

## Task 2-1

The screenshot displays the Burp Suite Professional interface. On the left, the 'Tasks' panel shows three active tasks: '1. Live passive crawl from Proxy (all traffic)', '2. Live audit from Proxy (all traffic)', and '3. Active scans'. The '3. Active scans' task is selected, showing a progress bar and a list of issues. The main panel displays a table of active scans with columns for Time, Source, Issue type, Host, Path, Insertion point, Severity, and Confidence. A specific issue is highlighted: a 'Cross-site scripting (reflected)' vulnerability on the path '/dwa/vulnerabilities/xss\_r/' with a severity of 'Medium' and confidence of 'Certain'. The 'Inspector' panel on the right shows the request details for the selected issue, including the request headers and the response body. The response body contains a cookie with a POC script: 'security=low; alert(1); 152f52f363; security=low; PHPSESSID=nko52u8wuh77cue3o2akea1360'.

Time	Source	Issue type	Host	Path	Insertion point	Severity	Confidence
01:45:44 17 Feb 2024	Task 3	Path-relative style sheet import	http://192.168.56.104	/dwa/vulnerabilities/xss_r/		Information	Firm
01:45:43 17 Feb 2024	Task 3	Input returned in response (reflected)	http://192.168.56.104	/dwa/vulnerabilities/xss_r/	URL path folder 3	Information	Certain
01:45:42 17 Feb 2024	Task 3	Input returned in response (reflected)	http://192.168.56.104	/dwa/vulnerabilities/xss_r/	URL path folder 2	Information	Certain
01:45:42 17 Feb 2024	Task 3	Input returned in response (reflected)	http://192.168.56.104	/dwa/vulnerabilities/xss_r/	URL path folder 1	Information	Certain
01:45:39 17 Feb 2024	Task 3	Cross-site scripting (reflected)	http://192.168.56.104	/dwa/vulnerabilities/xss_r/	security cookie	Medium	Certain
01:45:36 17 Feb 2024	Task 3	Input returned in response (reflected)	http://192.168.56.104	/dwa/vulnerabilities/xss_r/	security cookie	Information	Certain
01:45:36 17 Feb 2024	Task 3	Flash cross-domain policy	http://192.168.56.104	/crossdomain.xml		High	Certain
01:45:36 17 Feb 2024	Task 3	HTTP TRACE method is enabled	http://192.168.56.104	/		Information	Certain

Inspector

Request attributes: 2

Request cookies: 3

Request headers: 8

1 highlight

The cookie carries the POC script

## Task 2-2

### Without using credentials to login to DVWA

The screenshot shows the Burp Suite Professional v2023.12.15 interface. The 'Issues' tab is selected for Task 4: Crawl and audit of 192.168.56.104. The table below lists the issues found:

Time	Source	Issue type	Host	Path	Insertion point	Severity	Confidence
01:53:39 17 Feb 2024	Task 4	Client-side desync	https://192.168.56.104	/dwa/login.php		High	Tentative
01:53:34 17 Feb 2024	Task 4	Client-side desync	https://192.168.56.104	/dwa/dwa/css/login.css		High	Tentative
01:53:31 17 Feb 2024	Task 4	Flash cross-domain policy	https://192.168.56.104	/crossdomain.xml		High	Certain
01:53:31 17 Feb 2024	Task 4	TLS certificate	https://192.168.56.104	/		Medium	Certain
01:53:30 17 Feb 2024	Task 4	TLS cookie without secure flag set	https://192.168.56.104	/dwa/		Medium	Firm

High: 3  
Medium: 2  
Using credentials to login to DVWA

The screenshot shows the Burp Suite Professional v2023.12.15 interface. The 'Issues' tab is selected for Task 17: Crawl and audit of 192.168.56.104. The table below lists the issues found:

Time	Source	Issue type	Host	Path	Insertion point	Severity	Confidence
09:00:55 17 Feb 2024	Task 17	Cleartext submission of password	http://192.168.56.104	/dwa/vulnerabilities/captcha/		High	Certain
09:00:56 17 Feb 2024	Task 17	Cleartext submission of password	http://192.168.56.104	/dwa/vulnerabilities/brute/		High	Certain
09:00:56 17 Feb 2024	Task 17	Cleartext submission of password	http://192.168.56.104	/dwa/vulnerabilities/curl/		High	Certain
09:01:40 17 Feb 2024	Task 17	Cross-site scripting (reflected)	http://192.168.56.104	/dwa/vulnerabilities/curl/	security cookie	Medium	Certain
09:01:47 17 Feb 2024	Task 17	Cross-site scripting (reflected)	http://192.168.56.104	/dwa/vulnerabilities/sqli/	security cookie	Medium	Certain
09:01:47 17 Feb 2024	Task 17	Cross-site scripting (reflected)	http://192.168.56.104	/dwa/vulnerabilities/brute/	security cookie	Medium	Certain
09:01:47 17 Feb 2024	Task 17	File path traversal	http://192.168.56.104	/dwa/vulnerabilities/ff/	page parameter	High	Firm
09:01:53 17 Feb 2024	Task 17	Cross-site scripting (reflected)	http://192.168.56.104	/dwa/vulnerabilities/view_source.php	id parameter	High	Certain
09:01:53 17 Feb 2024	Task 17	Cross-site scripting (reflected)	http://192.168.56.104	/dwa/vulnerabilities/ff/	security cookie	Medium	Certain
09:02:03 17 Feb 2024	Task 17	Cross-site scripting (reflected)	http://192.168.56.104	/dwa/vulnerabilities/captcha/	security cookie	Medium	Certain
09:03:06 17 Feb 2024	Task 17	Cross-site scripting (reflected)	http://192.168.56.104	/dwa/vulnerabilities/sqli_blind/	security cookie	Medium	Certain
09:03:34 17 Feb 2024	Task 17	OS command injection	http://192.168.56.104	/dwa/vulnerabilities/exec/	ip parameter	High	Firm
09:04:06 17 Feb 2024	Task 17	Cross-site scripting (reflected)	http://192.168.56.104	/dwa/vulnerabilities/xxss_sl	name parameter	High	Certain
09:04:15 17 Feb 2024	Task 17	SQL injection	http://192.168.56.104	/dwa/vulnerabilities/brute/	username parameter	High	Certain
09:04:16 17 Feb 2024	Task 17	SQL injection	http://192.168.56.104	/dwa/vulnerabilities/sqli/	id parameter	High	Certain
09:05:28 17 Feb 2024	Task 17	Cross-site scripting (reflected)	http://192.168.56.104	/dwa/vulnerabilities/xxss_sl	txtName parameter	High	Certain
09:06:16 17 Feb 2024	Task 17	Cross-site scripting (reflected)	http://192.168.56.104	/dwa/vulnerabilities/exec/	security cookie	Medium	Certain
09:09:08 17 Feb 2024	Task 17	Cross-site request forgery	http://192.168.56.104	/dwa/vulnerabilities/xxss_sl		Medium	Tentative
09:09:25 17 Feb 2024	Task 17	Cross-site scripting (reflected)	http://192.168.56.104	/dwa/vulnerabilities/xxss_sl		High	Certain
09:10:02 17 Feb 2024	Task 17	Cross-site scripting (reflected)	http://192.168.56.104	/dwa/vulnerabilities/captcha/	mtaMessage parameter	Medium	Tentative
09:10:48 17 Feb 2024	Task 17	Cross-site request forgery	http://192.168.56.104	/dwa/vulnerabilities/captcha/	security cookie	Medium	Certain
09:11:28 17 Feb 2024	Task 17	Cross-site scripting (reflected)	http://192.168.56.104	/dwa/vulnerabilities/upload/		Medium	Tentative
09:12:49 17 Feb 2024	Task 17	Cross-site request forgery	http://192.168.56.104	/dwa/vulnerabilities/upload/	security cookie	Medium	Tentative
09:13:42 17 Feb 2024	Task 17	Cross-site scripting (reflected)	http://192.168.56.104	/dwa/vulnerabilities/xxss_sl		High	Certain
09:16:50 17 Feb 2024	Task 17	Cross-site scripting (stored)	http://192.168.56.104	/dwa/vulnerabilities/xxss_sl		High	Certain

High: 13  
Medium: 13