Log out   MY ACCOUNT

Professional and Community Edition   ⌄

🔍 Search Burp Suite documentation   ⟩

>   Testing multiple inputs

PROFESSIONAL

Testing multiple inputs with the Burp Collaborator client

🕐 **Last updated:** January 27, 2023   ⏱ **Read time:** 1 Minute

You can use the Burp Collaborator client to test multiple request inputs at once. To do this, you need to insert a different payload into each input. This enables you to easily identify which input causes an interaction with the Collaborator server.

To generate multiple payloads at once:

1. Go to the **Collaborator** tab. If this is the first time you've opened the **Collaborator** tab, click **Get started**.
2. Enter the number of Collaborator payloads that you want to generate in the **Payloads to generate** field.
3. Click **Copy to clipboard** to copy the specified number of payloads.
4. To access the payloads, paste them into a document.

> **Note**
>
> To include the full Collaborator server address in your payloads, select **Include Collaborator server location**. If this is not selected, only the Collaborator ID will be included in your payloads.

You can now insert the unique payloads manually into the specific inputs that you want to test. Follow the usual testing process:

1. Open the request into which you want to insert the payloads. Insert these into the appropriate locations.
2. Send the request.
3. Go to the **Collaborator** tab and click **Poll now**. Interactions received as a result of your Collaborator payloads are displayed.
4. To identify which input caused the interaction, cross-reference the interaction payload with the payloads used in the request.

Was this article helpful?

👍 YES, THANKS!   👎 NOT REALLY

Burp Suite

Web vulnerability scanner
Burp Suite Editions
Release Notes

Vulnerabilities

Cross-site scripting (XSS)
SQL injection
Cross-site request forgery
XML external entity injection
Directory traversal
Server-side request forgery

Customers

Organizations
Testers
Developers

Company

About
PortSwigger News
Careers
Contact
Legal
Privacy Notice

Insights

Web Security Academy
Blog
Research
The Daily Swig

PortSwigger

Follow us

© 2023 PortSwigger Ltd.