Drupal - Discovery & Enumeration

Drupal, launched in 2001 is the third and final CMS we'll cover on our tour through the world of common applications. Drupal is another open-source CMS that is popular among companies and developers. Drupal is written in PHP and supports using MySQL or PostgreSQL for the backend. Additionally, SQLite can be used if there's no DBMS installed. Like WordPress, Drupal allows users to enhance their websites through the use of themes and modules. At the time of writing, the Drupal project has nearly 43,000 modules and 2,900 themes and is the third most popular CMS by market share. Here are a few interesting statistics on Drupal gathered from various sources:

- Around 1.5% of sites on the internet run Drupal (over 1.1 million sites!), 5% of the top 1 million websites on the internet, and 7% of the top 10,000 sites
- Drupal accounts for around 2.4% of the CMS market
- It is available in 100 languages
- Drupal is community-oriented and has over 1.3 million members
- Drupal 8 was built by 3,290 contributors, 1,288 companies, and help from the community
- 33 of the Fortune 500 companies use Drupal in some way
- 56% of government websites across the world use Drupal
- 23.8% of universities, colleges, and schools use Drupal worldwide
- Some major brands that use Drupal include: Tesla and Warner Bros Records

According to the Drupal website there are just around 950,000 instances of Drupal in use at the time of writing (distributed from version 5.x through version 9.3.x, as of September 5, 2021). As we can see from these statistics, Drupal usage has held steadily between 900,000 and 1.1 million instances between June 2013 and September 2021. These statistics do not account for `EVERY` instance of Drupal in use worldwide, but rather instances running the Update Status module, which checks in with drupal.org daily to look for any new versions of Drupal or updates to modules in use.

Discovery/Footprinting

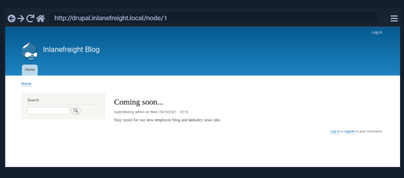
During an external penetration test, we encounter what appears to be a CMS, but we know from a cursory review that the site is not running WordPress or Joomla. We know that CMS' are often "juicy" targets, so let's dig into this one and see what we can uncover.

A Drupal website can be identified in several ways, including by the header or footer message `Powered by Drupal`, the standard Drupal logo, the presence of a `CHANGELOG.txt` file or `README.txt file`, via the page source, or clues in the robots.txt file such as references to `/node`.

```
Govardhan Gujji22@htb[/htb]$ curl -s http://drupal.inlanefreight.local | grep Drupal

<meta name="Generator" content="Drupal 8 (https://www.drupal.org)" />
      <span>Powered by <a href="https://www.drupal.org">Drupal</a></span>
```

Another way to identify Drupal CMS is through nodes. Drupal indexes its content using nodes. A node can hold anything such as a blog post, poll, article, etc. The page URIs are usually of the form `/node/<nodeid>`.



For example, the blog post above is found to be at `/node/1`. This representation is helpful in identifying a Drupal website when a custom theme is in use.

Note: Not every Drupal installation will look the same or display the login page or even allow users to access the login page from the internet.

Drupal supports three types of users by default:

1. `Administrator`: This user has complete control over the Drupal website.
2. `Authenticated User`: These users can log in to the website and perform operations such as adding and editing articles based on their permissions.
3. `Anonymous`: All website visitors are designated as anonymous. By default, these users are only allowed to read posts.

Enumeration

Once we have discovered a Drupal instance, we can do a combination of manual and tool-based (automated) enumeration to uncover the version, installed plugins, and more. Depending on the Drupal version and any hardening measures that have been put in place, we may need to try several ways to identify the version number. Newer installs of Drupal by default block access to the `CHANGELOG.txt` and `README.txt` files, so we may need to do further enumeration. Let's look at an example of enumerating the version number using the `CHANGELOG.txt` file. To do so, we can use `cURL` along with `grep`, `sed`, `head`, etc.

```
Govardhan Gujji22@htb[/htb]$ curl -s http://drupal-acc.inlanefreight.local/CHANGELOG.txt | gr

Drupal 7.57, 2018-02-21
```

Here we have identified an older version of Drupal in use. Trying this against the latest Drupal version at the time of writing, we get a 404 response.

```
Govardhan Gujji22@htb[/htb]$ curl -s http://drupal.inlanefreight.local/CHANGELOG.txt

<!DOCTYPE html><html><head><title>404 Not Found</title></head><body><h1>Not Found</h1><p>The
```

There are several other things we could check in this instance to identify the version. Let's try a scan with `droopescan` as shown in the Joomla enumeration section. `Droopescan` has much more functionality for Drupal than it does for Joomla.

Let's run a scan against the `http://drupal.inlanefreight.local` host.

```
Govardhan Gujji22@htb[/htb]$ droopescan scan drupal -u http://drupal.inlanefreight.local

[+] Plugins found:
    php http://drupal.inlanefreight.local/modules/php/
        http://drupal.inlanefreight.local/modules/php/LICENSE.txt

[+] No themes found.

[+] Possible version(s):
    8.9.0
    8.9.1

[+] Possible interesting urls found:
    Default admin - http://drupal.inlanefreight.local/user/login

[+] Scan finished (0:03:19.199526 elapsed)
```

This instance appears to be running version `8.9.1` of Drupal. At the time of writing, this was not the latest as it was released in June 2020. A quick search for Drupal-related vulnerabilities does not show anything apparent for this core version of Drupal. In this instance, we would next want to look at installed plugins or abusing built-in functionality.

Start Instance

∞ / 1 spawns left

Waiting to start...

Questions

Answer the question(s) below to complete this Section and earn cubes!

Cheat Sheet

Get VPN Key

Target: Click here to spawn the target system!

vHosts needed for these questions:

- `drupal.inlanefreight.local`
- `drupal-qa.inlanefreight.local`

+ 0 cubes Identify the Drupal version number in use on http://drupal-qa.inlanefreight.local

7.30

Submit

← Previous Next →

Mark Complete & Next

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left