

Nella lezione pratica di oggi vedremo come configurare una DVWA – ovvero damn vulnerable web application in Kali Linux. La DVWA ci sarà molto utile per i nostri test sia durante la build week 1 che durante lo sviluppo del modulo 2, dove vedremo da vicino le tecniche per sfruttare le vulnerabilità nella fase di exploit.

The screenshot shows the Burp Suite interface with a GET request to `/DVWA/index.php` and its response. The request is a standard HTTP GET with various headers including `Cache-Control: max-age=0`, `sec-ch-ua: max=0`, `sec-ch-ua-mobile: ?0`, `sec-ch-ua-platform: ''`, `Upgrade-Insecure-Requests: 1`, `Origin: http://127.0.0.1`, `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5798.171 Safari/537.36`, and `Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7`. The response is an HTML page titled "Welcome to Damn Vulnerable Web Application!" with a main content area containing a paragraph about DVWA's purpose and a section for general instructions.

The screenshot shows a POST request to `/DVWA/login.php` and its response. The request includes a `Content-Type: application/x-www-form-urlencoded` header and a body with `username=admin` and `password=admin`. The response is an HTML page titled "Login Failed" with a message "Login failed" and a link to the login page. The response also includes a `Cookie: PHPSESSID=...` and a `Set-Cookie: PHPSESSID=...` header.