HackerOne Letter of Attestation

Release date
October 14th, 2021

Author

Evan Hachenburg (Associate Solutions Architect, HackerOne)
ehachenburg@hackerone.com

For External Use

Executive Summary

Files.com engaged HackerOne to perform a HackerOne Pentest from September 13th, 2021 to September 27th, 2021.

Opinion

HackerOne conducts penetration tests using methodologies that have been developed from industry standards, best practices, and proprietary knowledge. HackerOne believes that the engagement performed against the assets listed in this report provides a thorough level of security assurance and an unbiased assessment of the state of security.

HackerOne's tests were conducted on the assets listed below from September 13th, 2021 to September 27th, 2021. Testers were provided test accounts to also conduct testing at the authenticated level.

Scope

During the preparation phase the following scope for the engagement was agreed upon:

IN SCOPE ASSETS
https://Pentest.files.com
https://pentest2.files.com
pentest.files.com
pentest2.files.com

Methodology

The security assessment was conducted using a crowdsourced penetration testing methodology. From its community of over 1,000,000 security researchers, HackerOne selected three top-tier researchers to focus on identifying vulnerabilities in Files.com scope during the agreed-upon testing window.

A HackerOne pentest engagement follows a series of methodologies, checklists, and guidelines to ensure a balance between consistent customer experience, coverage of testing, and depth of testing. HackerOne develops these tools using industry best practices such as OSSTMM, OWASP, NIST, PTES, and ISSAF; as well as, proprietary knowledge gained through HackerOne's platform that services thousands of on-going and/or timeboxed engagements and a community of over 1,000,000 hackers. Using this combination of best practices and proprietary experience HackerOne is confident that its penetration tests provide a thorough level of security assurance and an unbiased assessment of the state of security for its customers.

HackerOne uses a vulnerability taxonomy based on the industry-standard Common Weakness Enumeration (CWE). CWE is a community-developed list of common software security weaknesses. It serves as a common language, a measuring stick for software security tools, and as a baseline for weakness identification, mitigation, and prevention efforts. More information can be found on MITRE's website: https://cwe.mitre.org/.

Framework

HackerOne uses the industry-standard CVSS to calculate severity for each identified security vulnerability. CVSS provides a way to capture the principal characteristics of a vulnerability, and produce a numerical score reflecting its severity, as well as a textual representation of that score. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes. More information can be found on the Forum for Incident Response and Security Teams' (FIRST) website: https://www.first.org/cvss.

Findings

As of October 14th, 2021, Files.com has no known vulnerabilities within the assets engaged by HackerOne, as summarized in the chart below.

	Critical	High	Medium	Low	None	Σ
https://Pentest.files.com	0	0	0	0	0	0
https://pentest2.files.com	0	0	0	0	0	0
Pentest.files.com	0	0	0	0	0	0
pentest2.files.com	0	0	0	0	0	0
Total	0	0	0	0	0	0