هفته‌نامه خبری

دروپال من

منتخب اخبار هفته — برگزیده از رأی مخاطبان

شماره ۳

۱۴۰۵/۰۵/۲۳

تا ۱۴۰۵/۰۵/۳۰

فهرست مطالب

صاحب امتیاز: رضا سروری

سردبیر: رضا سروری

طراحی و صفحه‌آرایی: رضا سروری

ایمیل: info@mydrupal.ir

مدیرمسئول: رضا سروری

مدیر اجرایی: رضا سروری

تلفن: 09100048292

نشانی: تهران خ انقلاب

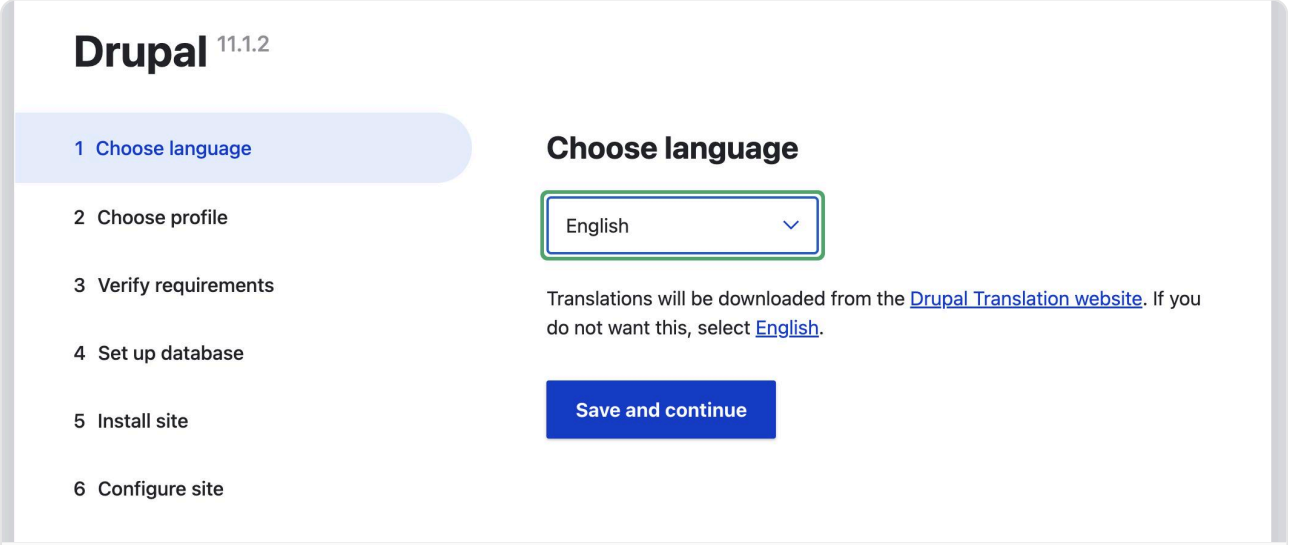
فهرست مطالب

دروپال من — شماره ۳ — ۱۴۰۵/۰۵/۲۳ تا ۱۴۰۵/۰۵/۳۰

خبر برگزیده هفته

آموزش نصب Drupal 10 و Drupal 11 روی سرور؛ راهنمای کامل نصب دروپال + ویدئو

آخرین خبر منتشر شده در این هفته



آموزش نصب Drupal 10 و Drupal 11 روی سرور؛ راهنمای کامل نصب دروپال + ویدئو

آموزش نصب Drupal 10 و Drupal 11

Drupal یکی از قدرتمندترین سیستم‌های مدیریت محتوای متن‌باز برای راه‌اندازی وب‌سایت‌های حرفه‌ای، سازمانی، خبری، فروشگاهی و پورتال‌های بزرگ است. برخلاف بسیاری از CMSهای ساده، دروپال معماری ماژولار و انعطاف‌پذیری دارد و می‌توان ساختار محتوا، کاربران، دسترسی‌ها، Views، API، جست‌وجو و بسیاری از بخش‌های سایت را متناسب با نیاز پروژه توسعه داد.

در این آموزش، نصب **Drupal 10** و **Drupal 11** را به‌صورت مرحله‌به‌مرحله بررسی می‌کنیم؛ از آماده‌سازی سرور و نصب PHP و دیتابیس گرفته تا دانلود Drupal با Composer، ایجاد دیتابیس، اجرای نصب از طریق مرورگر، تنظیم مجوزها، فعال‌سازی SSL و اقدامات ضروری پس از نصب.

اگر قصد راه‌اندازی یک سایت جدید را دارید، در شرایط فعلی **Drupal 11** انتخاب مناسب‌تری است؛ شاخه Drupal 11.4.x برای توسعه سایت‌های جدید هدف قرار گرفته و تا ژوئن ۲۰۲۷ پشتیبانی امنیتی خواهد داشت.

Drupal 10 یا Drupal 11؛ کدام نسخه را نصب کنیم؟

یکی از اولین سؤال‌ها قبل از نصب دروپال این است که از Drupal 10 استفاده کنیم یا Drupal 11.

برای پروژه‌های جدید، پیشنهاد کلی استفاده از **Drupal 11** است؛ البته در صورتی که ماژول‌ها و قالب‌های مورد نیاز پروژه با Drupal 11 سازگار باشند.

Drupal 10 همچنان برای پروژه‌هایی که به دلیل سازگاری ماژول‌ها، قالب‌ها یا کدهای اختصاصی نمی‌توانند به Drupal 11 مهاجرت کنند، کاربرد دارد. با این حال Drupal 10.6 آخرین شاخه فرعی Drupal 10 است و پایان عمر Drupal 10 برای ۹ دسامبر ۲۰۲۶ تعیین شده است.

مقایسه سریع Drupal 10 و Drupal 11

ویژگی	Drupal 10	Drupal 11
PHP حداقل	8.1	8.3
MySQL	+5.7.8	+8.0
MariaDB	+10.3.7	+10.6
PostgreSQL	+12	+16
SQLite	+3.26	+3.45
Composer	+2.3.6	نسخه‌های جدید Composer
مناسب پروژه جدید	قابل استفاده	**پیشنهاد اصلی**
وضعیت آینده	پایان پشتیبانی در 2026	شاخه اصلی فعلی

نیازمندی‌های دیتابیس و PHP مطابق مستندات رسمی Drupal هستند.

پیش‌نیازهای نصب Drupal

قبل از شروع نصب باید سرور شما شرایط لازم را داشته باشد.

Drupal روی Apache و Nginx قابل اجرا است و برای یک سایت واقعی بهتر است از Linux استفاده شود. مستندات رسمی Drupal نیز Linux یا سیستم‌های مشابه را برای میزبانی پیشنهاد می‌کنند.

یک ترکیب پیشنهادی برای سرور:

Ubuntu 22.04 یا Ubuntu 24.04

Apache یا Nginx

PHP 8.3 یا 8.4 برای Drupal 11

MySQL 8 یا MariaDB 10.6+

Composer

SSL/HTTPS

حداقل 1GB RAM برای کارهای Composer

فضای دیسک کافی برای فایل‌های سایت، دیتابیس، رسانه‌ها و Backup

Drupal حداقل 1GB حافظه برای اجرای Composer را توصیه می‌کند و مقدار RAM مورد نیاز در سایت‌های بزرگ‌تر با توجه به ماژول‌ها و سرویس‌هایی مانند Solr و Memcached افزایش پیدا می‌کند.

نیازمندی‌های PHP در Drupal 10 و Drupal 11

یکی از مهم‌ترین تفاوت‌های Drupal 10 و Drupal 11 نسخه PHP است.

Drupal 10 حداقل به PHP 8.1 نیاز دارد، در حالی که Drupal 11 به PHP 8.3 نیاز دارد. در شاخه‌های فعلی Drupal 11، PHP 8.4 نیز گزینه مناسبی است.

برای Drupal 11 بهتر است سرور جدید را روی PHP 8.4 تنظیم کنید؛ البته باید سازگاری ماژول‌ها و نرم‌افزارهای جانبی پروژه نیز بررسی شود.

برخی افزونه‌های مهم PHP عبارت‌اند از:

`php-cli`

`php-curl`

`php-gd`

`php-mbstring`

`php-mysql`

`php-xml`

`php-zip`

`php-intl`

`php-opcache`

Drupal برای ارتباط با دیتابیس به PDO و Driver مناسب دیتابیس نیاز دارد.

نصب PHP و ابزارهای مورد نیاز در Ubuntu

اگر سرور شما Ubuntu است، ابتدا سیستم را به‌روزرسانی کنید:

```
sudo apt update
sudo apt upgrade -y
```

برای نصب PHP و افزونه‌های رایج Drupal می‌توانید از دستور زیر استفاده کنید:

```
\ sudo apt install -y
\ php
\ php-cli
\ php-fpm
\ php-curl
\ php-gd
\ php-mbstring
\ php-mysql
\ php-xml
\ php-zip
\ php-intl
\ php-opcache
\ unzip
\ git
curl
```

سپس نسخه PHP را بررسی کنید:

```
php -v
```

برای Drupal 11 خروجی باید حداقل PHP 8.3 باشد.

نصب Composer

Drupal برای پروژه‌های مدرن خود استفاده از Composer را توصیه می‌کند. Composer وابستگی‌های Drupal، ماژول‌ها، قالب‌ها و کتابخانه‌های PHP را مدیریت می‌کند.

روش پیشنهادی Drupal برای ایجاد پروژه جدید استفاده از پکیج:

```
drupal/recommended-project
```

است. این روش همچنین ساختار پروژه‌ای ایجاد می‌کند که فایل‌های قابل دسترسی از وب در پوشه web قرار می‌گیرند.

ابتدا Composer را بررسی کنید:

```
composer --version
```

اگر Composer نصب نیست، می‌توان آن را از روش رسمی Composer نصب کرد.

پس از نصب:

```
composer --version
```

را اجرا کنید و مطمئن شوید نسخه Composer به‌روز و سازگار با PHP سرور است.

نصب Drupal 11 با Composer

برای یک پروژه جدید، روش پیشنهادی این است که Drupal را با Composer نصب کنیم.

مثلاً:

```
cd /var/www

drupal/recommended-project:^11 mysite
```

در این مثال پروژه داخل مسیر زیر ایجاد می‌شود:

```
var/www/mysite/
```

ساختار پروژه معمولاً چیزی شبیه این خواهد بود:

```
/mysite
composer.json —┤
composer.lock —┤
/vendor —┤
/web —└
/core —┤
/modules —┤
/profiles —┤
```

```
/sites ──┤
/themes ──└
```

نکته بسیار مهم این است که در این ساختار، **Document Root وب‌سرور باید روی پوشه web قرار بگیرد، نه روی ریشه پروژه.**

یعنی اگر پروژه در این مسیر قرار دارد:

`var/www/mysite/`

ریشه وب باید:

`var/www/mysite/web/`

باشد.

این ساختار از نظر امنیتی و مدیریت وابستگی‌ها بسیار بهتر از قرار دادن کل پروژه Composer در معرض وب است.

نصب Drupal 10 با Composer

برای نصب Drupal 10 نیز روش Composer مشابه است.

مثلاً:

```
cd /var/www

composer create-project drupal/recommended-project:^10 mysite
```

Composer نسخه سازگار Drupal 10 و وابستگی‌های آن را دریافت می‌کند.

در پروژه‌های واقعی بهتر است به‌جای نصب نسخه‌ای که صرفاً با یک Constraint کلی انتخاب می‌شود، وضعیت نسخه‌های موجود و سازگاری ماژول‌های پروژه را نیز بررسی کنید.

مستندات رسمی Drupal نیز استفاده از `drupal/recommended-project` را برای Drupal 10 و 11 توصیه می‌کند.

نصب Drupal با فایل ZIP

روش دوم نصب Drupal استفاده از فایل ZIP است.

در این روش ابتدا نسخه مورد نظر Drupal را از سایت رسمی دریافت می‌کنید، فایل را استخراج کرده و فایل‌های Drupal را داخل Document Root سرور قرار می‌دهید.

این روش برای بعضی هاست‌های اشتراکی و محیط‌هایی که Composer در دسترس نیست مناسب است.

با این حال برای پروژه‌های حرفه‌ای و قابل توسعه، **Composer انتخاب بهتری است**؛ زیرا Drupal و وابستگی‌های آن را مدیریت می‌کند و فرآیند نصب و به‌روزرسانی ماژول‌ها را استانداردتر می‌کند.

ایجاد دیتابیس برای Drupal

پس از آماده‌سازی PHP باید دیتابیس ایجاد شود.

برای Drupal 11 می‌توانید از MySQL 8 یا MariaDB 10.6 به بالا استفاده کنید. PostgreSQL 16 و SQLite 3.45 نیز در نسخه‌های فعلی Drupal 11 پشتیبانی می‌شوند.

برای مثال در MySQL:

```
CREATE DATABASE drupal_db
CHARACTER SET utf8mb4
COLLATE utf8mb4_general_ci;

CREATE USER 'drupal_user'@'localhost'
IDENTIFIED BY 'StrongPasswordHere';

GRANT ALL PRIVILEGES
ON drupal_db.*
TO 'drupal_user'@'localhost';

FLUSH PRIVILEGES;
```

اطلاعات زیر را برای مرحله نصب نگه دارید:

```
Database name: drupal_db
Username: drupal_user
Password: StrongPasswordHere
Host: localhost
```

برای سایت واقعی حتماً از یک رمز عبور طولانی و تصادفی استفاده کنید.

اجرای نصب Drupal از طریق مرورگر

پس از قرار دادن فایل‌های Drupal و تنظیم Virtual Host، آدرس دامنه خود را در مرورگر باز کنید.

مثلاً:

```
https://example.com
```

اگر تنظیمات درست باشد، صفحه نصب Drupal نمایش داده می‌شود.

فرآیند نصب معمولاً شامل مراحل زیر است:

انتخاب زبان
انتخاب Installation Profile
بررسی نیازمندی‌ها
تنظیم دیتابیس
نصب سایت
تنظیم اطلاعات سایت

مرحله اول؛ انتخاب زبان

در اولین مرحله زبان مورد نظر را انتخاب کنید.

برای سایت فارسی می‌توانید زبان فارسی را انتخاب کنید.

پس از انتخاب زبان روی:

Save and continue

کلیک کنید.

در این مرحله Drupal فایل‌های زبان مورد نیاز را دریافت یا آماده می‌کند و شما وارد مرحله بعد می‌شوید.

مرحله دوم؛ انتخاب Installation Profile

Drupal در زمان نصب از شما می‌خواهد Installation Profile را انتخاب کنید.

در بسیاری از پروژه‌ها استفاده از پروفایل استاندارد نقطه شروع مناسبی است.

اما اگر قصد دارید سایت را از ابتدا به‌صورت کاملاً سفارشی پیاده‌سازی کنید، انتخاب پروفایل مناسب به معماری پروژه بستگی دارد.

در نسخه‌های جدید Drupal 11 برخی تغییرات در محتوای پیش‌فرض Installation Profile استاندارد اعمال شده است؛ بنابراین نباید تصور کرد که همه Content Typeهای سنتی دقیقاً مانند نسخه‌های قدیمی در نصب اولیه ایجاد می‌شوند.

مرحله سوم؛ بررسی نیازمندی‌های Drupal

Drupal قبل از شروع نصب، سرور را بررسی می‌کند.

مواردی مانند:

- نسخه PHP
- افزونه‌های PHP
- دسترسی فایل‌ها
- دیتابیس
- تنظیمات وب‌سرور
- قابلیت‌های لازم PHP

بررسی می‌شوند.

اگر مشکلی وجود داشته باشد Drupal معمولاً آن را در همین مرحله نمایش می‌دهد.

برای مثال اگر PHP سرور روی 8.2 باشد و قصد نصب Drupal 11 را داشته باشید، نصب متوقف خواهد شد؛ زیرا Drupal 11 به PHP 8.3 یا بالاتر نیاز دارد.

مرحله چهارم؛ اتصال Drupal به دیتابیس

در این مرحله اطلاعات دیتابیس را وارد کنید.

مثلاً:

```
Database type: MySQL
Database name: drupal_db
Database username: drupal_user
Database password: ********
Database host: localhost
```

اگر دیتابیس روی سرور دیگری قرار دارد، مقدار Host را متناسب با سرور دیتابیس تغییر دهید.

در بخش Advanced Options نیز می‌توان مواردی مانند:

Database Host

Port

Table Prefix

را تنظیم کرد.

برای اکثر نصب‌های استاندارد، مقدار Host برابر `localhost` یا آدرس سرویس دیتابیس است.

مرحله پنجم؛ نصب Drupal

پس از اتصال موفق به دیتابیس، Drupal جداول مورد نیاز را ایجاد کرده و ماژول‌های Core را نصب می‌کند.

در این مرحله بهتر است صفحه مرورگر را Refresh نکنید و اجازه دهید فرآیند نصب کامل شود.

پس از پایان نصب، وارد مرحله تنظیم سایت می‌شوید.

مرحله ششم؛ تنظیم اطلاعات سایت

در این بخش اطلاعات اصلی سایت را وارد کنید:

Site name

نام سایت.

Site email address

ایمیل اصلی سایت.

Username

نام کاربری مدیر.

Password

رمز عبور مدیر.

Default country

کشور پیش‌فرض.

Default time zone

منطقه زمانی.

برای سایت فارسی که در ایران فعالیت می‌کند، تنظیم Time Zone اهمیت دارد؛ مخصوصاً برای:

- انتشار زمان‌بندی‌شده محتوا
- Cron
- نمایش تاریخ
- ثبت زمان محتوا
- گزارش‌ها

پس از تکمیل اطلاعات، روی **Save and continue** کلیک کنید.

تنظیم مجوز فایل‌های Drupal

یکی از حساس‌ترین قسمت‌های نصب Drupal تنظیم Permissionها است.

فایل‌های پروژه نباید بدون دلیل Writable باشند.

در ساختار Composer معمولاً پروژه در خارج از Document Root قرار دارد و فقط پوشه web از طریق وب در دسترس است.

پوشه زیر برای ذخیره فایل‌های آپلودی سایت استفاده می‌شود:

```
web/sites/default/files
```

این پوشه باید توسط وب‌سرور قابل نوشتن باشد.

برای مثال:

```
mkdir -p web/sites/default/files
```

و سپس مالکیت را متناسب با کاربر وب‌سرور تنظیم کنید.

در Ubuntu با Nginx یا Apache که با www-data اجرا می‌شود:

```
sudo chown -R www-data:www-data web/sites/default/files
```

اما نباید به‌صورت غیرضروری کل پروژه را Writable کنید.

تنظیم settings.php

فایل تنظیمات اصلی Drupal در مسیر زیر قرار دارد:

```
web/sites/default/settings.php
```

همچنین فایل اولیه معمولاً در این مسیر قرار دارد:

```
web/sites/default/default.settings.php
```

پس از نصب، settings.php شامل اطلاعات مهم سایت مانند اتصال دیتابیس است.

به همین دلیل نباید Permission آن را بدون دلیل بالا نگه داشت.

همچنین توصیه می‌شود بعد از پایان نصب، تنظیمات امنیتی لازم در settings.php اعمال شود.

تنظیم Trusted Host در Drupal

برای سایت‌های واقعی بهتر است Trusted Host Patterns را تنظیم کنید.

در فایل:

```
web/sites/default/settings.php
```

می‌توان دامنه‌های مجاز را مشخص کرد.

مثلاً:

```
$settings['trusted_host_patterns'] = [
  '^example\.com$',
  '^www\.example\.com$',
];
```

اگر سایت شما با چند دامنه یا Subdomain کار می‌کند باید الگوی مناسب برای آن‌ها تعریف شود.

این تنظیم یکی از اقدامات مهم امنیتی Drupal است.

تنظیم وب‌سرور برای Drupal

Apache

اگر از Apache استفاده می‌کنید، Document Root باید به پوشه web پروژه اشاره کند.

برای مثال:

```
var/www/mysite/web/
```

همچنین Rewrite باید فعال باشد.

نمونه فعال‌سازی:

```
sudo a2enmod rewrite
sudo systemctl restart apache2
```

Drupal برای Clean URLها به تنظیم صحیح Rewrite نیاز دارد.

تنظیم Nginx برای Drupal

در سرورهای پرترافیک معمولاً Nginx به همراه PHP-FPM انتخاب مناسبی است.

نمونه ساختار Virtual Host:

```
server {
    listen 80;
    server_name example.com www.example.com;

    root /var/www/mysite/web;
    index index.php index.html;

    location / {
        try_files $uri /index.php?$query_string;
    }

    location ~ '\.php$' {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/run/php/php8.4-fm.sock;
    }

    location ~* \.(css|js|jpg|jpeg|png|gif|ico|svg|webp|woff|woff2)$ {
        expires 7d;
        access_log off;
    }
}
```

مسیر PHP-FPM باید متناسب با نسخه PHP نصب‌شده روی سرور تغییر کند.

مثلاً برای PHP 8.3 ممکن است مسیر به شکل زیر باشد:

```
run/php/php8.3-fpm.sock/
```

و برای PHP 8.4:

```
run/php/php8.4-fpm.sock/
```

فعال کردن HTTPS برای Drupal

پس از نصب سایت، یکی از اولین اقدامات امنیتی باید فعال کردن HTTPS باشد.

برای این کار می‌توانید از Let's Encrypt استفاده کنید.

در Ubuntu با Certbot، پس از نصب ابزار مورد نیاز، گواهی SSL دریافت و روی وب‌سرور فعال می‌شود.

بعد از فعال شدن HTTPS بهتر است سایت را به‌گونه‌ای تنظیم کنید که نسخه HTTP به HTTPS Redirect شود.

مثلاً:

```
http://example.com
```

به

```
https://example.com
```

منتقل شود.

استفاده از HTTPS برای ورود کاربران، مدیریت سایت و انتقال اطلاعات دیتابیس و Sessionها اهمیت زیادی دارد.

نصب Drupal با Drush

پس از نصب Drupal می‌توان از Drush برای مدیریت سایت استفاده کرد.

در پروژه Composer:

```
composer require drush/drush
```

پس از نصب:

```
vendor/bin/drush status
```

را اجرا کنید.

در صورت نصب موفق، اطلاعات سایت، PHP، Drupal، Database و مسیرهای پروژه نمایش داده می‌شود.

برای استفاده راحت‌تر می‌توانید Drush را از مسیر پروژه اجرا کنید:

```
vendor/bin/drush cr
```

برای پاک‌سازی Cache:

```
vendor/bin/drush cr
```

و برای اجرای Update Database:

```
vendor/bin/drush updb
```

تنظیم Cron در Drupal

Cron برای اجرای وظایف دوره‌ای Drupal استفاده می‌شود.

از جمله:

پردازش Queueها

اجرای عملیات دوره‌ای

به‌روزرسانی برخی داده‌ها

پردازش Search

اجرای وظایف ماژول‌ها

برای سایت‌های واقعی بهتر است Cron را به‌صورت واقعی روی سرور تنظیم کنید، نه اینکه صرفاً به اجرای دستی آن وابسته باشید.

برای مثال:

```
cd /var/www/mysite && vendor/bin/drush cron */15 * * * *
```

این Cron هر ۱۵ دقیقه اجرا می‌شود.

بسته به نوع سایت ممکن است اجرای Cron در بازه‌های کوتاه‌تر یا بلندتر مناسب باشد.

تنظیم PHP Memory Limit

Drupal برای سایت‌های ساده و حرفه‌ای به یک Memory Limit مناسب نیاز دارد.

مقدار حداقلی PHP ممکن است برای نصب Core کافی باشد، اما در سایت‌هایی که تعداد زیادی ماژول، Views پیچیده، Commerce، پردازش تصویر یا ابزارهای جست‌وجو دارند، Memory Limit بیشتری لازم است.

برای بسیاری از سایت‌های حرفه‌ای مقدار:

```
memory_limit = 256M
```

نقطه شروع مناسبی است.

در سایت‌های بزرگ ممکن است نیاز به:

```
memory_limit = 512M
```

یا بیشتر وجود داشته باشد.

مقدار مناسب باید بر اساس مصرف واقعی سایت تعیین شود، نه صرفاً با افزایش بی‌دلیل Memory Limit.

فعال‌سازی OPcache

برای افزایش عملکرد PHP بهتر است OPcache فعال باشد.

در Ubuntu می‌توانید بسته مربوطه را نصب کنید:

```
sudo apt install php-opcache
```

سپس PHP-FPM را Restart کنید:

```
sudo systemctl restart php8.4-fpm
```

البته نسخه PHP را مطابق سرور خود تغییر دهید.

OPcache باعث می‌شود PHP مجبور نباشد در هر درخواست فایل‌های PHP را از ابتدا Parse و Compile کند.

نصب ماژول‌های Drupal با Composer

یکی از اشتباهات رایج در پروژه‌های Drupal این است که ماژول را به‌صورت دستی دانلود کرده و سپس با Composer مخلوط کنیم.

در پروژه‌های مدرن بهتر است ماژول‌ها را با Composer نصب کنید.

مثلاً برای نصب Token:

```
composer require drupal/token
```

یا:

```
composer require drupal/pathauto
```

پس از نصب، ماژول را با Drush فعال کنید:

```
vendor/bin/drush en token -y
```

یا:

```
vendor/bin/drush en pathauto -y
```

مستندات رسمی Drupal نیز مدیریت Core، ماژول‌ها، Themeها و وابستگی‌ها با Composer را توصیه می‌کند.

پاک کردن Cache در Drupal

یکی از مهم‌ترین دستورات مدیریتی Drupal:

```
vendor/bin/drush cr
```

است.

هر زمان تغییر مهمی در مواردی مانند:

- Theme
- Twig
- Routing
- Services
- Configuration
- Module
- CSS/JS aggregation

انجام می‌دهید، ممکن است نیاز باشد Cache را پاک کنید.

بررسی وضعیت سایت بعد از نصب

بعد از نصب وارد بخش:

```
admin/reports/status/
```

شوید.

در این صفحه Drupal مشکلات مهم سایت را نمایش می‌دهد.

مواردی مانند:

- PHP
- Database
- File System
- Security
- Cron
- Configuration
- Updates

را بررسی کنید.

نباید صرفاً به این دلیل که صفحه اصلی سایت باز می‌شود تصور کنید نصب کاملاً صحیح است.

تنظیمات مهم بعد از نصب Drupal

پس از نصب اولیه بهتر است این موارد را بررسی کنید:

1. HTTPS

گواهی SSL فعال باشد.

2. Trusted Host

دامنه‌های معتبر در `settings.php` تعریف شوند.

3. Cron

Cron روی سرور تنظیم شود.

4. Cache

کش Drupal فعال و صحیح تنظیم شود.

5. PHP OPcache

فعال باشد.

6. File Permissions

Permission فایل‌ها و پوشه‌ها بررسی شود.

7. Backup

برای دیتابیس و فایل‌های سایت Backup منظم داشته باشید.

8. Updates

Module ،Core و Themeها مرتب به‌روزرسانی شوند.

9. Admin Account

برای حساب مدیر از رمز عبور بسیار قوی استفاده شود.

10. حذف فایل‌ها و تنظیمات اضافی

فایل‌های موقت، Backupهای حساس و فایل‌هایی که نباید از طریق وب قابل دسترسی باشند در Document Root قرار نگیرند.

نصب Drupal روی هاست اشتراکی

اگر قصد نصب Drupal روی هاست اشتراکی دارید، ابتدا بررسی کنید هاست از موارد زیر پشتیبانی می‌کند:

PHP 8.3 برای Drupal 11

MySQL 8 یا MariaDB 10.6 برای Drupal 11

Composer

SSH

PHP Extensions مورد نیاز

- SSL
- Cron
- دسترسی مناسب فایل‌ها

اگر هاست Composer و SSH ارائه نمی‌کند، می‌توانید از روش ZIP استفاده کنید؛ اما برای پروژه‌های حرفه‌ای که مرتباً ماژول نصب و به‌روزرسانی می‌شوند، VPS یا سرور مدیریت‌شده انتخاب مناسب‌تری است.

نصب Drupal روی Ubuntu با معماری پیشنهادی

برای یک سایت حرفه‌ای می‌توان معماری زیر را در نظر گرفت:

```
Internet
   |
   ▼
Nginx
   |
   ▼
PHP-FPM
   |
   ▼
Drupal
   |
   ├── MySQL / MariaDB
   ├── Redis
   ├── Solr
   └── File Storage
```

برای سایت‌های کوچک نیازی به استفاده از تمام این سرویس‌ها نیست.

اما در پروژه‌های بزرگ، سرویس‌هایی مانند Redis و Solr می‌توانند نقش مهمی در Cache و Search داشته باشند.

تفاوت نصب Drupal 10 و Drupal 11

از نظر فرآیند کلی، نصب Drupal 10 و Drupal 11 بسیار شبیه است.

تفاوت اصلی در Platform Requirements و برخی تغییرات Core است.

برای Drupal 11 حداقل PHP 8.3 لازم است و دیتابیس‌های اصلی نیز نسخه‌های جدیدتری می‌خواهند؛ برای مثال MariaDB 10.6، MySQL 8.0 و PostgreSQL 16.

بنابراین اگر سرور قدیمی دارید، ممکن است Drupal 10 روی آن اجرا شود اما Drupal 11 نصب نشود.

خطاهای رایج هنگام نصب Drupal

خطای PHP version

اگر با خطایی مشابه زیر مواجه شدید:

```
Your PHP installation is too old
```

نسخه PHP را بررسی کنید:

```
php -v
```

برای Drupal 11 حداقل PHP 8.3 لازم است.

خطای PDO

اگر Drupal دیتابیس را تشخیص نمی‌دهد، بررسی کنید Driver مربوط به دیتابیس نصب شده باشد.

برای MySQL:

```
php -m | grep pdo
```

همچنین:

```
php -m | grep mysql
```

خطای Permission

اگر Drupal نمی‌تواند فایل ایجاد کند یا فایل آپلود کند، Permission پوشه:

```
sites/default/files
```

را بررسی کنید.

خطای 403

در صورت دریافت:

```
Forbidden 403
```

موارد زیر را بررسی کنید:

- Document Root
- Permission
- Nginx Configuration
- Apache Configuration
- SELinux در سرورهای مبتنی بر RHEL
- Rewrite Rules

خطای 404 برای صفحات داخلی

اگر صفحه اصلی باز می‌شود اما URLهای داخلی مانند:

```
about/
news/
contact/
```

با 404 مواجه می‌شوند، معمولاً باید تنظیمات Rewrite وب‌سرور بررسی شود.

در Nginx استفاده از:

```
/_files $uri /index.php?$query_string
```

یکی از قسمت‌های مهم Configuration است.

آیا نصب Drupal با Composer بهتر است؟

برای پروژه حرفه‌ای، پاسخ تقریباً همیشه **بله** است.

Composer مزایای مهمی دارد:

مدیریت نسخه Drupal

مدیریت وابستگی‌ها

نصب استاندارد Moduleها

نصب Themeها

مدیریت Libraryها

امکان Rollback بهتر

مدیریت Composer Lock

به‌روزرسانی کنترل‌شده

مناسب برای Git و CI/CD

ساختار `drupal/recommended-project` نیز باعث می‌شود فایل‌های قابل دسترسی از وب در پوشه `web` قرار بگیرند و بخش‌های دیگر پروژه از Document Root خارج باشند.

آیا Drupal 11 برای سایت جدید انتخاب بهتری است؟

اگر در سال ۱۴۰۵ قصد راه‌اندازی یک سایت جدید دارید، در حالت عادی **Drupal 11 انتخاب منطقی‌تری نسبت به Drupal 10 است**؛ به شرطی که ماژول‌ها و Theme مورد استفاده شما با Drupal 11 سازگار باشند.

شاخه Drupal 11.4.x برای توسعه سایت‌های جدید هدف قرار گرفته و در حال حاضر آخرین Patch Release این شاخه، Drupal 11.4.5 است. این شاخه تا ژوئن ۲۰۲۷ پشتیبانی امنیتی دریافت خواهد کرد.

Drupal 10 بیشتر زمانی انتخاب می‌شود که پروژه به دلایل سازگاری نرم‌افزاری، ماژول‌های قدیمی یا کدهای اختصاصی هنوز آماده Drupal 11 نباشد.

جمع‌بندی

نصب Drupal 10 و Drupal 11 از نظر مراحل کلی تفاوت زیادی ندارد، اما نیازمندی‌های سرور در Drupal 11 جدیدتر شده‌اند.

برای Drupal 11 بهتر است از محیطی مانند:

Linux

Nginx / Apache

PHP 8.4

MySQL 8 / MariaDB 10.6+

Composer

SSL

Cron

OPcache

استفاده شود.

برای پروژه‌های حرفه‌ای نیز پیشنهاد می‌شود Drupal را با Composer نصب کنید:

```
drupal/recommended-project:^11 mysite
```

و Document Root را روی:

```
mysite/web
```

قرار دهید.

بعد از نصب نیز تنظیم HTTPS، Trusted Host، Permissionها، Backup، OPcache، Cache، Cron و به‌روزرسانی منظم Core و Moduleها ضروری است.

در نهایت، اگر پروژه جدیدی را در سال ۱۴۰۵ شروع می‌کنید، انتخاب Drupal 11 به‌خصوص شاخه x.11.4 آینده‌نگرانه‌تر است؛ در حالی که Drupal 10 به پایان چرخه عمر خود نزدیک می‌شود.

سوالات متداول درباره نصب Drupal

برای نصب Drupal 11 چه نسخه PHP لازم است؟

Drupal 11 حداقل به PHP 8.3 نیاز دارد. برای پروژه‌های جدید، PHP 8.4 انتخاب مناسبی است؛ البته سازگاری

ماژول‌ها نیز باید بررسی شود.

آیا می‌توان Drupal 11 را روی MySQL 5.7 نصب کرد؟

خیر، MySQL 5.7 برای Drupal 11 پشتیبانی رسمی ندارد. Drupal 11 به MySQL 8.0 یا بالاتر نیاز دارد.

Drupal را با Composer نصب کنیم یا ZIP؟

برای سایت‌های حرفه‌ای Composer روش پیشنهادی است. نصب ZIP بیشتر برای محیط‌هایی مناسب است که Composer یا SSH در دسترس نیست.

آیا Drupal روی Nginx نصب می‌شود؟

بله. Drupal از Nginx پشتیبانی می‌کند و باید PHP-FPM و تنظیمات Rewrite/`try_files` به‌درستی پیکربندی شوند.

حداقل RAM مورد نیاز Drupal چقدر است؟

Drupal حداقل 1GB RAM را برای اجرای Composer توصیه می‌کند؛ سایت‌های بزرگ‌تر با ماژول‌های بیشتر یا سرویس‌هایی مانند Solr و Memcached به RAM بیشتری نیاز دارند.

آیا Drupal 10 هنوز قابل استفاده است؟

بله، اما Drupal 10 در سال ۲۰۲۶ به پایان چرخه عمر خود نزدیک شده است. طبق برنامه رسمی Drupal، Drupal 10 در ۹ دسامبر ۲۰۲۶ به پایان عمر می‌رسد؛ بنابراین برای پروژه جدید بهتر است Drupal 11 را در نظر بگیرید.

آیا بعد از نصب Drupal باید Cron تنظیم کنیم؟

بله. برای سایت‌های واقعی بهتر است Cron به‌صورت منظم روی سرور اجرا شود تا وظایف دوره‌ای Drupal و ماژول‌ها بدون نیاز به اجرای دستی انجام شوند.

منابع رسمی

برای بررسی آخرین نیازمندی‌ها و نسخه‌های Drupal، بهتر است همیشه مستندات رسمی Drupal را نیز بررسی کنید:

مستندات رسمی نصب Drupal

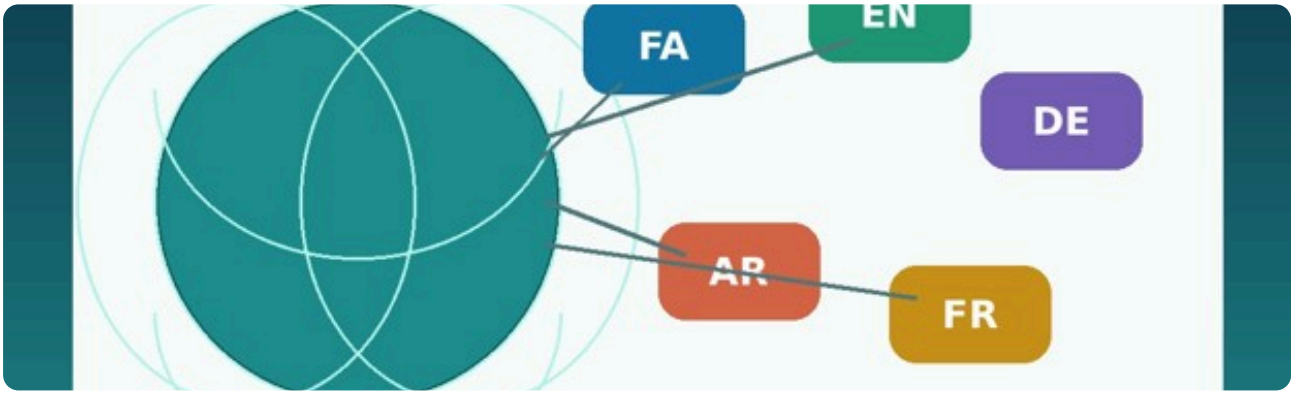
نیازمندی‌های سیستم Drupal

مستندات رسمی Composer در Drupal

صفحه نسخه‌های Drupal Core

دیگر اخبار هفته

طراحی سایت چندزبانه در دروپال؛ چرا ترجمه ماشینی به‌تنهایی کافی نیست؟



اگر قصد دارید یک **وب‌سایت چندزبانه با دروپال** راه‌اندازی کنید، صرفاً فعال کردن قابلیت ترجمه یا اتصال سایت به یک موتور هوش مصنوعی کافی نیست. بسیاری از مدیران وب تصور می‌کنند با نصب ماژول‌های ترجمه، تجربه کاربری

مطلوبی ایجاد خواهد شد؛ اما پژوهش‌های جدید نشان می‌دهد کیفیت ترجمه، بومی‌سازی محتوا و سئو بین‌المللی نقش بسیار مهم‌تری در موفقیت یک سایت چندزبانه دارند.

پژوهشی که در سال ۲۰۲۶ در مجله **Language Resources and Evaluation** منتشر شد، رفتار **۴۲۱۷ کاربر در شش کشور اروپایی** را بررسی کرده و نشان داده است که اگرچه بیشتر کاربران از ترجمه ماشینی استفاده می‌کنند، اما کیفیت پایین ترجمه باعث کاهش اعتماد آن‌ها به وب‌سایت می‌شود.

کاربران ترجمه ماشینی را استفاده می‌کنند، اما همیشه به آن اعتماد ندارند

بر اساس نتایج این پژوهش:

۸۲ درصد کاربران برای مطالعه صفحات وب از ابزارهای ترجمه آنلاین استفاده می‌کنند.
۷۵ درصد قابلیت ترجمه داخلی مرورگر را فعال کرده‌اند.

- نزدیک به ۴۰ درصد کیفیت ترجمه را متوسط یا ضعیف ارزیابی کرده‌اند.
- مشکل تنها ترجمه اشتباه واژه‌ها نیست. بسیاری از موتورهای ترجمه در انتقال لحن برند، اصطلاحات تخصصی، شوخی‌ها، مفاهیم فرهنگی یا حتی واحدهای اندازه‌گیری عملکرد مناسبی ندارند.

- به همین دلیل، ترجمه ماشینی تنها **دسترسی اولیه** ایجاد می‌کند؛ در حالی که **بومی‌سازی (Localization)** اعتماد کاربران، نرخ تبدیل و وفاداری آن‌ها را افزایش می‌دهد.

اهمیت این موضوع برای سایت‌های دروپال

یکی از مهم‌ترین مزایای **Drupal**، معماری قدرتمند آن برای مدیریت سایت‌های چندزبانه است.

در یک پروژه واقعی ممکن است بخش‌های زیر نیاز به ترجمه داشته باشند:

مقالات
محصولات
صفحات خدمات
منوها
بلاک‌ها
طبقه‌بندی‌ها (Taxonomy)
فرم‌ها
ایمیل‌های ارسالی
پیام‌های سیستمی
متن دکمه‌ها

اگر فقط محتوای اصلی ترجمه شود، بخش زیادی از رابط کاربری همچنان به زبان اصلی باقی می‌ماند و تجربه‌ای نامناسب برای کاربران ایجاد خواهد شد.

معماری صحیح چندزبانه در دروپال

یکی از اشتباهات رایج این است که چندزبانه بودن سایت بعد از تولید محتوا در نظر گرفته می‌شود.

در حالی که معماری صحیح باید از همان ابتدای طراحی پروژه تعریف شود.

در این مرحله باید مشخص شود:

- کدام فیلدها ترجمه شوند.
- چه داده‌هایی مشترک بمانند.
- چه اصطلاحاتی در تمام زبان‌ها ثابت باشند.
- گردش کار ترجمه چگونه انجام شود.

به عنوان نمونه:

- کد محصول ترجمه نمی‌شود.
- عنوان محصول ترجمه می‌شود.
- توضیحات ترجمه می‌شود.
- ویژگی‌ها ترجمه می‌شوند.
- متن دکمه‌ها ترجمه می‌شوند.
- پیام‌های خطا نیز باید ترجمه شوند.

تفاوت ترجمه و بومی‌سازی (Localization)

بسیاری این دو مفهوم را یکسان می‌دانند، در حالی که تفاوت زیادی دارند.

ترجمه فقط متن را از یک زبان به زبان دیگر تبدیل می‌کند.

اما **بومی‌سازی** موارد زیر را نیز متناسب با کشور مقصد تغییر می‌دهد:

- تاریخ

واحد پول

شماره تلفن

آدرس

جهت متن

تصاویر

رنگ‌ها

مثال‌ها

روش پرداخت

پیشنهاد محصولات

در زبان‌های راست‌به‌چپ مانند فارسی و عربی نیز باید موارد زیر بررسی شوند:

آیکن‌ها

فلش‌ها

فاصله‌ها

ترتیب ستون‌ها

محل قرارگیری منوها

صرفاً راست‌چین کردن متن کافی نیست.

بهترین روش ترجمه در سایت‌های دروپال

پژوهش ۲۰۲۶ پیشنهاد می‌کند از مدل **Machine Translation + Human Review** استفاده شود.

مراحل پیشنهادی عبارت‌اند از:

محتوای اصلی را ساده و قابل ترجمه بنویسید.

واژه‌نامه اختصاصی برند تهیه کنید.

ترجمه اولیه را با هوش مصنوعی انجام دهید.

صفحات مهم توسط مترجم انسانی بازبینی شوند.

امکان ثبت بازخورد کاربران فراهم شود.

هنگام تغییر متن اصلی، وضعیت ترجمه سایر زبان‌ها نیز به‌روزرسانی شود.

سئو سایت چندزبانه در دروپال

یکی از مهم‌ترین بخش‌های **Drupal Multilingual**، رعایت اصول سئو است.

اگر تنظیمات سئو به درستی انجام نشود، موتورهای جستجو ممکن است:

نسخه اشتباه صفحه را ایندکس کنند.

- صفحات را محتوای تکراری تشخیص دهند.
- زبان مناسب را به کاربران نمایش ندهند.

برای جلوگیری از این مشکلات:

- برای هر زبان URL مستقل ایجاد کنید.
- از تگ **hreflang** استفاده کنید.
- عنوان صفحات را ترجمه کنید.
- Meta Description هر زبان را جداگانه بنویسید.
- متن ALT تصاویر را ترجمه کنید.
- داده‌های ساختاریافته (Structured Data) را نیز ترجمه کنید.
- از Canonical صحیح استفاده کنید.
- نقشه سایت XML هر زبان را تولید کنید.
- تحقیق کلمات کلیدی را برای هر زبان جداگانه انجام دهید.
- Core Web Vitals را در تمام زبان‌ها بررسی کنید.

ماژول‌های مورد نیاز برای چندزبانه کردن دروپال

برای اغلب پروژه‌ها این ماژول‌های هسته دروپال کافی هستند:

- Language
- Content Translation
- Interface Translation
- Configuration Translation

سپس بسته به پروژه می‌توان:

- گردش کار ترجمه
- نقش کاربران
- وضعیت انتشار
- اتصال به سرویس‌های ترجمه
- اتصال به مدل‌های هوش مصنوعی

را به پروژه اضافه کرد.

گردش کار حرفه‌ای ترجمه در دروپال

یک فرآیند استاندارد معمولاً به این شکل است:

1. نویسنده محتوای اصلی را منتشر می‌کند.
2. سیستم وظیفه ترجمه ایجاد می‌کند.
3. موتور ترجمه یا مترجم نسخه اولیه را آماده می‌کند.
4. ویراستار محلی کیفیت متن را بررسی می‌کند.

مدیر محتوا نسخه نهایی را منتشر می‌کند.
این روش از انتشار ترجمه‌های ناقص جلوگیری می‌کند.

چگونه محتوایی تولید کنیم که بهتر ترجمه شود؟

طبق نتایج پژوهش، هرچه متن ساده‌تر باشد، کیفیت ترجمه ماشینی بیشتر خواهد بود.

پیشنهاد می‌شود:

جملات کوتاه بنویسید.
اصطلاحات ثابت استفاده کنید.
مخفف‌های نامشخص را حذف کنید.
واژه‌های تخصصی را استانداردسازی کنید.
راهنمای نگارش برای تیم محتوا تهیه کنید.
این کار علاوه بر افزایش کیفیت ترجمه، هزینه بازبینی انسانی را نیز کاهش می‌دهد.

اشتباهات رایج در پروژه‌های چندزبانه دروپال

ترجمه خودکار تمام صفحات بدون بازبینی
ترجمه نکردن منوها و پیام‌های سیستمی
استفاده از تصاویر یکسان برای تمام کشورها
تغییر مداوم ساختار URL زبان‌ها
ترجمه مستقیم کلمات کلیدی بدون تحقیق بازار
ترکیب بخش‌های راست‌چین و چپ‌چین در یک صفحه
فراموش کردن تنظیمات hreflang
نداشتن فرآیند مدیریت نسخه‌های ترجمه
جمع‌بندی

دروپال یکی از قدرتمندترین سیستم‌های مدیریت محتوا برای پیاده‌سازی وب‌سایت‌های چندزبانه است، اما موفقیت پروژه تنها به فعال کردن قابلیت ترجمه وابسته نیست. ترکیب **ترجمه ماشینی، بازبینی انسانی، بومی‌سازی، معماری صحیح محتوا و سئو بین‌المللی** باعث می‌شود کاربران احساس کنند سایت دقیقاً برای زبان و فرهنگ آن‌ها طراحی شده است؛ موضوعی که در نهایت به افزایش اعتماد، نرخ تبدیل و رشد ترافیک ارگانیک منجر خواهد شد.

پرسش‌های متداول

آیا دروپال به‌صورت پیش‌فرض از چند زبان پشتیبانی می‌کند؟

بله. هسته دروپال شامل ابزارهای مدیریت زبان، ترجمه محتوا، ترجمه رابط کاربری و ترجمه تنظیمات است؛ اما برای دستیابی به یک سایت چندزبانه حرفه‌ای باید ساختار محتوا، قالب، گردش کار و تنظیمات سئو نیز به‌درستی پیکربندی شوند.

آیا ترجمه هوش مصنوعی برای همه صفحات مناسب است؟

خیر. برای صفحات اطلاع‌رسانی یا محتوای کم‌ریسک می‌توان از ترجمه ماشینی استفاده کرد، اما صفحات فروش، حقوقی، پزشکی، مالی و محتوای برندمحور باید حتماً توسط مترجم یا ویراستار انسانی بازبینی شوند.

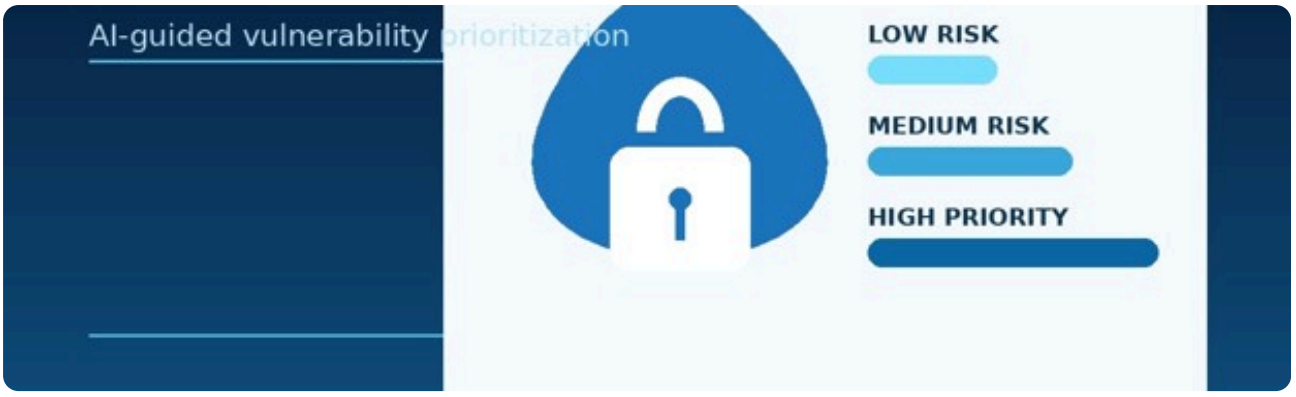
hreflang چه تأثیری بر سئو دارد؟

تگ **hreflang** به موتورهای جستجو اعلام می‌کند هر نسخه از صفحه برای کدام زبان یا منطقه جغرافیایی طراحی شده است و از نمایش نسخه اشتباه یا ایجاد مشکل محتوای تکراری جلوگیری می‌کند.

بهترین ساختار URL برای سایت چندزبانه چیست؟

در بیشتر پروژه‌های دروپال، استفاده از زیرپوشه‌های زبانی مانند `/en/`، `/fa/` و `/ar/` ساده‌ترین و قابل‌مدیریت‌ترین روش است؛ هرچند در پروژه‌های بین‌المللی ممکن است استفاده از زیردامنه یا دامنه مجزا بر اساس استراتژی کسب‌وکار انتخاب بهتری باشد.

امنیت دروپال در ۲۰۲۶؛ اولویت‌بندی هوشمند آسیب‌پذیری‌ها با هوش مصنوعی توضیح‌پذیر



امنیت دروپال در سال ۲۰۲۶؛ چگونه با هوش مصنوعی آسیب‌پذیری‌های Drupal را اولویت‌بندی کنیم؟

امنیت دروپال (Drupal Security) دیگر فقط به نصب آخرین نسخه هسته محدود نمی‌شود. مدیران وب‌سایت‌های مبتنی بر Drupal هر روز با ده‌ها هشدار امنیتی، آسیب‌پذیری (CVE)، به‌روزرسانی ماژول‌ها و وابستگی‌های Composer روبه‌رو هستند. سؤال اصلی این است که **کدام آسیب‌پذیری باید همین امروز برطرف شود و کدام مورد می‌تواند تا چرخه نگهداری بعدی منتظر بماند؟**

پژوهشی که در سال ۲۰۲۶ در مجله **International Journal of Information Security** منتشر شده است، با ترکیب **هوش مصنوعی توضیح‌پذیر (Explainable AI)**، **امتیاز شدت آسیب‌پذیری (CVSS)** و **احتمال بهره‌برداری واقعی (EPSS)** روشی دقیق‌تر برای مدیریت ریسک سایبری ارائه می‌دهد. این پژوهش می‌تواند برای مدیران و توسعه‌دهندگان **Drupal** که مسئول امنیت وب‌سایت‌های سازمانی و فروشگاهی هستند، بسیار کاربردی باشد.

چرا تنها به‌روزرسانی دروپال برای امنیت کافی نیست؟

- بسیاری از مدیران تصور می‌کنند با نصب آخرین نسخه هسته دروپال، امنیت سایت تضمین می‌شود؛ اما در عمل امنیت یک وب‌سایت Drupal به عوامل متعددی وابسته است، از جمله:
- نسخه هسته Drupal
- ماژول‌های مشارکتی (Contributed Modules)
- کتابخانه‌ها و وابستگی‌های Composer
- نسخه PHP
- تنظیمات وب‌سرور
- نوع پایگاه داده
- سطح دسترسی کاربران
- تنظیمات امنیتی سرور

به همین دلیل، **به‌روزرسانی هسته تنها بخشی از فرآیند امنیت دروپال است.**

چرا CVSS به‌تنهایی برای اولویت‌بندی آسیب‌پذیری‌ها کافی نیست؟

تقریباً تمام آسیب‌پذیری‌های امنیتی دارای **امتیاز CVSS** هستند. این امتیاز شدت فنی یک ضعف امنیتی را مشخص می‌کند، اما لزوماً نشان نمی‌دهد که مهاجمان تا چه اندازه از آن در دنیای واقعی سوءاستفاده می‌کنند.

برای مثال ممکن است:

- یک آسیب‌پذیری با امتیاز **۹.۸** نیازمند شرایط پیچیده‌ای برای بهره‌برداری باشد.

در مقابل، آسیب‌پذیری دیگری با امتیاز **۸.۲** به‌صورت گسترده توسط ربات‌های اینترنتی اسکن و مورد سوءاستفاده قرار گیرد.

بنابراین تصمیم‌گیری صرفاً بر اساس **CVSS** همیشه بهترین انتخاب نیست.

EPSS چیست و چه کمکی به امنیت Drupal می‌کند؟

EPSS (Exploit Prediction Scoring System) احتمال بهره‌برداری واقعی از یک آسیب‌پذیری را پیش‌بینی می‌کند.

در حالی که CVSS شدت فنی آسیب‌پذیری را اندازه‌گیری می‌کند، EPSS نشان می‌دهد:

احتمال حمله واقعی چقدر است.
آیا مهاجمان در حال سوءاستفاده از این آسیب‌پذیری هستند؟
آیا این ضعف باید فوراً وصله شود؟
برای مدیران سایت‌های **Drupal**، ترکیب CVSS و EPSS باعث می‌شود منابع امنیتی روی مهم‌ترین تهدیدها متمرکز شوند.

بررسی Drupalgeddon2؛ یکی از خطرناک‌ترین آسیب‌پذیری‌های دروپال

یکی از نمونه‌های مطرح‌شده در مقاله، آسیب‌پذیری مشهور **CVE-2018-7600** یا **Drupalgeddon2** است.

این آسیب‌پذیری امکان **اجرای کد از راه دور (Remote Code Execution)** را بدون احراز هویت فراهم می‌کرد و یکی از مهم‌ترین رخدادهای امنیتی تاریخ Drupal محسوب می‌شود.

بر اساس نتایج پژوهش:

امتیاز **EPSS حدود ۰٫۹۶** برای این آسیب‌پذیری گزارش شده است.
احتمال بهره‌برداری عملی بسیار بالا ارزیابی شده است.
حتی با گذشت چند سال، اگر نسخه آسیب‌پذیر هنوز روی سرور وجود داشته باشد، همچنان در اولویت فوری قرار دارد.

نتیجه مهم: قدیمی بودن یک CVE به معنای بی‌اهمیت بودن آن نیست.

نقش هوش مصنوعی توضیح‌پذیر در مدیریت امنیت دروپال

پژوهشگران برای تحلیل آسیب‌پذیری‌ها از مدل **CodeBERT** استفاده کرده‌اند.

این مدل توانسته در فرآیند آموزش و اعتبارسنجی دقتی نزدیک به **۹۷ درصد** در شناسایی آسیب‌پذیری‌های قابل بهره‌برداری به دست آورد.

اما مهم‌تر از دقت، استفاده از روش **SHAP** است.

SHAP مشخص می‌کند هر عامل چه میزان در تصمیم مدل نقش داشته است؛ از جمله:

- احتمال بهره‌برداری
- بردار حمله
- سطح دسترسی مهاجم
- نیاز یا عدم نیاز به تعامل کاربر
- تأثیر بر محرمانگی اطلاعات
- تأثیر بر یکپارچگی داده‌ها

این شفافیت باعث می‌شود مدیران امنیت بتوانند تصمیمات خود را مستند و قابل دفاع کنند.

نمونه واقعی سال ۲۰۲۶؛ آسیب‌پذیری CVE-2026-9082

در ماه مه ۲۰۲۶ تیم امنیت Drupal آسیب‌پذیری **CVE-2026-9082** را منتشر کرد.

این ضعف امنیتی از نوع **SQL Injection** بود و روی سایت‌هایی اثر می‌گذاشت که از **PostgreSQL** استفاده

می‌کردند.

پیامدهای احتمالی این آسیب‌پذیری عبارت بودند از:

- افشای اطلاعات
- افزایش سطح دسترسی
- اجرای کد از راه دور در برخی شرایط

شدت این آسیب‌پذیری توسط تیم امنیت Drupal **۲۳ از ۲۵** اعلام شد و پس از مشاهده تلاش‌های بهره‌برداری واقعی، فوریت نصب وصله امنیتی افزایش یافت.

این نمونه نشان می‌دهد شناخت دقیق زیرساخت سایت اهمیت بسیار بیشتری از واکنش صرف به یک هشدار امنیتی دارد؛ زیرا وب‌سایت‌هایی که از **MySQL** یا **MariaDB** استفاده می‌کنند، در مسیر اصلی این حمله قرار نمی‌گیرند.

چگونه آسیب‌پذیری‌های دروپال را اولویت‌بندی کنیم؟

برای مدیریت مؤثر امنیت Drupal، پیشنهاد می‌شود مراحل زیر را اجرا کنید.

۱. دارایی‌های سایت را مستندسازی کنید

موارد زیر را ثبت کنید:

- نسخه هسته Drupal
- ماژول‌ها
- قالب‌ها
- PHP
- Composer
- پایگاه داده
- سرویس‌های متصل

---

۲. اطلاعیه‌های امنیتی رسمی را دنبال کنید

همیشه این منابع را بررسی کنید:

- Drupal Security Advisories
- پایگاه CVE
- هشدارهای Composer
- اطلاعیه‌های امنیتی کتابخانه‌ها

---

۳. شدت و احتمال حمله را همزمان بررسی کنید

بهترین تصمیم زمانی گرفته می‌شود که:

- CVSS شدت آسیب‌پذیری را مشخص کند.
- EPSS احتمال سوءاستفاده را نشان دهد.

---

۴. ارزش دارایی را در نظر بگیرید

اولویت وصله برای این بخش‌ها بیشتر است:

- صفحه ورود مدیر
- صفحه پرداخت
- اطلاعات کاربران
- APIها
- سرویس‌های حیاتی

---

۵. مسیر حمله را تحلیل کنید

سؤالات زیر را بررسی کنید:

- آیا حمله از اینترنت قابل انجام است؟
- آیا نیاز به احراز هویت دارد؟
- آیا WAF فعال است؟
- آیا مهاجم به سطح دسترسی اولیه نیاز دارد؟

---

۶. تصمیم‌ها را مستندسازی کنید

برای هر آسیب‌پذیری مشخص کنید:

- فوری
- مهم
- قابل تعویق

و دلیل این تصمیم را ثبت کنید.

---

۷. پس از نصب وصله، آزمون انجام دهید

بعد از هر به‌روزرسانی موارد زیر را بررسی کنید:

- فرم‌ها

ورود کاربران

API

Cron

Queue

کش

سرویس‌های خارجی

چک‌لیست امنیت دروپال

قبل از پایان هر چرخه نگهداری، این موارد را بررسی کنید:

هسته Drupal روی نسخه پشتیبانی‌شده قرار دارد.

ماژول‌های مشارکتی به‌روز هستند.

وابستگی‌های Composer بررسی شده‌اند.

احراز هویت چندمرحله‌ای برای مدیران فعال است.

نسخه پشتیبان خارج از سرور نگهداری می‌شود.

پایگاه داده از اینترنت عمومی قابل دسترسی نیست.

گزارش‌های PHP، Drupal، وب‌سرور و WAF به‌صورت متمرکز ذخیره می‌شوند.

ماژول‌های بدون استفاده حذف شده‌اند.

فرآیند واکنش به وصله‌های امنیتی بحرانی از قبل تعریف شده است.

ارتباط امنیت دروپال با سئو

بسیاری تصور می‌کنند امنیت و سئو ارتباطی با یکدیگر ندارند؛ در حالی که یک نفوذ امنیتی می‌تواند تأثیر مستقیمی بر رتبه سایت در گوگل داشته باشد.

از جمله پیامدهای رایج:

ایجاد صفحات اسپم

ریدایرکت‌های مخرب

سرقت محتوا

کاهش سرعت سایت

قرار گرفتن هشدار امنیتی در نتایج جستجو

حذف صفحات آلوده از ایندکس گوگل

به همین دلیل، امنیت Drupal بخشی از استراتژی سئو و نگهداری حرفه‌ای وب‌سایت محسوب می‌شود.

جمع‌بندی

مدیریت امنیت دروپال در سال ۲۰۲۶ دیگر به نصب وصله‌های امنیتی محدود نیست. استفاده همزمان از **EPSS**، **CVSS**، هوش مصنوعی توضیح‌پذیر و شناخت دقیق معماری سایت، به مدیران کمک می‌کند منابع خود را روی مهم‌ترین تهدیدها متمرکز کنند.

پژوهش منتشرشده در **International Journal of Information Security** نشان می‌دهد که آینده مدیریت آسیب‌پذیری‌ها به سمت تصمیم‌گیری هوشمند، داده‌محور و قابل توضیح حرکت می‌کند؛ رویکردی که می‌تواند امنیت وب‌سایت‌های Drupal را به شکل قابل توجهی افزایش دهد.

پرسش‌های متداول

آیا نصب آخرین نسخه دروپال برای امنیت کافی است؟

خیر. علاوه بر هسته Drupal، باید ماژول‌ها، وابستگی‌های Composer، تنظیمات PHP، وب‌سرور، پایگاه داده و دسترسی کاربران نیز به‌صورت منظم بررسی شوند.

تفاوت CVSS و EPSS چیست؟

CVSS شدت فنی یک آسیب‌پذیری را اندازه‌گیری می‌کند، در حالی که EPSS احتمال بهره‌برداری واقعی از آن را پیش‌بینی می‌کند.

آیا همه آسیب‌پذیری‌های بحرانی باید فوراً وصله شوند؟

در بیشتر موارد بله، اما اولویت نهایی به معماری سایت، نوع پایگاه داده، میزان دسترسی مهاجم و کنترل‌های امنیتی موجود بستگی دارد.

آیا هوش مصنوعی جایگزین متخصص امنیت می‌شود؟

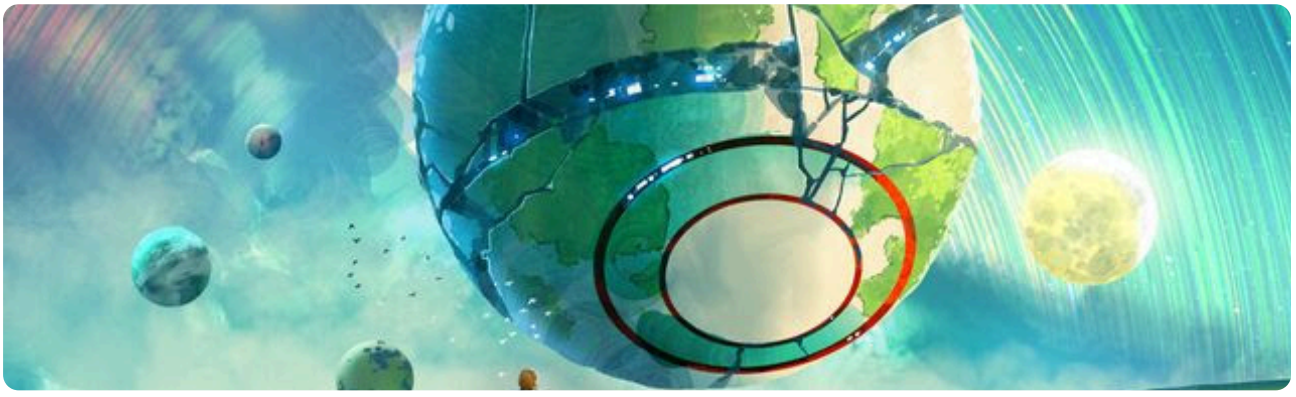
خیر. هوش مصنوعی می‌تواند تحلیل و اولویت‌بندی آسیب‌پذیری‌ها را سرعت ببخشد، اما تصمیم نهایی همچنان نیازمند دانش فنی و شناخت زیرساخت سازمان است.

منبع علمی

این پژوهش آسیب‌پذیری مشهور **Drupalgeddon2 (CVE-2018-7600)** را تحلیل کرده و در کنار آن، اطلاعیه رسمی **SA-CORE-2026-004** درباره **CVE-2026-9082** نیز به‌عنوان نمونه‌ای از مدیریت ریسک در Drupal قابل بررسی است.

عنوان انگلیسی	Explainable AI based dynamic cybersecurity risk management for cyber insurability
مجله و نمایه	International Journal of Information Security | Web of Science Core Collection | SCIE
تاریخ/شماره	انتشار: ۲۲ ژانویه ۲۰۲۶؛ جلد ۲۵، مقاله ۳۶
DOI	10.1007/s10207-025-01189-8
ارتباط با دروپال	Drupalgeddon2 را تحلیل می‌کند. منبع تکمیلی رسمی: SA-CORE-2026-004 درباره CVE-2026-9082، منتشرشده در ۲۰ مه ۲۰۲۶.

مهاجرت از وردپرس به دروپال؛ چرا سازمان‌های بزرگ Drupal را انتخاب می‌کنند؟



در سال‌های اخیر، بسیاری از سازمان‌های بزرگ در جهان یک تصمیم استراتژیک مشابه گرفته‌اند: **انتقال وب‌سایت‌های خود از وردپرس و سایر سیستم‌های مدیریت محتوا به Drupal**.

این تغییر فقط به دلیل امکانات فنی دروپال نیست؛ بلکه یک مسئله مهم‌تر در پشت این تصمیم وجود دارد: **هزینه‌های پنهان استفاده از چند CMS مختلف در یک سازمان.**

دریس بایترت (Dries Buytaert)، بنیان‌گذار Drupal، در مقاله‌ای با عنوان «مالیات چندپارگی CMS» (The CMS Fragmentation Tax) توضیح می‌دهد که بسیاری از سازمان‌ها به دلیل استفاده هم‌زمان از چند پلتفرم مدیریت محتوا، هزینه‌های زیادی را متحمل می‌شوند.

مشکل اصلی: چند CMS یعنی چند برابر شدن هزینه‌ها

بسیاری از سازمان‌های بزرگ دارای ده‌ها یا حتی صدها وب‌سایت هستند. در طول زمان، هر تیم ممکن است بر اساس نیاز خود یک CMS انتخاب کند:

- یک سایت با WordPress راه‌اندازی شود.
- یک سایت سازمانی با Drupal ساخته شود.

یک پلتفرم دیگر مانند Contentful برای تیم دیگری استفاده شود.

در ابتدا این تصمیم‌ها منطقی به نظر می‌رسند؛ اما در مقیاس سازمانی مشکلات شروع می‌شوند.

فرض کنید سازمان تصمیم می‌گیرد یک سیستم مدیریت دارایی دیجیتال (DAM) جدید به وب‌سایت‌های خود متصل کند.

- اگر سازمان فقط یک CMS داشته باشد، یک پروژه Integration خواهد داشت.

اما اگر سه CMS مختلف داشته باشد، باید:

سه اتصال جداگانه توسعه داده شود.

سه تیم متخصص درگیر شوند.

سه فرآیند تست و نگهداری ایجاد شود.

سه مدل امنیتی بررسی شود.

در نتیجه، یک قابلیت جدید به جای یک پروژه، تبدیل به چند پروژه موازی و پرهزینه می‌شود.

هزینه پنهان استفاده از چند سیستم مدیریت محتوا

چندپارگی CMS فقط هزینه توسعه اولیه ایجاد نمی‌کند؛ بلکه یک هزینه دائمی برای سازمان به وجود می‌آورد.

این هزینه شامل موارد زیر است:

۱. افزایش هزینه توسعه و نگهداری

- هر CMS معماری، افزونه‌ها، روش توسعه و نیازهای فنی متفاوتی دارد.

تیم‌های توسعه باید دانش چند پلتفرم را حفظ کنند و مشکلات هر سیستم را جداگانه مدیریت کنند.

۲. پیچیده‌تر شدن امنیت

هر CMS دارای:

فرآیندهای امنیتی متفاوت

چرخه بروزرسانی متفاوت

افزونه‌ها و آسیب‌پذیری‌های مخصوص به خود است.

- مدیریت امنیت چند CMS برای سازمان‌های بزرگ بسیار دشوارتر است.

۳. کاهش سرعت نوآوری

امروزه سازمان‌ها به سرعت باید قابلیت‌های جدیدی مانند:

- هوش مصنوعی
- شخصی‌سازی محتوا
- تحلیل رفتار کاربران
- اتوماسیون بازاریابی
- سیستم‌های پیشنهاددهنده

را به وب‌سایت‌های خود اضافه کنند.

اما وقتی زیرساخت دیجیتال پراکنده باشد، هر قابلیت جدید باید چند بار پیاده‌سازی شود.

چرا Drupal برای سازمان‌های بزرگ جذاب شده است؟

دروپال سال‌هاست که در پروژه‌های سازمانی بزرگ استفاده می‌شود، اما یکی از تغییرات مهم اخیر، ساده‌تر شدن تجربه کاربری آن برای بازاریابان و مدیران محتوا است.

معرفی **Drupal CMS** باعث شده فاصله بین قدرت فنی Drupal و نیازهای تیم‌های بازاریابی کمتر شود.

امروزه Drupal تلاش می‌کند دو نیاز مهم سازمان‌ها را هم‌زمان پاسخ دهد:

- سادگی برای تولیدکنندگان محتوا
- انعطاف‌پذیری برای تیم‌های فنی

یک CMS مشترک، اما با مدل‌های عملیاتی متفاوت

یکی از نکات مهم مطرح‌شده توسط Dries Buytaert این است که استانداردسازی روی یک CMS به معنی یکسان‌سازی همه سایت‌ها نیست.

یک سازمان ممکن است صدها سایت داشته باشد که نیازهای متفاوتی دارند.

برای مثال:

یک سایت کمپین بازاریابی ممکن است نیاز داشته باشد:

- سریع راه‌اندازی شود.
- بدون وابستگی زیاد به برنامه‌نویسان مدیریت شود.

اما یک سامانه سازمانی بزرگ ممکن است نیازمند:

ماژول‌های اختصاصی
Integrationهای پیچیده
کنترل کامل کد
باشد.

- راهکار پیشنهادی Drupal این است که یک پایه مشترک وجود داشته باشد، اما مدل استفاده متفاوت باشد.

تفاوت Acquia Source و Acquia Cloud چیست؟

Acquia برای پاسخ به این نیاز دو مدل ارائه کرده است:

Acquia Source؛ مدل SaaS برای سرعت بیشتر

- این مدل برای سازمان‌هایی مناسب است که:

سرعت راه‌اندازی اهمیت زیادی دارد.
تیم بازاریابی باید استقلال بیشتری داشته باشد.
نیاز به مدیریت زیرساخت وجود ندارد.
در این مدل، مدیریت زیرساخت توسط Acquia انجام می‌شود و کاربران بیشتر از طریق رابط کاربری و ابزارهای آماده سایت را توسعه می‌دهند.

Acquia Cloud؛ مدل PaaS برای کنترل بیشتر

- این مدل برای پروژه‌هایی مناسب است که نیاز دارند:

ماژول اختصاصی Drupal توسعه دهند.
از ماژول‌های جامعه Drupal استفاده کنند.
کد را با Git مدیریت کنند.
فرآیند CI/CD داشته باشند.
Integrationهای پیچیده ایجاد کنند.
مفهوم Open SaaS؛ ترکیب قدرت متن‌باز و راحتی SaaS

یکی از مفاهیم مهم مطرح‌شده توسط Dries Buytaert، اصطلاح **Open SaaS** است.

یعنی سازمان‌ها بتوانند از راحتی سرویس‌های SaaS استفاده کنند، اما همچنان مالکیت و قابلیت انتقال اطلاعات خود را حفظ کنند.

در این مدل:

- سازمان وابسته به یک CMS بسته نمی‌شود.
- امکان مهاجرت وجود دارد.
- داده‌ها و کد قابل انتقال هستند.

مسیر رشد فناوری حفظ می‌شود.
آینده متعلق به سازمان‌هایی است که یک پایه دیجیتال مشترک دارند

در آینده، سازمان‌ها بیش از گذشته به فناوری‌هایی مانند:

- هوش مصنوعی مولد
- موتورهای شخصی‌سازی
- تحلیل داده
- اتوماسیون محتوا

نیاز خواهند داشت.

اگر هر وب‌سایت روی یک CMS جداگانه باشد، اجرای این قابلیت‌ها دشوار و پرهزینه خواهد شد.

اما داشتن یک پایه مشترک مانند Drupal باعث می‌شود سازمان بتواند:

- تجربه‌های طراحی را دوباره استفاده کند.
- امنیت را استاندارد کند.
- Integrationها را یک‌بار توسعه دهد.
- دانش تیم‌ها را به اشتراک بگذارد.

جمع‌بندی: کاهش هزینه دیجیتال با انتخاب یک CMS استراتژیک

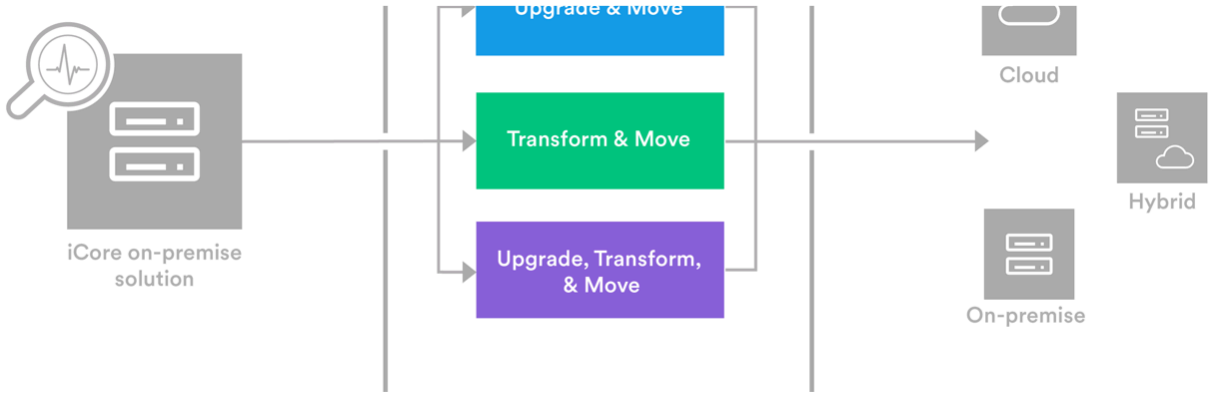
موضوع اصلی مهاجرت سازمان‌ها از WordPress و سایر CMSها به Drupal فقط انتخاب یک فناوری نیست؛ بلکه یک تصمیم مدیریتی برای کاهش پیچیدگی دیجیتال است.

استفاده از یک CMS استاندارد در کنار مدل‌های عملیاتی مختلف، به سازمان‌ها اجازه می‌دهد:

هزینه توسعه و نگهداری را کاهش دهند.
امنیت را بهتر مدیریت کنند.
سریع‌تر قابلیت‌های جدید اضافه کنند.
از سرمایه‌گذاری‌های قبلی خود دوباره استفاده کنند.

به همین دلیل، بسیاری از سازمان‌های بزرگ در حال بازنگری معماری دیجیتال خود و حرکت به سمت یک پلتفرم مشترک مانند Drupal هستند.

راهنمای کامل مهاجرت از دروپال ۹/۱۰ به دروپال ۱۱



اگر هنوز روی دروپال ۹ یا نسخه‌های اولیه ۱۰ هستید، وقت آن رسیده که مسیر مهاجرت به دروپال ۱۱ را جدی بگیرید. دروپال ۹ سال‌هاست از رده پشتیبانی خارج شده و دروپال ۱۰ هم برنامه پایان عمر مشخصی دارد. در این مقاله مسیر عملی و بدون دردسر مهاجرت را قدم‌به‌قدم بررسی می‌کنیم.

چرا مهاجرت به دروپال ۱۱ ضروری است؟

دروپال ۱۱ نسل جدیدی از وابستگی‌های نرم‌افزاری، بهبود قابل توجه در عملکرد و پایه‌ای پایدارتر برای سال‌های آینده ارائه می‌دهد. علاوه بر این، بسیاری از ماژول‌های کانتریب دیگر برای نسخه‌های قدیمی‌تر پشتیبانی فعال ارائه نمی‌کنند و همین موضوع ریسک امنیتی سایت شما را بالا می‌برد.

پیش‌نیازهای فنی مهاجرت

پیش از هر اقدامی باید نسخه PHP سرور خود را به ۸.۳ ارتقا دهید، چون دروپال ۱۱ به این نسخه نیاز دارد. همچنین باید مطمئن شوید پایگاه داده (معمولاً MySQL یا MariaDB) نسخه‌ای سازگار دارد.

چک‌لیست پیش‌نیاز:

- ارتقای PHP به نسخه ۸.۳
- بک‌آپ کامل از دیتابیس و فایل‌ها
- بررسی سازگاری ماژول‌های کانتریب با دروپال ۱۱
- تست محیط Staging جدا از سایت اصلی

مسیر پیشنهادی مهاجرت

اگر روی دروپال ۹ هستید، ابتدا باید به دروپال ۱۰.۳ ارتقا پیدا کنید؛ این نسخه عملاً از نظر ساختار API با دروپال ۱۱ یکسان است و تنها کدهای منسوخ‌شده (Deprecated) را هنوز پشتیبانی می‌کند. پس از رسیدن به ۱۰.۳، مهاجرت به ۱۱ یک پرش کوچک و کم‌ریسک خواهد بود.

مراحل عملی:

1. ارتقای پله‌ای به دروپال ۱۰.۳
2. اجرای Drupal Rector برای شناسایی کدهای منسوخ در ماژول‌های سفارشی
3. رفع وابستگی‌های Composer ناسازگار
4. تست کامل عملکرد سایت در محیط Staging
5. اجرای نهایی ارتقا در سایت زنده در زمان کم‌ترافیک

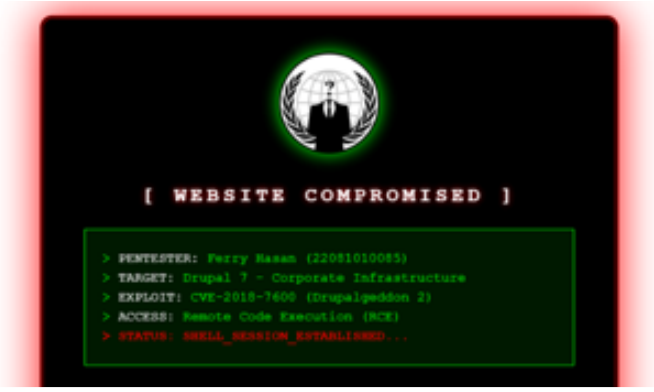
ماژول‌های سفارشی؛ نقطه حساس مهاجرت

بیشترین زمان صرف‌شده در مهاجرت واقعی معمولاً مربوط به ماژول‌های سفارشی است، نه هسته دروپال. توابع منسوخ‌شده، تغییر امضای متدها در سرویس‌ها، و وابستگی به کتابخانه‌های قدیمی از رایج‌ترین مشکلات هستند. توصیه می‌شود پیش از شروع، فهرستی از تمام هوک‌ها و سرویس‌های استفاده‌شده در ماژول‌های خودتان تهیه کنید.

جمع‌بندی

مهاجرت به دروپال ۱۱ یک پروژه یک‌شبه نیست، اما با برنامه‌ریزی درست و تست کافی در محیط Staging، می‌توان آن را بدون افت عملکرد یا از دست رفتن داده انجام داد. شروع زودهنگام، مهم‌ترین عامل موفقیت در این مسیر است.

تحلیل آسیب‌پذیری اجرای کد از راه دور CVE-2018-7600 در دروپال با Metasploit



CVE-2018-7600 یکی از خطرناک‌ترین آسیب‌پذیری‌های کشف‌شده در هسته دروپال است. این نقص امنیتی که با نام Drupalgeddon 2 شناخته می‌شود، در شرایط خاص امکان اجرای کد از راه دور و تصاحب سامانه را فراهم می‌کند. در این مقاله، علت فنی، پیامدها، نتایج یک آزمایش کنترل‌شده و راهکارهای پیشگیری از این تهدید بررسی شده است.

تحلیل آسیب‌پذیری اجرای کد از راه دور CVE-2018-7600 در دروپال با Metasploit

آسیب‌پذیری **CVE-2018-7600 در دروپال** که بیشتر با نام **Drupalgeddon 2** شناخته می‌شود، یکی از جدی‌ترین نقص‌های امنیتی هسته Drupal است. این آسیب‌پذیری می‌تواند در نسخه‌های قدیمی و به‌روزرسانی‌نشده دروپال، امکان اجرای کد از راه دور یا Remote Code Execution را برای مهاجم فراهم کند.

در صورت بهره‌برداری موفق، مهاجم ممکن است بدون ورود به حساب کاربری، کد دلخواه خود را با سطح دسترسی وب‌سرور اجرا کند. چنین دسترسی‌ای می‌تواند امنیت فایل‌ها، پایگاه داده، اطلاعات کاربران و حتی دسترس‌پذیری کامل وب‌سایت را تهدید کند.

اطلاعیه رسمی Drupal این نقص را یک آسیب‌پذیری اجرای کد از راه دور با درجه خطر «بسیار بحرانی» معرفی کرده است. این آسیب‌پذیری می‌توانست چند بخش از هسته دروپال را تحت‌تأثیر قرار دهد و در نهایت باعث تصاحب کامل وب‌سایت شود.

هشدار حقوقی و اخلاقی: مطالب این مقاله فقط با هدف آموزش امنیت، تحلیل آسیب‌پذیری و آزمایش در محیط کنترل‌شده منتشر شده‌اند. هرگونه آزمایش امنیتی باید فقط روی سامانه‌ای انجام شود که مالک آن هستید یا برای ارزیابی آن مجوز رسمی و کتبی دارید.

در این مقاله چه می‌خوانید؟

در ادامه، موضوعات زیر بررسی می‌شوند:

Drupalgeddon 2 چیست؟

اجرای کد از راه دور یا RCE چه مفهومی دارد؟

کدام نسخه‌های دروپال تحت‌تأثیر قرار گرفتند؟

علت فنی CVE-2018-7600 چیست؟

Metasploit چه نقشی در آزمایش این آسیب‌پذیری دارد؟

پیامدهای این نقص برای امنیت اطلاعات چیست؟

چگونه می‌توان از وب‌سایت‌های دروپالی محافظت کرد؟

Drupalgeddon 2 چیست؟

Drupalgeddon 2 نامی است که برای آسیب‌پذیری **CVE-2018-7600** انتخاب شده است. این نقص امنیتی در تاریخ ۲۸ مارس ۲۰۱۸ با شناسه امنیتی **SA-CORE-2018-002** منتشر شد.

بر اساس اطلاعات ثبت‌شده در پایگاه ملی آسیب‌پذیری‌های آمریکا، نسخه‌های زیر در زمان انتشار وصله تحت‌تأثیر قرار داشتند:

Drupal 7 پیش از نسخه 7.58

Drupal 8.3 پیش از نسخه 8.3.9

Drupal 8.4 پیش از نسخه 8.4.6

Drupal 8.5 پیش از نسخه 8.5.1

این نسخه‌ها به‌دلیل نقصی که چند زیرسامانه هسته دروپال را درگیر می‌کرد، امکان اجرای کد دلخواه از راه دور را فراهم می‌کردند.

نسخه 7.58 فقط نسخه‌ای تاریخی است که در سال ۲۰۱۸ این نقص مشخص را برطرف کرد و نباید آن را نسخه‌ای مناسب برای استفاده امروزی در نظر گرفت. پشتیبانی رسمی Drupal 7 در تاریخ ۵ ژانویه ۲۰۲۵ پایان یافته است و این شاخه دیگر به‌روزرسانی امنیتی رسمی دریافت نمی‌کند. بنابراین، مدیران وب‌سایت‌های باقی‌مانده روی Drupal 7 باید برای انتقال به یک نسخه پشتیبانی‌شده برنامه‌ریزی کنند.

اجرای کد از راه دور یا RCE چیست؟

اجرای کد از راه دور یا **Remote Code Execution** نوعی آسیب‌پذیری امنیتی است که به مهاجم اجازه می‌دهد از طریق شبکه، دستور یا کد دلخواه خود را روی سرور هدف اجرا کند.

در یک حمله موفق RCE، مهاجم ممکن است بتواند:

- فایل‌های حساس را مشاهده کند؛
- اطلاعات پیکربندی را تغییر دهد؛
- به پایگاه داده دسترسی پیدا کند؛
- داده‌های کاربران را سرقت کند؛
- فایل‌های مخرب روی سرور قرار دهد؛
- ظاهر و محتوای وب‌سایت را تغییر دهد؛
- سرویس را از دسترس خارج کند.

شدت خطر به سطح دسترسی فرایند وب‌سرور و پیکربندی سیستم‌عامل بستگی دارد. اجرای وب‌سرور با دسترسی محدود می‌تواند بخشی از خسارت را کاهش دهد، اما جایگزین نصب وصله و به‌روزرسانی نرم‌افزار نیست.

علت فنی آسیب‌پذیری CVE-2018-7600

ریشه Drupalgeddon 2 به پردازش ناامن ورودی‌ها در چند زیرسامانه دروپال مربوط بود. یکی از بخش‌های مهم درگیر، سازوکار فرم‌ها و آرایه‌های قابل‌نمایش در دروپال بود.

دروپال برای ایجاد فرم‌ها و اجزای پویا از ساختارهایی استفاده می‌کند که بعضی ویژگی‌های آن‌ها می‌توانند عملیات مشخصی را در زمان پردازش محتوا اجرا کنند. در نسخه‌های آسیب‌پذیر، کنترل و پاک‌سازی بعضی ورودی‌های کاربر به‌اندازه کافی سخت‌گیرانه نبود.

در نتیجه، ورودی دستکاری‌شده می‌توانست به‌عنوان یک ویژگی اجرایی تفسیر شود و باعث اجرای عملیات ناخواسته روی سرور شود. ماژول Drupalgeddon 2 در Metasploit نیز این مسئله را به‌عنوان تزریق ویژگی در Forms API معرفی می‌کند.

به زبان ساده، مشکل زمانی رخ می‌داد که سیستم بخشی از داده ورودی کاربر را به‌جای «داده معمولی»، مانند یک دستور قابل‌اجرا پردازش می‌کرد.

نقش Metasploit در تحلیل Drupalgeddon 2

Metasploit Framework یک چارچوب شناخته‌شده برای ارزیابی امنیت و تست نفوذ است. این ابزار مجموعه‌ای از ماژول‌ها را برای شناسایی و بررسی آسیب‌پذیری‌های مختلف ارائه می‌کند.

برای CVE-2018-7600 نیز یک ماژول آزمایش امنیتی در Metasploit وجود دارد که به متخصصان اجازه می‌دهد در یک محیط آزمایشگاهی و دارای مجوز، بررسی کنند که آیا نسخه قدیمی دروپال در برابر این نقص آسیب‌پذیر است یا خیر.

طبق مستندات Rapid7، این ماژول برای سامانه‌های مبتنی بر Linux ،PHP و Unix طراحی شده است. به همین دلیل، استفاده از محموله‌های مخصوص ویندوز برای یک هدف لینوکسی یا کانتینر لینوکسی انتخاب فنی مناسبی نیست.

در این مقاله، جزئیات اجرایی و فرمان‌های عملیاتی بهره‌برداری ارائه نمی‌شوند. برای ارزیابی امنیتی واقعی باید از مستندات رسمی، محیط ایزوله و مجوز کتبی مالک سامانه استفاده شود.

معماری محیط آزمایش

برای تحلیل کنترل‌شده آسیب‌پذیری، می‌توان یک آزمایشگاه محلی و جدا از اینترنت ایجاد کرد. ساختار آزمایش مورد بررسی از سه بخش اصلی تشکیل شده بود:

۱. سیستم میزبان

یک رایانه دارای Windows 11 به‌عنوان سیستم اصلی برای اجرای ابزارهای مجازی‌سازی، WSL و کانتینرها استفاده شد.

۲. محیط ارزیابی امنیت

Kali Linux در بستر WSL 2 به‌عنوان محیط تحلیل و اجرای ابزارهای امنیتی در نظر گرفته شد. Metasploit Framework نیز در همین محیط اجرا شد.

۳. سامانه هدف آزمایشگاهی

یک کانتینر Docker شامل نسخه قدیمی و آسیب‌پذیر Drupal 7.54 به‌عنوان هدف آزمایش استفاده شد. وب‌سرور، PHP و پایگاه داده نیز در شبکه محلی و ایزوله قرار گرفتند.

استفاده از شبکه جداشده مانع از آن می‌شود که آزمایش به سامانه‌های واقعی یا اینترنت عمومی آسیب برساند.

روش کلی ارزیابی آسیب‌پذیری

فرایند پژوهش با رویکرد آزمایشی ـ توصیفی انجام شد و شامل مراحل کلی زیر بود:

1. راه‌اندازی نسخه آسیب‌پذیر دروپال در محیط کنترل‌شده؛
2. بررسی نسخه و پیکربندی سامانه هدف؛
3. انتخاب ابزار ارزیابی سازگار با CVE-2018-7600؛
4. انجام آزمایش فقط در شبکه محلی و دارای مجوز؛
5. بررسی سطح دسترسی به‌دست‌آمده؛
6. تحلیل پیامدهای امنیتی؛
7. مستندسازی راهکارهای پیشگیری و کاهش خطر.

هدف این آزمایش، اثبات وجود آسیب‌پذیری و بررسی اثر آن بود؛ نه ایجاد دسترسی پایدار یا آسیب‌رساندن به سامانه.

نتایج آزمایش کنترل‌شده

نتایج آزمایش نشان داد که نسخه قدیمی Drupal 7.54 در برابر CVE-2018-7600 آسیب‌پذیر است. در محیط آزمایشگاهی، اجرای موفق تست باعث ایجاد یک نشست از راه دور با سطح دسترسی فرایند وب‌سرور شد.

به‌دست‌آوردن چنین نشستی به این معناست که مهاجم می‌تواند در محدوده مجوزهای وب‌سرور، بخش‌هایی از سیستم را مشاهده یا تغییر دهد.

شناسایی اطلاعات سیستم

پس از ایجاد نشست آزمایشگاهی، اطلاعاتی مانند موارد زیر قابل مشاهده بود:

- نوع سیستم‌عامل؛
- معماری پردازنده؛
- نسخه هسته سیستم‌عامل؛
- نام میزبان؛
- نام کاربر اجراکننده وب‌سرور؛

مسیر فعلی برنامه.

این اطلاعات به مهاجم کمک می‌کنند ساختار سامانه و سطح دسترسی موجود را بهتر شناسایی کند.

دسترسی به ساختار فایل‌های دروپال

در صورت تنظیم نادرست مجوزها، مهاجم ممکن است به پوشه‌های اصلی دروپال دسترسی پیدا کند؛ از جمله:

پوشه ماژول‌ها؛

پوشه قالب‌ها؛

پوشه فایل‌های بارگذاری‌شده؛

فایل‌های تنظیمات؛

فایل‌های پشتیبان باقی‌مانده روی سرور.

قرارگرفتن فایل‌های پشتیبان یا تنظیمات در مسیرهای قابل‌دسترسی می‌تواند شدت حمله را افزایش دهد.

افشای فایل تنظیمات

یکی از مهم‌ترین خطرها، دسترسی احتمالی به فایل تنظیمات دروپال است. این فایل می‌تواند شامل اطلاعات اتصال به پایگاه داده، نام پایگاه داده و سایر داده‌های حساس باشد.

افشای این اطلاعات ممکن است به مهاجم اجازه دهد دامنه حمله را از وب‌سرور به پایگاه داده گسترش دهد. به همین دلیل، محدودکردن مجوز خواندن فایل تنظیمات و جداسازی دسترسی‌های پایگاه داده اهمیت زیادی دارد.

خطر تغییر یا بارگذاری فایل

چنانچه کاربر وب‌سرور مجوز نوشتن گسترده داشته باشد، مهاجم ممکن است بتواند فایل‌های وب‌سایت را تغییر دهد یا فایل جدیدی در مسیرهای قابل‌دسترسی قرار دهد.

این وضعیت می‌تواند به پیامدهایی مانند موارد زیر منجر شود:

تغییر ظاهر سایت؛

تزریق محتوای جعلی؛

انتشار بدافزار؛

ایجاد صفحات فیشینگ؛

باقی‌ماندن دسترسی غیرمجاز؛

تغییر فایل‌های اصلی برنامه.

به همین دلیل، وب‌سرور نباید روی تمام پوشه‌های هسته و قالب‌ها مجوز نوشتن داشته باشد.

اثر CVE-2018-7600 بر مثلث CIA

مثلث CIA از سه اصل محرمانگی، یکپارچگی و دسترس‌پذیری تشکیل شده است. یک آسیب‌پذیری RCE مانند Drupalgeddon 2 می‌تواند هر سه اصل را هم‌زمان تهدید کند.

نقض محرمانگی

محرمانگی یعنی اطلاعات فقط در اختیار کاربران مجاز قرار بگیرند. در صورت بهره‌برداری موفق، موارد زیر ممکن است افشا شوند:

- اطلاعات حساب کاربران؛
- داده‌های شخصی؛
- اطلاعات اتصال به پایگاه داده؛
- فایل‌های پیکربندی؛
- اسناد سازمانی؛
- نسخه‌های پشتیبان؛
- اطلاعات تراکنش‌ها.

نقض یکپارچگی

یکپارچگی یعنی اطلاعات و فایل‌ها بدون مجوز تغییر نکنند. مهاجم ممکن است بتواند:

- محتوای وب‌سایت را تغییر دهد؛
- فایل‌های برنامه را دستکاری کند؛
- اطلاعات پایگاه داده را تغییر دهد؛
- سطح دسترسی کاربران را عوض کند؛
- حساب غیرمجاز ایجاد کند؛
- کدهای مخرب را به برنامه اضافه کند.

نقض دسترس‌پذیری

دسترس‌پذیری یعنی سرویس در زمان موردنیاز کاربران قابل استفاده باشد. حمله می‌تواند باعث موارد زیر شود:

- توقف وب‌سرور؛
- حذف فایل‌های حیاتی؛
- مصرف بیش از اندازه منابع؛
- خرابی پایگاه داده؛

از دسترس خارج‌شدن سایت؛

رمزگذاری یا تخریب اطلاعات.

ریسک اعلام‌شده برای SA-CORE-2018-002 برابر با ۲۴ از ۲۵ و در سطح «بسیار بحرانی» بوده است. همچنین این CVE در فهرست آسیب‌پذیری‌های شناخته‌شده و مورد بهره‌برداری قرار گرفته است.

پیامدهای Drupalgeddon 2 برای کسب‌وکارها

موفقیت یک حمله RCE فقط یک مشکل فنی نیست و می‌تواند تمام بخش‌های سازمان را تحت‌تأثیر قرار دهد.

خسارت عملیاتی

از دسترس خارج‌شدن وب‌سایت یا سامانه‌های وابسته می‌تواند فعالیت عادی سازمان را متوقف کرده و بهره‌وری کارکنان را کاهش دهد.

افشای اطلاعات

اطلاعات کاربران، اسناد داخلی، داده‌های مالی و اطلاعات راهبردی سازمان ممکن است سرقت یا منتشر شوند.

هزینه‌های مالی

سازمان ممکن است با هزینه‌های زیر روبه‌رو شود:

بررسی فنی و جرم‌یابی دیجیتال؛

بازیابی سرورها و اطلاعات؛

خرید تجهیزات یا خدمات امنیتی؛

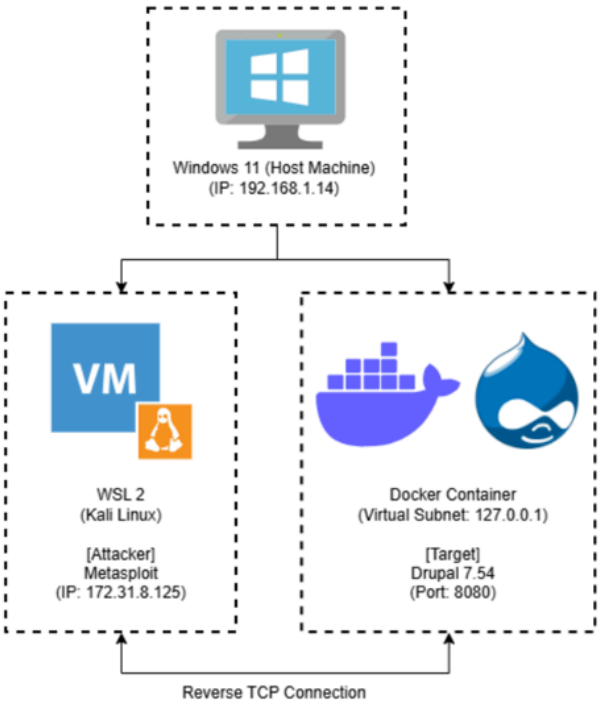
جبران خسارت کاربران؛

توقف فروش و خدمات آنلاین؛

جریمه‌های احتمالی مرتبط با حفاظت از داده.

آسیب به اعتبار سازمان

اعلام عمومی نفوذ به وب‌سایت می‌تواند اعتماد مشتریان، همکاران و سرمایه‌گذاران را کاهش دهد. بازیابی اعتبار ازدست‌رفته گاهی بسیار پرهزینه‌تر از اصلاح فنی سامانه است.



چگونه CVE-2018-7600 را شناسایی کنیم؟

مدیران سامانه ابتدا باید نسخه Drupal Core را بررسی کنند. مشاهده نسخه‌های قدیمی به‌تنهایی اثبات نمی‌کند که سامانه هک شده است، اما نشان‌دهنده نیاز فوری به ارزیابی امنیتی است.

بررسی‌های دفاعی پیشنهادی عبارت‌اند از:

- شناسایی نسخه هسته Drupal؛
- بررسی افزونه‌ها و قالب‌های قدیمی؛
- کنترل تاریخچه ورود مدیران؛
- بررسی حساب‌های کاربری ناشناس؛
- کنترل تغییرات غیرمنتظره فایل‌ها؛
- جست‌وجوی فایل‌های جدید در پوشه بارگذاری؛
- بررسی گزارش‌های وب‌سرور؛
- بررسی ارتباطات خروجی غیرعادی؛
- مقایسه فایل‌های هسته با نسخه اصلی؛
- اجرای اسکن آسیب‌پذیری مجاز.

وجود Drupal 7 روی یک سامانه فعال، به‌دلیل پایان پشتیبانی رسمی این شاخه، باید به‌عنوان یک خطر جدی در نظر گرفته شود.

راهکارهای جلوگیری از Drupalgeddon 2

به‌روزرسانی یا مهاجرت به نسخه پشتیبانی‌شده

- مهم‌ترین اقدام، استفاده از نسخه‌ای است که همچنان پشتیبانی امنیتی دریافت می‌کند. مدیران سایت‌های Drupal 7 باید به‌جای اکتفا به نصب وصله‌های قدیمی، برنامه مشخصی برای مهاجرت داشته باشند.

استفاده از دیوار آتش برنامه وب

- دیوار آتش برنامه وب یا WAF می‌تواند برخی درخواست‌های مخرب و الگوهای شناخته‌شده حمله را مسدود کند.

با این حال، WAF نباید جایگزین به‌روزرسانی هسته شود. این ابزار فقط یک لایه دفاعی تکمیلی است و ممکن است در برابر روش‌های جدید یا تغییرشکل‌یافته حمله کافی نباشد.

اجرای اصل کمترین سطح دسترسی

- فرایند وب‌سرور باید فقط به فایل‌ها و پوشه‌هایی دسترسی داشته باشد که برای عملکرد عادی سایت ضروری هستند.

پیشنهاد می‌شود:

- وب‌سرور با حساب مدیر یا root اجرا نشود؛
- مجوز نوشتن روی فایل‌های هسته حذف شود؛
- دسترسی نوشتن فقط به پوشه‌های ضروری محدود شود؛
- حساب پایگاه داده فقط به پایگاه موردنیاز دسترسی داشته باشد؛
- اطلاعات حساس از مسیرهای عمومی وب جدا شوند.

محافظت از فایل تنظیمات

فایل تنظیمات Drupal باید فقط برای کاربران و فرایندهای ضروری قابل خواندن باشد. اطلاعات پایگاه داده نیز نباید در گزارش‌ها، نسخه‌های پشتیبان عمومی یا مخزن کد منتشر شوند.

در صورت احتمال نفوذ، تغییر رمزهای پایگاه داده و سایر کلیدهای امنیتی ضروری است.

پایش گزارش‌های امنیتی

- گزارش‌های وب‌سرور، پایگاه داده و سیستم‌عامل باید به‌صورت منظم بررسی شوند.

موارد مهم برای پایش عبارت‌اند از:

- درخواست‌های POST غیرعادی؛
- افزایش ناگهانی خطاهای وب‌سرور؛
- ایجاد فایل در مسیرهای غیرمنتظره؛
- تغییر فایل‌های اصلی Drupal؛
- حساب‌های مدیریتی جدید؛
- ارتباط خروجی ناشناس از وب‌سرور؛
- فعالیت خارج از ساعت معمول سازمان.

استفاده از سامانه مدیریت رویداد و اطلاعات امنیتی یا SIEM می‌تواند جمع‌آوری و تحلیل مرکزی این گزارش‌ها را آسان‌تر کند.

تهیه نسخه پشتیبان ایمن

نسخه‌های پشتیبان باید:

- به‌صورت منظم تهیه شوند؛
- رمزگذاری شوند؛
- خارج از سرور اصلی نگهداری شوند؛
- فقط برای کاربران مجاز قابل دسترسی باشند؛
- به‌صورت دوره‌ای آزمایش بازیابی شوند.

نسخه پشتیبانی که امکان بازیابی آن بررسی نشده باشد، در زمان حادثه قابل‌اعتماد نیست.

ارزیابی امنیتی دوره‌ای

سازمان باید اسکن آسیب‌پذیری و تست نفوذ مجاز را به‌صورت دوره‌ای انجام دهد. همچنین نسخه هسته، افزونه‌ها، قالب‌ها و کتابخانه‌های جانبی باید در یک فهرست دارایی ثبت شوند.

این فهرست کمک می‌کند پس از انتشار یک آسیب‌پذیری جدید، سامانه‌های تحت‌تأثیر سریع‌تر شناسایی شوند.

تدوین برنامه واکنش به حادثه

برنامه واکنش به حادثه باید پیش از وقوع حمله آماده شود و شامل موارد زیر باشد:

- مشخص‌کردن مسئول هر اقدام؛

روش قطع دسترسی مهاجم؛

حفظ شواهد دیجیتال؛

بررسی دامنه نفوذ؛

تغییر اطلاعات ورود؛

بازیابی سامانه؛

اطلاع‌رسانی داخلی و خارجی؛

مستندسازی درس‌های آموخته‌شده.

اقدامات ضروری در صورت احتمال نفوذ

چنانچه احتمال می‌دهید وب‌سایت دروپالی شما از طریق CVE-2018-7600 یا آسیب‌پذیری مشابهی نفوذ شده است، تنها به به‌روزرسانی هسته اکتفا نکنید. نصب وصله، دسترسی قبلی مهاجم یا فایل‌های ایجادشده را حذف نمی‌کند.

اقدامات دفاعی مناسب شامل موارد زیر است:

جداکردن سامانه مشکوک از شبکه؛

تهیه نسخه جرم‌یابی از سیستم؛

حفظ گزارش‌ها و شواهد؛

بررسی تغییرات فایل‌ها و پایگاه داده؛

تغییر تمام رمزهای عبور و کلیدهای دسترسی؛

حذف حساب‌های غیرمجاز؛

بازیابی از یک نسخه پشتیبان سالم؛

نصب نسخه پشتیبانی‌شده Drupal؛

بررسی سایر سرورهای متصل؛

پایش سامانه پس از بازیابی.

جمع‌بندی

آسیب‌پذیری **CVE-2018-7600 در دروپال** نشان داد که یک نقص در اعتبارسنجی ورودی‌ها می‌تواند به تصاحب کامل یک وب‌سایت منجر شود. Drupalgeddon 2 بدون نیاز به احراز هویت قابل بهره‌برداری بود و محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات را هم‌زمان تهدید می‌کرد.

تحلیل آزمایشگاهی با Metasploit نشان می‌دهد که نسخه‌های قدیمی و آسیب‌پذیر Drupal می‌توانند دسترسی قابل‌توجهی در اختیار مهاجم قرار دهند. بااین‌حال، هدف از چنین آزمایش‌هایی باید فقط ارزیابی دفاعی و افزایش امنیت سامانه‌های دارای مجوز باشد.

به‌روزرسانی مستمر، مهاجرت از نسخه‌های پایان‌یافته، محدودکردن مجوزها، استفاده از WAF، پایش گزارش‌ها، تهیه نسخه پشتیبان و تدوین برنامه واکنش به حادثه، مهم‌ترین اقدامات برای کاهش خطر این نوع حملات هستند.

پرسش‌های متداول

CVE-2018-7600 چیست؟

CVE-2018-7600 یک آسیب‌پذیری اجرای کد از راه دور در نسخه‌های قدیمی Drupal Core است که با نام Drupalgeddon 2 نیز شناخته می‌شود.

آیا Drupalgeddon 2 بدون ورود به سایت قابل بهره‌برداری بود؟

بله. یکی از دلایل شدت بالای این آسیب‌پذیری، امکان سوءاستفاده بدون احراز هویت در پیکربندی‌های رایج بود.

آیا Drupal 7 هنوز امن است؟

پشتیبانی امنیتی رسمی Drupal 7 از ۵ ژانویه ۲۰۲۵ پایان یافته است. ادامه استفاده از آن بدون خدمات پشتیبانی تخصصی و برنامه مهاجرت، خطر امنیتی بالایی دارد.

آیا نصب WAF به‌تنهایی کافی است؟

خیر. WAF یک لایه دفاعی تکمیلی است و جایگزین نصب به‌روزرسانی، مهاجرت به نسخه پشتیبانی‌شده و اصلاح مجوزهای سرور نمی‌شود.

آیا استفاده از Metasploit قانونی است؟

خود ابزار Metasploit قانونی است، اما استفاده از آن روی سامانه دیگران بدون اجازه می‌تواند غیرقانونی باشد. آزمایش باید فقط روی سامانه شخصی، آزمایشگاه ایزوله یا سیستمی انجام شود که برای آن مجوز کتبی دارید.

چگونه متوجه شویم سایت قبلاً هک شده است؟

باید گزارش‌های وب‌سرور، تغییرات فایل‌ها، حساب‌های مدیریتی، ارتباطات خروجی، فرایندهای فعال و اطلاعات پایگاه داده بررسی شوند. در موارد جدی، استفاده از متخصص پاسخ‌گویی به حادثه و جرم‌یابی دیجیتال توصیه می‌شود.

منابع معتبر

اطلاعیه امنیتی SA-CORE-2018-002 تیم امنیت Drupal.

اطلاعات CVE-2018-7600 در پایگاه ملی آسیب‌پذیری‌ها.

3. مستندات ماژول Drupalgeddon 2 در Rapid7 Metasploit.
4. اعلام رسمی پایان پشتیبانی Drupal 7.

آینده Drupal در 2026؛ آیا هنوز ارزش یادگیری دارد؟

تغییر جایگاه Drupal

امروزه Drupal بیشتر در این پروژه‌ها استفاده می‌شود:

پورتال‌های سازمانی

سامانه‌های دولتی

LMSهای حرفه‌ای

فروشگاه‌های پیچیده

Headless CMS

API Platform

Drupal و AI

یکی از مهم‌ترین ترندهای جدید، ادغام AI با CMSها است.

Drupal به دلیل معماری ماژولار، قابلیت اتصال بسیار خوبی به:

OpenAI API

RAG Systems

AI Search

Smart Content

Recommendation Engine

دارد.

آینده بازار کار Drupal

توسعه‌دهندگان حرفه‌ای Drupal کمتر از WordPress هستند، اما پروژه‌ها تخصصی‌تر و درآمدها معمولاً بالاتر است.

مهارت‌های مهم:

- Drupal Backend
- Twig
- Symfony
- Decoupled Drupal
- API Development
- Security
- DevOps

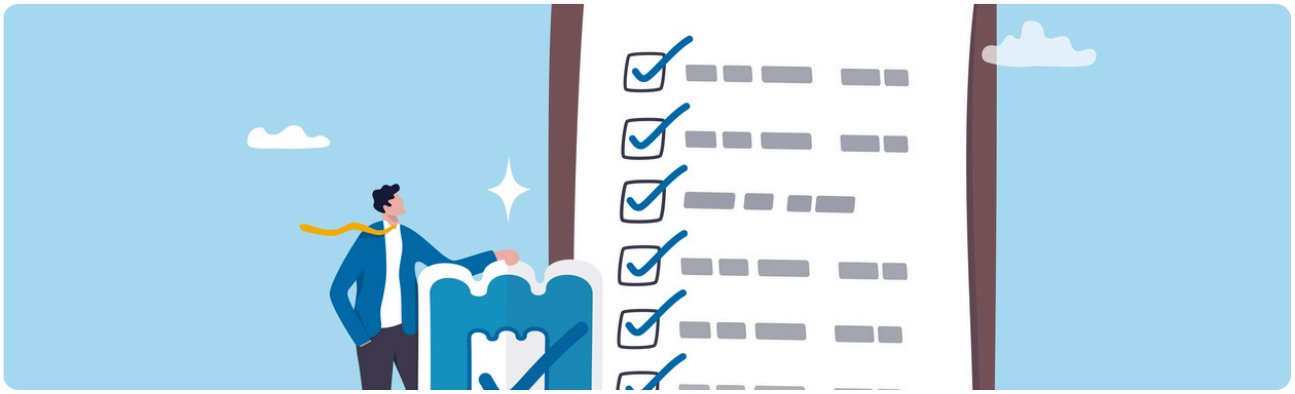
آیا یادگیری Drupal هنوز منطقی است؟

اگر هدف شما ساخت سایت‌های ساده است، شاید گزینه‌های دیگری سریع‌تر باشند. اما اگر می‌خواهید وارد پروژه‌های Enterprise شوید، Drupal همچنان یکی از قوی‌ترین گزینه‌هاست.

نتیجه‌گیری

Drupal دیگر CMS عمومی برای همه پروژه‌ها نیست؛ بلکه به یک پلتفرم حرفه‌ای برای سیستم‌های بزرگ، امن و مقیاس‌پذیر تبدیل شده است.

چک‌لیست امنیتی Drupal برای جلوگیری از هک شدن سایت



به‌روزرسانی هسته و ماژول‌ها

مهم‌ترین اصل:

همیشه Core را آپدیت نگه دارید

ماژول‌های بدون پشتیبانی را حذف کنید

Security Advisoryها را بررسی کنید

محدودسازی دسترسی‌ها

- بسیاری از هک‌ها به دلیل Permission اشتباه رخ می‌دهند.

نکات مهم:

Anonymous User محدود شود

Roleهای اضافی حذف شوند

دسترسی Admin فقط برای افراد ضروری باشد

محافظت از فرم‌ها

برای فرم‌های حساس:

CAPTCHA فعال شود

Rate Limit اعمال شود

OTP استفاده شود

Login Attempt محدود شود

امنیت سرور

تنها امن بودن Drupal کافی نیست.

سرور نیز باید:

- Firewall داشته باشد
- Fail2Ban فعال باشد
- SSH محدود شود
- PHP Harden شود
- Headerهای امنیتی فعال باشند

بررسی OWASP

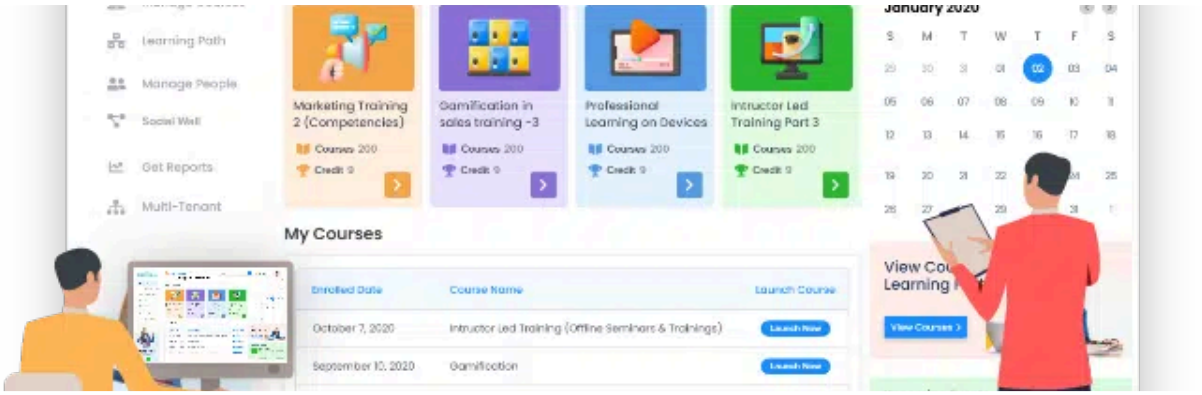
سایت Drupal باید در برابر موارد زیر تست شود:

- XSS
- CSRF
- SQL Injection
- File Upload Abuse
- Broken Access Control

نتیجه‌گیری

بیشتر سایت‌های هک‌شده به دلیل ضعف پیکربندی هستند، نه ضعف خود Drupal. اگر اصول امنیتی رعایت شوند، Drupal می‌تواند یکی از امن‌ترین CMSهای دنیا باشد.

چگونه Drupal را به یک LMS حرفه‌ای تبدیل کنیم؟



مزیت اصلی Drupal در LMS

Drupal در مدیریت کاربران و محتوا بسیار قدرتمند است.

شما می‌توانید:

دوره تعریف کنید

- استاد تعریف کنید
- کلاس آنلاین بسازید
- آزمون برگزار کنید
- گواهینامه صادر کنید

ویدیوها را مدیریت کنید

اتصال به BigBlueButton

BigBlueButton یکی از بهترین پلتفرم‌های آموزش آنلاین متن‌باز است.

مزایا:

ذخیره جلسات

- اشتراک صفحه
- تخته سفید
- سیستم چت

Poll

Breakout Rooms

Drupal می‌تواند به صورت کامل با BBB یکپارچه شود.

امنیت اطلاعات آموزشی

یکی از مشکلات سرویس‌های آماده، ذخیره اطلاعات روی سرورهای شخص ثالث است.

اما در معماری اختصاصی:

- فایل‌ها روی سرور خودتان ذخیره می‌شوند
- اطلاعات دانشجو در اختیار شماست
- امکان کنترل Backup وجود دارد
- سطح دسترسی‌ها قابل مدیریت است

سیستم عضویت و پرداخت

Drupal Commerce می‌تواند برای فروش دوره‌ها استفاده شود.

امکانات:

- اشتراک ماهانه
- فروش دوره
- تخفیف
- کیف پول
- فاکتور رسمی

نتیجه‌گیری

Drupal فقط یک CMS نیست؛ بلکه می‌تواند هسته یک سامانه آموزش مجازی کاملاً اختصاصی و حرفه‌ای باشد.

مقایسه Drupal Commerce با ووکامرس برای فروشگاه‌های حرفه‌ای

تفاوت معماری

WooCommerce اساساً یک افزونه فروشگاهی روی WordPress است.

اما Drupal Commerce بخشی از معماری Drupal محسوب می‌شود.

این موضوع باعث می‌شود:

- مدیریت داده حرفه‌ای‌تر باشد
- توسعه API راحت‌تر شود
- ساختار سفارشات انعطاف بیشتری داشته باشد
- سفارشی‌سازی عمیق‌تر شود

سیستم محصول در Drupal Commerce

در Drupal Commerce محصول فقط یک آیتم ساده نیست.

شما می‌توانید:

- Product Variation بسازید
- Attribute سفارشی تعریف کنید
- Workflow اختصاصی ایجاد کنید
- قیمت‌گذاری پیچیده داشته باشید
- انبار چندگانه تعریف کنید

مناسب برای فروشگاه‌های B2B

یکی از مهم‌ترین مزایای Drupal Commerce، قابلیت‌های B2B است.

مثلاً:

- قیمت اختصاصی برای هر مشتری
- نقش‌های فروشگاهی مختلف
- فرآیند تأیید سفارش
- سیستم اعتباری
- API سازمانی

امنیت فروشگاه

در فروشگاه‌های بزرگ، امنیت حیاتی است.

Drupal Commerce مزایای امنیتی مهمی دارد:

- Permission دقیق
- کنترل فرم‌ها
- سیستم Cache حرفه‌ای
- سازگاری بهتر با استانداردهای امنیتی

نتیجه‌گیری

اگر فروشگاه شما کوچک و ساده است، ووکامرس می‌تواند سریع‌تر راه‌اندازی شود. اما برای پروژه‌های بزرگ، سازمانی و توسعه‌پذیر، Drupal Commerce انتخاب حرفه‌ای‌تری محسوب می‌شود.