Identify & Impose more Security in Drupal

Security In Drupal By Snehamay & Monoj

Implement Basic Securities :

- **Use**

  - Most updated module versions

  - Secure communication like SSH, sFTP, FTPS, and HTTPS

  - Strong Case sensitive Passwords

  - Secure communication like SSH, sFTP, FTPS, and HTTPS

- **Keep CHANGELOG.txt file updated**

- **Backup contents regularly**

Relieved ????

Identify Your Application Status?

Security review :

A wonderful community module that examines & publish reports for :

- File system permissions
- Input formats
- Content (Nodes and Comments and fields in Drupal 7)
- Error reporting
- Private files
- Allowed upload extensions
- Database errors
- Failed logins
- Drupal admin permissions
- Username as password
- Password included in user emails
- PHP access

Project : http://drupal.org/project/security_review

Drupal Application Security Types :

We can classify any Drupal applications mainly in 3 types:

- **User Account Security**
  - Login security
  - Oauth
  - Password Policy
  - Automated Logout

- **Content Access Security**
  - ACL
  - Content Access
  - Taxonomy Access Control
  - Menu Admin per Menu

- **Security from various Attacks**
  - Spamspan filter
  - Captcha & Re-Captcha
  - Security Kit

UH OH...

User Account Securities …

Login security :

With Login Security module, a site administrator may :

- **Protect and restrict access by adding access control features to the login forms through :**

  - Limiting the number of invalid login attempts
  - Denying access by IP address, temporarily or permanently

- **Set notifications like :**

  - Password and account guessing
  - Brute force login attempts
  - Unexpected behavior with the login operation

Project : http://drupal.org/project/login_security

Oauth :

Oauth is an advanced tool for the authorization used in Drupal for security purposes. It provides a secure access to server resources. Two-level and three-level user identifications are involved to secure the website against any malicious attack.

When a user submits an authorization request to the server, this tool judges whether the user is a legitimate client for a particular website. The server then issues an approval for content usage to the visitors.

This module implements the OAuth 1.0 standard for use with Drupal and acts as a support module for other modules that wish to use OAuth.

Project : http://www.drupal.org/project/oauth

Password Policy :

Password Policy module provides :

- **Set of constraints which must be met before a user password change will be accepted :**

  - Character types
  - Digit
  - Letter/Digit (Alphanumeric)
  - Length
  - Uppercase/Lowercase/Punctuation
  - Username
  - Digit placement
  - History

- **Password Hints**

Project : http://www.drupal.org/project/password_policy

Automated Logout :

As Drupal don’t have auto logout feature, this module provides a site administrator the ability to log users out after a specified time of inactivity.

It provides features like :

- Enabling/Disabling timeouts based on role
- Permission for users to set their own timeout
- Includes developer hooks to allow users to remain logged in
- Optional integration with JavaScript Timer

Project : http://www.drupal.org/project/autologout

Content Access Security…

Access Control List (ACL) :

A Drupal API to be used with other modules.

The purpose is to create a list of users for a website and assign them privileges.

This tool has no user interface of its own and works only in coordination with other Drupal modules already in use.

Following modules uses ACL :

- Flexi Access
- Forum Access
- Image Gallery Access
- Content Access(Optionally)

Project : http://www.drupal.org/project/acl

Content Access:

Allows you to set a specific view for an author or a role.
It provides features like :

- Manage permissions for content types by Role/Author
- Allows you to specify Custom View/Edit/Delete Permissions for each content type
- Provides permission to enable per content access settings to customize the access for each content node

Project : http://drupal.org/project/content_access

Taxonomy Access Control :

As Drupal don’t have auto logout feature, this module provides a site administrator the ability to log users out after a specified time of inactivity.

It provides features like :

- Automatically controls access to nodes (based on their taxonomy terms)
- Provides configuration page for each user role
- Three node access permission types: View, Update, Delete
- Two term access types: View tag, Add tag

Project : http://www.drupal.org/project/taxonomy_access

Menu Admin Per Menu :

By default, Drupal allows only users with “Administer Menu Permission" to Add/Modify/Delete menu items.

This module allows administer to give roles per menu admin permissions without giving them full admin permission.

Project :
http://www.drupal.org/project/menu_admin_per_menu

Security from various Attacks …

Spamspan Filter :

The SpamSpan module obfuscates email addresses to help prevent spambots from collecting them.

SpamSpan however will produce clickable links if JavaScript is enabled, and will show the email address as *example [at] example [dot] com* if the browser does not support JavaScript or if JavaScript is disabled.

Project : http://www.drupal.org/project/spamspan

Captcha & Re-Captcha :

As the name suggests the purpose of CAPTCHA is to block form submissions by spambots, which are automated scripts that post spam content everywhere they can.

The CAPTCHA module provides this feature to virtually any user facing web form on a Drupal site.

Additional CAPTCHA Modules are :

- CAPTCHA Pack
- Text CAPTCHA
- Captcha Riddler
- Hidden CAPTCHA
- KeyCAPTCHA
- Draggable CAPTCHA
- Image CAPTCHA refresh

Re-Captcha uses the Google reCAPTCHA web service to improve the CAPTCHA system and protect email addresses

Projects :

https://www.drupal.org/project/captcha
https://www.drupal.org/project/recaptcha

Security Kit :

Provides Drupal installation with various security hardening options. This lets your mitigate the risks of exploitation of different web application vulnerabilities

It provides features to avoid :

- Cross-site Scripting
- Cross-site Request Forgery
- Clickjacking
- SSL/TLS

Project : https://www.drupal.org/project/seckit

Queries ?

Thank You…