



Web Security

Exploiting and patching
vulnerabilities on the
web.





OUTLINE FOR TODAY

01

Required Software

Please install Burp Suite if you have not already!

02

Overview of Burp Suite

Tools like Repeater, Intruder, etc.

03





OWASP Juice Shop

Attack a live insecure website, fix security bugs

Install Burp Suite Community Edition

 PortSwigger

LOGIN

Products  Solutions  Research | Academy | Support  



Burp Suite Enterprise Edition

The enterprise-enabled dynamic web vulnerability scanner.



Burp Suite Professional

The world's #1 web penetration testing toolkit.



Burp Suite Community Edition

The best manual tools to start web security testing.



Dastardly, from Burp Suite

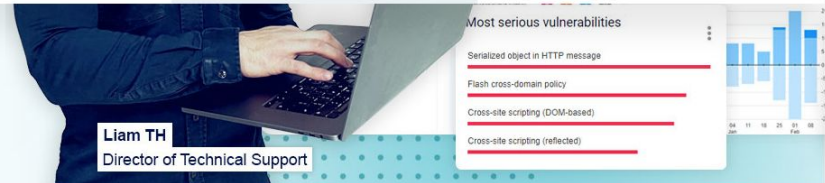
Free, lightweight web application security scanning for CI/CD.

[View all product editions](#) →

[FIND OUT MORE](#)

Account and subscription management

Information on ordering, pricing, and more.



Liam TH
Director of Technical Support

Most serious vulnerabilities

- Serialized object in HTTP message
- Flash cross-domain policy
- Cross-site scripting (DOM-based)
- Cross-site scripting (reflected)



"Best in class for security testing"



"A must-have tool for security engineers"



Install Burp Suite Community Edition

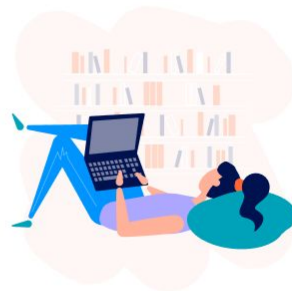
Burp Suite Community Edition

Start your web security testing journey for free - download our essential manual toolkit.

Enter your email to download

DOWNLOAD

[Go straight to downloads →](#)



Professional / Community 2023.2.3

Stable

10 March 2023 at 14:29 UTC

Burp Suite Community Edition ▾

Windows (64-bit) ▾

DOWNLOAD

[show checksums](#)

This release provides improved support for WebSocket functionality in the Montoya API, as well as a number of minor improvements and bug fixes.

Why Use Burp Suite?

- Keep a log of web traffic
- View and modify HTTP requests/responses on a website
- Suite of tools:
 - Proxy
 - View all traffic routed through the Burp proxy
 - Intercept and modify requests
 - Intruder
 - Brute force HTTP requests by parameters, endpoints, HTTP headers, etc.
 - Repeater
 - Repeating a previous HTTP request with modifications
 -
 -
 -

Burp Suite Proxy



Browser

Request is sent from the browser to Burp Suite.



Burp Suite

Allows for the modification of request data.
Forwards the request to the web server.

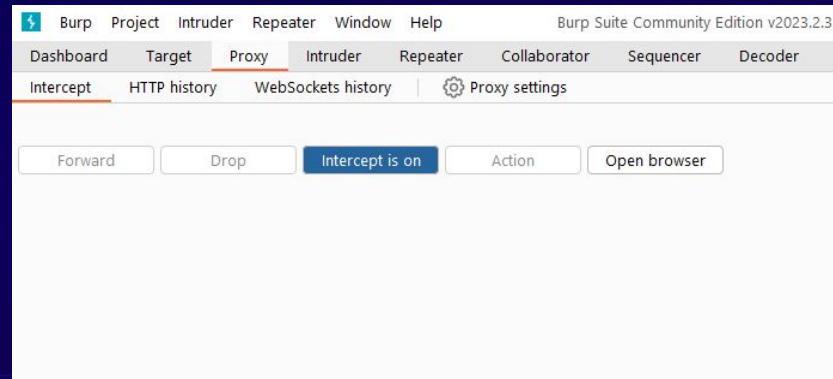


Web Server

The web application response is sent back to the Burp proxy.



Quick Intercept Demo



Place an order that makes you rich

- Make the shop pay you



SQL Injection

User input fields may be used as arguments in an SQL query. If these input fields are not sanitized or validated correctly, an attacker may be able to modify the query maliciously.

SQLi - Login as Admin

- Analyzing SQL queries and crafting an SQLi string
- Brute forcing SQLi strings with Burp Intruder

SQL Injection

```
SELECT * FROM Users WHERE email = '$EMAIL' AND password = '$PASSWORD' AND deletedAt IS NULL
```

```
EMAIL = "admin@domain.com" --"
```

```
SELECT * FROM Users WHERE email = 'admin@domain.com' -- ' AND password = '$PASSWORD' AND deletedAt IS NULL
```

[OWASP Juice Shop login.ts](https://github.com/jhewit/OWASP-Juice-Shop/blob/master/login.ts)

Access the Administration Section

- Find the URL to the administration section

Register an Admin Account

- Find the parameter required to register an admin account
- Craft a registration request with this parameter

THANK YOU

Any questions?



@gdscutm



@utmmcss

CREDITS

This is where you give credit to the ones who are part of this project.

- ◀ Presentation template by [Slidesgo](#)
- ◀ Icons by [Flaticon](#)
- ◀ Infographics by [Freepik](#)
- ◀ Author introduction slide photo created by Freepik
- ◀ Text & Image slide photo created by Freepik.com