



Browsershot 3.57.2 – Server Side XSS to LFR via URL

Summary



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Allow all cookies](#)

[Show details](#)

Affected versions	Version 3.57.2
State	Public
Release date	2022-10-28

Vulnerability

Kind	Server Side XSS
Rule	425. Server Side XSS
Remote	Yes
CVSSv3 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVSSv3 Base Score	7.5
Exploit available	Yes
CVE ID(s)	CVE-2022-41706

Description

Browsershot version 3.57.2 allows an external attacker to remotely obtain arbitrary local files. This is possible because the application does not validate the URL protocol passed to the `Browsershot::url` method.

Vulnerability

This vulnerability occurs because the application does not validate the URL protocol passed to the `Browsershot::url` method. Thanks to this, an attacker can point to internal server files, which will be reflected in the PDF that will be generated.

Exploitation

Vendor Confirmed the vulnerability.

✓ 2022-10-25
Vulnerability patched.

✓ 2022-10-28
Public Disclosure.



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details

Services

Continuous Hacking

One-shot Hacking

Comparative

Solutions

DevSecOps

Secure Code Review

Red Teaming

Breach and Attack Simulation

Security Testing

Penetration Testing

Ethical Hacking

Vulnerability Management

Blog

Certifications

Partners

Careers

Advisories

FAQ

Documentation

Contact