(·>papaki HELP

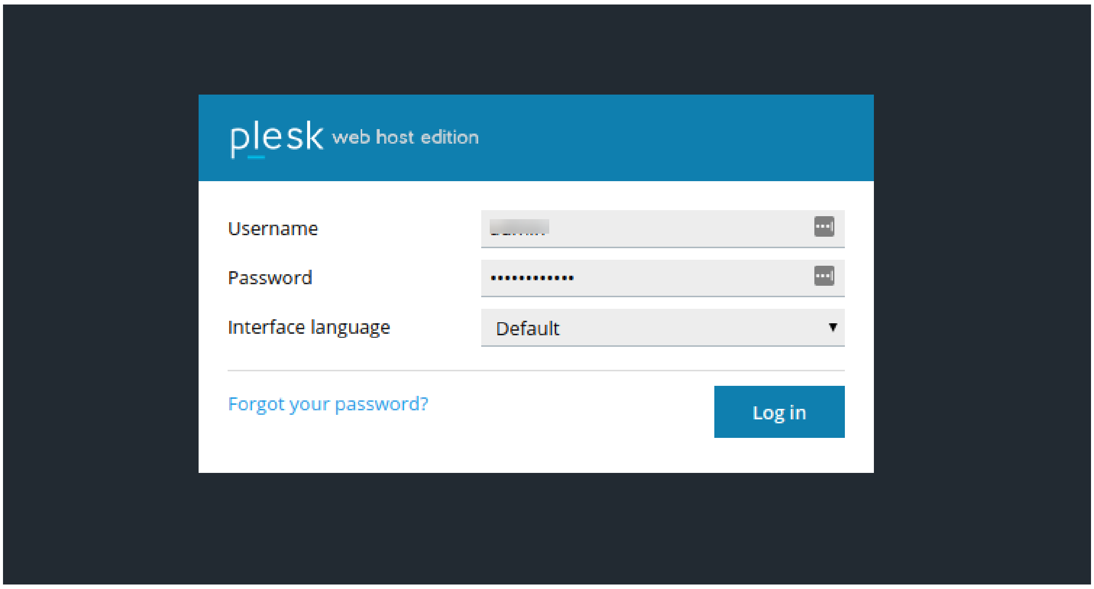
Knowledgebase > Plesk > Γενικά > How can I use ImunifyAV to scan my website for malwares

How can I use ImunifyAV to scan my website for malwares

Alexandros Karagiannis - 2022-12-28 - Γενικά

In case you use Plesk server on Linux, you have the ability to scan your files for potentially malicious content using **ImunifyAV**.

Firstly, login to Plesk with your credentials.

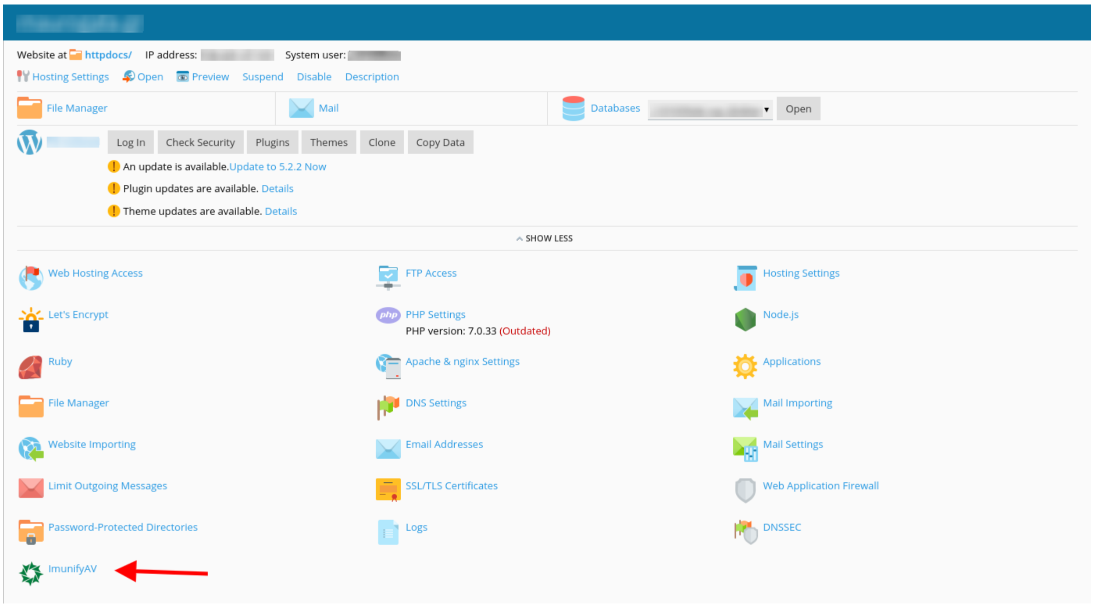


Username [redacted]

Password ••••••••••••

Interface language Default ▾

You can then select **Website & Domains** from the left list and click on **ImunifyAV**.



Website at httpdocs/ IP address: [redacted] System user: [redacted]

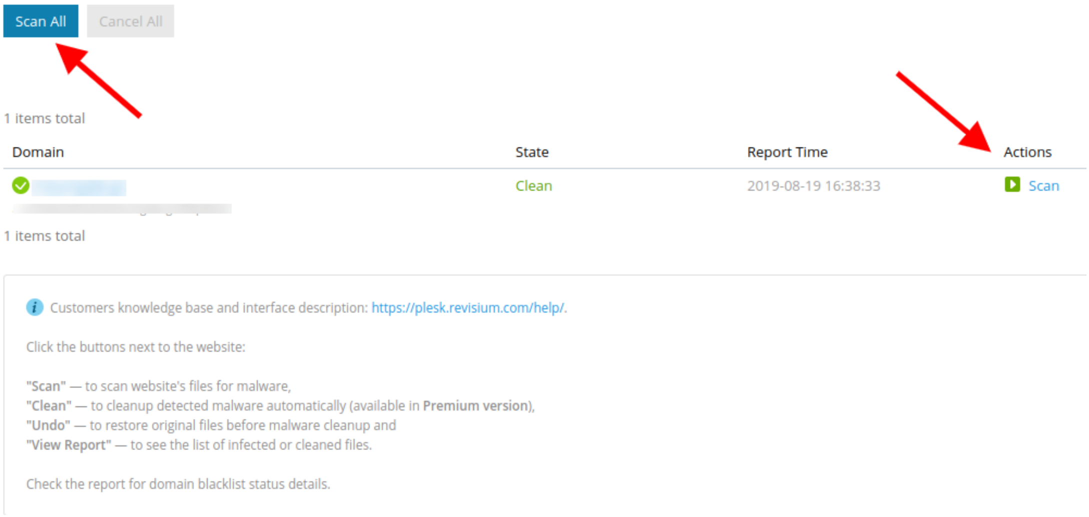
! An update is available.Update to 5.2.2 Now

! Plugin updates are available. Details

! Theme updates are available. Details

PHP version: 7.0.33 (Outdated)

To start scanning, select **Scan** to apply it on your website.
Otherwise, if your plan contains more than one domain and you wish to scan them all, select **Scan All**.



1 items total

Domain	State	Report Time	Actions
✓ [redacted] [redacted]	Clean	2019-08-19 16:38:33	Scan

1 items total

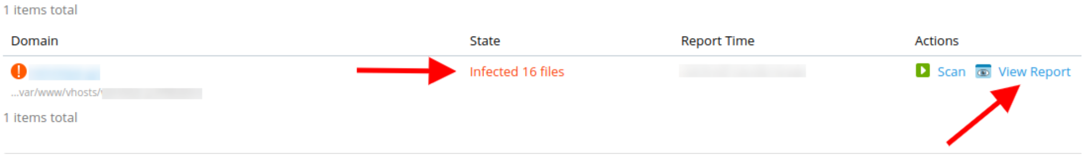
Customers knowledge base and interface description: https://plesk.revisium.com/help/.

Click the buttons next to the website:

"Scan" — to scan website's files for malware,
"Clean" — to cleanup detected malware automatically (available in **Premium version**),
"Undo" — to restore original files before malware cleanup and
"View Report" — to see the list of infected or cleaned files.

Check the report for domain blacklist status details.

If ImunifyAV does not detect any malware in your website, then a **Clean** indication will appear in the field **State**.
In case malware or security gaps have been detected, then an **Infected** indication will appear in the field **State**.



1 items total

Domain	State	Report Time	Actions
! [redacted] ...var/www/vhosts/[redacted]	Infected 16 files	[redacted]	Scan View Report

1 items total

You can see the ImunifyAV report containing potential security gaps or malware by clicking on **View Report**.

Summary

Finished at: [redacted]
Spent time: 1m43s
Number of scanned files: 6218
Available for auto-cleanup: 16

Public Vulnerabilities

File	Vulnerability
/homedir/public_html/wp-content/plugins/wp_rokbox/thumb.php	RCE : TIMTHUMB : CVE-2011-4106,CVE-2014-4663
/homedir/public_html/wp-content/plugins/wp_rokstories/thumb.php	RCE : TIMTHUMB : CVE-2011-4106,CVE-2014-4663
/homedir/public_html/wp-content/plugins/wp_roknewspager/thumb.php	RCE : TIMTHUMB : CVE-2011-4106,CVE-2014-4663

16 items total

Pages: First << 1 2 >> Last

Entries per page: 10 25 10

ID	Type	Action	Signature ID	File	Size	Modified
1	SRV	⚠ Ignore	SMW-INJ-03406-bkdr.eval-0	/homedir/public_html/wp-admin/admin-footer.php ...|<?php...	14 KB	2018-05-16 15:07:46
2	SRV	⚠ Ignore	SMW-INJ-03406-bkdr.eval-0	/homedir/public_html/wp-admin/custom-background.php ...|<?php...	24 KB	2018-05-16 15:07:47
3	SRV	⚠ Ignore	SMW-INJ-03406-bkdr.eval-0	/homedir/public_html/wp-content/plugins/contact-form-7/includes/capabilities.php ...|<?php...	9 KB	2018-05-16 15:10:51
4	SRV	⚠ Ignore	SMW-INJ-03406-bkdr.eval-0	/homedir/public_html/wp-content/plugins/roknewsflash/CHANGELOG.php ...|<?php...	11 KB	2018-05-16 15:08:55
5	SRV	⚠ Ignore	SMW-INJ-03406-bkdr.eval-0	/homedir/public_html/wp-content/plugins/gantry/gizmos/rokstyle.php ...|<?php...	13 KB	2018-05-16 15:11:20
6	SRV	⚠ Ignore	SMW-INJ-03548-bkdr-3	/homedir/public_html/wp-content/uploads/wysija/themes/tmp/LgOgu.php.suspected ...<?php info();?> |<?php eval($_POST['pass3s']);?...	49 b	2018-05-16 15:56:13
7	SRV	⚠ Ignore	SMW-SA-04420-wshll-0	/homedir/public_html/wp-content/uploads/wysija/themes/KGWsBsuCMA/index.php ...<?php if(md5($_POST['password'])=='e191ee875c345f5adaf7e3c448f1a230'){ |preg_repl...	237 b	2018-05-16 15:56:09
8	SRV	⚠ Ignore	SMW-SA-04420-wshll-0	/homedir/public_html/wp-content/uploads/wysija/themes/hxqJTacnwG/index.php ...<?php if(md5($_POST['password'])=='0240387be81a74fca223bf3002502b8c'){ |preg_repl...	237 b	2018-05-16 15:56:08