

JOOMLA!



JOOMLA

Joomla is an open-source content management system (CMS) which uses to build websites. It is written in PHP, MySQL database to store content. Joomla is known for its flexibility, user friendly, easy to use and for its extensibility. Using Joomla, we can use variety of website whether it can a blog as well as complex corporate website. Joomla also supports multiple language, extensions as well as plugins.

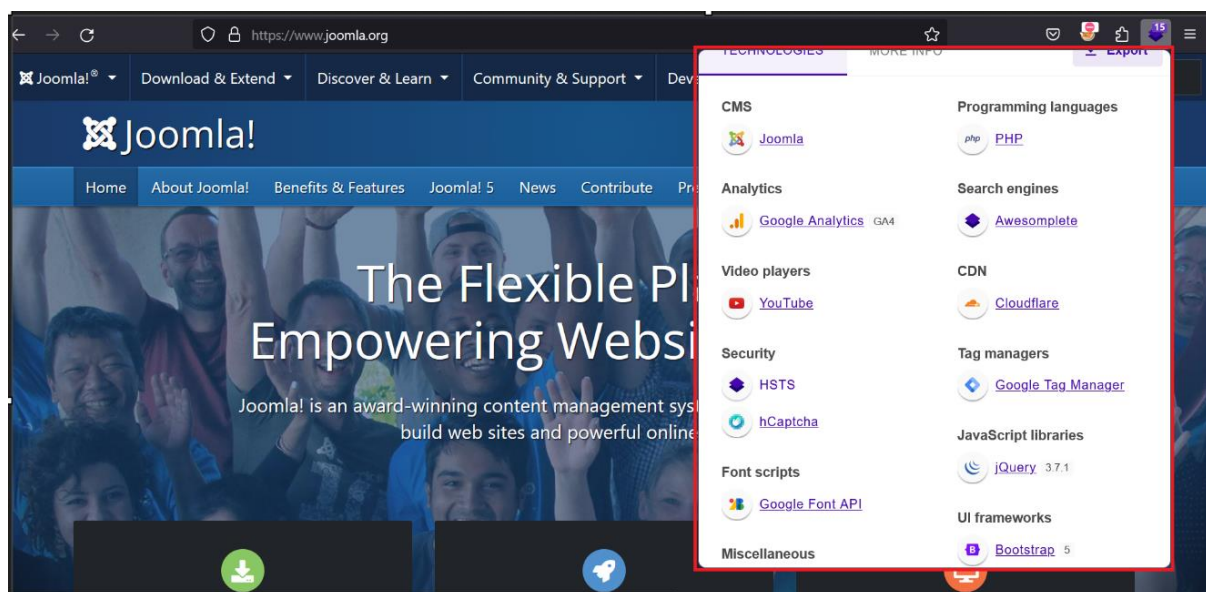
Since this is an open-source content management system, user can create website without coding skills.

Also, there are multiple CMS are available in market such as WordPress, Drupal, Joomla, Weebly and Wix.

EXTRACT INFORMATION ABOUT BACKEND TECHNOLOGY USING TOOLS FOR JOOMLA

A penetration tester can use different passive techniques to find out what technologies has been used in background to run this website.

- **Wappalyzer.**



SCREENSHOT: WAPPALYZER EXTENSION IN FIREFOX

Wappalyzer is an extension of Mozilla firefox and easy to add in. It shows what technology has been used in backend so user can check what is the technology and what version the website is using currently so according to current vulnerability in that technology penetration tester can exploit.

WHAT IS JOOMLA VULNERABILITIES

1. **SQL Injection Vulnerability:** Basically SQL Injection is vulnerability where attacker can play with the database information i.e., modify or delete the database information using SQL Injection queries. Also, attacker can compromise the back-end infrastructure using this attack. This vulnerability for the particular website Joomla is also listed in CVE website as well as NVD. Here is the case details CVE-2023-49708. The Joomla version which is impacted is version 3.7.
- **Impact:** If the attacker is successfully able to attack using SQL Injection then it can simply compromise the user's password, credit card details as well as personal information which is valuable.
 - **Techniques to Find Vulnerability:**
 - You can use single quote (') at the end of the URL and hit enter, now check if there are any changes in the website behaviour or changes of data in the webpage.
 - You can also use Boolean operator to check i.e., OR 1=1, OR 1=2 at the end of the URL to see the changes in the webpage.
 - You can also take help from github to get the queries and try applying on the website to check the changes in the data of the webpage.

CVE-ID	
CVE-2023-49708 Learn more at National Vulnerability Database (NVD)	
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information	
Description	
SQLi vulnerability in Starshop component for Joomla.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
<ul style="list-style-type: none">• MISC:https://extensions.joomla.org/extension/starshop/• URL:https://extensions.joomla.org/extension/starshop/	
Assigning CNA	
The Joomla! Project	
Date Record Created	
20231130	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20231130)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	

SCREENSHOT: CVE RECORD OF JOOMLA

2. **Reflected Cross-Site Scripting (XSS):** Recently as per the CVE report in 2023 Joomla has faced 5 cross-site scripting issues in the system. It means when the application receives the data and it is already stored some data for immediate response, this considered as unsafe way to function any website. You can find the reported case id here. CVE-2023-40659, CVE-2023-40658, CVE-2023-40657, CVE-2023-40656, CVE-2023-40655.
- **Impact:** It may be a huge impact for the sites which stores banking details as well as privileges. It can compromise the data and go into the wrong hand if the firm do not patch to latest security.
 - **Techniques to Find Vulnerability:**
 - You can search for any input option in website which gives response and use the simple scripts to find out if the webpage is vulnerable to XSS or not.
 - For example, you can a simple payload `<script>alert1</script>` in any entry point of the webpage which provides response.

CVE-2023-40659	A reflected XSS vulnerability was discovered in the Easy Quick Contact module for Joomla.	V3.1: 6.1 MEDIUM V2.0:(not available)
Published:	December 14, 2023; 4:15:41 AM -0500	
CVE-2023-40658	A reflected XSS vulnerability was discovered in the Clicky Analytics Dashboard module for Joomla.	V3.1: 6.1 MEDIUM V2.0:(not available)
Published:	December 14, 2023; 4:15:41 AM -0500	
CVE-2023-40657	A reflected XSS vulnerability was discovered in the Joomdoc component for Joomla.	V3.1: 6.1 MEDIUM V2.0:(not available)
Published:	December 14, 2023; 4:15:41 AM -0500	
CVE-2023-40656	A reflected XSS vulnerability was discovered in the Quickform component for Joomla.	V3.1: 6.1 MEDIUM V2.0:(not available)
Published:	December 14, 2023; 4:15:41 AM -0500	
CVE-2023-40655	A reflected XSS vulnerability was discovered in the Proforms Basic component for Joomla.	V3.1: 6.1 MEDIUM V2.0:(not available)
Published:	December 14, 2023; 4:15:41 AM -0500	

SCREENSHOT: NVD OF XSS FOR JOOMLA

I have provided the screenshot above of National Vulnerability Database Record which shows the case details, descriptions of issue, Version of web application as well as severity.

You can follow the below link to access the database record of CVE & NVA.

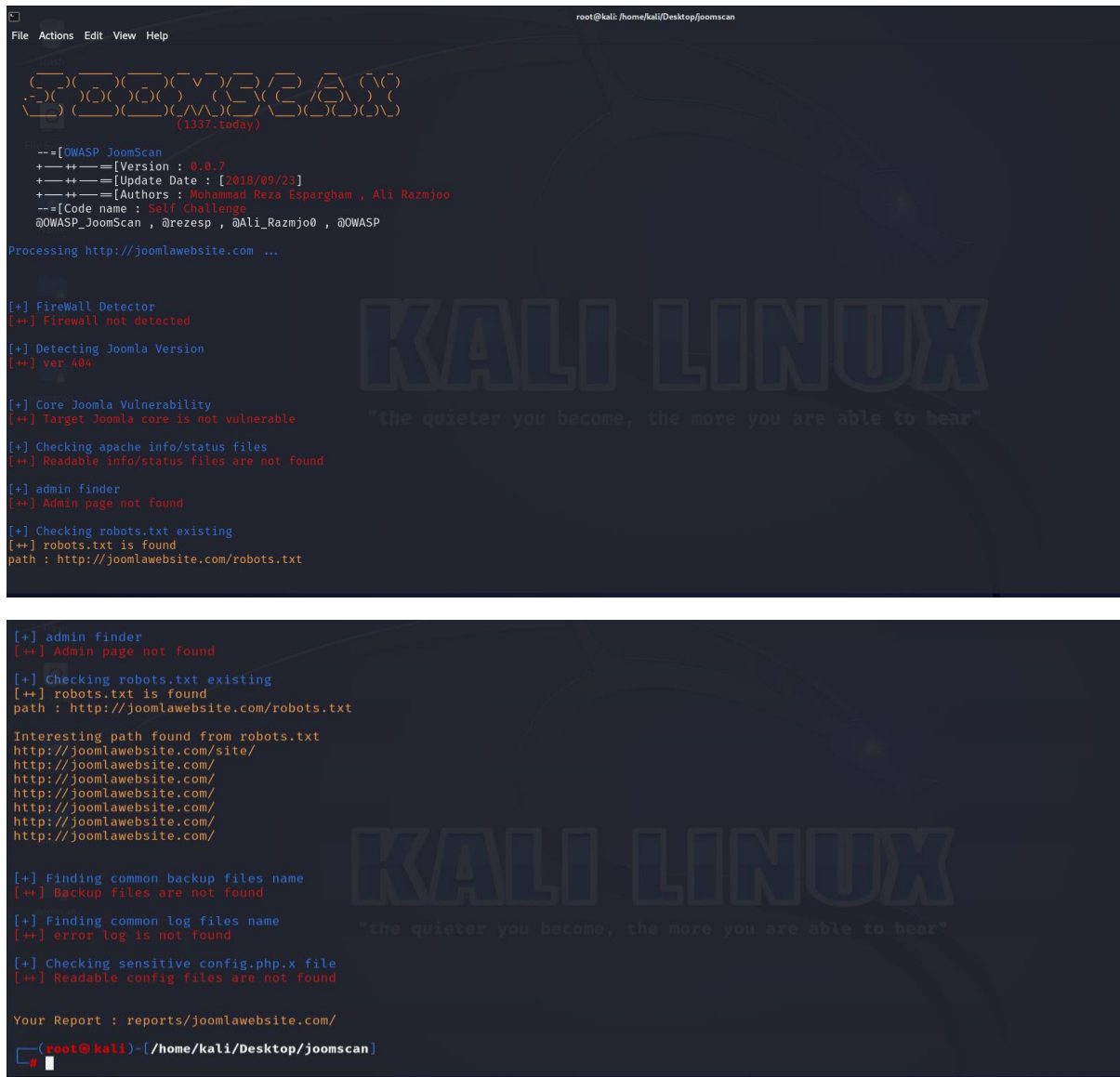
https://cve.mitre.org/cve/search_cve_list.html

<https://nvd.nist.gov/vuln/detail/CVE-2023-49708>

TOOLS FOR SCANNING JOOMLA WEBSITE

1. **SecurityCheck:** It is an extension which can be add to your Joomla application than prevents from 90 different attack patterns. Also, scans the website to check if there is any issue on going.
2. **Joomscan:** It is one of the most popular open-source tool which provides core information about Joomla. You can use this tool in windows as well as in kali linux.
 - You can use the following command to run the test in Joomscan in kali linux.

Perl joomscan.pl -u <http://joomlawebsite.com>



```
root@kali: /home/kali/Desktop/joomscan
File Actions Edit View Help

--=[OWASP JoomScan
+--++--=[Version : 0.0.7
+--++--=[Update Date : [2018/09/23]
+--++--=[Authors : Mohammad Reza Espargham , Ali Razmjoo
+--++--=[Code name : Self Challenge
@OWASP_JoomScan , @rezesp , @Ali_Razmjoo , @OWASP

Processing http://joomlawebsite.com ...

[+] FireWall Detector
[++] Firewall not detected

[+] Detecting Joomla Version
[++] ver 404

[+] Core Joomla Vulnerability
[++] Target Joomla core is not vulnerable

[+] Checking apache info/status files
[++] Readable info/status files are not found

[+] admin finder
[++] Admin page not found

[+] Checking robots.txt existing
[++] robots.txt is found
path : http://joomlawebsite.com/robots.txt

[+] admin finder
[++] Admin page not found

[+] Checking robots.txt existing
[++] robots.txt is found
path : http://joomlawebsite.com/robots.txt

Interesting path found from robots.txt
http://joomlawebsite.com/site/
http://joomlawebsite.com/
http://joomlawebsite.com/
http://joomlawebsite.com/
http://joomlawebsite.com/
http://joomlawebsite.com/
http://joomlawebsite.com/

[+] Finding common backup files name
[++] Backup files are not found

[+] Finding common log files name
[++] error log is not found

[+] Checking sensitive config.php.x file
[++] Readable config files are not found

Your Report : reports/joomlawebsite.com/

root@kali)~[/home/kali/Desktop/joomscan]
```

SCREENSHOT: JOOMSCAN RESULTS

3. **Pentest-Tools:** It is a web based tool which is powered by JoomVS Tool. User simply need to enter the URL in the search box and hit enter. This tool automatically scans the URL and check all the possible templates and module to find out the vulnerability. Also, the beauty of this tool is that it's generates report based on the search and user can make a use of it to understand it.

<https://pentest-tools.com/cms-vulnerability-scanning/joomla-scanner>

4. **SUCURI:** This tool is also a web based tool which provides information about malware and security issues in the website. i.e., Blacklisting, SPAM and any defacement. Also, gives information about the web server, links and scripts.

https://sitecheck.sucuri.net/?cjevent=a6ee96bcc07f11ee827400010a18ba72&cj_aid=13942195&cj_pid=8517397&cj_cid=4761150

5. **Joomla Anti Malware Scan Script (JAMSS):** Basically user have to install this script in their website root location so that it can identify any finger prints, traces that could have been compromised. Installing JAMSS is nothing but uploading JAMSS.php file in your webroot location.

<http://www.your-joomla-site.com/jamss.php>

6. **Detectify:** It is one of the most useful tool for Content Management System (CSM) as it contains top 10 OWASP which benefits to provide more than 1000 vulnerabilities. It not only checks the Joomla security, but also checks for WordPress, Drupal, etc.

<https://detectify.com/cms-security>

7. **SiteGuarding:** It is a cloud-based website security scanner which is an extension also for the Joomla web application. Basically it works like an Anti-Virus for the website.

8. **Hacker Target:** It contains two different options to scan.

- **Passive Scan:** It uses passive scan method to gather information about security which basically extracts using Dorking method, External Links, Directory Index Lookup and Geo-location & Web-Hosting Lookup.
- **Aggressive Scan:** It basically requires a membership to perform aggressive scan which provides details information about the security vulnerability in themes, modules, extensions and in components.

<https://hackertarget.com/joomla-security-scan/>

MITIGATION

1. **Update to Latest Version:** It is always recommended to users to use latest version of web application or software as there are chances in previous version there might be any security issue which is patched in latest version. So, make sure you read the complete description of latest version and use.
2. **Update Extension:** Like software's, extensions also get updates for better performance and other factors which contains security patches as well. So it is essential to keep updated your software extension on time. Also, use the selected extension which is necessary.
3. **Enable Two-Factor Authentication:** It provides a layer of security for the user who uses two-factor or multi-factor authentication on their applications and prevents by getting easily hacked from attackers.

REFERENCE

<https://geekflare.com/joomla-security-vulnerability-scanner/>

<https://portswigger.net/>