The Hague

Rules of
ENGAGEMENT

HÂCK
THE HAGUE
2023 // 5TH EDITION

hackthehague.com

RULES OF **ENGAGEMENT 2023**

Method, monitoring and disruptions

Hâck The Hague 2023 takes place in the live environments. Every contestant will receive a network connection for a public IP address within the municipality's own IP-range that must be used during the event.

About 120 ethical Hackers will explore and search the IT environment at the same time. The excessive generating of traffic with automatic tools such as Dirbuster, Nmap, Skipfish and so on to scan the environment broadly, must therefore be limited (non-intrusive).

The following methods are NOT permitted:
• any form of Denial-of-Service attack;
• brute-forcing and "flood based" attacks;
• emptying of databases or changing records.

> If you suspect that you may have caused a disruption, stop your work immediately and inform the jury or someone from the organisation.

GENERAL RULES

• Findings may not be exploited beyond the minimum requirement.
• Demonstrate the vulnerability with a Proof of Concept.
• Your findings may only be shared on the Zerocopter platform, and within your own team.
• Your work must be stopped immediately at the organisation's request.

No points will be awarded for the following:
• Missing cookie-flags on non-sensitive cookies;
• Reports about insecure SSL/TLS configurations (unless you can clearly demonstrate why this is important);
• Missing HTTP security headers (unless you can clearly demonstrate why this is important);
• Social engineering (including phishing);
• Bulk creation of accounts, files or folders;
• Client-side and self-inflicted XSS vulnerabilities.

Reporting findings

Findings need to be reported using the Zerocopter platform. Make sure you register on the Zerocopter platform with the same email address used in the registration form, so we can trace the findings to the right person or team. Teams must work with one joint account in Zerocopter. The jury will only assess the findings that are submitted through an account and look at the argumentation of your finding. If you submit a fully automated report, you need to fill in a description of what you did. Please check that your finding has been accepted, as the description may not be adequate or the finding may have already been found by someone else. The Municipality of The Hague has a Coordinated Vulnerability Disclosure . The rules in this policy also apply to Hâck The Hague 2023.

Scope

The scope will be shared with the contestants during the kick-off.

Important: Any environment/system/port that is not named in the list we share during the kick-off is not included in the scope. Intentionally starting a test or a scan outside the scope will result in automatic disqualification.

Media

The organisation has the right to record and/or stream video during the award ceremony, including the use of images for promotional purposes of Hâck The Hague.

In addition, the press or organisation might ask a few team captains or hackers for an interview. The organisation will only approach the teams who let us know via the registration form that they are willing to talk with the press. We strive to limit these distractions during the event as much as possible.

In case you have any questions, please reach out to the organisation at: hackthehague@denhaag.nl