Πώς μπορώ να εξαιρέσω κανόνα του Mod_Security ;

- 2021-05-25 - Γενικά

Σε περίπτωση που το site σας εμφανίζει 403 Forbidden, αυτό σημαίνει πως το Mod_security κόβει αιτήματα που τα θεωρεί κακόβουλα.

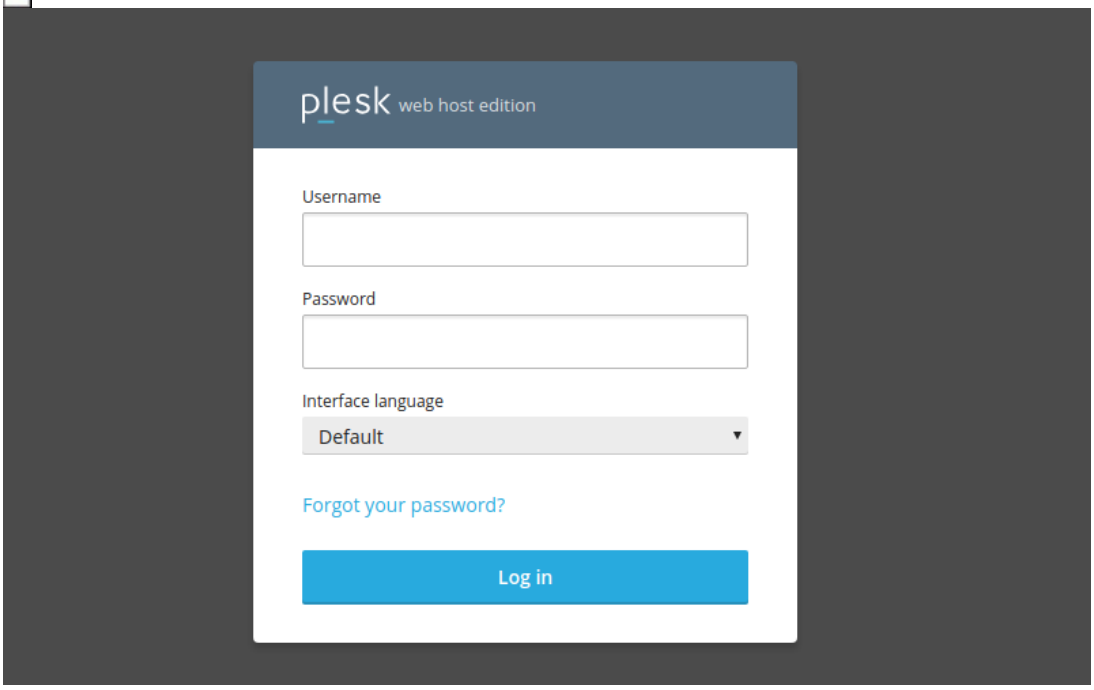
Το Mod_security (Web Application Firewall) είναι το firewall σε επίπεδο cms όπως το wordpress ή το Joomla. Εξετάζει τα αιτήματα (requests) που γίνονται στον server και το κατηγοριοποιεί ως κακόβουλα ή όχι. Μέσα από τα error logs του PLesk, καταγράφεται ο κανόνας όπως και το id του. Το σφάλμα θα είναι της παρακάτω μορφής :

"\[Thu Jun 02 14:31:04 2016\] \[error\] \[client 213.16.178.247] ModSecurity: Access denied with code 403 (phase 2). Pattern match "(?:\\\\b(?:c(?:d(?:\\\\b[^a-zA-Z0-9_]{0,}?[/\\\\]|[^a-zA-Z0-9_]{0,}?\\\\.\\\\.)|hmod.{0,40}?\\\\+.{0,3}x|md(?:\\\\b[^a-zA-Z0-9_]{0,}?/c|(?:\\\\.exe|32)\\\\b))|(?:echo\\\\b[^a-zA-Z0-9_]{0,}?\\\\by{1,}|n(?:et(?:\\\\b[^a-zA-Z0-9_]{1,}?\\\\blocalgroup|\\\\.exe)|(?:c|map)\\\\.exe)|t(?:c ..." at ARGS:snippet. [file "/etc/httpd/conf/modsecurity.d/rules/comodo/01_Global_Generic.conf"\] \[line "59"\]\[id "211210"][rev "6"\] \[msg "COMODO WAF: System Command Injection|36pos.eoo.gr|"\] \[data "Matched Data: \`[[\*id found within ARGS:snippet: [[++site_start:is=\`[[*id]]\`:then=\` [title][[++site_name]][/title]\`:else=\` [title][[++site_name]] - [[*pagetitle]][/title]\`]] [meta charset=utf-8/] [meta name = format-detection content = telephone=no/] [[$metas]\] \[[$ogs\]] [link rel=icon href=\[[++site_url]]assets/theme/images/favicon36.ico type=image/x-icon/] [link rel=alternate type=application/rss+xml title=[[++site_name]] :: rss feed href=[[++site_url]\]\[[~39\]]/] \[[$css]\] \[[$js\]] \[[$google analytics]]

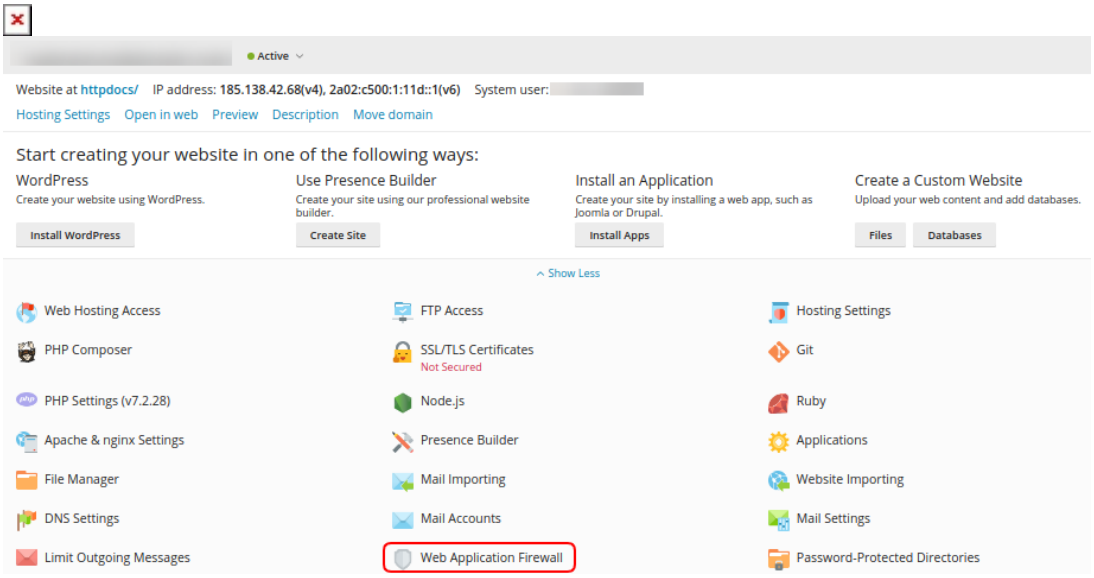
Το Plesk, δίνει τη δυνατότητα να προσθέσετε στις εξαιρέσεις τον κανόνα μέσω του Web Application Firewall

Για να προσθέσετε ένα κανόνα (id), μέσα στο Web Application Firewall, ακολουθείστε τις οδηγίες που περιγράφονται παρακάτω :

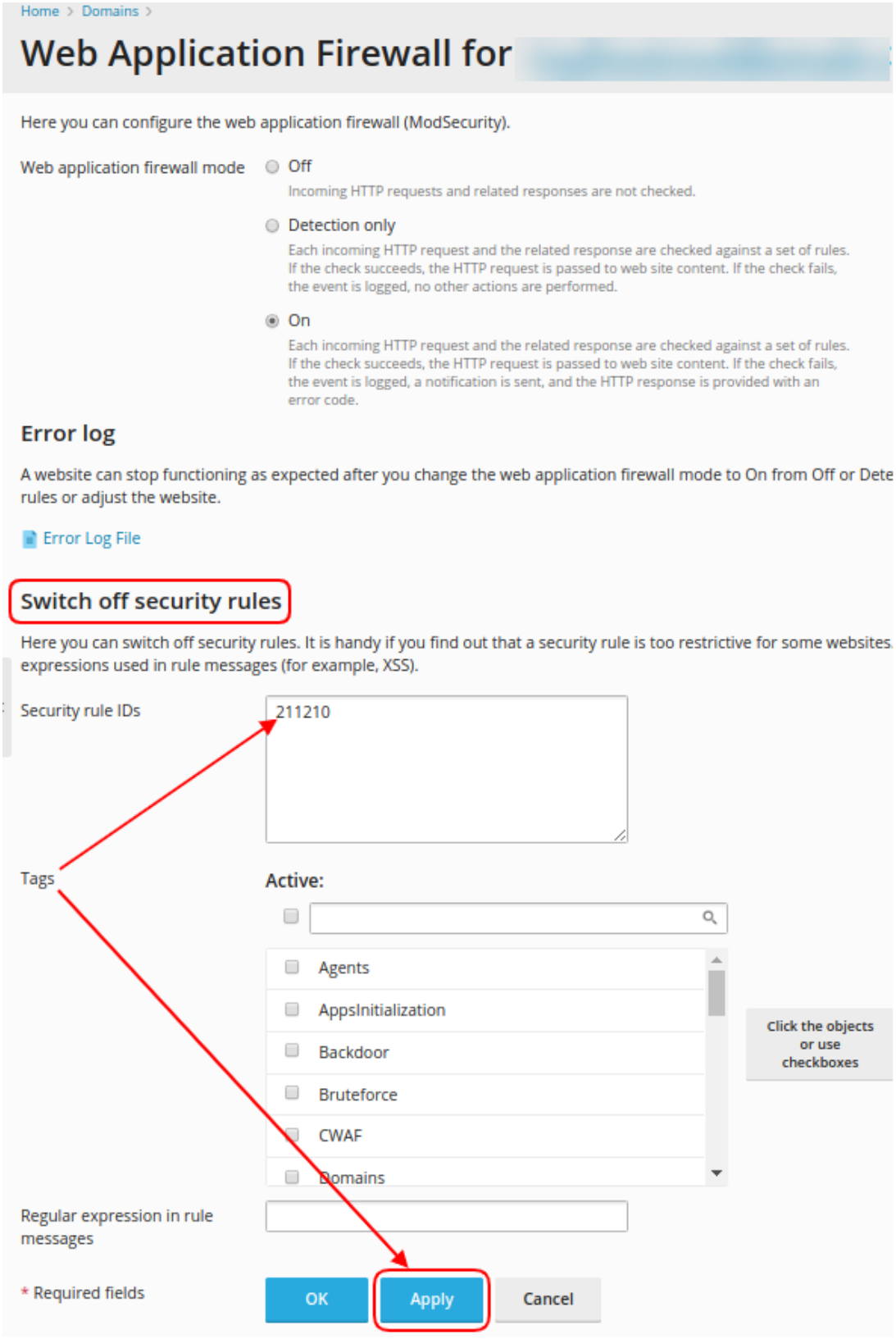
1. Συνδεθείτε στο **Plesk** με τα στοιχεία πρόσβασης σας.



2. Στην καρτέλα **Websites & Domains**, επιλέξτε **Web Application Firewall.**



3. Στο πεδίο **Security rules IDs** (στην κατηγορία **Switch Off Security rules**) , δηλώστε το Id που θα δείτε στο error log (όπως στο παραπάνω παράδειγμα), επιλέξτε **Apply** και **Ok.**



ΠΡΟΣΟΧΗ : Σε περίπτωση που υπάρχουν παραπάνω από μία εξαιρέσεις, προσθέτετε το ID το ένα κάτω από το άλλο και όχι το ένα δίπλα στο άλλο.