

Forum:[Hack Forums](#)

Thread: [\[Mass Exploit\] Joomla 3.2 to 3.4 SQL Injection](#)

makmaniac - October 28, 2015, 8:44 pm

Hello HF ?

I love to automate stuff. I wrote this demo exploit to automate SQL injection vulnerability in open source CMS joomla (3.2 to 3.4.4) found by Trust Wave Labs. CVE-2015-7297, CVE-2015-7857, and CVE-2015-7858 cover this SQL Injection vulnerability.

I have used [Google Scraper and Mass Exploiter](#) from one of my previous projects which works as a dork scanner and performs mass exploitation on hundreds of URLs in a matter of seconds.

Here's a preview.

[\[img=500x400\]http://mukarramkhalid.com/wp-content/uploads/2015/10/joomla1.png\[/img\]](#)

Requirements

Python version 3.4.x or higher

A third party package – [Requests](#)

GitHub Repository

[Joomla 3.2 to 3.4.4 Remote SQL Injection Mass Exploit](#)

Blog Post

[\[Mass Exploit\] Joomla 3.2 to 3.4 SQL Injection](#)

Last Scan Results

Code [+] Starting dork scanner for : inurl:"/component/tags/"

[+] Total URLs found : 452

[+] URLs written to urls.txt

[+] Trying Joomla SQL Injection exploit on 452 urls

....REMOVED....

....REMOVED....

....REMOVED....

Total URLs Scanned : 452

Vulnerable URLs Found : 66

Script Execution Time : 291.078248500824 seconds

Video Demo

[Video: <https://vimeo.com/143520589>]

Please check the blog post for some known issues in the script.

.
.

lilsamzy - *October 29, 2015, 5:36 am*

thanks man u made it alot easier to use this exploit ?

HaxOr? - *October 29, 2015, 8:30 am*

Can you inject a specific list or it needs to be dorked first?

cruxxy - *October 31, 2015, 6:02 am*

OMFG thankyou so much youre my hero <3

wiros4bleng - *November 13, 2017, 6:37 am*

Wow! great. Thanks for share