# Submit #551123: demtec.sk Graphlytics 5.0.7 Cross Site Scripting

**Title** demtec.sk Graphlytics 5.0.7 Cross Site Scripting

**Description** [ Reflected XSS on Graphytics v5.0.7 ]
Graphytics version 5.0.7 is vulnerable to Reflected Cross-Site Scripting (XSS), allowing attackers to execute malicious JavaScript in a victim's browser. This can lead to session hijacking, as the application does not enforce the HttpOnly flag on session cookies, making them accessible to client-side scripts. Exploiting this vulnerability could result in unauthorized access to user sessions and sensitive information.

The issue was tested in the Dockerized version of Graphytics, following the installation guide provided at: https://graphlytic.com/doc/latest/Install_with_Docker_on_Ubuntu.html

Payload used:
http://{graphlytic-ip}:8080/visualization?name`;alert(document.cookie);`=1

Refer complete POC published on the Git repo.

Note:
If possible please add Adamya Varma (varma.adamya@gmail.com) as co-researcher for the vulnerability

**Source** ⚠ https://github.com/HexC0d3/graphlytic-xss-exploits/blob/main/reflected_xss.md

**User** 0xc0de (UID 83444)

**Submission** 04/04/2025 09:15 AM (11 days ago)

**Moderation** 04/14/2025 11:17 PM (11 days later)

**Status** Accepted

**VulDB Entry** 304671 [Demtec Graphytics 5.0.7 HTTP GET Parameter /visualization cross site scripting]

**Points** 20

## Notice

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

## Documentation

- Submission Policy
- Data Processing
- CVE Handling