Directory Indexing

HACKING WORDPRESS CO

Active plugins should not be our only area of focus when assessing a WordPress website. Even if a plugin is deactivated, it may still be accessible, and therefore we can gain access to its associated scripts and functions. Deactivating a vulnerable plugin does not improve the WordPress site's security. It is best practice to either remove or keep up-to-date any unused plugins.

The following example shows a disabled plugin.



If we browse to the plugins directory, we can see that we still have access to the Mail Masta plugin.

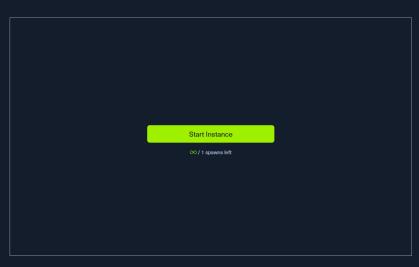


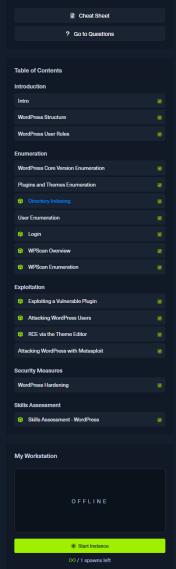
We can also view the directory listing using cURL and convert the HTML output to a nice readable format using html2text.



This type of access is called <code>Oirectory Indexing</code>. It allows us to navigate the folder and access files that may contain sensitive information or vulnerable code. It is best practice to disable directory indexing on web servers so a potential attacker cannot gain direct access to any files or folders other than those necessary for the website to function properly.







Page 6 / Directory Indexing

