WordPress Core Version Enumeration

It is always important to know what type of application we are working with. An essential part of the enumeration phase is uncovering the software version number. This is helpful when searching for common misconfigurations such as default passwords that may be set for certain versions of an application and searching for known vulnerabilities for a particular version number. We can use a variety of methods to discover the version number manually. The first and easiest step is reviewing the page source code. We can do this by right-clicking anywhere on the current page and selecting "View page source" from the menu or using the keyboard shortcut `[CTRL + U]`.

We can search for the `meta generator` tag using the shortcut `[CTRL + F]` in the browser or use `cURL` along with `grep` from the command line to filter for this information.

WP Version - Source Code

Code: html

```html
...SNIP...
<link rel='https://api.w.org/' href='http://blog.inlanefreight.com/index.php/wp-json/' />
<link rel="EditURI" type="application/rsd+xml" title="RSD" href="http://blog.inlanefreight.com/xmlrpc.ph
<link rel="wlwmanifest" type="application/wlwmanifest+xml" href="http://blog.inlanefreight.com/wp-includ
<meta name="generator" content="WordPress 5.3.3" />
...SNIP...
```

WP Version - Source Code

```shell
Avenger666@htb[/htb]$ curl -s -X GET http://blog.inlanefreight.com | grep '<meta name="generator"'

<meta name="generator" content="WordPress 5.3.3" />
```

Aside from version information, the source code may also contain comments that may be useful. Links to CSS (style sheets) and JS (JavaScript) can also provide hints about the version number.

WP Version - CSS

Code: html

```html
ght.com/wp-content/themes/ben_theme/css/bootstrap.css?ver=5.3.3' type='text/css' media='all' />
lanefreight.com/wp-content/themes/ben_theme/style.css?ver=5.3.3' type='text/css' media='all' />
lanefreight.com/wp-content/themes/ben_theme/css/colors/default.css?ver=5.3.3' type='text/css' media='all'
ight.com/wp-content/themes/ben_theme/css/jquery.smartmenus.bootstrap.css?ver=5.3.3' type='text/css' media=
```

WP Version - JS

Code: html

```html
g.inlanefreight.com/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp'></script>
g.inlanefreight.com/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1'></script>
g.inlanefreight.com/wp-content/plugins/mail-masta/lib/subscriber.js?ver=5.3.3'></script>
g.inlanefreight.com/wp-content/plugins/mail-masta/lib/jquery.validationEngine-en.js?ver=5.3.3'></script>
g.inlanefreight.com/wp-content/plugins/mail-masta/lib/jquery.validationEngine.js?ver=5.3.3'></script>
```

In older WordPress versions, another source for uncovering version information is the `readme.html` file in WordPress's root directory.

← Previous Next → ✓ Mark Complete & Next

Cheat Sheet

Table of Contents

Introduction

Enumeration

Exploitation

Security Measures

Skills Assessment

Summary

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left