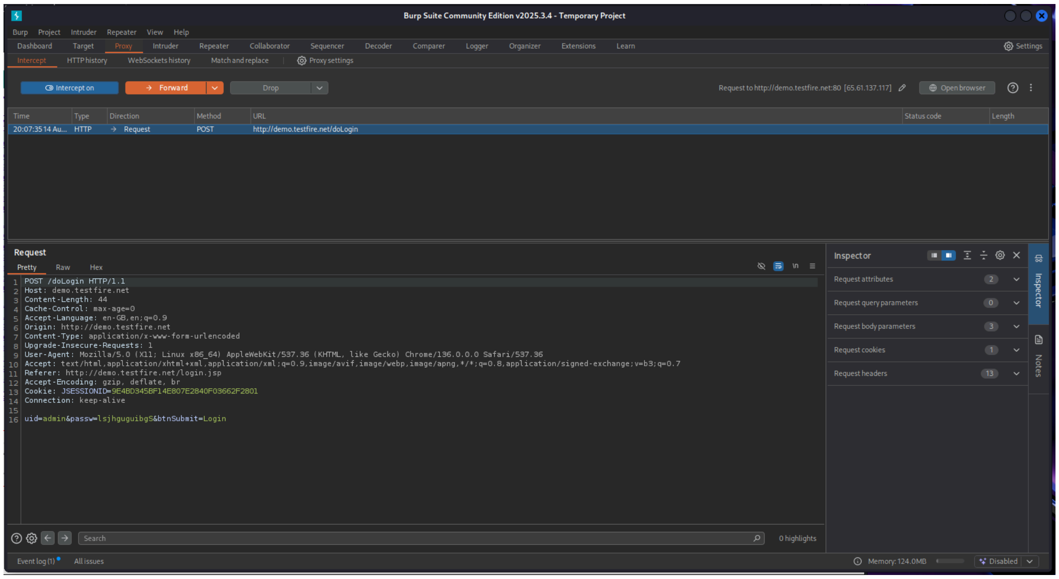
Password: ••••••••••••

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, 2025, HCL Technologies, Ltd., All rights reserved.

6. Now switch back to the burpsuite and click on the intercepted package.

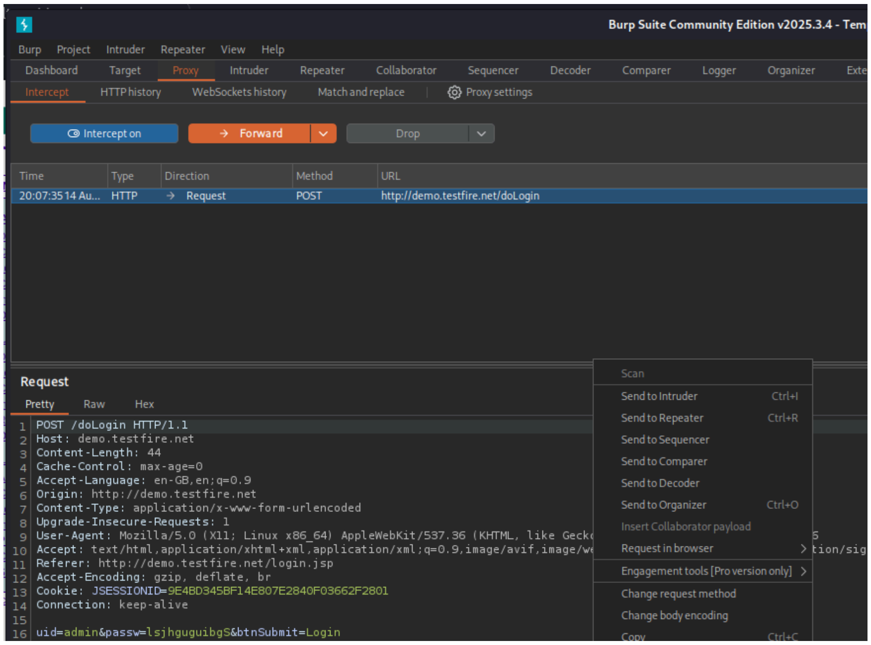

Burp Suite Community Edition v2025.3.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to http://demo.testfire.net:80 [65.61.137.117]
Open browser
Request
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 1
Request headers 13
Search
0 highlights
Event log (1) All issues
Memory: 124.0MB
Disabled
Inspector
Notes

Time	Type	Direction	Method	URL	Status code	Length
20:07:35 14 Au...	HTTP	→ Request	POST	http://demo.testfire.net/doLogin		

```
POST /doLogin HTTP/1.1
Host: demo.testfire.net
Content-Length: 44
Cache-Control: max-age=0
Accept-Language: en-GB,en;q=0.9
Origin: http://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://demo.testfire.net/login.jsp
Accept-Encoding: gzip, deflate, br
Cookie: JSESSIONID=9E4BD345BF14E807E2840F03662F2801
Connection: keep-alive

uid=admin&passw=lsjhguguibgS&btnSubmit=Login
```

7. Right click on the content of the package and select the ‘Send to intruder’ option.

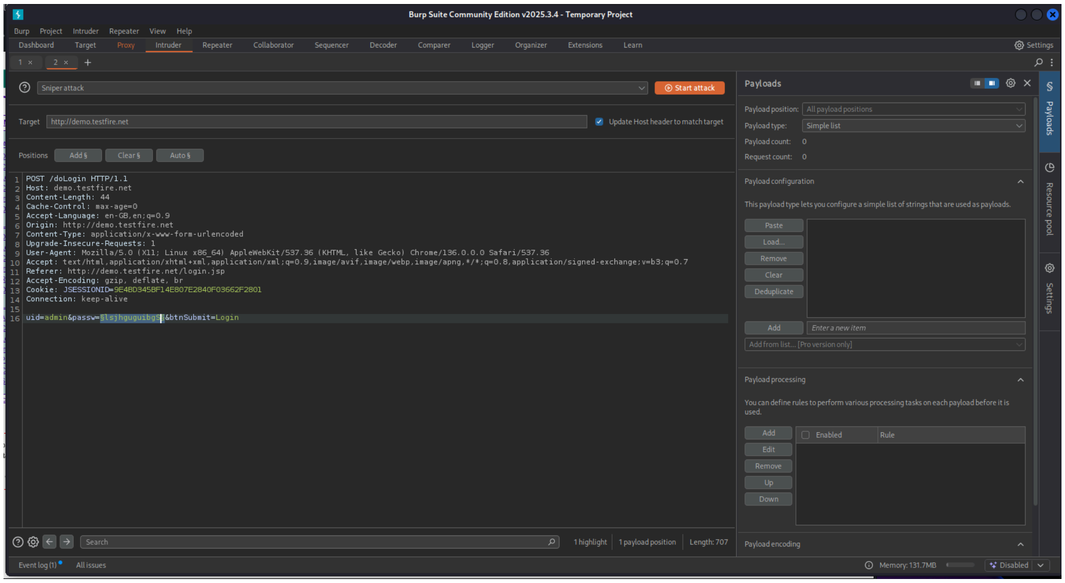

Burp Suite Community Edition v2025.3.4 - Tem
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Exte
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request
Pretty Raw Hex
Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Send to Organizer Ctrl+O
Insert Collaborator payload
Request in browser
Engagement tools [Pro version only]
Change request method
Change body encoding
Copy Ctrl+C

Time	Type	Direction	Method	URL
20:07:35 14 Au...	HTTP	→ Request	POST	http://demo.testfire.net/doLogin

```
POST /doLogin HTTP/1.1
Host: demo.testfire.net
Content-Length: 44
Cache-Control: max-age=0
Accept-Language: en-GB,en;q=0.9
Origin: http://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko                         5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w                          tion/sig
Referer: http://demo.testfire.net/login.jsp
Accept-Encoding: gzip, deflate, br
Cookie: JSESSIONID=9E4BD345BF14E807E2840F03662F2801
Connection: keep-alive

uid=admin&passw=lsjhguguibgS&btnSubmit=Login
```

8. Now go to Intruder and select the value of password and click on ‘Add §’ to select the content for payload.



Sniper attack

Target: http://demo.testfire.net

☑ Update Host header to match target

```
POST /doLogin HTTP/1.1
Host: demo.testfire.net
Content-Length: 44
Cache-Control: max-age=0
Accept-Language: en-GB,en;q=0.9
Origin: http://demo.testfire.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://demo.testfire.net/login.jsp
Accept-Encoding: gzip, deflate, br
Cookie: JSESSIONID=9E4BD345BF14E807E2840F03662F2801
Connection: keep-alive

uid=admin&passw=§lsjhguguibgS§&btnSubmit=Login
```

1 highlight | 1 payload position | Length: 707

Payload position: All payload positions
Payload type: Simple list
Payload count: 0
Request count: 0

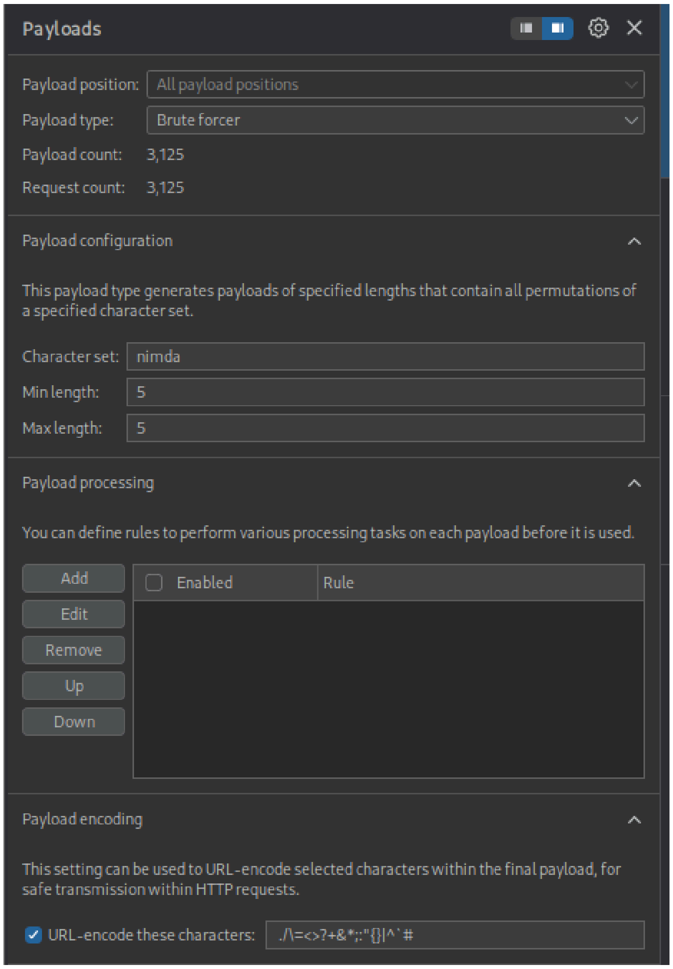
This payload type lets you configure a simple list of strings that are used as payloads.

You can define rules to perform various processing tasks on each payload before it is used.

☐ Enabled	Rule

Memory: 131.7MB

9. Choose brute forcer as payload type, select character set and the min and max length possible for the password.



Payloads

Payload position: All payload positions

Payload type: Brute forcer

Payload count: 3,125

Request count: 3,125

Payload configuration

This payload type generates payloads of specified lengths that contain all permutations of a specified character set.

Character set: nimda

Min length: 5

Max length: 5

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

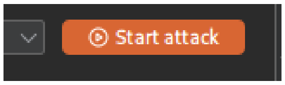
□ Enabled	Rule

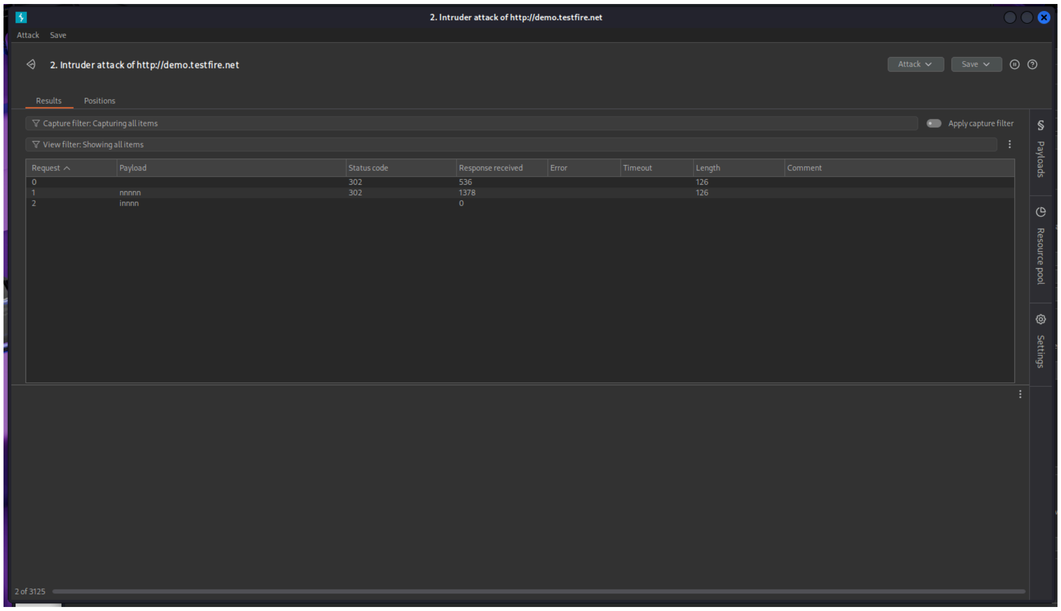
Payload encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☑ URL-encode these characters: ./\=<>?+&*;:"{}|^`#

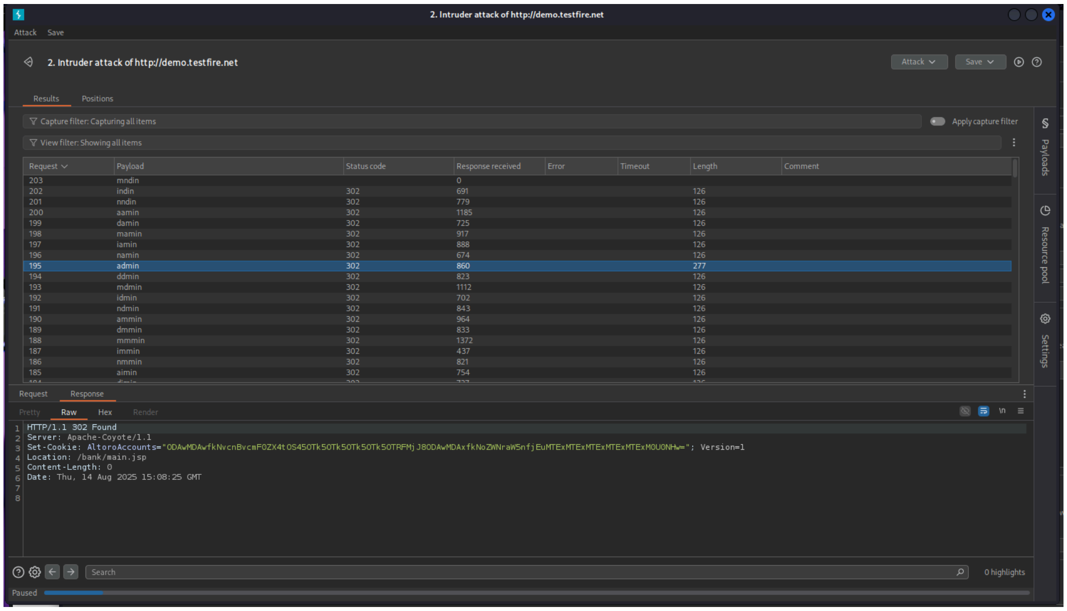
10. Now, to start brute forcing, click the ‘start attack’ button and wait for the process to finish.




2. Intruder attack of http://demo.testfire.net
Attack
Save
2. Intruder attack of http://demo.testfire.net
Attack
Save
Results
Positions
Capture filter: Capturing all items
Apply capture filter
View filter: Showing all items
Payloads
Resource pool
Settings
2 of 3125

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		302	536			126	
1	nnnnn	302	1378			126	
2	innnn		0				

11. The payload, for which the returned packet length is largest, is the correct password.

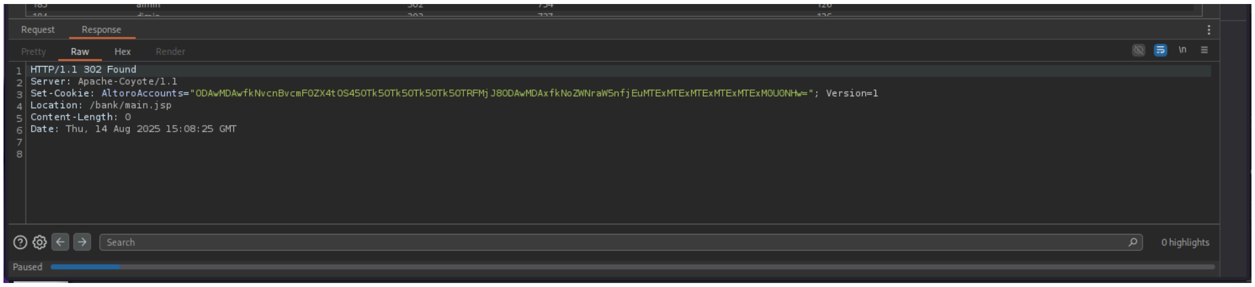

2. Intruder attack of http://demo.testfire.net
Attack
Save
2. Intruder attack of http://demo.testfire.net
Attack
Save
Results
Positions
Capture filter: Capturing all items
Apply capture filter
View filter: Showing all items
Payloads
Resource pool
Settings
Request
Response
Pretty
Raw
Hex
Render
Search
0 highlights
Paused

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
203	mndin		0				
202	indin	302	691			126	
201	nndin	302	779			126	
200	aamin	302	1185			126	
199	damin	302	725			126	
198	mamin	302	917			126	
197	iamin	302	888			126	
196	namin	302	674			126	
195	admin	302	860			277	
194	ddmin	302	823			126	
193	mdmin	302	1112			126	
192	idmin	302	702			126	
191	ndmin	302	843			126	
190	ammin	302	964			126	
189	dmmin	302	833			126	
188	mmmin	302	1372			126	
187	immin	302	437			126	
186	nmmin	302	821			126	
185	aimin	302	754			126	

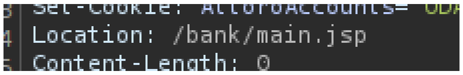
```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Set-Cookie: AltoroAccounts="ODAwMDAwfkNvcnBvcmF0ZX4tOS45OTk5OTk5OTk5OTk5OTRFMjJ8ODAwMDAxfkNoZWNraW5nfjEuMTExMTExMTExMTExMTExM0U0NHw="; Version=1
Location: /bank/main.jsp
Content-Length: 0
Date: Thu, 14 Aug 2025 15:08:25 GMT
```

12. Now, check the response that you received from the correct password, if it contains a path then you may (or may not if they already have taken necessary measures to prevent it) be able to access the page without logging in by just adding the path in the url.

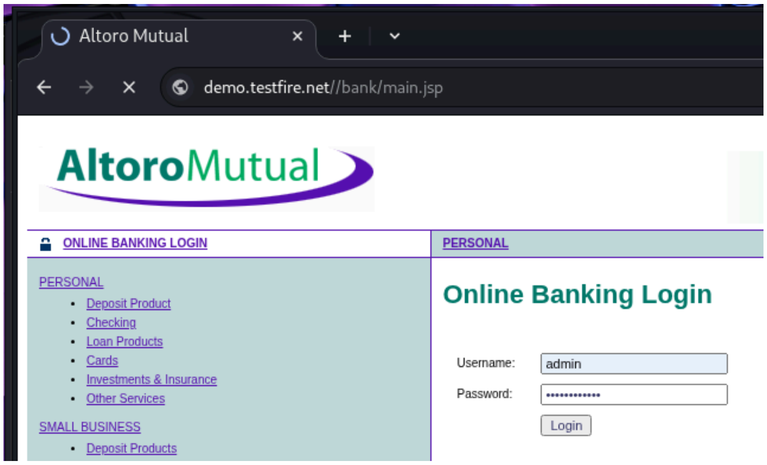
    Note : Remember to turn off intercept before performing this step.



```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Set-Cookie: AltoroAccounts="ODAwMDAwfkNvcnBvcmF0ZX4tOS45OTk5OTk5OTk5OTRFMjJ8ODAwMDAxfkNoZWNraW5nfjEuMTExMTExMTExMTExMTExM0U0NHw="; Version=1
Location: /bank/main.jsp
Content-Length: 0
Date: Thu, 14 Aug 2025 15:08:25 GMT
```



```
Set-Cookie: AltoroAccounts= ODA
Location: /bank/main.jsp
Content-Length: 0
```

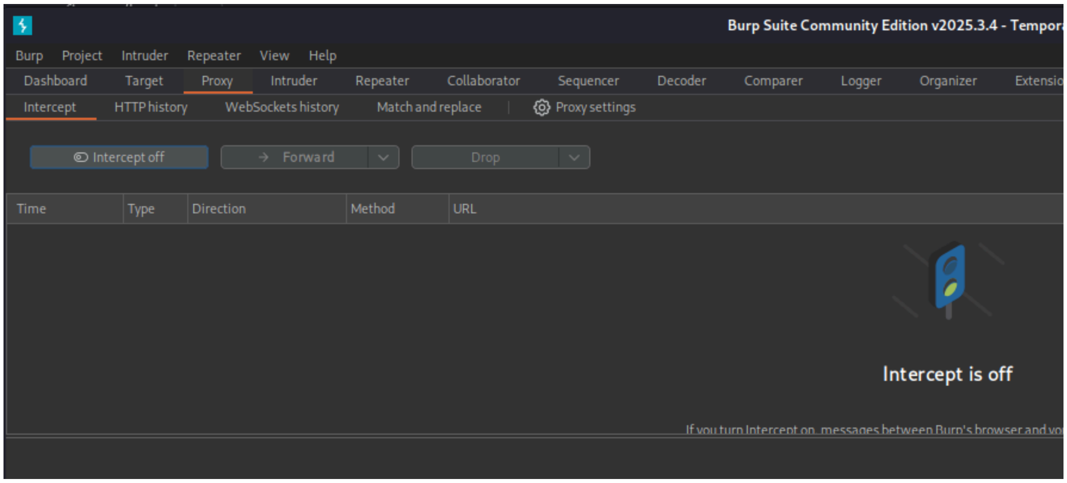


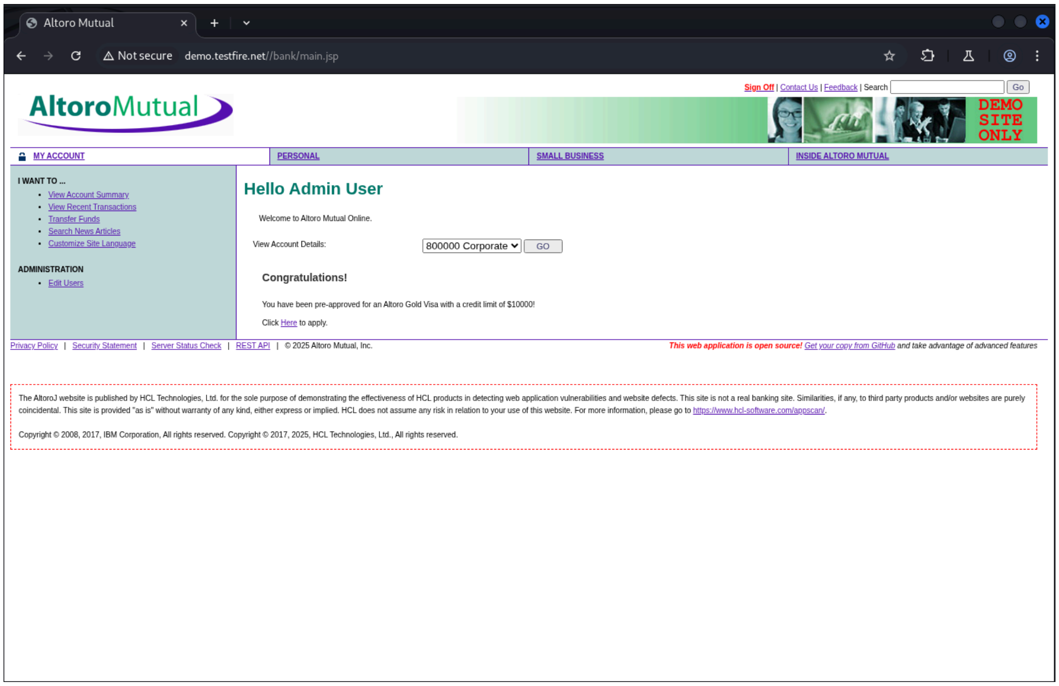
Online Banking Login

Username: admin

Password: ••••••••••••

Login





I WANT TO ...

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

ADMINISTRATION

- Edit Users

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate GO

Congratulations!

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

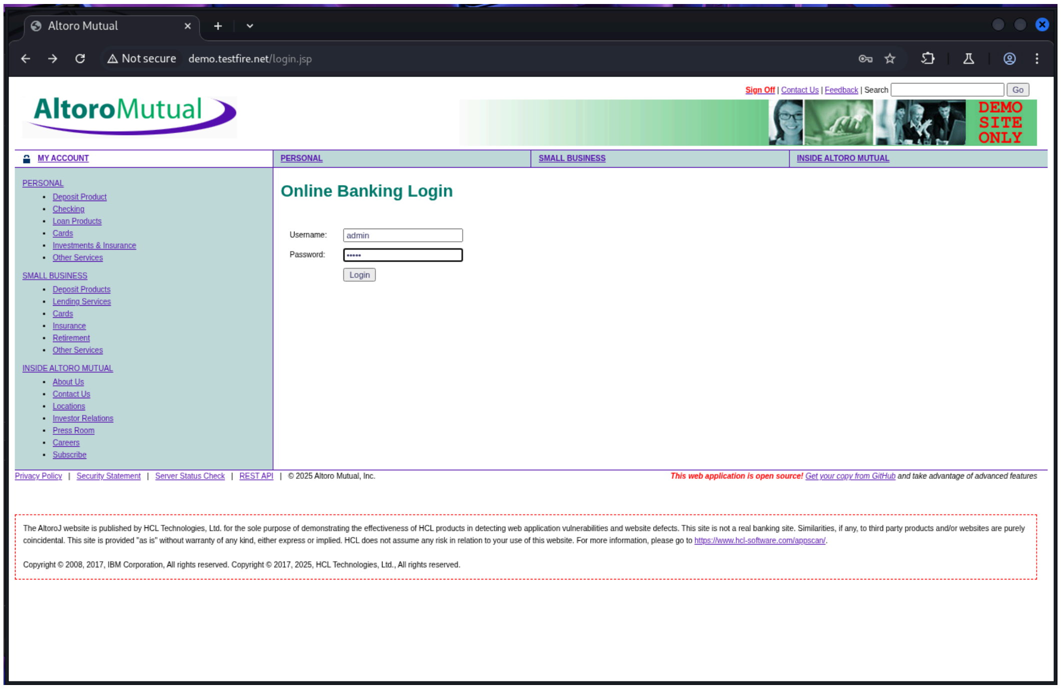
Click Here to apply.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2025 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, 2025, HCL Technologies, Ltd., All rights reserved.

13. And if step 12 fails, you can just login using the password through the normal way.



PERSONAL

- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL

- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Online Banking Login

Username: admin

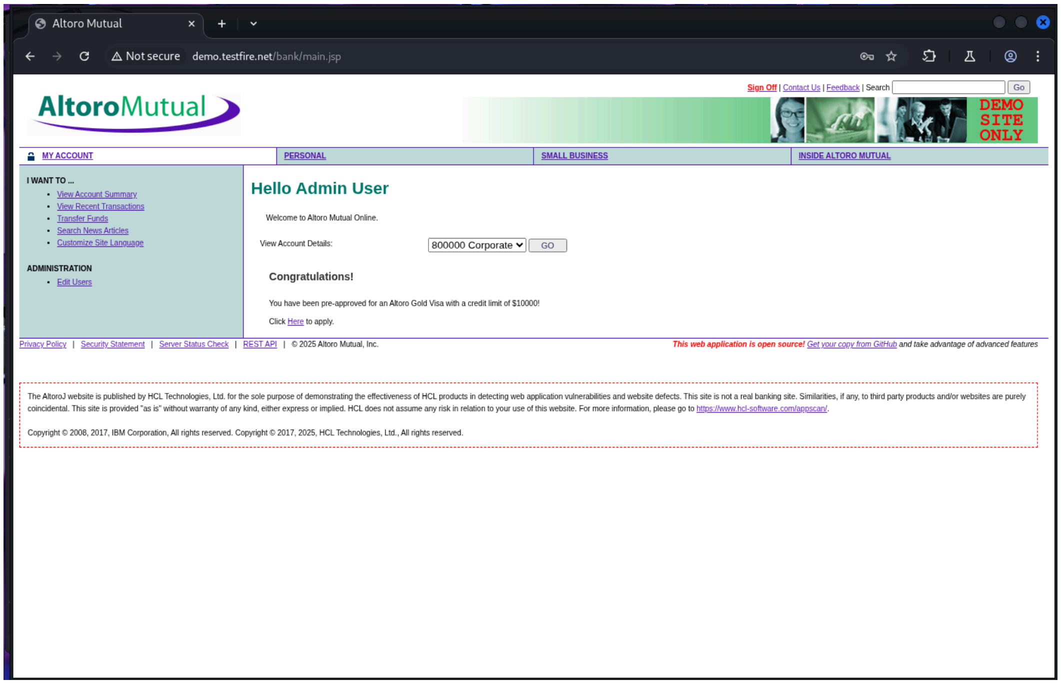
Password: •••••

Login

Privacy Policy | Security Statement | Server Status Check | REST API | © 2025 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, 2025, HCL Technologies, Ltd., All rights reserved.



Sign Off | Contact Us | Feedback | Search [ ] Go

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

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate GO

Congratulations!

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

Click Here to apply.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2025 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, 2025, HCL Technologies, Ltd., All rights reserved.