OWASP
Open Web Application
Security Project

OWASP JoomScan Project

Mohammad Reza Espargham & Esmaeil Rahimian

Blackhat Asia Arsenal 2018

Project Leaders

- Mohammad Reza Espargham @rezesp
- Ali Razmjoo Qalaei @Ali_Razmjo0

Joomla !

- Joomla is the second most popular content management system used by 7% (26,474 million installed) of the CMS based websites. The first version of Joomla was released in 2005 as the rebranding of the Mambo CMS by an Australian Company. Among the three CMS platforms compared here, Joomla seems the youngest, however, it has already earned lots of public interest as it offers an amazing platform for building websites

Slow Loris & JoomScan

What is OWASP JoomScan?

- OWASP JoomScan (short for [Joom]la Vulnerability [Scan]ner) is an opensource project in perl programming language to detect Joomla CMS vulnerabilities and analysis them.

WHY?

- If you want to do a penetration test on a Joomla CMS, OWASP JoomScan is Your best shot ever! This Project is being faster than ever and updated with the latest Joomla vulnerabilities.

Influenced

OWASP VBScan Project

https://www.owasp.org/index.php/OWASP_VBScan_Project

https://github.com/rezasp/vbscan

- VBScan (short for [VB]ulletin Vulnerability [Scan]ner) is a project to detect VBulletin CMS vulnerabilities and analysis them.

What sort of tools?

- Update with latest published exploits
- Easy to use
- PowerFul
- Free and open-source software
- Written in perl programming language
- Support
- Extensibility
- Cross platform
- Fast
- User Friendly Report
- Under active development
- Involvement actively encouraged

The Features:

- Version enumerator
- Vulnerability enumerator (based on version)
- Components enumerator (1205 most popular by default)
- Components vulnerability enumerator (based on version)(+950 exploit)
- Reporting to Text & HTML output
- Finding common log files name
- Finding common backup files name

The Features:

- Configuration files finder
- Checking robots.txt existing
- Admin page finder
- Directory listing checker
- Debug mode status checker
- Random agent and customized agent support
- Customized cookie support
- Other Joomla misconfigurations check

Latest Version

OWASP JoomScan 0.0.5

Codename: KLOT

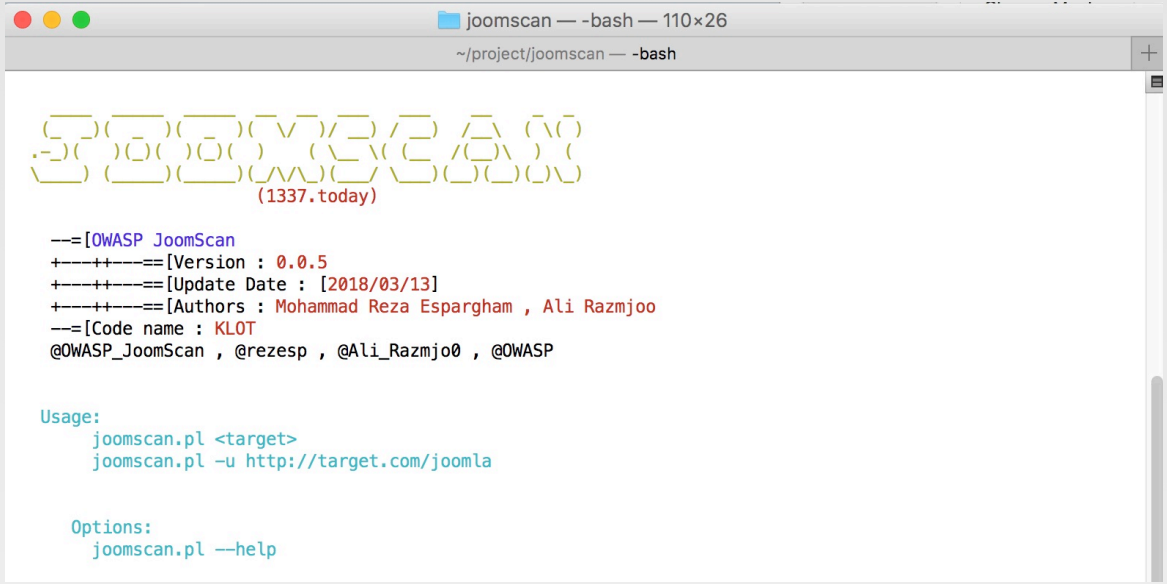
Audience:

- Security Researchers
- Penetration testers
- Teachers and Students (OWASP top 10 or other methodology methods)
- Joomla contributors
- and you ☺
- …

TODO

- Powerful REST based API
- Tor support
- Bypass firewalls
- Enhanced scanners to detect more vulnerabilities
- Technology detection
- Validation Scan
- What do you want?? ☺

UI


joomscan — -bash — 110×26
~/project/joomscan — -bash
(1337.today)
--=[OWASP JoomScan
+---++---==[Version : 0.0.5
+---++---==[Update Date : [2018/03/13]
+---++---==[Authors : Mohammad Reza Espargham , Ali Razmjoo
--=[Code name : KLOT
@OWASP_JoomScan , @rezesp , @Ali_Razmjo0 , @OWASP
Usage:
joomscan.pl <target>
joomscan.pl -u http://target.com/joomla
Options:
joomscan.pl --help

HTML Report

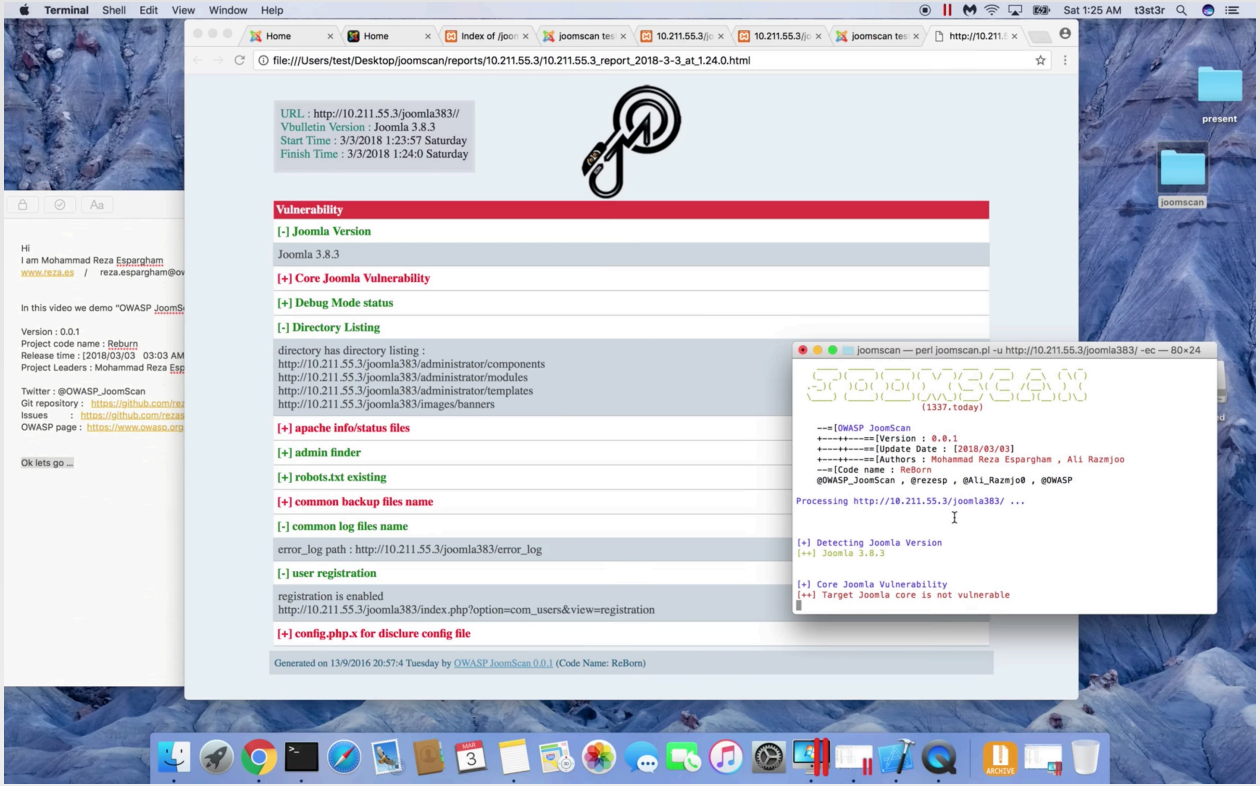
/joomscan/reports/10.211.55.3/10.211.55.3_report_2018-3-16_at_4.12.59.html

URL : http://10.211.55.3/joomla383//
Joomla Version : Joomla 3.8.3
Start Time : 2018-3-16 4:12:40 Friday
Finish Time : 16/3/2018 4:12:59 Friday

Vulnerability
[+] Joomla Version
[+] Core Joomla Vulnerability
[+] Debug Mode status
[+] Directory Listing
[+] apache info/status files
[+] admin finder
[+] robots.txt existing
[+] common backup files name
[+] common log files name
[+] user registration
[+] sensitive config.php.x file
[+] Enumeration component (com_ajax)
[+] Enumeration component (com_banners)
[+] Enumeration component (com_contact)
[+] Enumeration component (com_content)
[+] Enumeration component (com_contenthistory)
[+] Enumeration component (com_fields)
[+] Enumeration component (com_finder)
[+] Enumeration component (com_mailto)
[+] Enumeration component (com_media)
[+] Enumeration component (com_newsfeeds)
[+] Enumeration component (com_search)
[+] Enumeration component (com_users)
[+] Enumeration component (com_wrapper)

Generated on 13/9/2016 20:57:4 Tuesday by OWASP JoomScan 0.0.5 (Code Name: KLOT)

Demo time



https://youtu.be/Ik2CJ9LkuoI

OWASP
Open Web Application Security Project

https://www.owasp.org/index.php/Category:OWASP_Joomla_Vulnerability_Scanner_Project

https://github.com/rezasp/joomscan

@OWASP_JoomScan

Any Questions?

@rezesp

@Ali_Razmjo0