

[Home](#) [About](#) [Contact](#) [Logout](#)

Binary Biceps

Binary Biceps is a web-based penetration testing tool designed to help ethical hackers and security professionals identify and exploit vulnerabilities in web applications.

Instances

Binary Biceps currently has 1 instance available for testing.

Information Gathering:

As part of the initial reconnaissance phase, we will automatically gather information about the target website, including its IP address, port, and basic configuration details.

Web Enumeration:

Once we have gathered basic information, we will perform a more detailed enumeration of the website's structure and content, identifying any additional pages or resources that may be present.

Source Code Analysis:

Reviewing the source code of the website can reveal many potential vulnerabilities. We will analyze the code for any suspicious patterns or logic that could be exploited.

Exploitation:

If we find a vulnerability, we will attempt to exploit it to gain access to the system. This may involve crafting specific input to trigger a buffer overflow or other type of exploit.

Post-exploitation:

Once we have gained access, we will use the tools available to us to further explore the system and extract sensitive information.

SQL Injection - Secret Querying - Admin Secret signature:

SQL injection is a common vulnerability that allows attackers to manipulate database queries. In this instance, we are targeting a secret query that is used by the application to verify user credentials.

Hashdump - Hash Length Extension Attack - Admin Cookie:

Hash length extension attacks are used to compromise hashed passwords. In this instance, we are targeting an admin cookie that is hashed using a weak algorithm.

