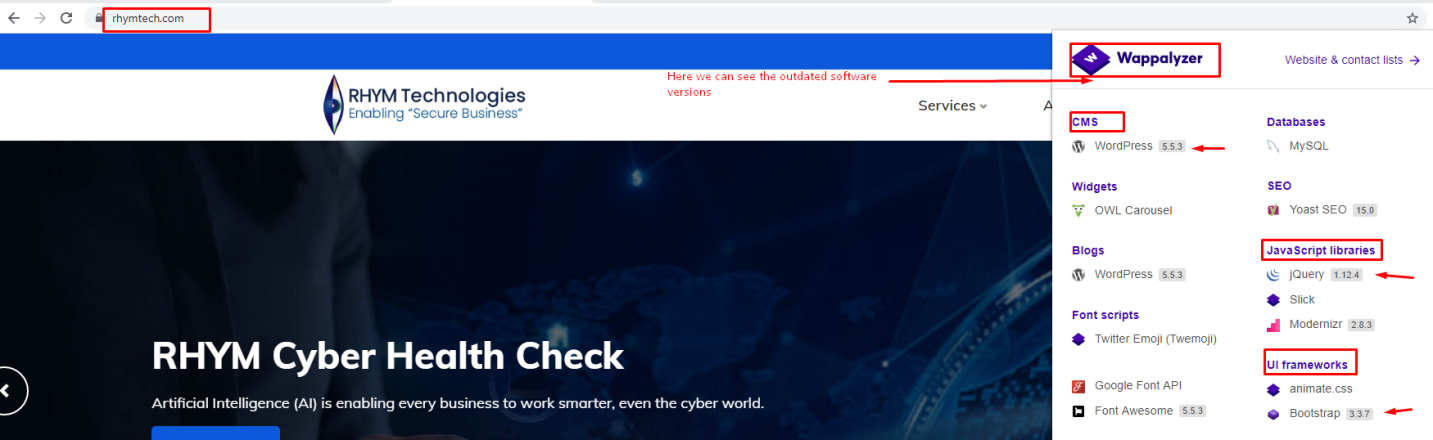
**PATCH RHYTHM**

1. **Insecure Software Versions:**
2. **Outdated/Obsolete Software**

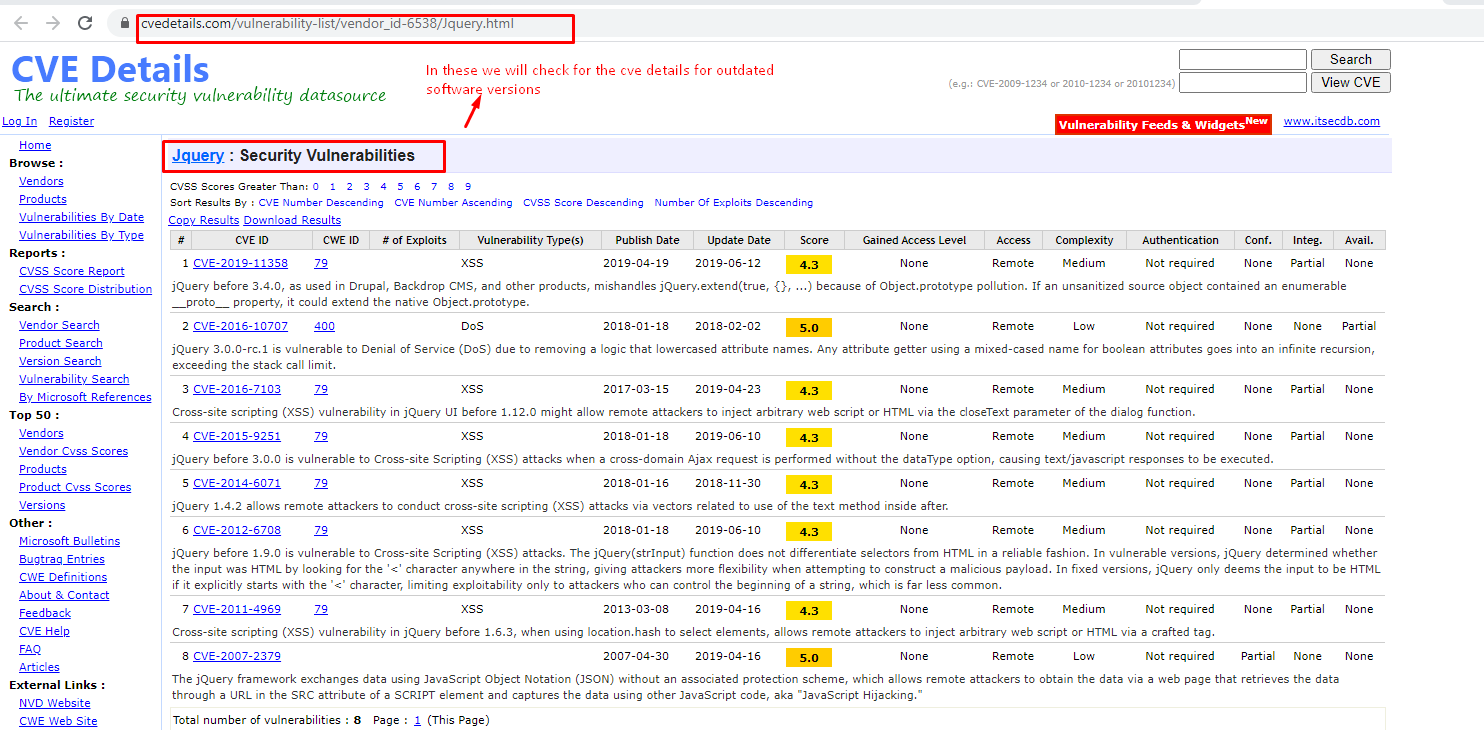
URL to check obsolete software’s [**wappalyzer.com**](https://wappalyzer.com/) **(Chrome Extension)**

**Step-1:** Enter the Domain name in search field and open the wappalyzer extension then it will show the Website Built in Technologies



**Step-2:** collect the insecure software versions using wappalyzer extension and check the software version in CVE details weather it is patched or unpatched.

**Step-3:** Open CVE details **https://www.cvedetails.com/** to check the insecure software versions and consider software versions as input

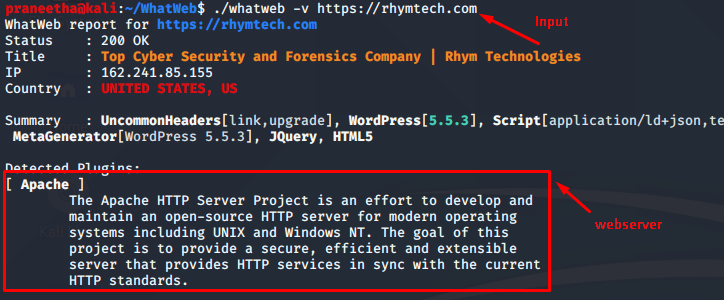


**Step-4:**If insecure software versions are detected Consider alert severity as **HIGH** and with alert score **7**

1. **Unpatched versions:**
2. **Web servers**

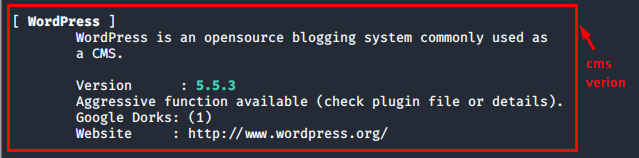
Tool to check Unpatched versions **https://github.com/urbanadventurer/WhatWeb.git**

**Step-1:** Enter the domain name using command. /whatweb -v domain name consider domain name as Input



**Step-2:** If unpatched web server version Detected consider alert severity as **HIGH** with alert score **7**

**Step-3:** If the webserver is PatchedConsider alert severity **as INFORMATIONAL** and with alert score **0**

****

1. **DNS servers**

Tool to check DNS server versions **fpdns** default tool in Kali Linux 2020

**Step-1:** Enter the domain name using command fpdns -d domain name consider domain name as input

**Step-2:** If an unpatched DNS server is detected consider alert severity as HIGH and with alert score of **7**

**Step-3:** if an secure DNS server is detected consider alert severity as **INFORMATIONAL** and with alert score of **0**

