Linuxhackingid

EXPLOIT DATABASE

PRACTICAL DOCUMENTATION

2025

PROPOSED BY :

Linuxhackingid Team

+628953213885780

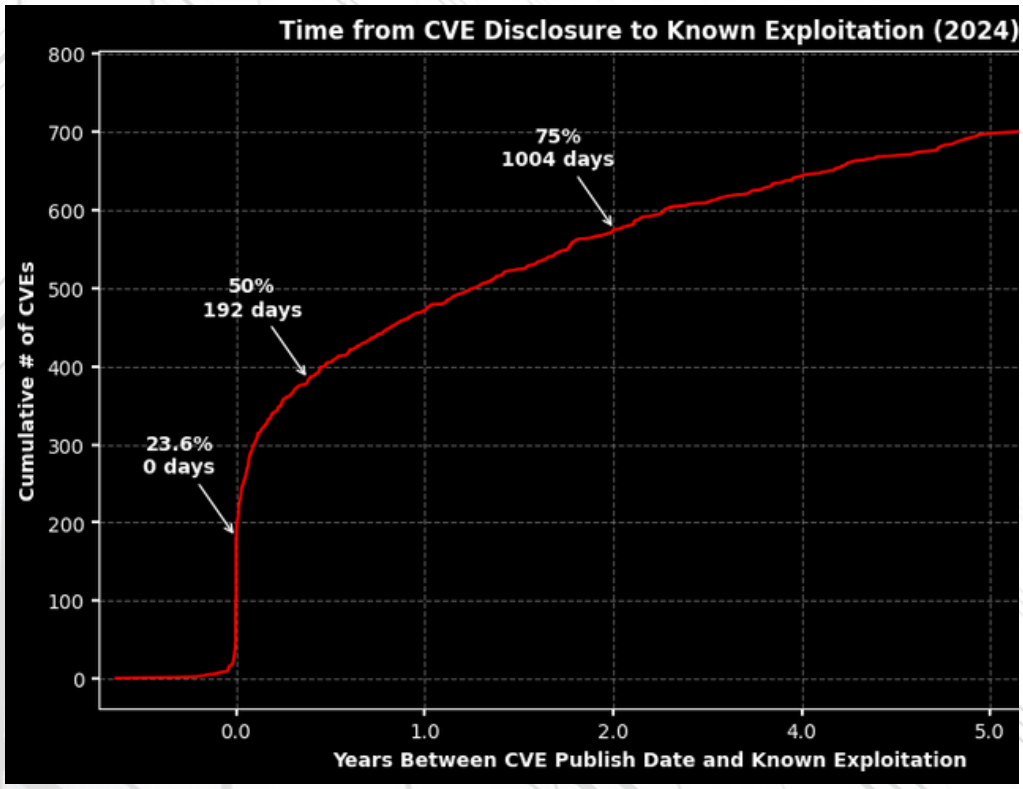
www.linuxhackingid.com

EXPLOIT

Apa itu Exploit?

Exploit adalah kode atau metode yang digunakan untuk mengeksploitasi kelemahan (vulnerability) dalam sistem, aplikasi, atau jaringan dengan tujuan mendapatkan akses tidak sah, meningkatkan hak akses, atau menyebabkan kerusakan.

Menurut data dari Vulncheck tahun 2024, sebanyak 23,6% KEV dieksploitasi pada atau sebelum CVE-nya diumumkan, turun dari 27% di 2023. Temuan ini menunjukkan bahwa eksploitasi dapat terjadi kapan saja, tidak hanya pada zero-day.

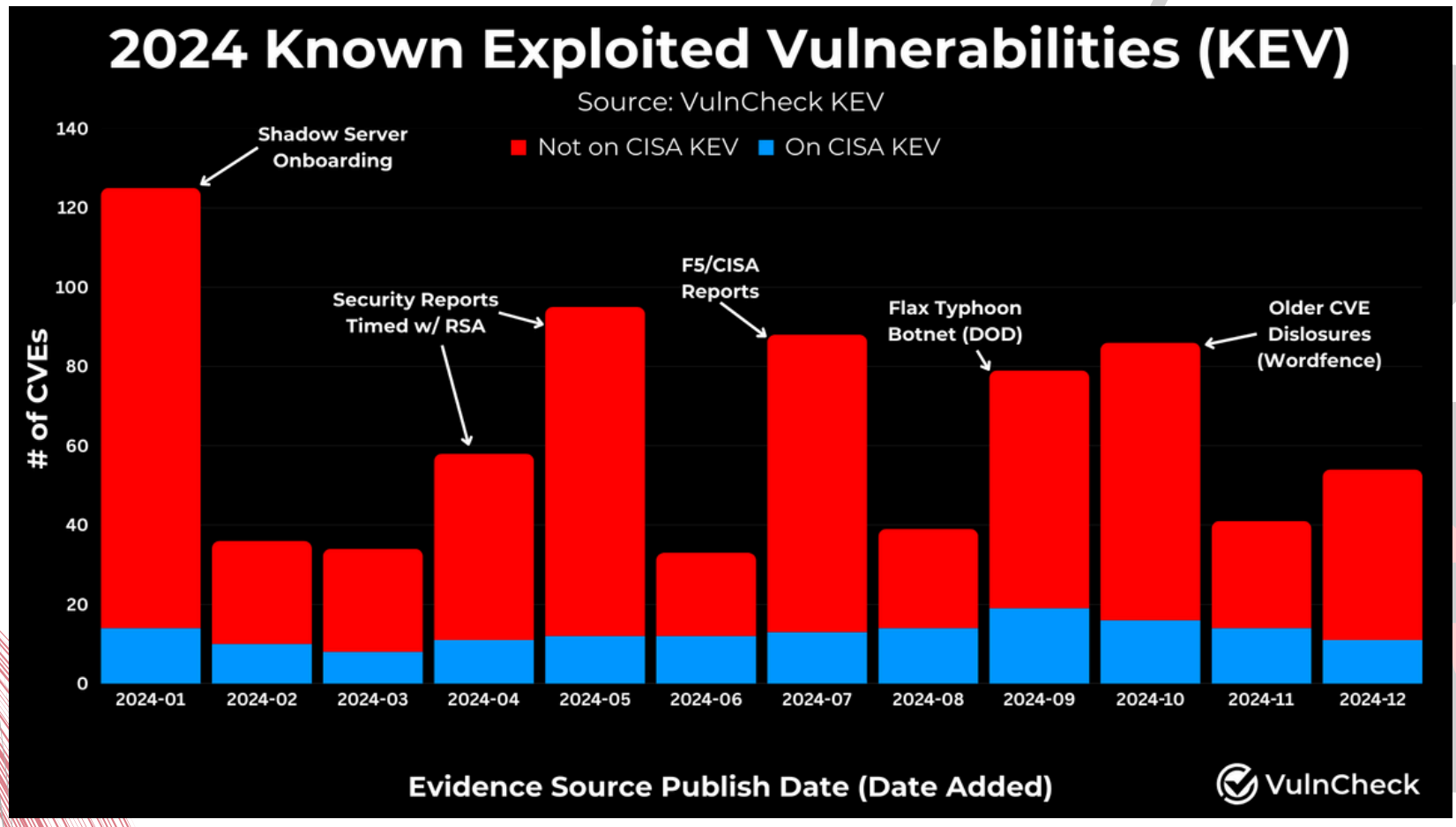


Linuxhackingid

WORDPRESS VULNERABILITY

GROWTH IN PUBLICLY REPORTED EXPLOITATION

Pada 2024, 768 CVE pertama kali dilaporkan dieksploitasi, meningkat 20% dari 2023. Sebanyak 1% CVE yang dipublikasikan dilaporkan dieksploitasi, dan jumlah ini kemungkinan bertambah seiring waktu.



SUMMARY

Eksploitasi CVE meningkat 20% pada 2024, dengan 768 kasus pertama kali dilaporkan. Sekitar 1% CVE yang dipublikasikan dieksploitasi, dan jumlah ini diperkirakan terus bertambah.

VULNERABILITY HIGHLIGHTS

Beberapa sorotan utama mencakup bug "RegreSSHion" pada OpenSSH yang memungkinkan eksekusi kode jarak jauh, serta "Sinkclose" pada prosesor AMD yang membuka celah untuk eskalasi hak istimewa.

SEARCHSPLOIT

Linuxhackingid

- **Mencari Exploit**
  - searchsploit **Windows**

```
┌──(kali㉿kali)-[~]
└─$ searchsploit Windows
```

Exploit Title	Path
(Gabriel's FTP Server) Open & Compact FTP Server 1.2 - 'PORT' Remote Denial of Service	windows/dos/12698.py
(Gabriel's FTP Server) Open & Compact FTP Server 1.2 - Authentication Bypass / Directory Traversal SAM Retrieval	windows/remote/27401.py
(Gabriel's FTP Server) Open & Compact FTP Server 1.2 - Full System Access	windows/remote/13932.py
(Gabriel's FTP Server) Open & Compact FTP Server 1.2 - Universal Denial of Service	windows/dos/12741.py
(Gabriel's FTP Server) Open & Compact FTPd 1.2 - Buffer Overflow (Metasploit)	windows/remote/11742.rb
(Gabriel's FTP Server) Open & Compact FTPd 1.2 - Crash (PoC)	windows/dos/11391.py
(Gabriel's FTP Server) Open & Compact FTPd 1.2 - Remote Overflow	windows/remote/11420.py
.NET Framework - Tilde Character Denial of Service	windows/dos/19575.txt
.NET Remoting Services - Remote Command Execution	windows/remote/35280.txt
.NET Runtime Optimization Service - Local Privilege Escalation	windows/local/16940.c
0irc-client 1345 build20060823 - Denial of Service	windows/dos/3547.c
1 Click Audio Converter 2.3.6 - Activex Local Buffer Overflow	windows/local/37211.html
1 Click Extract Audio 2.3.6 - Activex Buffer Overflow	windows/local/37212.html
10-Strike Bandwidth Monitor 3.7 - Local Buffer Overflow (SEH)	windows/local/45085.py
10-Strike Bandwidth Monitor 3.9 - Buffer Overflow (SEH) (ASLR + DEP Bypass)	windows/local/48570.py
10-Strike LANState 8.8 - Local Buffer Overflow (SEH)	windows/local/45086.py
10-Strike Network File Search Pro 2.3 - Local Buffer Overflow (SEH)	windows/local/40903.py
10-Strike Network Inventory Explorer - 'srvInventoryWebServer' Unquoted Service Path	windows/local/48251.txt
10-Strike Network Inventory Explorer 8.54 - 'Add' Local Buffer Overflow (SEH)	windows/local/48253.py
10-Strike Network Inventory Explorer 8.54 - 'Registration Key' Buffer Overflow (SEH)	windows_x86/local/44840.py
10-Strike Network Inventory Explorer 8.54 - Local Buffer Overflow (SEH)	windows_x86/local/44838.py
10-Strike Network Inventory Explorer 8.54 - Local Buffer Overflow (SEH) (DEP Bypass)	windows/local/46283.py
10-Strike Network Inventory Explorer 8.65 - Buffer Overflow (SEH)	windows/local/49134.py
10-Strike Network Inventory Explorer 9.03 - 'Read from File' Buffer Overflow (SEH) (ROP)	windows/local/48264.py
10-Strike Network Inventory Explorer Pro 9.05 - Buffer Overflow (SEH)	windows/local/49322.py
10-Strike Network Inventory Explorer Pro 9.31 - 'srvInventoryWebServer' Unquoted Service Path	windows/local/50494.txt
10-Strike Network Inventory Explorer Pro 9.31 - Buffer Overflow (SEH)	windows/local/50472.py
10-Strike Network Scanner 3.0 - Local Buffer Overflow (SEH)	windows_x86/local/44841.py
10Strike LANState 9.32 - 'Force Check' Buffer Overflow (SEH)	windows/local/48277.py
123 FlashChat 7.8 - Multiple Vulnerabilities	windows/remote/14658.txt
1by1 1.67 - '.m3u' Local Stack Overflow (PoC)	windows/dos/8484.pl
1C: Arcadia Internet Store 1.0 - Arbitrary File Disclosure	windows/remote/20947.txt
1C: Arcadia Internet Store 1.0 - Denial of Service	windows/dos/20949.c
1C: Arcadia Internet Store 1.0 - Path Disclosure	windows/remote/20948.txt
1CLICK DVD Converter 2.1.7.1 - Multiple DLL Loading Arbitrary Code Execution Vulnerabilities	windows/remote/34848.c

- **Download Exploit**
  - searchsploit -m **ID**

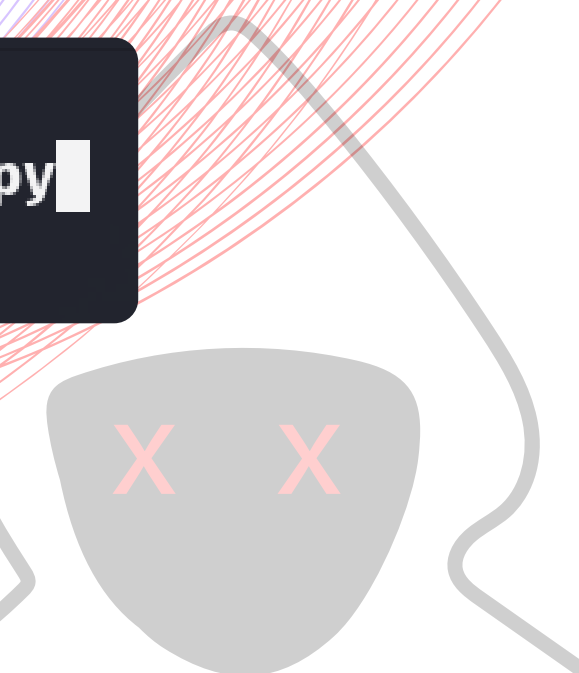
```
┌──(kali㉿kali)-[~]
└─$ searchsploit -m 12698
  Exploit: (Gabriel's FTP Server) Open & Compact FTP Server 1.2 - 'PORT' Remote Denial of Service
      URL: https://www.exploit-db.com/exploits/12698
     Path: /usr/share/exploitdb/exploits/windows/dos/12698.py
    Codes: N/A
 Verified: True
File Type: ASCII text
Copied to: /home/kali/12698.py
```

SEARCHSPLOIT

Linuxhackingid

- **Test Exploit**
  - python3 **file-exploit.py**

```
┌──(kali㉿kali)-[~]
└─$ python3 /home/kali/12698.py
```



Note: Ketika menjalankan, perhatikan bahasa pemograman Exploit

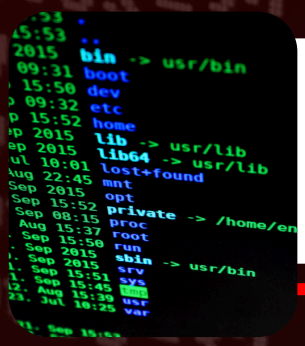
OUR PRACTICAL COURSES

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

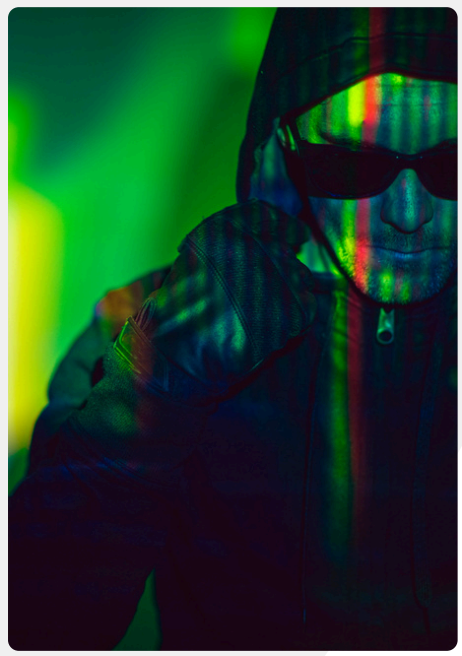
Linuxhackingid

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+	8000+	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