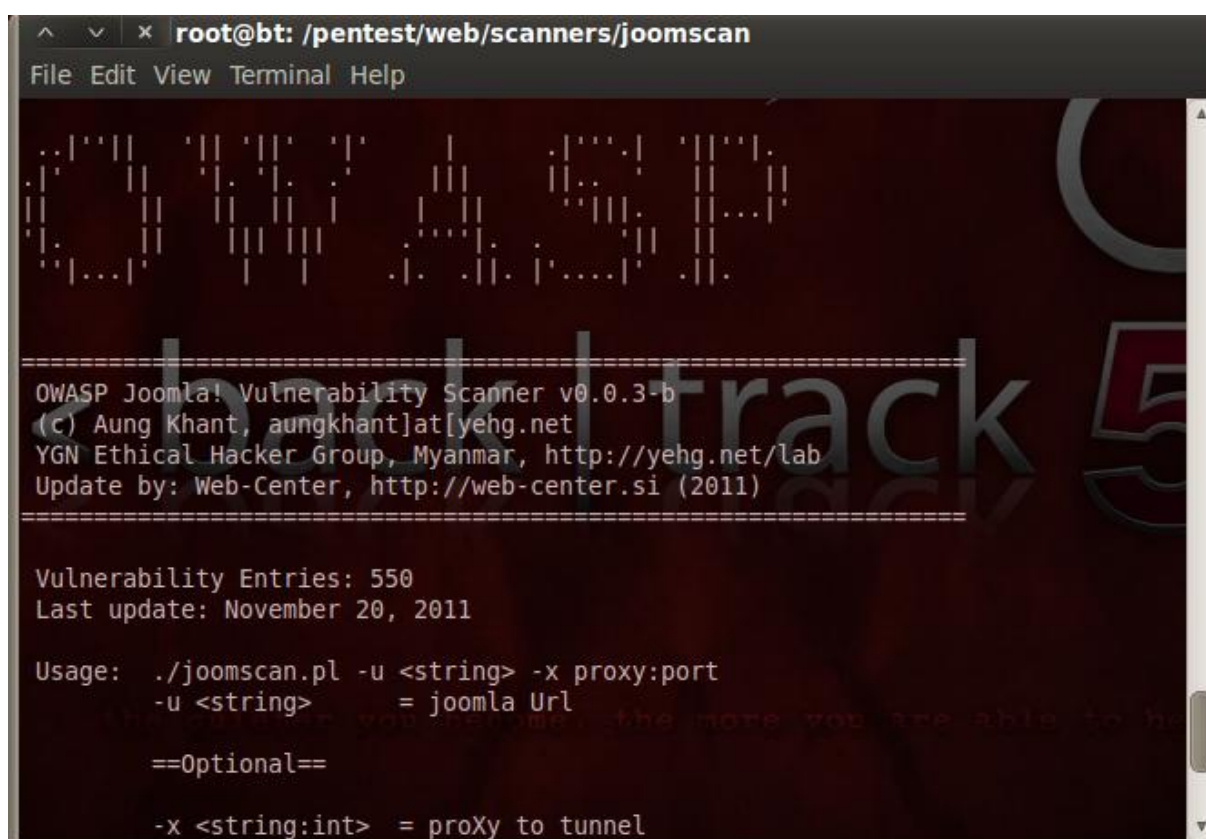


# Navodila za uporabo

## Orodje za pregledovanje Joomla (Joomscan)

Joomscan je orodje za testiranje ranljivosti spletnih strani, ki uporabljajo brezplačni sistem za urejanje spletne vsebine 'Joomla'. Joomscan vam omogoča pregledovanje oz. testiranje vaše spletne strani na tki. napade XSS, SQL Injection, LFI, RFI, BruteForce itd. V zadnji posodobitvi je bilo v bazi vpisanih 466 ranljivih komponent, danes pa baza šteje že 550 vpisanih ranljivosti. V seznam smo vključili ranljivosti Joomla kot sistema, komponente ipd. iz leta 2010 in pa 2011.



```
root@bt: /pentest/web/scanners/joomscan
File Edit View Terminal Help

OWASP

OWASP Joomla! Vulnerability Scanner v0.0.3-b
(c) Aung Khant, aungkhant[at]yehg.net
YGN Ethical Hacker Group, Myanmar, http://yehg.net/Lab
Update by: Web-Center, http://web-center.si (2011)

Vulnerability Entries: 550
Last update: November 20, 2011

Usage: ./joomscan.pl -u <string> -x proxy:port
       -u <string>      = joomla Url
       ==Optional==
       -x <string:int> = proXy to tunnel
```

Prenesi:

<http://web-center.si/joomscan/joomscan.rar> (Windows)

<http://web-center.si/joomscan/joomscan.tar.gz> (Linux)

1. Najprej si orodje prenesete na svoj računalnik, ga odprete in prenesete v mapo "/pentest/web/scanners/joomscan/". V Windows okolju zadevo opravite nekoliko drugače. Najprej si namestite program ActivePerl (navodila si lahko ogledate na naslednji povezavi: <http://web-center.si/splosno/154-namestitev-perl-a>). Po opravljeni namestitvi programa ActivePerl, orodje shranite npr. na namizije in v konzoli vpišete naslednje:

- cd desktop
- cd joomscan
- joomscan.pl



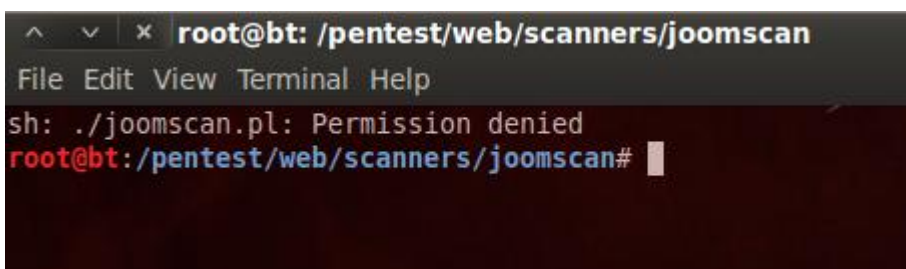
2. V mapo joomscan lahko prenesete vse datoteke ali pa samo skripto joomscan.pl.

Razlika je v tem da v prvem primeru ne bo potrebno opraviti posodobitev, medtem ko v drugem primeru bo to potrebno.



(Tale korak ne velja za Windows okolje)

3. Zadevo zaženete, nato ji dodelite pravice 777, z ukazom: `chmod 0777 joomscan.pl`, kot je na sliki spodaj:



```
root@bt:/pentest/web/scanners/joomscan# chmod 0777 joomscan.pl
root@bt:/pentest/web/scanners/joomscan#
```

(Tale korak ne velja za Windows okolje)

4. Sedaj je potrebno opraviti še posodobitev baze (velja za tiste, ki so prenesli v mapo joomscan samo datoteko joomscan.pl), tako kot je na sliki spodaj:

```
=====
OWASP Joomla! Vulnerability Scanner v0.0.3-b
(c) Aung Khant, aungkhant[at]yehg.net
YGN Ethical Hacker Group, Myanmar, http://yehg.net/lab
Update by: Web-Center, http://web-center.si (2011)
=====
Vulnerability Entries: 466
Last update: August 18, 2009

Usage: ./joomscan.pl -u <string> -x proxy:port
       -u <string>      = joomla Url
```

```
root@bt:/pentest/web/scanners/joomscan# ./joomscan.pl update
```

5. Če ste do sedaj vse pravilno opravili, bi zadeva morala izgledati kot na sliki, s posodobljeno bazo:

```
OWASP Joomla! Vulnerability Scanner Database Update
(c) Aung Khant, http://yehg.net/lab
Update by: Web-Center, http://web-center.si

Remote Database Entries: 550
Remote Last Update: November 20, 2011

Local Database Entries: 466
Local Last update: August 18, 2009

~Updating..

~Done successfully. have fun!
```

6. Sedaj lahko uspešno uporabljate orodje in pregledujete vaše spletne strani.

```
Target: http://www.web-center.si
Server: Apache
X-Powered-By: PHP/5.2.17

## Checking if the target has deployed an Anti-Scanner measure
[!] Scanning Passed ..... OK
```

**OPOMBA: Orodje Joomscan je izključno namenjeno za testiranje ranljivosti spletnih strani in nikakor za zlonamerno uporabo!**

Naj še opomnimo, da bomo posodobitve izdajali predvidoma vsak mesec oz. po potrebi.

Za dodatna vprašanja ali predloge nam lahko pišete na email naslov: [info@web-center.si](mailto:info@web-center.si)

Web-Center 2011, <http://web-center.si>