

What is Burp Suite? An Introduction to Web Security Testing

In today's digital landscape, web application security has become paramount. Burp Suite stands as one of the most trusted and widely-used platforms for identifying vulnerabilities before malicious actors can exploit them. Whether you're a budding security researcher, an experienced penetration tester, or simply curious about how professionals secure the web applications we use daily, understanding Burp Suite is an essential step in your cybersecurity journey.



Burp Suite: The Cybersecurity Swiss Army Knife

Developed by PortSwigger, Burp Suite has established itself as the gold standard in web application security testing. This comprehensive platform brings together an integrated suite of tools that work in harmony to identify, analyse, and exploit vulnerabilities in web applications and APIs.

With a user base exceeding 70,000 security professionals worldwide, Burp Suite has proven its worth across industries—from financial institutions protecting customer data to tech companies securing their platforms. What sets Burp Suite apart is its unique blend of manual testing capabilities and automated features, allowing security professionals to leverage both human intuition and computational power.

The platform's architecture is designed to support the entire security testing workflow, from initial reconnaissance and mapping to deep vulnerability analysis and exploitation. This holistic approach ensures that no stone is left unturned when assessing an application's security posture.

70,000+

Security professionals worldwide trust Burp Suite

Manual + Automated

Best of both testing approaches



Burp Suite Editions: Community vs Professional

Community Edition

Cost: Completely free

Best For: Students, beginners, hobbyists, and those learning web security fundamentals

Key Characteristics: Focuses on manual testing with core tools that teach foundational pentesting skills. No time limits or feature expiration—use it as long as you need to develop your expertise.

- Full access to Proxy, Repeater, and Intruder (with throttling)
- Target site mapping capabilities
- Perfect for small-scale testing and learning environments

Professional Edition

Cost: £350 per year (approximately £29/month)

Best For: Professional penetration testers, security consultants, and organisations conducting comprehensive security assessments

Key Characteristics: Adds enterprise-grade automation, advanced scanning engines, and productivity multipliers that dramatically accelerate testing workflows.

- Automated vulnerability scanning with smart detection
- Advanced session handling and macro recording
- Extensibility through BApp Store extensions
- Comprehensive reporting and collaboration features

The Community Edition provides an excellent foundation for understanding web security testing methodologies. As your skills progress and testing requirements grow more complex, the Professional Edition offers the advanced capabilities needed for enterprise-level assessments. Many security professionals begin with Community Edition to master the fundamentals before transitioning to Professional for commercial work.

Core Features of Burp Suite Community Edition

The Community Edition provides four essential tools that form the backbone of manual web application security testing. Each tool serves a distinct purpose in the security assessment workflow, and together they create a powerful testing environment.



Proxy

The foundation of all Burp Suite testing. Intercept, inspect, and modify HTTP/S traffic flowing between your browser and the target application. See everything your browser sends and receives.

- Intercept mode for real-time request modification
- HTTP history for reviewing past traffic
- Match and replace rules for automated modifications



Target

Automatically constructs a comprehensive site map as you interact with the application. Visualise the application's structure and identify all discoverable endpoints within your defined scope.

- Tree view of application structure
- Scope definition to focus testing efforts
- Detailed information about each discovered endpoint



Repeater

Your manual testing laboratory. Send requests repeatedly whilst modifying parameters, headers, or body content. Observe how subtle changes affect server responses—perfect for deep-dive vulnerability analysis.


- Side-by-side request and response viewing
- Syntax highlighting for easy reading
- Request history within each Repeater tab



Intruder

Automate customised attacks by defining payload positions and attack patterns. Excellent for fuzzing, credential testing, and discovering how applications handle various inputs.

- Multiple attack types (Sniper, Battering ram, Pitchfork, Cluster bomb)
- Built-in payload lists and generators
- Results sorting and filtering capabilities

 **Pro Tip:** Master these four tools and you'll have the foundation for 80% of manual web application security testing. The key is understanding when and how to use each tool in your testing workflow.

How Proxy Works in Community Edition

The Proxy tool is your window into the communication between browser and server—acting as an intelligent man-in-the-middle that captures every HTTP and HTTPS request. This visibility is fundamental to understanding how web applications truly work beneath their polished interfaces.

Key Capabilities

- **Intercept Mode:** Pause requests before they reach the server, allowing you to modify headers, parameters, cookies, or body content on the fly. This is invaluable for testing how applications handle unexpected or malicious input.
- **Traffic Inspection:** Examine the complete anatomy of each request and response—from HTTP methods and status codes to every header and byte of data transmitted.
- **SSL/TLS Decryption:** Burp Suite's CA certificate enables inspection of encrypted HTTPS traffic, ensuring no communication escapes analysis.
- **History Logging:** Every request and response is logged, creating an audit trail you can review and analyse at any time during your assessment.

01

Configure Browser

Set browser proxy settings to route traffic through Burp (typically localhost:8080)

02

Install CA Certificate

Import Burp's certificate to enable HTTPS interception

03

Enable Intercept

Turn on intercept mode to begin capturing traffic

04

Analyse & Modify

Inspect requests, make changes, and forward to server

Practical Example: Testing Authentication Security

Imagine you're testing a login form. With Proxy intercept enabled, you submit credentials and capture the authentication request. You might discover the application sends passwords in Base64 encoding (easily decoded) rather than proper encryption. You could modify the request to test for SQL injection by adding ' OR '1'='1 to the username field. You might also test whether the application properly validates session tokens by modifying or removing authentication cookies. Each of these tests begins with intercepting traffic through the Proxy—your first line of insight into application security.

Using the Target Tab: Mapping Your Attack Surface

Understanding your target application's structure is crucial before diving into security testing. The Target tab in Burp Suite Community Edition provides an automatic reconnaissance capability that builds a comprehensive map of the application as you interact with it through your browser.

Automatic Site Mapping

As traffic flows through Burp's Proxy, the Target tab intelligently catalogues every URL, parameter, and endpoint discovered. This creates a hierarchical tree view of the application's structure, revealing:

- All accessible pages and directories
- Query string parameters and their values
- Form fields and hidden inputs
- API endpoints and their methods
- Static resources (JavaScript, CSS, images)

This automated mapping saves countless hours of manual reconnaissance and ensures you don't overlook potential testing targets.

Scope Definition

Professional testing requires focus. The Target tab allows you to define exactly which hosts and URLs are "in scope" for your assessment. This is critical for:

- **Legal compliance:** Ensuring you only test authorised systems
- **Noise reduction:** Filtering out third-party resources (CDNs, analytics, ads)
- **Efficiency:** Concentrating efforts on relevant application components

Use regex patterns or simple URL matching to define scope boundaries. Burp Suite will then highlight in-scope items throughout the interface, keeping your assessment focused and organised.

Discovery Example: Hidden Admin Panels

Whilst browsing a public-facing website, the Target map reveals an unlinked `/admin` directory. This hidden endpoint, not accessible through normal navigation, becomes a high-priority testing target. Perhaps it lacks proper authentication, or uses default credentials—vulnerabilities you'd never find without comprehensive mapping.

Discovery Example: Undocumented APIs

Modern applications heavily rely on API calls invisible to users. The Target tab captures these background requests, exposing REST endpoints like `/api/v1/users` or `/api/orders`. These APIs often have different security controls than the main application and may reveal sensitive data or allow unauthorized actions when tested directly.

Repeater: Manual Testing Powerhouse

Repeater is where hypothesis becomes verification. This tool transforms Burp Suite from a passive observer into an active testing laboratory, allowing you to craft and refine attacks with surgical precision.

How Repeater Works

Right-click any request in Proxy history or Target map and select "Send to Repeater." The request appears in a new Repeater tab where you have complete control. Modify any aspect of the request—URL parameters, POST data, headers, cookies—then click "Send" to dispatch it to the server. The response appears immediately alongside your request for analysis.

This rapid iteration cycle—modify, send, analyse, repeat—enables deep exploration of application behaviour. Unlike one-off Proxy intercepts, Repeater lets you test variations systematically, building understanding of how the application processes input and generates output.

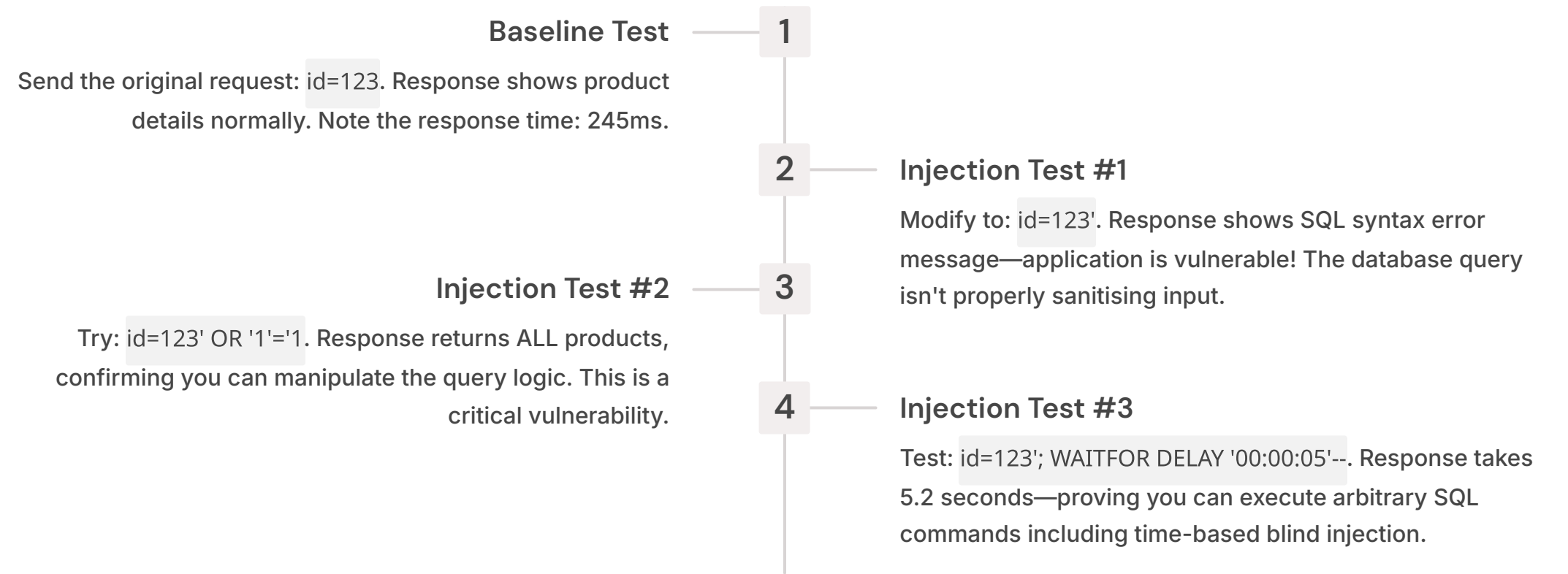
Key Features

- **Multiple tabs:** Test different endpoints simultaneously
- **Request history:** Navigate back through previous iterations
- **Syntax highlighting:** HTML, JSON, XML formatting for readability
- **Comparison mode:** Diff responses to spot subtle changes



Practical Example: Testing for SQL Injection

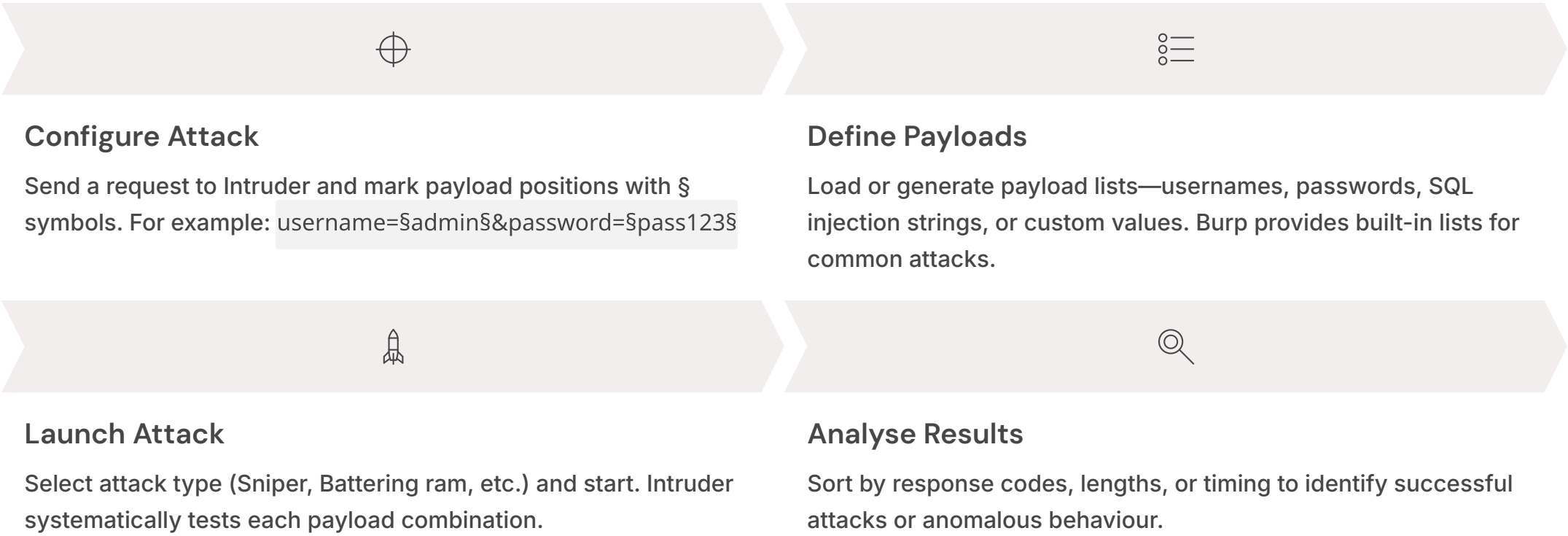
You've captured a product search request: `GET /products?id=123`. Send it to Repeater and begin systematic testing:



☐ **Security Note:** SQL injection consistently ranks among the most critical web vulnerabilities (OWASP Top 10). Repeater's methodical testing approach helps you not only identify the vulnerability but also understand its severity and exploitability.

Intruder: Automating Attacks in Community Edition

Whilst Repeater excels at targeted manual testing, Intruder brings automation to repetitive testing tasks. By defining payload positions and attack patterns, you can test hundreds or thousands of variations systematically.




Attack Types in Community Edition

<h3>Sniper</h3> <p>Tests one payload position at a time whilst keeping others static. Perfect for testing individual parameters.</p> <p>Use case: Testing password complexity by trying variations on a known username.</p>	<h3>Battering Ram</h3> <p>Uses the same payload in all positions simultaneously. Useful when parameters must match.</p> <p>Use case: Testing systems where username equals password (common default configurations).</p>	<h3>Pitchfork</h3> <p>Pairs payloads from multiple lists, testing them together in sequence.</p> <p>Use case: Testing username/password pairs from a credential stuffing list.</p>	<h3>Cluster Bomb</h3> <p>Tests all possible combinations of payloads across positions.</p> <p>Use case: Brute-forcing login with separate username and password lists.</p>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Practical Example: Account Enumeration

You're testing a login form at `/login`. You suspect the application reveals which usernames exist based on error messages. Configure Intruder with position: `username=$test$&password=wrongpass`. Load a payload list of common usernames (admin, user, test, administrator, etc.). Launch a Sniper attack.

Most responses return "Invalid credentials" with status 401. However, responses for "admin" and "administrator" return "Incorrect password" with status 200. This subtle difference reveals these accounts exist—an information disclosure vulnerability that aids targeted attacks.

 **Community Edition Limitation:** Intruder in Community Edition is throttled to prevent abuse, running at reduced speed. Despite this, it remains highly effective for testing moderate-sized payload sets and discovering vulnerabilities through automated fuzzing.

Limitations of Community Edition & When to Upgrade

Community Edition provides exceptional value for learning and manual testing, but understanding its limitations helps you recognise when your needs have outgrown the free tier.

Community Edition Constraints

No Automated Scanning

No passive or active vulnerability scanner. You must manually identify and test for vulnerabilities using Proxy, Repeater, and Intruder.

Throttled Intruder

Attack speed is intentionally limited, making large-scale fuzzing or brute-forcing impractical for time-sensitive assessments.

No Extensions

Cannot install BApp Store extensions that add specialized testing capabilities (e.g., CSRF token handling, advanced payloads, custom scanners).

Limited Automation

No session handling rules, macros, or scan scheduling. Manual intervention required for complex authentication flows.

No Collaboration

Cannot share projects or findings with team members. No built-in reporting for client deliverables.

Basic Scanner Detection

No intelligent vulnerability detection or exploitation assistance for complex attacks.

Professional Edition Advantages



Upgrading to Professional Edition (£350/year) unlocks enterprise capabilities:

- **Automated Scanning:** State-of-the-art vulnerability scanner detects SQL injection, XSS, SSRF, and dozens more vulnerability classes automatically
- **Full-Speed Intruder:** Unrestricted attack speeds for efficient large-scale testing
- **BApp Extensions:** Access hundreds of community and official extensions adding specialized testing capabilities
- **Session Handling:** Sophisticated macros handle complex authentication and maintain sessions during automated testing
- **Collaboration:** Share projects, save state, and generate professional reports
- **Scanner Insertion Points:** Advanced configuration for testing complex application architectures
- **Active Scan Optimization:** Intelligent scanning reduces false positives and testing time

When to Upgrade

Consider Professional if you're conducting commercial penetration tests, need to scale testing across multiple applications, require compliance reporting, or find manual testing bottlenecking your productivity. For learning, practicing, and occasional testing, Community Edition remains perfectly adequate.

Summary: Why Use Burp Suite Community Edition?

Burp Suite Community Edition represents an exceptional opportunity to develop professional web application security testing skills without financial barrier. It's a complete toolkit that provides everything needed to understand how modern web applications work—and how they break.

💰 Zero Cost, Maximum Value

Completely free with no trial periods, feature expiration, or hidden costs. Learn at your own pace with professional-grade tools.

🎓 Perfect Learning Platform

Master fundamental pentesting methodologies with Proxy, Repeater, Intruder, and Target—the same tools professionals use daily.

🔍 Real Vulnerability Discovery

Despite being free, Community Edition finds real vulnerabilities. SQL injection, XSS, authentication flaws—all discoverable through manual testing.

📈 Career Development

Burp Suite proficiency is a required skill for cybersecurity careers. Community Edition provides hands-on experience valued by employers.

Your Path Forward

1. **Download and Install:** Get Burp Suite Community Edition from PortSwigger's official website
2. **Practice Environments:** Use legal practice platforms like OWASP WebGoat, HackTheBox, or TryHackMe
3. **Master the Core Four:** Focus on Proxy, Target, Repeater, and Intruder until they become second nature
4. **Study Vulnerabilities:** Understand OWASP Top 10 vulnerabilities and how to test for them manually
5. **Document Everything:** Develop reporting skills by documenting findings, reproduction steps, and remediation advice
6. **Join Communities:** Engage with the cybersecurity community through forums, Discord servers, and bug bounty platforms

When your skills advance and professional opportunities arise, upgrading to Professional Edition adds automation and productivity features that transform how you work. But that journey begins here, with Community Edition—your gateway to professional web application security testing.



📌 **Remember:** With great power comes great responsibility. Only test applications you own or have explicit written permission to assess. Unauthorised security testing is illegal and unethical. Use Burp Suite to build a safer internet, not to cause harm.