

ASSIGNMENT 4

TO USE AND LEARN BURSUIE

Introduction

Burp Suite is a widely recognized and highly regarded cybersecurity tool designed for web application security testing and assessment. It is an essential component of any cybersecurity professional's toolkit due to its versatility, robust feature set, and effectiveness in identifying vulnerabilities in web applications. This report explores what Burp Suite is, why it is used in cybersecurity, and its key features.

What is Burp Suite?

Burp Suite, developed by PortSwigger, is a comprehensive platform used for web security testing and penetration testing of web applications. It is primarily employed by security professionals, ethical hackers, and penetration testers to identify and remediate vulnerabilities in web applications, APIs, and other web services. The tool has gained popularity for its user-friendly interface and powerful capabilities, making it an indispensable tool for securing web applications.

Why is Burp Suite Used in Cybersecurity?

Burp Suite is used in cybersecurity for several compelling reasons:

1. Web Application Vulnerability Scanning:

One of the primary use cases for Burp Suite is to identify and assess vulnerabilities in web applications. It can automatically scan web applications for common security issues such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and more. By discovering these vulnerabilities, cybersecurity professionals can address them before malicious actors exploit them.

2. Manual Testing and Exploitation:

Burp Suite provides a powerful proxy tool that allows security experts to intercept and modify web traffic between the client and the web application server. This feature is particularly valuable for manual testing and exploiting vulnerabilities that automated scanners may miss. Ethical hackers can manipulate requests and responses to identify hidden flaws and weaknesses in the application.

3. Web Application Mapping:

Burp Suite assists in mapping the structure and functionality of web applications. It creates a detailed site map, providing insights into the application's architecture, endpoints, and potential attack surfaces. This mapping is crucial for planning security assessments and targeting specific areas of interest.

4. Reporting and Documentation:

The tool offers robust reporting capabilities, enabling users to generate detailed reports of identified vulnerabilities and their impact. These reports can be shared with development teams, allowing them to prioritize and fix security issues effectively.

5. Extensibility and Automation:

Burp Suite can be extended through its extensibility framework, which supports the development of custom plugins and scripts. This flexibility allows cybersecurity professionals to automate repetitive tasks, tailor the tool to their specific needs, and integrate it into their existing security workflow.

Features of Burp Suite

Burp Suite boasts a wide range of features that contribute to its popularity and effectiveness in cybersecurity:

1. Proxy:

Intercept and manipulate HTTP requests and responses. Control and analyze web traffic for security assessment.

2. Scanner:

Automated scanning for common vulnerabilities. Customizable scanning profiles. Real-time feedback and vulnerability identification.

3. Spider:

Automated web application mapping. Identifies links, parameters, and potential vulnerabilities. Creates an organized site map.

4. Intruder:

Automated and customizable payload-based testing. Brute force, fuzzing, and other attack techniques. Detailed results and data analysis.

5. Repeater:

Manual request/response editing and replay. Fine-grained control over HTTP requests. Efficient testing of specific vulnerabilities.

6. Sequencer:

Analyzes the quality of randomness in tokens and session identifiers. Helps identify predictable patterns.

Essential for session management and authentication testing.

7. Extensibility:

Supports custom extensions and plugins. API for automation and integration with other tools. A vibrant community creating and sharing extensions.

Conclusion


Burp Suite is a versatile and powerful cybersecurity tool trusted by professionals worldwide for web application security testing and penetration testing. Its extensive features, including scanning, proxying, mapping, and customization, make it an essential asset in identifying and mitigating vulnerabilities in web applications, contributing significantly to the overall security posture of organizations. Staying current with Burp Suite and its evolving capabilities is crucial for cybersecurity experts aiming to protect web applications effectively.

BYPASSING LOGIN USING BURPSUITE:


The image shows a screenshot of the Burp Suite interface. The top menu bar includes Burp, Project, Intruder, Repeater, View, and Help. The main toolbar contains Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. The Sequencer tab is active, showing a list of HTTP history items. Below the toolbar, there's a section for 'Intercept is off' with buttons for Forward, Drop, Intercept is off, Action, and Open browser. A message states: 'When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.' There are links for 'Learn more' and 'Open browser'.


Below the Burp Suite interface, there's a screenshot of a web browser displaying the Altoro Mutual website. The browser's address bar shows 'testfire.net'. The website has a green header with the Altoro Mutual logo and navigation links: Sign In, Contact Us, Feedback, Search, and Go. A 'DEMO SITE ONLY' banner is visible on the right. The main content area is divided into four columns: ONLINE BANKING LOGIN, PERSONAL, SMALL BUSINESS, and INSIDE ALTORO MUTUAL. The PERSONAL column includes links for Deposit Products, Checking, Loan Products, Cards, Investments & Insurance, and Other Services. The SMALL BUSINESS column includes links for Deposit Products, Lending Services, Cards, Insurance, Retirement, and Other Services. The INSIDE ALTORO MUTUAL column includes links for about Us, Contact Us, Locations, Investor Relations, Press Room, Careers, and Subscribe. The footer contains links for Privacy Policy, Security Statement, Server Status Check, REST API, and copyright information for Altoro Mutual, Inc. A disclaimer states: 'This web application is open source! Get your copy from GitHub and take advantage of advanced features.'


We go to sign in page:



[Sign In](#) | [Contact Us](#) | [Feedback](#) | Search






 ONLINE BANKING LOGIN	PERSONAL	SMALL BUSINESS	INSIDE ALTORO MUTUAL
<div> PERSONAL <ul style="list-style-type: none"> • Deposit Product • Checking • Loan Products • Cards • Investments & Insurance • Other Services </div> <div> SMALL BUSINESS <ul style="list-style-type: none"> • Deposit Products • Lending Services • Cards • Insurance • Retirement • Other Services </div> <div> INSIDE ALTORO MUTUAL <ul style="list-style-type: none"> • About Us • Contact Us • Locations • Investor Relations • Press Room • Careers • Subsidiary </div>	<div> <h2>Online Banking Login</h2> <div> Username: <input type="text"/> </div> <div> Password: <input type="password"/> </div> <div> <input type="button" value="Login"/> </div> </div>		

[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [BEST API](#) | © 2023 Altoro Mutual, Inc.






This web application is open source! [Get your copy from Github](#) and take advantage of advanced features


We assume that we only know the username and not the password of some user.

So we enter the username and any random password.



[Sign In](#) | [Contact Us](#) | [Feedback](#) | Search [Go](#)


ONLINE BANKING LOGIN

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

PERSONAL


SMALL BUSINESS

INSIDE ALTORO MUTUAL

Online Banking Login

Username:

Password:


This connection is not secure.
Logins entered here could be compromised. [Learn More](#)

[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [BEST API](#) | © 2023 Altoro Mutual, Inc.

This web application is open source! [Get your copy from GitHub](#) and take advantage of advanced features

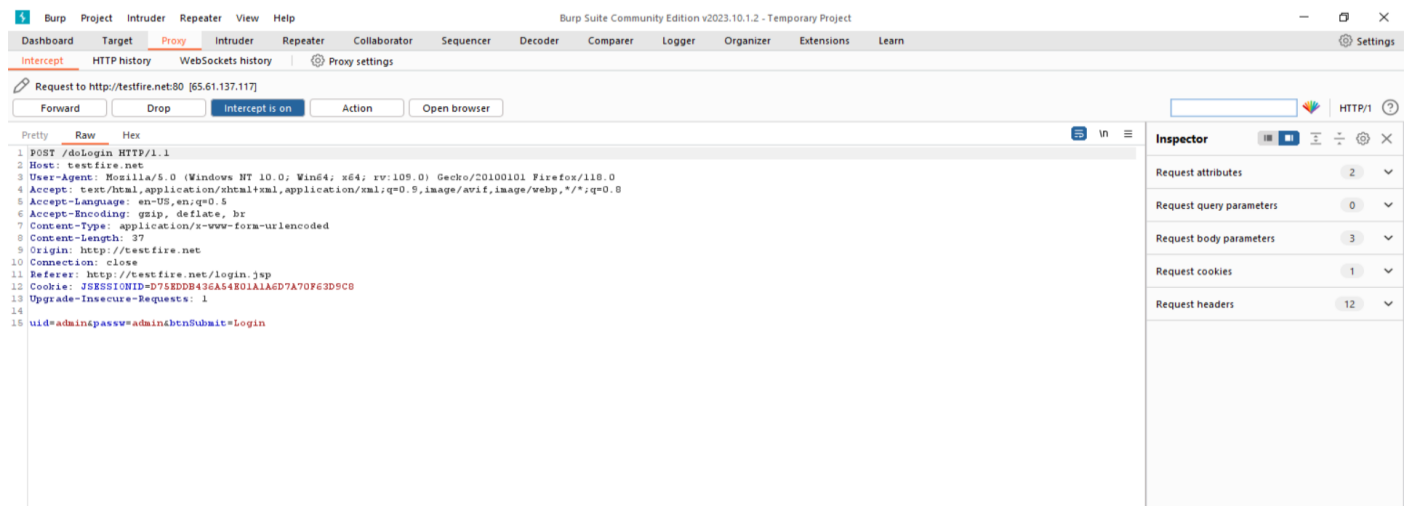
The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/us/en/subcategory/SW110>.

Copyright © 2008, 2023, IBM Corporation, All rights reserved.

Intercept is turned on:

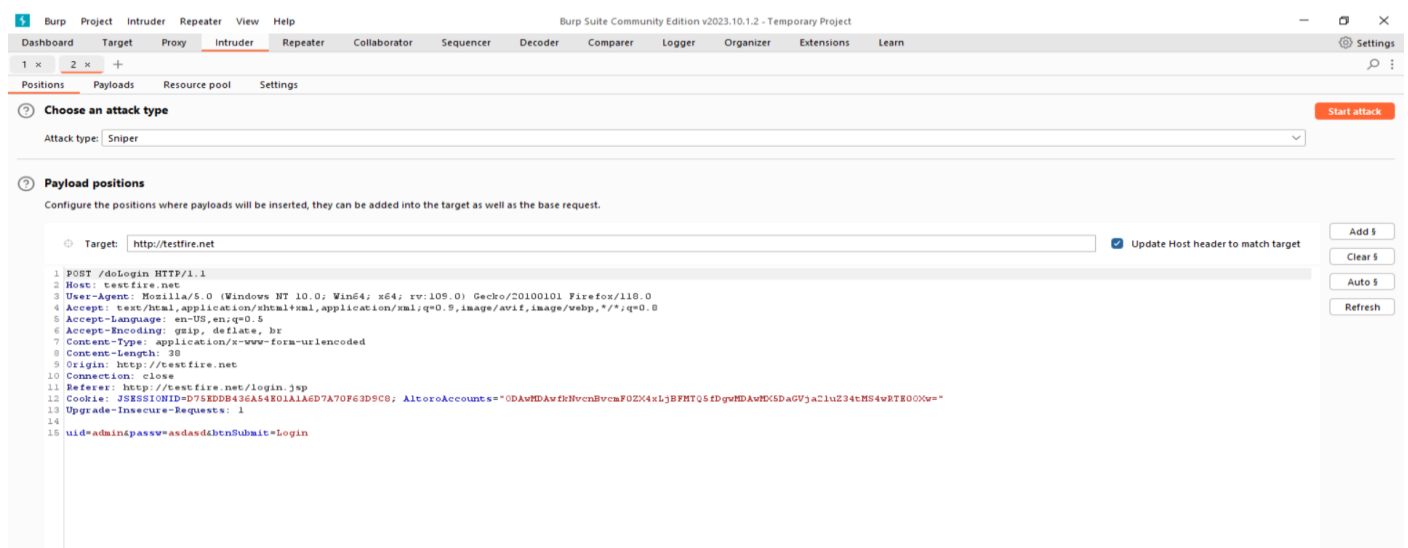
A screenshot of the Burp Suite web interface. At the top, there is a navigation bar with buttons: 'Forward', 'Drop', 'Intercept is on' (highlighted in blue), 'Action', and 'Open browser'. Below this, the main content area is mostly empty, with a large, faint watermark in the background that reads 'Burp Suite'. In the center of the page, there is a blue shield icon with a white padlock, indicating that interception is active. Below the icon, the text 'Intercept is on' is displayed in bold. Further down, a paragraph explains: 'Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.' At the bottom of this section, there are two buttons: 'Learn more' and 'Open browser'.

Now we click on the login button and get the request before it is sent to the server:

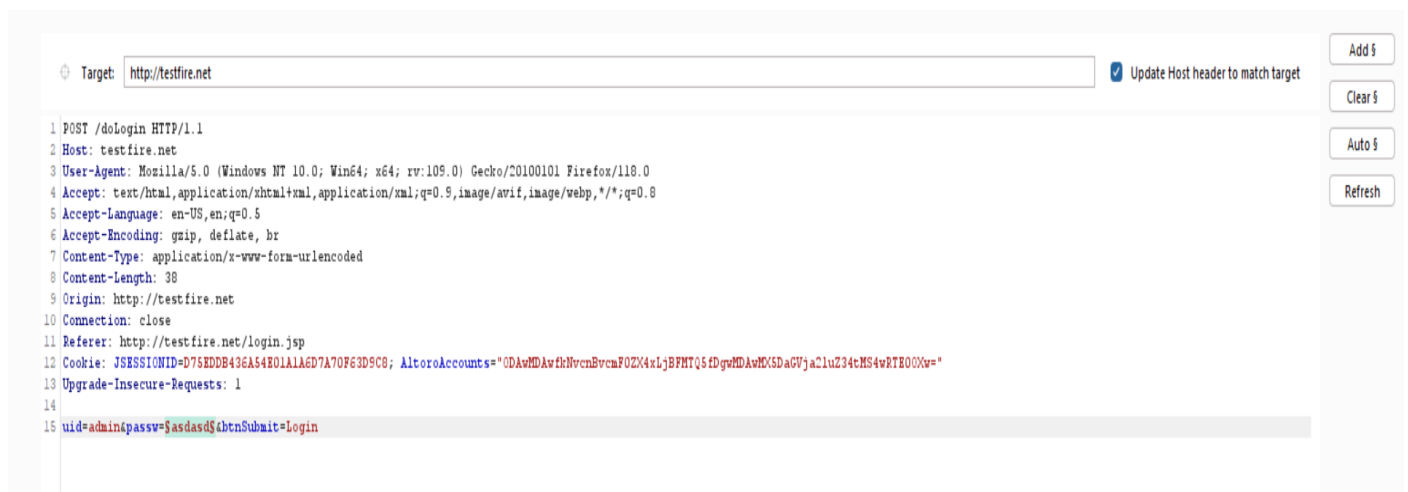


As we can see, we have several options like forward, drop or transfer the request.

We sent the request to the intruder and turn off the intercept:



We highlight the password and click on ADD:



Now we go to payloads and load our password list which contains all the possible combinations of passwords:

1 x2 x+

PositionsPayloadsResource poolSettings

?

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set:1

Payload count:15

Payload type:Simple list

Request count:15

?

Payload settings [Simple list]

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

Paste

Load ...

Remove

Clear

Deduplicate

Add

Add from list ... [Pro version only]

1234

password

4321

asdasd

lvndkvdf

mohit

abhau

Password

Pass

Enter a new item

?

Payload processing

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

Add

Edit

Remove

Up

Down

Enabled

Rule

We start our attack:

1 x2 x+

DashboardTargetProxyIntruderRepeaterViewHelp

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerOrganizerExtensionsLearn

PositionsPayloadsResource poolSettings

?

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set:1

Payload count:15

Payload type:Simple list

Request count:15

?

Payload settings [Simple list]

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

Paste

Load ...

Remove

Clear

Deduplicate

Add

Add from list ... [Pro version only]

1234

password

4321

asdasd

lvndkvdf

mohit

abhau

Password

Pass

Enter a new item

?

Payload processing

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

Add

Edit

Remove

Up

Down

Enabled

Rule

AttackSaveColumns2. Intruder attack of http://testfire.net - Temporary attack - Not saved to project file

ResultsPositionsPayloadsResource poolSettings

Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length	Comment
4	asdasd	302			126	
5	lvndkvdf	302			126	
6	mohit	302			126	
7	abhau	302			126	
8	Password	302			126	
9	Pass	302			126	
10	Blue	302			126	
11	Red	302			126	
12	Yellow	302			126	
13	admin	302			241	
14	ADMIN	302			241	
15	Admin	302			241	

Finished


Now we see in the finished result of our attack, three passwords have different values. So one of these three can be our correct password.

Results	Positions	Payloads	Resource pool	Settings		
Filter: Showing all items						
Request ^	Payload	Status code	Error	Timeout	Length	Comment
4	asdasd	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
5	lvndkvdf	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
6	mohit	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
7	abhau	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
8	Password	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
9	Pass	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
10	Blue	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
11	Red	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
12	Yellow	302	<input type="checkbox"/>	<input type="checkbox"/>	126	
13	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	241	
14	ADMIN	302	<input type="checkbox"/>	<input type="checkbox"/>	241	
15	Admin	302	<input type="checkbox"/>	<input type="checkbox"/>	241	

We again go to the sign in page and try our first possible password as “admin”:

AltoroMutual

[Sign Off](#) | [Contact Us](#) | [Feedback](#) | Search



DEMO
SITE
ONLY

MY ACCOUNT

PERSONAL

SMALL BUSINESS

INSIDE ALTORO MUTUAL

PERSONAL

SMALL BUSINESS

INSIDE ALTORO MUTUAL

Deposit Product

Checking

Loan Products

Cards

Investments & Insurance

Other Services

Deposit Products

Lending Services

Cards

Insurance

Retirement

Other Services

About Us

Contact Us

Locations

Investor Relations

Press Room

Careers

Subscribe

Online Banking Login

Username:

Password:


Privacy Policy | Security Statement | Server Status Check | [BEST API](#) | © 2023 Altoro Mutual, Inc.

This web application is open source! [Get your copy from GitHub](#) and take advantage of advanced features

We get successfully log in!!

AltoroMutual

[Sign Off](#) | [Contact Us](#) | [Feedback](#) | Search



DEMO
SITE
ONLY

MY ACCOUNT

PERSONAL

SMALL BUSINESS

INSIDE ALTORO MUTUAL

I WANT TO ...

ADMINISTRATION

View Account Summary

View Recent Transactions

Transfer Funds

Search News Articles

Customize Site Language

Edit Users

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details:

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 | [BEST API](#) | © 2023 Altoro Mutual, Inc.

This web application is open source! [Get your copy from GitHub](#) and take advantage of advanced features

The AltoroI website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM 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. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/us/en/subcategory/SW110>.

Copyright © 2008, 2023, IBM Corporation, All rights reserved.