XSS in description field

Moderate **bigprof** published **GHSA-rm79-5596-r7q4** on Jan 21, 2021

Package

No package listed

Affected versions

4.0

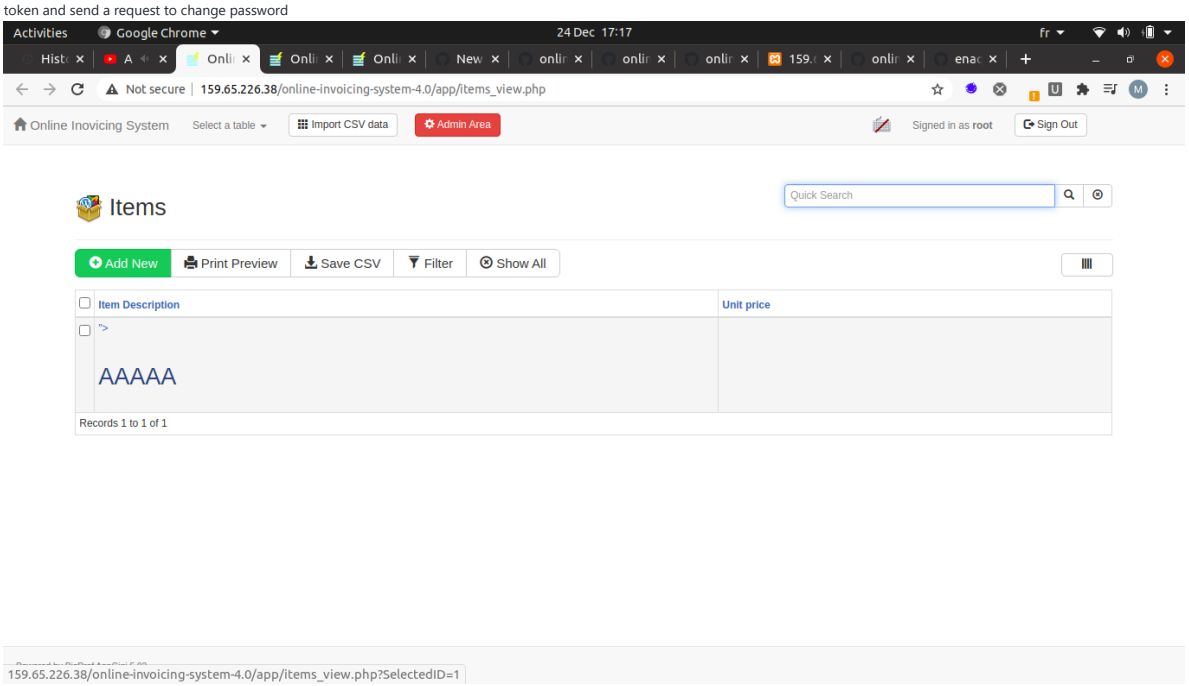
Patched versions

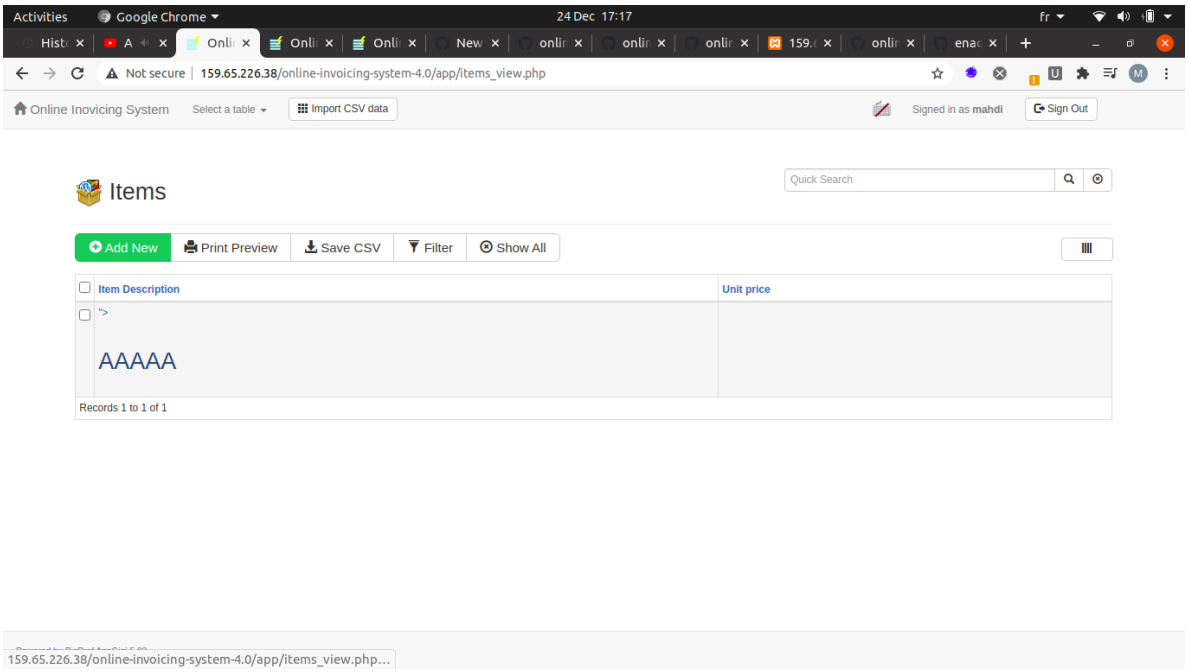
4.1

Description

As reported by @MMrhassel

Hey I've found that Item description is reflected without sanitize in app/items_view.php which can make an malicious user takeover the admin account through a payload that is extract csrf token and send a request to change password





Severity

Moderate

CVE ID

CVE-2021-21260

Weaknesses

No CWEs