SCANTRAP: Protecting Content Management Systems from Vulnerability Scanners with Cyber Deception and Obfuscation

Daniel Reti, Karina Elzer and Hans Dieter Schotten

German Research Center for Artificial Intelligence, Kaiserslautern, Germany

{firstname}.{lastname}@dfki.de

Introduction

Content Management Systems (CMS) have become a notable part of today's web, with almost half of the websites using some sort of CMS. Specifically, some popular CMSs have emerged: WordPress (WP) is the most popular CMS, with a market share of 63.3%. Shopify, Wix and Squarespace, as paid alternatives, together have 12.4% of the market share. The most popular open-source alternatives, Joomla and Drupal, are used in 4.3% of websites using CMS. [4]
With such popularity, however, they also become an attractive target for attackers. Due to the addition of third-party extensions, these platforms leave a large attack surface. In the field of penetration testing, different tools have emerged that reduce the effort of scanning and exploitation of popular CMSs. This makes reconnaissance possible with low effort, enabling the threat from so-called 'script kiddies' and bots.
Therefore, it is desirable to increase the effort of attackers in regards to attacking CMS by using different defence strategies. This starts with the attacker's capability of scanning CMSs.

Cyber Deception

The approach of this work is based on cyber deception to disguise valuable information, by hiding the real and presenting false information. Regarding strategies for web services, the following methods were looked at, based on the work of [2]:

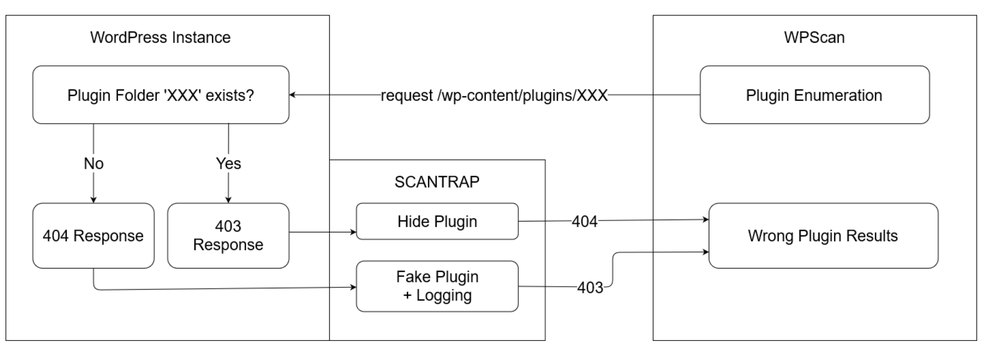
- Version Trickery
- Disallow Injection
- Virtual Honey Files
- Code Obfuscation
- Cookie Scrambling
- Content Modification
- Status Code Tampering
- Latency Adaption

Scanner	CMS	Module Enum	Version Detection	User Enum	Misconfigs	URLs	Exposed Files	Login Attacks	Exploits	Code Analysis
Droopescan	multiple	✓	✓	-	-	✓	✓	-	-	-
CMSmap	multiple	✓	✓	✓	✓	✓	✓	✓	-	-
CMSeek	multiple	✓	✓	✓	✓	-	✓	-	-	-
WPScan	WordPress	✓	✓	✓	✓	✓	✓	✓	-	-
WPSeku	WordPress	✓	-	-	✓	-	✓	✓	-	✓
JoomScan	Joomla	✓	✓	-	✓	-	✓	-	-	-
JoomlaVS	Joomla	✓	✓	-	✓	-	-	-	-	-
JScanner	Joomla	-	✓	✓	-	-	-	-	-	-
Drupwn	Drupal	✓	✓	✓	-	-	✓	-	✓	-

Comparing different CMS scanners functionality [3]

SCANTRAP

For evaluating the ability to evade CMS scanners, we used WordPress as the CMS and WPScan as the CMS scanner and created a plugin for WordPress that focused on the four main scans of WPScan.



Demonstration of response manipulation of request for plugin folder 'XXX' with WP plugin 'SCANTRAP'.

Plugin Detection

- Fakes plugins by changing the 404 response code to 403
- Adds customized text to the response body to add version detection
- Logs fake plugin requested
- Hides plugins by changing the response code to plugin folder requests to 404

Theme Detection

- Same methods as for the plugin detection
- Main theme detection not evaded

Version Detection

- Removes WordPress Head
- Removes WordPress Generator
- Removes Version Query
- Changes fingerprints of files
- Removes version from file content

User Enumeration

- Disables Rest API
- Disables JSON API
- Removes Author Class
- Removes RSS Author Tag
- Disables Login Error
- Disables URL Queries
- Removes Author URL

Pugin/ Caption	Hide/Fake Users	Hide/Fake Plugins	Hide/Fake Themes	Hide/Fake ‚wp-content'	Hide/Fake Login Path	Hide/Fake Login Error	Hide/Fake Version	Hide WP	Hide/Fake robots.txt	Detect/ Block Attackers
SCANTRAP	✓/-	✓/✓	✓/✓	-/-	-/-	✓/-	✓/-	-	-/-	✓/-
Blackhole	-/-	-/-	-/-	-/-	-/-	-/-	-/-	-	-/✓	✓/✓
WP Ghost	✓/-	✓/-	✓/-	✓/-	✓/✓	-/-	-/-	✓	-/-	✓/✓
Don Security	✓/-	✓/-	-/-	-/-	-/-	-/-	✓/-	-	✓/-	-/-
Stop User Enum	✓/-	-/-	-/-	-/-	-/-	-/-	-/-	-	-/-	-/-
WP Smart Security	-/-	✓/-	✓/-	✓/-	✓/-	✓/-	✓/✓	✓	-/-	✓/✓
Titan	-/-	-/-	-/-	-/-	✓/-	-/-	✓/-	-	-/-	✓/✓
tinyShield (deprecated)	✓/-	-/-	-/-	-/-	-/-	-/-	-/-	-	-/-	✓/✓
block-wpscan	-/-	-/-	-/-	-/-	-/-	-/-	-/-	-	-/-	✓/✓
NovaSense	-/-	-/-	-/-	-/-	-/-	-/-	-/-	-	-/-	✓/✓
Astra Security	-/-	-/-	-/-	-/-	-/-	-/-	-/-	-	-/-	✓/✓
BlogSafe Honeypot	-/-	-/-	-/-	-/-	-/-	-/-	-/-	-	-/-	✓/-

Comparing different WordPress security plugins [1] regarding their dissimulation and simulation features.

Github: https://github.com/dfki-in-sec/SCANTRAP

Conclusion

In this paper, we have presented a WordPress plugin that manipulates the output of WPScan scans, in order to counter reconnaissance. This plugin can hide the existence of plugins, themes and users from the enumeration process and present false plugins and themes.
The results support the idea that cyber deception and obfuscation methods are applicable to the CMS enumeration process, and can also help to detect attacks at an early stage. This could be effective to protect from 'script kiddies', bots or attackers that use automation to gather information.
Future work could generalize this approach and transfer it to other CMS than WordPress. It should be noted that scanning tools could be adapted to be more resilient against cyber deception, representing a cat-and-mouse game.

References

[1] https://wordpress.org/plugins/
[2] Daniel Fraunholz, Daniel Reti, Simon Duque Anton, and Hans Dieter Schotten.
Cloxy: A Context-Aware Deception-as-a-Service Reverse Proxy for Web Services.
In Proceedings of the 5th ACM Workshop on Moving Target Defense, MTD '18, page 40–47. ACM, 2018.
[3] InfosecMatter. CMS Vulnerability Scanners for WordPress, Joomla, Drupal, Moodle, Typo3.. https://www.infosecmatter.com/cms-vulnerability-scanners-for-wordpress-joomla-dru
2020. Accessed: 2022-09-21.
[4] W3Techs (2022). Usage statistics of content management systems.
https://w3techs.com/technologies/overview/content\ management. Accessed: 2022-09-21.

Acknowledgements

This research was supported by the German Federal Ministry of Education and Research (BMBF) through the Open6GHub project (Grant 16KISK003K).