

## Out-of-Date Version (Apache)

---

Reported to : internshipstudio.com  
Reported at : 18 August 2021  
Asset : zero.webappsecurity.com  
URL : http://zero.webappsecurity.com/login.html  
Weakness : Out-of-Date Version  
Severity : Critical  
Participants : Roshan More

---

### **Summary:**

The out-of-date version can lead attackers get unauthorized access to the website and can retrieve any sensitive information through Cross Site Scripting.

### **Steps to Reproduce:**

- Enter URL <http://zero.webappsecurity.com/login.html>
- Enter your username and password
- Click 'Sign in'
- After user clicks 'Sign in', attacker can get access to the site because of the version not getting updated.

## Impact:

An attacker can get unauthorized access to the site because of old version the site is using.

## Mitigation:

- Always upgrade and use latest version.
- User's login credentials should be stored using HTTPS.

## Supporting Material/References:

Screenshots and video recording has been submitted with this report.

The screenshot displays the Netsparker 5.8.1.28119 interface. The main window shows a vulnerability report for 'Out-of-date Version (Apache)' with a 'CRITICAL' severity. The report includes details such as the URL (<https://zero.webappsecurity.com/>), identified version (2.2.6), and latest version (2.4.48). It also lists various classification standards like PCI DSS 3.2, OWASP 2013, OWASP 2017, CWE, CAPEC, HIPAA, and ISO27001. The impact section states: 'Since this is an old version of the software, it may be vulnerable to attacks.' The remediation section is partially visible. On the right, a 'Netsparker Assistant' panel shows a warning about 'DOM Simulation Timeout/Exception'.

**Out-of-date Version (Apache)**  
**CRITICAL**

Certainty : ☐  
URL : <https://zero.webappsecurity.com/>  
Identified Version : 2.2.6  
Latest Version : 2.4.48 (in this branch)  
Vulnerability Database : Result is based on 08/17/2021 20:30:00 vulnerability database content.

**Vulnerability Details**  
Netsparker identified you are using an out-of-date version of Apache.

**Impact**  
Since this is an old version of the software, it may be vulnerable to attacks.

**Remedv**

**CLASSIFICATION**  
PCI DSS 3.2 [6.2](#)  
OWASP 2013 [A9](#)  
OWASP 2017 [A9](#)  
CWE [829](#)  
CAPEC [310](#)  
HIPAA [164.308\(A\)\(1\)\(i\)](#)  
ISO27001 [A.14.1.2](#)

**DOM Simulation Timeout/Exception**  
Netsparker has detected that the configured DOM Simulation Timeout value is insufficient to completely simulate some of the pages in your scan. You may want to increase this value to keep the scan coverage at its best.  
Adjust in Scan Policy

