# Red Hawk

## Target information

**Domain**
joomla.org

**IP Address**
104.26.14.15

**Date**
09/01/2021 6:14 p.m.

## Shodan

## Gathered information

**Technology:**

- IP: 104.26.14.15
- Service Provider: Cloudflare, Inc.
- Operating System: None

## Ports

**443**
Info: HTTP/1.1 400 Bad Request Server: cloudflare Date: Wed, 01 Sep 2021 12:32:56 GMT Content-Type: text/html Content-Length: 655 Connection: close CF-RAY: -

**2083**
Info: HTTP/1.1 400 Bad Request Server: cloudflare Date: Wed, 01 Sep 2021 02:01:07 GMT Content-Type: text/html Content-Length: 655 Connection: close CF-RAY: -

**8443**
Info: HTTP/1.1 400 Bad Request Server: cloudflare Date: Wed, 01 Sep 2021 02:00:28 GMT Content-Type: text/html Content-Length: 655 Connection: close CF-RAY: -

**2087**
Info: HTTP/1.1 400 Bad Request Server: cloudflare Date: Wed, 01 Sep 2021 01:59:46 GMT Content-Type: text/html Content-Length: 655 Connection: close CF-RAY: -

**80**
Info: HTTP/1.1 403 Forbidden Date: Wed, 01 Sep 2021 01:54:16 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 3748 Connection: close X-Frame-Options: SAMEORIGIN Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Expires: Thu, 01 Jan 1970 00:00:01 GMT Vary: Accept-Encoding Server: cloudflare CF-RAY: 687adea4df36367f-LAX

**8880**
Info: HTTP/1.1 403 Forbidden Date: Wed, 01 Sep 2021 01:53:52 GMT Content-Type: text/plain; charset=UTF-8 Content-Length: 16 Connection: close X-Frame-Options: SAMEORIGIN Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Expires: Thu, 01 Jan 1970 00:00:01 GMT Server: cloudflare CF-RAY: 687ade0fba743625-LAX error code: 1003

**2082**
Info: HTTP/1.1 403 Forbidden Date: Wed, 01 Sep 2021 01:52:27 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 3748 Connection: close X-Frame-Options: SAMEORIGIN Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Expires: Thu, 01 Jan 1970 00:00:01 GMT Vary: Accept-Encoding Server: cloudflare CF-RAY: 687adbf96f9631bb-LAX

**2086**
Info: HTTP/1.1 403 Forbidden Date: Wed, 01 Sep 2021 01:50:09 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 3748 Connection: close X-Frame-Options: SAMEORIGIN Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Expires: Thu, 01 Jan 1970 00:00:01 GMT Vary: Accept-Encoding Server: cloudflare CF-RAY: 687ad89b1be93163-LAX

**8080**
Info: HTTP/1.1 403 Forbidden Date: Wed, 01 Sep 2021 01:47:52 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 3748 Connection: close X-Frame-Options: SAMEORIGIN Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Expires: Thu, 01 Jan 1970 00:00:01 GMT Vary: Accept-Encoding Server: cloudflare CF-RAY: 687ad546fca352b3-LAX

**2052**
Info: HTTP/1.1 403 Forbidden Date: Tue, 31 Aug 2021 00:39:25 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 3750 Connection: close X-Frame-Options: SAMEORIGIN Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Expires: Thu, 01 Jan 1970 00:00:01 GMT Vary: Accept-Encoding Server: cloudflare CF-RAY: 6872339eadfd0517-LAX

**2053**
Info: HTTP/1.1 400 Bad Request Server: cloudflare Date: Tue, 31 Aug 2021 00:27:05 GMT Content-Type: text/html Content-Length: 655 Connection: close CF-RAY: -

**2095**
Info: HTTP/1.1 403 Forbidden Date: Tue, 31 Aug 2021 00:00:23 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 3750 Connection: close X-Frame-Options: SAMEORIGIN Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Expires: Thu, 01 Jan 1970 00:00:01 GMT Vary: Accept-Encoding Server: cloudflare CF-RAY: 6871fa749b690c9f-LAX

**2096**
Info: HTTP/1.1 400 Bad Request Server: cloudflare Date: Mon, 30 Aug 2021 23:53:30 GMT Content-Type: text/html Content-Length: 655 Connection: close CF-RAY: -

### Vulnerabilities

**The host which you are trying to scan seems to be no vulnerable in Shodan**

## Wapiti - Web Application Vulnerability Scanner

**The host which you are trying to scan is unreachable, there is a WAF blocking the requests or you chose Discovery or CMS scanning mode**

## WPScan - WordPress Vulnerability Scanner

### Gathered Information

**It seems that host is reachable but it isn't running WordPress as CMS**

## CMSeek - CMS Scanner

### Gathered information

**CMS: joomla - Version : ['2.5']**

### Vulnerabilities

**Name: Joomla! 'redirect.php' SQL Injection Vulnerability**

Description: ['EDB : https://www.exploit-db.com/exploits/36913/']

**Name: Joomla! 2.5.0 < 2.5.1 - Time Based SQL Injection**

Description: ['EDB : https://www.exploit-db.com/exploits/18618/']

**Name: Joomla! 'highlight.php' PHP Object Injection**

Description: ['CVE : CVE-2013-1453', 'EDB : https://www.exploit-db.com/exploits/24551/']

**Name: Joomla! 'remember.php' PHP Object Injection**

Description: ['CVE : CVE-2013-3242', 'EDB : https://www.exploit-db.com/exploits/25087/']

**Name: Joomla! 1.5 < 3.4.5 - Object Injection Remote Command Execution**

Description: ['CVE : CVE-2015-8562', 'EDB : https://www.exploit-db.com/exploits/38977/']

**Name: Joomla! 1.0 < 3.4.5 - Object Injection 'x-forwarded-for' Header Remote Code Execution**

Description: ['CVE : CVE-2015-8562 , CVE-2015-8566 ', 'EDB : https://www.exploit-db.com/exploits/39033/']

---

**Name: Joomla! Core Remote Privilege Escalation Vulnerability**

Description: ['CVE : CVE-2016-9838', 'EDB : https://www.exploit-db.com/exploits/41157/']

---

**Name: Joomla! 1.6/1.7/2.5 privilege escalation vulnerability**

Description: ['CVE : CVE-2012-1563', 'EDB : https://www.exploit-db.com/exploits/41156/']

---

**Name: Joomla! Component Akeeba Kickstart - Unserialize Remote Code Execution**

Description: ['CVE : CVE-2014-7228', 'EDB : https://www.exploit-db.com/exploits/35033/']

---

**Name: Joomla! 'media.php' Arbitrary File Upload Vulnerability**

Description: ['CVE : CVE-2013-5576', 'EDB : https://www.exploit-db.com/exploits/27610/']

---

**Name: Joomla! Clickjacking Security Bypass Vulnerability**

Description: ['CVE : CVE-2012-5827', 'https://developer.joomla.org/security/news/543-20121101-core-clickjacking.html', 'https://developer.joomla.org/security/news/544-20121102-core-clickjacking.html']

---

**Name: Joomla! Highlighter Plugin Unspecified Cross-Site Scripting Vulnerability**

Description: ['CVE : CVE-2013-3267 ', 'https://developer.joomla.org/security/86-20130407-core-xss-vulnerability.html']

---

**Name: Joomla! Security Bypass Vulnerability**

Description: ['CVE : CVE-2013-3056', 'http://www.securityfocus.com/bid/59490/info']

---

**Name: Joomla! Information Disclosure Vulnerability**

Description: ['CVE : CVE-2013-3057', 'http://www.securityfocus.com/bid/59489', 'http://developer.joomla.org/security/82-20130402-core-information-disclosure.html']

---

**Name: Joomla! Unspecified Cross-Site Scripting Vulnerability**

Description: ['CVE : CVE-2013-3058', 'http://www.securityfocus.com/bid/59483', 'http://developer.joomla.org/security/81-20130403-core-xss-vulnerability.html']

---

**Name: Joomla! Unspecified Cross-Site Scripting Vulnerability**

Description: ['CVE : CVE-2013-3059', 'https://developer.joomla.org/security/80-20130405-core-xss-vulnerability.html']

---

**Name: Joomla! Core Authentication Bypass Vulnerability**

Description: ['CVE :CVE-2014-6632', 'http://developer.joomla.org/security/594-20140902-core-unauthorised-logins.html']

---

**Name: Joomla! Core Remote Denial of Service Vulnerability**

Description: ['CVE : CVE-2014-7229', 'https://developer.joomla.org/security/596-20140904-core-denial-of-service.html']

---

**Name: Joomla! Open Redirection Vulnerability**

Description: ['CVE : CVE-2015-5608', 'http://www.securityfocus.com/bid/76496']

---

**Name: Joomla! Cross Site Request Forgery Vulnerability**

Description: ['CVE : CVE-2015-5397', 'https://developer.joomla.org/security-centre/618-20150602-core-remote-code-execution.html']

---

**Name: Joomla! Core Security Bypass Vulnerability**

Description: ['CVE : CVE-2015-7859', 'https://developer.joomla.org/security-centre/629-20151002-core-acl-violations.html']

---

**Name: Joomla! Directory Traversal Vulnerability**

Description: ['CVE : CVE-2015-8565', 'https://developer.joomla.org/security-centre/635-20151214-core-directory-traversal-2.html']

---

**Name: Joomla! Core Cross Site Request Forgery Vulnerability**

Description: ['CVE : CVE-2015-8563', 'https://developer.joomla.org/security-centre/633-20151214-core-csrf-hardening.html']

---

**Name: Joomla! Information Disclosure Vulnerability**

Description: ['CVE : CVE-2016-9837', 'https://developer.joomla.org/security-centre/666-20161203-core-information-disclosure.html']

---

**Name: PHPMailer Remote Code Execution Vulnerability**

Description: ['CVE : CVE-2016-10033', 'https://www.rapid7.com/db/modules/exploit/multi/http/phpmailer_arg_injection', 'https://github.com/opsxcq/exploit-CVE-2016-10033', 'EDB : https://www.exploit-db.com/exploits/40969/']

---

**Name: PPHPMailer Incomplete Fix Remote Code Execution Vulnerability**

Description: ['CVE : CVE-2016-10045', 'https://www.rapid7.com/db/modules/exploit/multi/http/phpmailer_arg_injection', 'EDB : https://www.exploit-db.com/exploits/40969/']

---