Name Of Bug

Name	FirstLast\LastName\Username
Email	test@gmail.com
Severity	Critical\High\Medium\Low
Severity Desc.	Why was this level of criticality determined?
Host	The endpoint host resource where the vulnerability was found. It can be an API server, file storage, website, etc. As a rule, this is the resource from the last PoC request/exploit.

01. Summary

What does this vulnerability do/exploit?
What consequences can an attacker have on the system?
Briefly, where is this vulnerability located, what is its functionality? General information about the type of vulnerability identified and the reasons for its occurrence.
What privileges are required?
To use this template comfortably, we recommend filling out your report in Google Docs.
Use indents for better text formatting.
Does the exploit require any actions to be performed by the victim (e.g., clicking a link, submitting a form, opening a page)?

02. Details

Provide a **detailed, step-by-step explanation** of how the vulnerability can be exploited.

- Include **screenshots** and **direct links** to vulnerable pages where applicable.
- Clearly describe **each action** the attacker must perform to reproduce the issue.

If the vulnerability involves PoC exploits (e.g., JavaScript payloads, SQLi, command injection), **include the exact payloads** used.
If the vulnerability involves **Linux-based exploitation**, provide the **exact shell commands** used during the process.
Embed or link an **MP4 video** recording of the exploitation process to demonstrate how the vulnerability works in real-time.
If HTTP requests were used (via **BurpSuite** or **OWASP ZAP**), include the **full raw request and response**.

03. Recommendation

Provide your own thoughts and technical recommendations on how to fix the vulnerability in the most effective and secure way.

- Suggest **specific code-level fixes**, configuration changes, or architectural improvements.
- If applicable, mention **relevant libraries**, **security headers**, **framework settings**, or **best practices** (e.g., OWASP ASVS).
- Justify why the proposed fix is effective and how it mitigates the root cause — not just the symptom.

04. Impact

What can an attacker do with this vulnerability? What information can they access? How does it affect the system? Clearly justify why the vulnerability is of this severity level and not lower.