

# HackGATE Pentest Audit Report

## Penetration Testing Monitoring for COMPANY

**HackGATE™'s dashboard provides a clear view of ethical hacking projects, enabling companies to monitor ethical hackers while having full control over the traffic.**

### SCOPE

**<https://staging-webapp.company.com>**

### TIMEFRAME

**17 June, 2024 - 28 June, 2024**

### MONITORING TOOL

**HackGATE by Hackrate**

### APPROACH

This document presents a set of security testing monitoring controls developed by Hackrate, a cybersecurity company that has developed HackGATE, an industry-first solution for monitoring ethical hacking projects. These controls are designed to provide a comprehensive overview of any ethical hacking project and enable companies to monitor their penetration test projects effectively. For further details, visit HackGATE's website: <https://www.hackgate.io>

## HackGATE Pentest Audit Report

### Report for COMPANY

Penetration Testing Scope

staging-webapp.company.com



HackGATE URL

staging-webapp.company.hackgate.net

#### Scope of the assessment

The scope of the penetration test was defined as the domain staging-webapp.company.com. The corresponding HackGATE URL was staging-webapp.company.hackgate.net.



#### SECURITY TESTING MONITORING REQUIREMENTS

The following section presents a control framework for cybersecurity testing monitoring. The controls cover various aspects of ethical hacking and provide a comprehensive assessment of the security testing projects, ensuring its alignment with established cybersecurity standards.

#### CONTROL ID: 01-QUALITY-FRAMEWORK

RESULT: VALIDATED

Control: Quality Assessment Framework of the Security Testing

Control Description: Establish and manage a framework for assessing the quality of penetration testing activities, independent of the severity of identified vulnerabilities, in accordance with ISO27001 A.12.6.1, SOC2 CC6.1, and NIST 800-53 Rev5 CA-8.

Result: The assessment indicated that the testing process was sufficiently thorough and effective, meeting the standards set by the control framework.

#### CONTROL ID: 02-TESTING-TRAFFIC-MONITORING

RESULT: VALIDATED

Control: Minimum Security Testing Traffic

Control Description: Ensure continuous monitoring of the security testing traffic generated during the penetration test, encompassing both manual and automated testing activities, in compliance with ISO27001 A.12.6.1, SOC2 CC6.1, and NIST 800-53 Rev5 CA-8.

Result: The observed traffic, although not high, was deemed appropriate for the scope of the test, maintaining a balance between manual and automated testing, thereby ensuring comprehensive coverage.

## HackGATE Pentest Audit Report

### Report for COMPANY

#### CONTROL ID: 03-SECURITY-TESTING-TECHNIQUES

RESULT: VALIDATED

Control: Adherence to Testing Techniques

Control Description: Ensure and evaluate the variety of testing techniques employed, benchmarked against the OWASP guidelines, in line with ISO27001 A.12.6.1, SOC2 CC6.1, and NIST 800-53 Rev5 CA-8.

Result: The ethical hackers utilized a diverse array of techniques, ensuring a thorough examination of the system's security, in accordance with established guidelines.

#### CONTROL ID: 04-TESTING-DURATION

RESULT: VALIDATED

Control: Security Testing Duration

Control Description: Monitor the duration of the test and the assets tested in accordance with ISO27001 A.12.6.1, SOC2 CC6.1, and NIST 800-53 Rev5 CA-8.

Result: The test was conducted over a period of 26 days, with multiple assets within the scope being tested. This ensured that the test was not rushed, and each asset received due attention.

#### CONTROL ID: 05-SCOPE-COVERAGE

RESULT: VALIDATED

Control: Scope Coverage Monitoring

Control Description: Ensure comprehensive coverage of the scope in accordance with ISO27001 A.12.6.1, SOC2 CC6.1, and NIST 800-53 Rev5 CA-8.

Result: HackGATE results showed that the main functionalities of the target web application were tested. HackGATE used API definition to compare the tested API endpoints.



#### REPORT SUMMARY

In conclusion, the penetration test was found to be satisfactory based on the controls monitored by HackGATE. The test maintained its scope, generated appropriate traffic, used various techniques, and tested the target over a suitable duration. The test was deemed appropriate based on HackGATE's quality assessment framework.