Burp Suite Introduction

Enterprise Content Operations

Exported on 11/14/2022

Table of Contents

What is Burp Suite?

Burp Suite Enterprise Edition is a web-based application that allows you to use Burp Scanner's cutting-edge web scanning logic to uncover dozens of different types of vulnerability. It is designed for automated scanning at any scale, and integration with software development processes.

What Will You Need to Access Burp Suite?

- Burp Suite Enterprise Edition OR access to reports via the email queue

Viewing Scan Details:

For scans that are currently in progress or that have finished, the following information is displayed:

1 Dashboard

The **Dashboard** tab contains a collection of graphs that show key information about the scan. The dashboard enables you to get a quick overview of the scan results:

- The issues found grouped by risk and confidence level.
- The number of URLs scanned.
- A list of the most serious vulnerabilities found.
- A chart of the issue severity over time.

2 Timeline

The **Timeline** tab shows you the progress of a running scan. You can scroll down to see more details about each stage of the scan. If there is an error, you can scroll down to see more detailed information, including suggestions to remedy the error.

You can also use the timeline tab to review completed scans.

The Timeline tab shows the following information:

- The scan status.
- The start time.
- The **End time**, for completed scans.
- The **Time remaining**, for running scans.

3 Issues

The **Issues** tab shows a list of security issues that were found by the scan. Select an issue from the list to view detailed information about it, including remediation advice and a log of the request that the issue was found in.

You can mark an issue as a false positive from this page. If you have configured an integration with an issue tracking platform, you can also use the **Raise ticket** drop-down to raise Jira tickets, GitLab issues, and Trello cards for the issue.

The issues found are grouped by type. The number next to each issue indicates how many instances of this issue type were found. If a particular issue type is found on more than one URL, you can click on the issue to see a list of the relevant URLs. Click a URL to view detailed information for that particular issue instance.

4 Scanned URLs

The **Scanned URLs** tab shows information about which URLs Burp Scanner[1] attempted to scan and what issues the scanner found at each URL. The default view is a list of URLs. You can also select a tree view, which shows URLs in a hierarchy. Both views show the number of requests made by the scan to each URL.

1 https://portswigger.net/burp/vulnerability-scanner

5 Scan statistics

The **Scan statistics** tab shows detailed information about the issues found by the scan, including:

- A list of issues found, grouped by severity.
- A **Changes** section showing how many of those issues were new, repeated, regressed, or resolved.
- A **Traffic** section showing the number of URLs scanned, how many of those URLs had errors, and the total number of requests made.
- Details of the scanning machines and scanner version used.

6 Settings

The **Settings** tab displays the site-level settings that were used for the scan. These include:

- The scan scope - the site scanned, the seed URL, and any URLs that were explicitly included or excluded.
- Any preset scan modes or custom scan configurations that were applied.
- Any application logins that were used.
- Any extensions that were used
- Details of the schedule (if any) that the scan was run on.

For a more detailed view of scheduling information, click **View schedule**.

7 Reporting

The **Reporting** tab allows you to download reports in HTML format. This is useful for sharing scan reports with colleagues who may not have access to Burp Suite Enterprise Edition[2] themselves.

From the **Reporting** tab, you can specify a detailed report, summary report or compliance report. For detailed or summary reports you can also specify which issue severities to include, and whether you want to include or exclude false positive results.

2 https://portswigger.net/burp/enterprise

8 Logging

From the **Logging** tab, you can download scan event and scan debug logs. Scan event logs provide details about the progress of a scan and may be useful in determining why a scan failed. Scan debug logs may be useful if you need to contact our Support team to help diagnose problems.

Note that the scan log is only available for scans that:

- Were successfully assigned to a scanning machine.
- Have run or started running since you upgraded to Burp Suite Enterprise Edition[3] 2020.12.
- Are less than 10 days old.

3 https://portswigger.net/burp/enterprise

9 Failed Scans

A scan assumes a status of **failed** if it is terminated early. For example, it could be that the scan never started because Burp Scanner was unable to connect to any of the URLs specified.

If the scan began but was terminated early then the failed scan details page shows much of the same information as a completed scan. In this case the **Scanned URLs** tab lists the URLs that caused the scan to fail.