Target information

Domain
epes.com

IP Address
64.190.62.111

Date
08/31/2021 11:03 a.m.

Shodan

Gathered information

Technology:
- IP: 64.190.62.111
- Service Provider: SEDO GmbH
- Operating System: None

Ports

443
Info: HTTP/1.1 200 OK Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Content-Type: text/html; charset=UTF-8 Date: Tue, 31 Aug 2021 11:03:18 GMT Expires: Mon, 26 Jul 1997 05:00:00 GMT Last-Modified: Tue, 31 Aug 2021 11:03:18 GMT Pragma: no-cache Server: NginX Vary: Accept-Encoding X-Adblock-Key:
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANnylWw2vLY4hUn9w06zQKbhKBfvjFUCsdFlb6TdQhxb9RXWXuI4t31c+o8fYOv/s8q1LGPga3DE1L/tHU4LENMCAwEAAQ==_uJsavDDltZ+oJKHJmCETfWSZWvUtGeBLUmvmofqhsLv4ex415lYCJK7T
X-Cache-Miss-From: parking-6cf5fb6c75-l2xj9 Transfer-Encoding: chunked

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

Technology:
- Server: Apache
- Proxy-Connection: Keep-Alive

WordPress version
- Version: 5.1.1
- Launch date: 2019-03-13
- Version status: insecure
- Method: Rss Generator (Passive Detection)

Interesting Findings

http://www.epes.es/robots.txt

Description: robots.txt found: http://www.epes.es/robots.txt

Type: robots_txt

Method: Robots Txt (Aggressive Detection)

http://www.epes.es/xmlrpc.php

Description: XML-RPC seems to be enabled: http://www.epes.es/xmlrpc.php

Type: xmlrpc

Method: Link Tag (Passive Detection)

http://www.epes.es/readme.html

Description: WordPress readme found: http://www.epes.es/readme.html

Type: readme

Method: Direct Access (Aggressive Detection)

http://www.epes.es/wp-content/debug.log

Description: Debug Log found: http://www.epes.es/wp-content/debug.log

Type: debug_log

Method: Direct Access (Aggressive Detection)

http://www.epes.es/wp-cron.php

Description: The external WP-Cron seems to be enabled: http://www.epes.es/wp-cron.php

Type: wp_cron

Method: Direct Access (Aggressive Detection)

Themes

Name: ultimatum

Evidence: False

Directory list: False

Method: Urls In Homepage (Passive Detection)

Plugins

Name: cred-frontend-editor

Evidence: http://www.epes.es/wp-content/plugins/cred-frontend-editor/

Method: Urls In Homepage (Passive Detection)

Name: indeed-social-media

Evidence: http://www.epes.es/wp-content/plugins/indeed-social-media/

Method: Urls In Homepage (Passive Detection)

Name: js_composer

Evidence: http://www.epes.es/wp-content/plugins/js_composer/

Method: Body Tag (Passive Detection)

Name: LayerSlider

Evidence: http://www.epes.es/wp-content/plugins/LayerSlider/

Method: Urls In Homepage (Passive Detection)

Name: responsive-lightbox

Evidence: http://www.epes.es/wp-content/plugins/responsive-lightbox/

Method: Urls In Homepage (Passive Detection)

Name: search-filter

Evidence: http://www.epes.es/wp-content/plugins/search-filter/

Method: Urls In Homepage (Passive Detection)

Name: types

Evidence: http://www.epes.es/wp-content/plugins/types/

Method: Urls In Homepage (Passive Detection)

Name: ubermenu

Evidence: http://www.epes.es/wp-content/plugins/ubermenu/

Method: Urls In Homepage (Passive Detection)

Name: wp-views

Evidence: http://www.epes.es/wp-content/plugins/wp-views/

Method: Urls In Homepage (Passive Detection)

CMSeek - CMS Scanner (Joomla)

Gathered information

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