**Lab9 – Mod\_security**

**Joni korpihalkola**

Document your commands or take screenshots. Answer questions in english or finnish.

Use Ubuntu server on Virtual box. Use Bridged network adapter.

Main idea is to Install LAMP on server, then set it up so we can try injections on it.

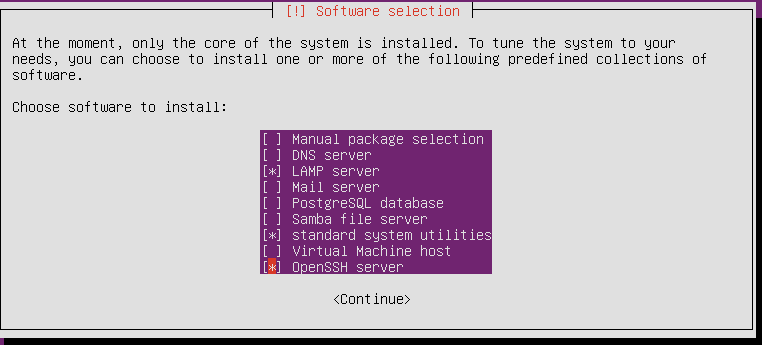
Next we install mod\_security and change settings so it doesn’t allow injections.

Then we create custom form to submit data. After that we make custom rules to prevent usage of specific words.

This all can be done by following this tutorial: <https://www.digitalocean.com/community/tutorials/how-to-set-up-mod_security-with-apache-on-debian-ubuntu>

1p for Installing LAMP

Latasin netistä Ubuntu Serverin ja asensin siihen LAMP stackin ja ssh serverin.



1p for setting up database & login site, and proving login & injection works.

1p for installing mod\_secure + preventing injection (NOTE where guide says: “nano /etc/apache2/mods-enabled/modsecurity.conf” depending how you installed it might be /etc/apache2/mods-enabled/security2.conf or something like that.)

Modsecurityn asennus ja käyttöönotto





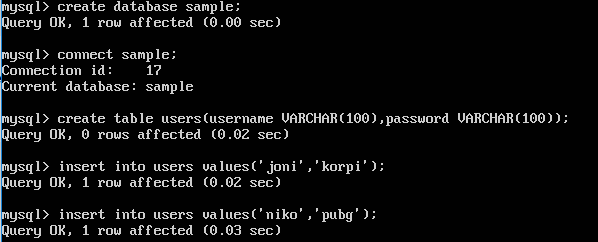


Modsecurity.conf muokkaukset

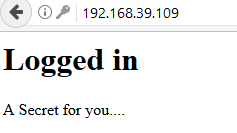
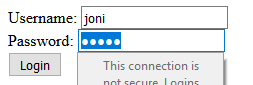




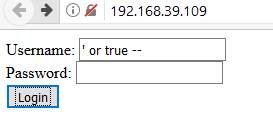
Mysql users taulun luonti, jolla kirjaudutaan sisään



Login sivu toimii luoduilla käyttäjätunnuksilla

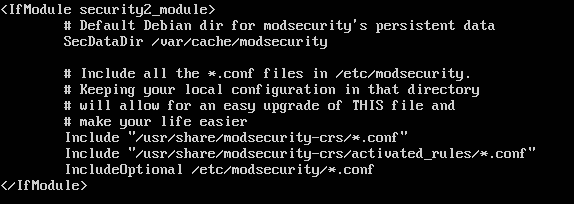


Ja myös injektiolla



1p for creating custom form + creating custom rule to block specific words from it, prove that it works.

Security2.conf muokkaukset



Symbolinen linkki

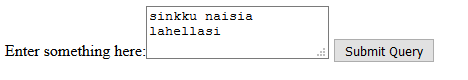


Nyt kun injektiolla yritetään kirjautua sisään, sitä ei päästetä



Luodaan form.php ja sille omat custom rules tarkistamaan tekstikentän sisältö





Säännöt blockkaavat, koska tekstistä löytyy blockattavia sanoja.



1p for proving that you can Exclude some directories from rules. For example, create custom form to other directory (/var/www/html/notblocked/form.php) and prove that it doesn’t get checked by rules even original form.php is checked

Muokkasin security2.conf



Jolloin notblocked polussa olevaa form.php:n sisältöä ei blockata.

