



# 27 Use Cases



# Burp Suite



## *for Penetration Testers*



Rajneesh Gupta  
[@rajneeshcyber](#)

# TABLE OF CONTENT

Topic	Page
Introduction to Burp Suite	3
Key Modules in Burp Suite	4
Burp Suite Pro vs Community	5
27 Use Cases of Burp-Suite for Penetration Tester	6
Conclusion	34

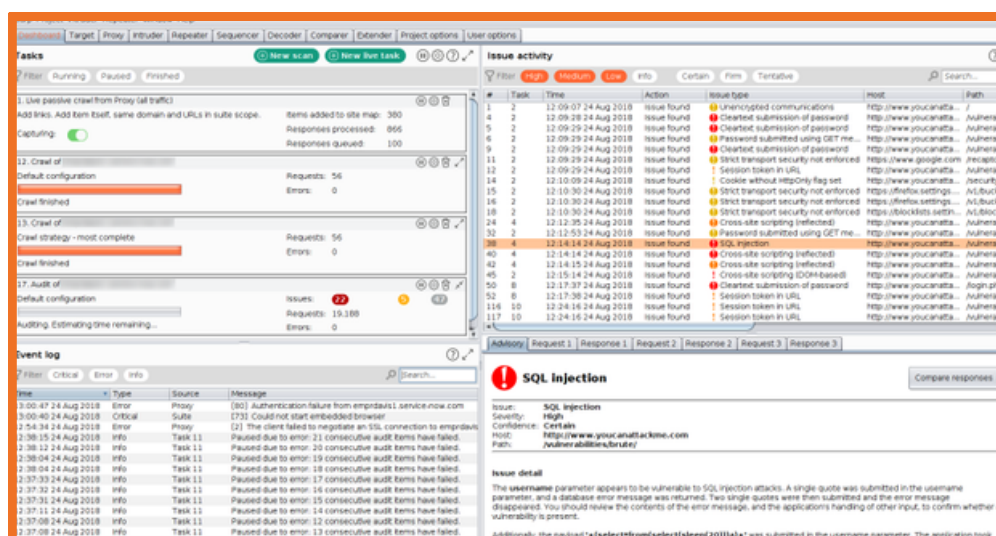
# INTRODUCTION TO BURP SUITE

## What is Burp Suite?

- Burp Suite is a powerful web application security testing tool.
- It provides both manual and automated testing options.
- Widely used by security professionals and pen testers for identifying vulnerabilities.

## Key Features

- Proxy for intercepting traffic between browser and web applications.
- Manual Testing Tools like Repeater and Intruder for precise attacks.
- Automated Scanner in Pro version for comprehensive vulnerability detection.



# KEY MODULES IN BURP SUITE

## *Proxy*

- Intercepts and inspects all HTTP/S traffic between browser and server.
- Allows manual modification of requests and responses.

## *Repeater*

- Used to send and modify individual HTTP requests repeatedly for testing.
- Useful for testing input parameters and observing server behavior.

## *Intruder*

- Automates attacks like brute-force, fuzzing, and parameter manipulation.
- Allows for sending large volumes of requests with custom payloads.

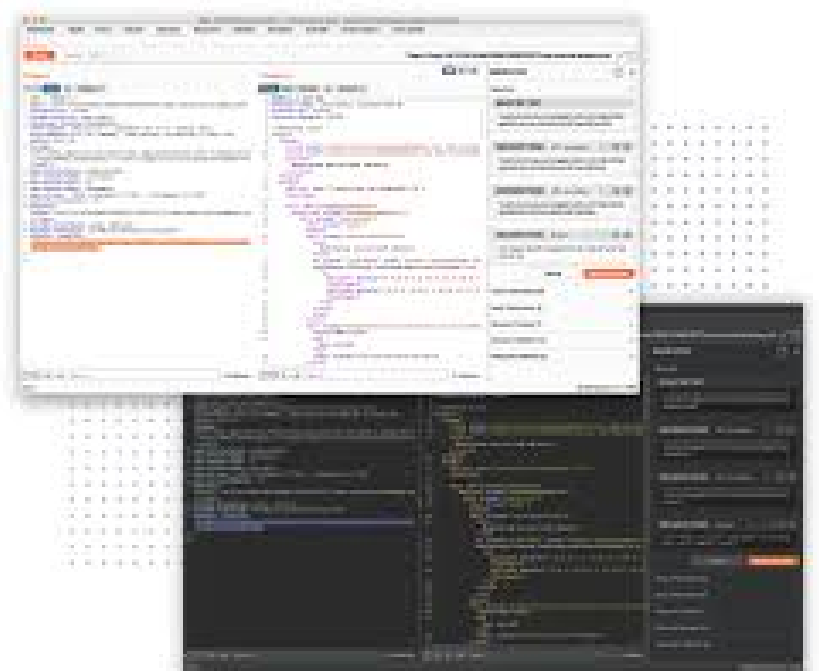
# BURP SUITE PRO VS COMMUNITY

## *Community Version*

- Provides essential manual testing tools like Proxy, Repeater, and Intruder.
- Suitable for beginners and manual penetration testers.

## *Pro Version*

- Includes all features of Community, plus Automated Scanning for vulnerabilities.
- Supports CI/CD integration, fuzzing, and advanced test configurations.
- Ideal for comprehensive, automated security testing in professional environments.



# 27 USE CASES OF BURP-SUITE

*for Penetration Testers*

NEXT





# AUTOMATED VULNERABILITY SCANNING

## *Purpose*

Identify common vulnerabilities automatically across web applications.

## *How Burp Suite Helps*

- Use the Pro Scanner to run a comprehensive vulnerability scan.
- Customize scans for specific web architectures and functionality.
- Schedule scans to run automatically for continuous security monitoring.

## *Analysis*

Review scan reports, prioritize high-risk issues, and manually verify to reduce false positives.

License: Pro



 **HANDS-ON GUIDE**

# 2

## MANUAL PENETRATION TESTING

### *Purpose*

Perform hands-on testing to explore specific areas of a web app.

### *How Burp Suite Helps*

- Use Repeater to manually craft and send HTTP requests repeatedly.
- Set Breakpoints to intercept and modify HTTP requests/responses.
- Test different input scenarios using Intruder to simulate attacks.

### *Analysis*

Analyze server responses and behavior to detect weaknesses, document findings, and propose security fixes.

License: Community and Pro

CLICK  
HERE

👉 **HANDS-ON GUIDE**



# 3

## MANUAL PENETRATION TESTING

### *Purpose*

Perform hands-on testing to explore specific areas of a web app.

### *How Burp Suite Helps*

- The Pro Scanner automatically scans for reflected, stored, and DOM-based XSS.
- Use Intruder to inject XSS payloads into form fields and URL parameters.
- Manually test potential XSS vectors using Repeater for targeted checks.

### *Analysis*

Verify that user input is properly sanitized or encoded, and implement Content Security Policy (CSP) headers to mitigate XSS risks.

License: Community and Pro



 **HANDS-ON GUIDE**

# 4

## SQL INJECTION DETECTION

### *Purpose*

Detect SQL injection vulnerabilities that allow attackers to manipulate backend databases.

### *How Burp Suite Helps*

- Use Intruder to inject SQL payloads into form fields, headers, and URLs.
- The Pro Scanner automates SQLi detection during scans.
- Manually test query parameters in Repeater to observe database interaction

### *Analysis*

Inspect responses for database error messages or abnormal behavior. Recommend using parameterized queries or stored procedures to prevent SQL injection.

License: Community and Pro



 **HANDS-ON GUIDE**

# 5

## SESSION MANAGEMENT TESTING

### *Purpose*

Test the security of session management, such as session fixation and hijacking.

### *How Burp Suite Helps*

- Modify session cookies and tokens using Repeater and check for security issues.
- Use Passive Scanning to inspect cookie attributes like Secure and HttpOnly.
- Test for session fixation vulnerabilities by altering session IDs.

### *Analysis*

Ensure that session cookies have secure attributes and that sessions are properly invalidated upon logout. Implement secure session management practices.

License: Community and Pro



 **HANDS-ON GUIDE**

# 6

## SSL/TLS MISCONFIGURATION DETECTION

### *Purpose*

Detect SSL/TLS configuration issues that weaken encryption.

### *How Burp Suite Helps*

- The Pro Scanner checks for weak ciphers and insecure SSL configurations.
- Use Passive Scanning to identify expired certificates or weak protocols like TLS 1.0.
- Manually inspect SSL/TLS traffic and certificates in Repeater.

### *Analysis*

Ensure strong encryption protocols (e.g., TLS 1.2 or higher) and up-to-date certificates are in use. Enable HTTP Strict Transport Security (HSTS) to enforce secure connections.

License: Community and Pro



 **HANDS-ON GUIDE**



# CSRF (CROSS-SITE REQUEST FORGERY) DETECTION

## *Purpose*

Identify CSRF vulnerabilities that allow unauthorized actions by tricking authenticated users.

## *How Burp Suite Helps*

- The Pro Scanner automatically tests forms and endpoints for missing CSRF tokens.
- Manually inspect sensitive actions with Repeater by omitting or modifying CSRF tokens.
- Test the validity of anti-CSRF measures by attempting to replay requests.

## *Analysis*

Verify that all sensitive actions are protected by anti-CSRF tokens. Recommend implementing token-based CSRF prevention mechanisms.

License: Community and Pro



 **HANDS-ON GUIDE**

# 8

## AUTHENTICATION TESTING

### *Purpose*

Assess the robustness of authentication mechanisms and check for vulnerabilities like weak passwords and session fixation.

### *How Burp Suite Helps*

- Use Intruder to brute force login forms using a common password list.
- Manually test login responses and session handling using Repeater.
- Use Passive Scanning to detect weak password policies and insecure session cookies.

### *Analysis*

Ensure strong password policies, enforce multi-factor authentication (MFA), and use session expiration after inactivity.

License: Community and Pro



 **HANDS-ON GUIDE**

# 9

## FILE UPLOAD TESTING

### *Purpose*

Ensure that file upload functionality is secure to avoid issues like remote code execution.

### *How Burp Suite Helps*

- Use Intruder to test file uploads with various payloads (e.g., executable files, large files).
- Manually upload files through Repeater and inspect server responses.
- Test upload restrictions by modifying file names and content types.

### *Analysis*

Verify that file types are properly restricted and stored securely. Recommend implementing file scanning and size limits.

License: Community and Pro



**HANDS-ON GUIDE**

# DIRECTORY TRAVERSAL DETECTION

## *Purpose*

Detect vulnerabilities that allow unauthorized access to directories or files via path traversal.

## *How Burp Suite Helps*

- Use Intruder to inject directory traversal payloads (e.g., ../../etc/passwd).
- The Pro Scanner automatically detects directory traversal vulnerabilities.
- Test file paths manually with Repeater to validate restricted access.

## *Analysis*

Ensure that user input is properly sanitized and sensitive directories are protected. Implement access controls to block unauthorized file access.

License: Community and Pro



 **HANDS-ON GUIDE**



# DENIAL OF SERVICE (DOS) TESTING

## *Purpose*

Test for vulnerabilities that allow DoS attacks to overwhelm a web server.

## *How Burp Suite Helps*

- Use Intruder to simulate large volumes of requests to stress-test specific endpoints.
- Upload large files via Repeater and observe server response times.
- Integrate Pro-only extensions to simulate various DoS attack vectors.

## *Analysis*

Review server performance under load and implement rate limiting, resource throttling, and DoS prevention mechanisms.

License: Pro



 **HANDS-ON GUIDE**

# INPUT VALIDATION TESTING

## *Purpose*

Test the web application's input validation mechanisms for weaknesses.

## *How Burp Suite Helps*

- Use Intruder to inject various payloads, such as HTML tags, JavaScript, and SQL statements, to test input validation.
- Manually submit crafted inputs using Repeater and observe responses.
- The Pro Scanner checks input fields for common vulnerabilities.

## *Analysis*

Review the application's response to malformed inputs and verify that inputs are properly sanitized and validated server-side.

License: Community and Pro



 **HANDS-ON GUIDE**

# ERROR HANDLING TESTING

## *Purpose*

Ensure that error messages do not reveal sensitive information, such as stack traces or system details.

## *How Burp Suite Helps*

- Use Intruder to send invalid inputs and observe error messages.
- Manually trigger errors via Repeater and analyze the responses.
- The Pro Scanner identifies verbose error messages that may leak sensitive information.

## *Analysis*

Ensure error messages are generic and do not expose internal details. Recommend implementing secure error handling practices to avoid information leakage.

License: Community and Pro

# BRUTE FORCE ATTACK SIMULATION

## *Purpose*

Test login forms for susceptibility to brute force attacks.

## *How Burp Suite Helps*

- Use Intruder to perform a brute force attack by testing various username/password combinations.
- Adjust request timing and parameters to mimic realistic brute force attempts.
- Monitor login page behavior in Repeater during brute force attempts.

## *Analysis*

Detect weak authentication mechanisms and implement account lockout policies, CAPTCHA, and multi-factor authentication to mitigate brute force attacks.

License: Community and Pro



 **HANDS-ON GUIDE**

# URL MANIPULATION TESTING

## *Purpose*

Test URL parameters for manipulation that could lead to unauthorized access or data exposure.

## *How Burp Suite Helps*

- Use Intruder to manipulate URL parameters systematically.
- Manually modify URL parameters using Repeater and observe responses.
- The Pro Scanner flags issues related to parameter tampering automatically.

## *Analysis*

Ensure the application validates URL parameters server-side and does not rely solely on client-side controls. Implement strict access controls for sensitive resources.

License: Community and Pro

# HTTP SECURITY HEADER TESTING

## *Purpose*

Ensure HTTP security headers, such as CSP and HSTS, are properly implemented to mitigate attacks like XSS and clickjacking.

## *How Burp Suite Helps*

- Use Passive Scanning to analyze HTTP responses for missing or weak security headers.
- The Pro Scanner detects missing or misconfigured security headers automatically.
- Manually review headers in HTTP responses using Repeater.

## *Analysis*

Ensure proper implementation of headers like Content Security Policy (CSP), X-Frame-Options, and Strict-Transport-Security (HSTS). Add missing security headers and refine existing ones.

License: Community and Pro

# API SECURITY TESTING

## *Purpose*

Test REST and SOAP APIs for vulnerabilities, such as injection attacks and unauthorized access.

## *How Burp Suite Helps*

- Use Repeater to manually craft and send API requests for testing.
- The Pro Scanner automatically detects vulnerabilities in API endpoints.
- Use Intruder to test API parameters for injections and authentication bypass.

## *Analysis*

Ensure API endpoints enforce proper authentication and validation. Secure APIs with token-based authentication and validate all inputs.

License: Community and Pro



 **HANDS-ON GUIDE**

# SERVER-SIDE REQUEST FORGERY (SSRF) DETECTION

## *Purpose*

Detect SSRF vulnerabilities that allow attackers to make unauthorized server-side requests.

## *How Burp Suite Helps*

- Use Intruder to send crafted URLs targeting internal systems or sensitive resources.
- Manually craft requests with potential SSRF payloads using Repeater.
- The Pro Scanner detects SSRF issues during automated scans.

## *Analysis*

Check if internal resources or URLs are accessible via crafted SSRF requests. Ensure proper input validation and restrict outbound requests to internal systems.



License: Community and Pro

 **HANDS-ON GUIDE**



# INFORMATION DISCLOSURE DETECTION

## *Purpose*

Ensure no sensitive data is exposed in headers, error messages, or server responses.

## *How Burp Suite Helps*

- Use Passive Scanning to detect sensitive information leaks, like server names or internal paths.
- The Pro Scanner automatically flags information disclosure vulnerabilities.
- Manually inspect responses in Repeater to check for sensitive data exposure.

## *Analysis*

Review responses for exposed internal details (e.g., server stack traces, API keys). Apply secure error handling and minimize sensitive information exposure.

License: Community and Pro

# CONTENT SECURITY POLICY (CSP) TESTING

## *Purpose*

Ensure that CSP headers are properly implemented to mitigate XSS and other injection attacks.

## *How Burp Suite Helps*

- Use Passive Scan to check for missing or misconfigured CSP headers in HTTP responses.
- The Pro Scanner flags weak or missing CSP headers during automated scans.
- Manually inspect HTTP responses in Repeater for CSP configurations.

## *Analysis*

Ensure that CSP restricts content sources to trusted domains. Review and refine the CSP to prevent inline scripts and unsafe resources.

License: Community and Pro



 **HANDS-ON GUIDE**

# FORCEFUL BROWSING DETECTION

## *Purpose*

Detect if sensitive resources like admin panels or backup files are accessible without proper authorization.

## *How Burp Suite Helps*

- Use Intruder to send requests for hidden resources (e.g., /admin, /backup.zip).
- The Pro Scanner detects unprotected files and directories during automated scans.
- Manually browse unlinked files using Repeater or Spider.

## *Analysis*

Ensure that sensitive resources are properly protected by authentication mechanisms. Apply access control measures and secure directory structures.

License: Community and Pro

# HTTP PARAMETER POLLUTION (HPP) TESTING

## *Purpose*

Identify vulnerabilities caused by multiple HTTP parameters with the same name leading to unpredictable behavior.

## *How Burp Suite Helps*

- Use Intruder to send requests with duplicate parameters.
- The Pro Scanner automatically detects HPP vulnerabilities in web applications.
- Manually test HPP vectors using Repeater to see how the server processes multiple parameters.

## *Analysis*

Ensure that the application handles duplicate parameters securely and does not merge or ignore them incorrectly. Implement input validation and normalization.

License: Community and Pro

# BROKEN ACCESS CONTROL TESTING

## *Purpose*

Identify access control issues where users can access resources they should not be authorized for.

## *How Burp Suite Helps*

- Use Intruder to manipulate access control parameters or tokens.
- Manually alter session tokens or user IDs in Repeater to test for privilege escalation.
- The Pro Scanner detects common access control vulnerabilities automatically.

## *Analysis*

Ensure proper role-based access control is enforced server-side. Test for broken access controls and recommend implementing the least privilege principle.

License: Community and Pro



 **HANDS-ON GUIDE**

# JSON WEB TOKEN (JWT)

## SECURITY TESTING

### *Purpose*

Identify access control issues where users can access resources they should not be authorized for.

### *How Burp Suite Helps*

- Use Repeater to send requests with manipulated JWTs and check for signature verification failures.
- The Pro Scanner flags weak or misconfigured JWTs during scans.
- Manually inspect token contents in Repeater and alter the payload or signature.

### *Analysis*

Ensure JWTs use strong encryption algorithms (e.g., HS256) and verify the signature on the server side. Implement secure storage for tokens.



License: Community and Pro

 **HANDS-ON GUIDE**

# HTTP FUZZING

## *Purpose*

Test endpoints by sending numerous variations of inputs to detect potential vulnerabilities.

## *How Burp Suite Helps*

- Use Intruder to send custom payloads or crafted input combinations to test input fields.
- Set payload positions in Intruder to test different parameters systematically.
- The Pro Scanner automates fuzzing with built-in payload lists.

## *Analysis*

Review responses for unexpected server behavior or crashes. Refine input validation to handle unusual or malformed inputs safely.

License: Community and Pro



 **HANDS-ON GUIDE**

# INPUT LENGTH TESTING

## *Purpose*

Identify vulnerabilities caused by excessively long inputs, such as buffer overflows.

## *How Burp Suite Helps*

- Use Intruder to send inputs with varying lengths to test how the server handles them.
- Manually send long input strings through Repeater and observe server responses.
- The Pro Scanner checks for issues related to input size and overflows.

## *Analysis*

Verify that the server correctly handles input length and does not crash or behave unexpectedly. Implement input length restrictions to prevent buffer overflows.

License: Community and Pro



# INPUT LENGTH TESTING

## *Purpose*

Identify server and application misconfigurations that could lead to vulnerabilities.

## *How Burp Suite Helps*

- Use the Pro Scanner to detect misconfigurations like open directories or insecure HTTP methods.
- Inspect HTTP responses for configuration issues like verbose server banners or outdated software versions.
- Use Passive Scanning to flag missing security headers or exposed server details.

## *Analysis*

Review server and application configurations for misconfigurations and vulnerabilities. Recommend applying best practices such as disabling unnecessary HTTP methods and securing server banners.

License: Community and Pro

# CONCLUSION

Burp Suite provides essential tools for robust web application security testing, making it a go-to solution for both manual and automated assessments. Key highlights include:

- Comprehensive vulnerability detection across both Community and Pro versions.
- Intruder and Repeater enable advanced payload testing and request manipulation.
- Pro Scanner automates complex security tests for broader coverage.
- Session, SSL, and authentication testing enhance the security of sensitive components.
- Fuzzing and brute-force tools help discover hidden vulnerabilities.
- Easy integration with CI/CD pipelines for continuous security testing.



Reach us at  
**hi@haxsecurity.com**

### Security Consulting

- Risk assessment
- Security Architecture
- SOC Set up

### Penetration testing

- Internal Pentest
- External Pentest
- Web App Pentest

### Training and Courses

- SOC Training
- Certification Training
- Vendor-specific learning

### Labs

- Hands-on Labs
- Career Path Labs
- Cyberrange for businesses