

Customization Summary

The Exploit-DB Python PoC was customized by updating the target URL and port, modifying request headers to match the server configuration, and encoding the payload to bypass input filtering. Hardcoded parameters were removed, timeout handling was improved, and verbose logging was added to reliably confirm successful exploitation.

Chained Exploit on Web Server

Findings:

- CVE-2021-22205
- Affected Host: 192.168.108

Sanitize and validate all user inputs

Apply the latest GitLab security updates and patches

Subject: Critical Finding: CVE-2021-22205 Leading to Remote Code Execution

Dear Development Team,

During the recent penetration testing exercise, a critical vulnerability (CVE-2021-22205) was identified on host 192.168.1.100. An initial web-based weakness enabled further exploitation, ultimately resulting in Remote Code Execution using a customized exploit. Successful exploitation allowed command execution with elevated privileges, posing a serious risk to system confidentiality and integrity.

Immediate remediation is strongly recommended, including sanitizing all user inputs, applying the latest GitLab security patches, and reviewing access controls. After fixes are applied, a validation scan should be conducted to ensure the vulnerability has been fully mitigated.

Regards,
Shashank M
VAPT Analyst