# [CVE-2021-35976] Plesk Obsidian on Linux is vulnerable to reflected XSS via the /plesk-site-preview/ path

The feature to preview a website in **Plesk Obsidian 18.0.0 through 18.0.32** on Linux is vulnerable to **reflected XSS** via the `/plesk-site-preview/` path, aka PFSI-62467. The attacker could execute JavaScript code in the victim's browser by using the link to preview sites hosted on the server. **Authentication is not required to exploit the vulnerability**.

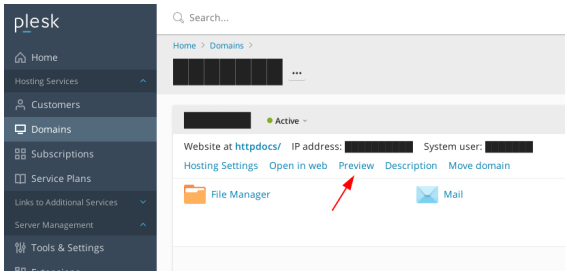
## Steps to reproduce

After you uploaded website files to the subscription, you can check how your site will look in a web browser, even before the information about the new site has spread in the Domain Name System.

To preview a website:

**1-** Go to Websites & Domains.

**2-** Click **Preview** below the domain name of the website that you want to preview.




Your site will open in a new browser window via the `/plesk-site-preview/` path.

### By default

```
http://<server_ip>/plesk-site-preview/<domain.tld>/https/<server_ip>
```

### Exploitation

```
http://<server_ip>/plesk-site-preview/<payload>/https/<server_ip>
```

Payload e.g.: `"><svg/onload=alert()>`

## Additional note

An attacker's JavaScript can be executed in the context of the origin which is used for website preview only (not for the rest part of Plesk panel).

## References

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35976
- https://support.plesk.com/hc/en-us/articles/4402990507026