UNIVERSITATEA "TITU MAIORESCU" DIN BUCUREȘTI
FACULTATEA DE INFORMATICĂ

PREZENTARE
LUCRARE DE DISERTAȚIE

Securitatea în WordPress

COORDONATOR ȘTIINȚIFIC:
Conf.univ.dr. Iustin Priescu

ABSOLVENT:
Olivian-Claudiu Breda

SESIUNEA IUNIE 2020

Cuprins lucrare

Obiectiv

să testăm cât de sigură este o implementare de WordPress, în varianta standard (implicită).

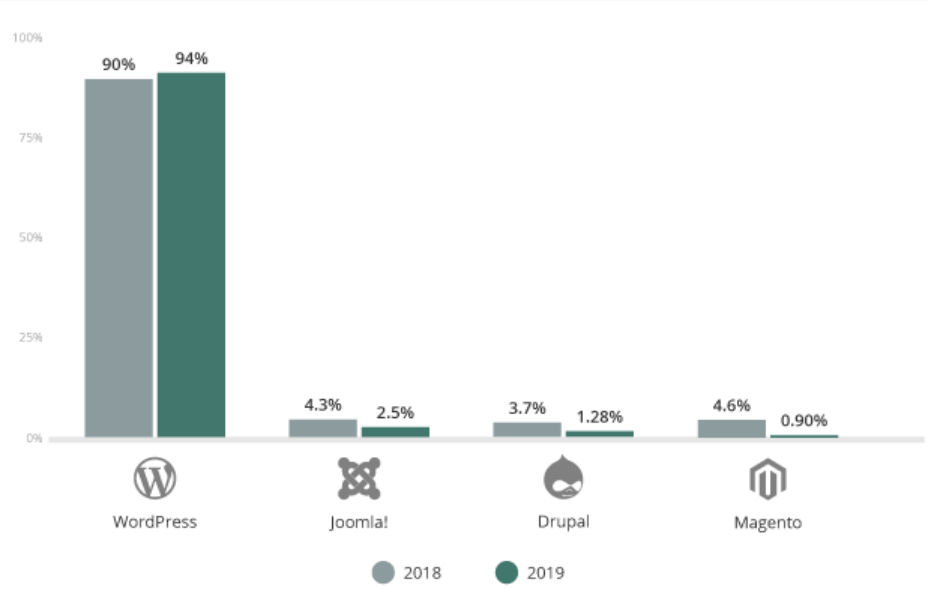
Motivație

#1 Mai mult de unul din 3 site-uri de pe Internet (36,1%) folosesc WordPress drept CMS.

W3techs.com. 2020. Usage Statistics And Market Share Of Wordpress, mai 2020. [online] Disponibil la: <https://w3techs.com/technologies/details/cm-wordpress> [Accesat 12 mai 2020].

#2 Tendință de creștere a infecțiilor pe WordPress: de la 90% la 94% în intervalul 2018-2019.

Sucuri. fără dată. Sucuri - Website Threat Report 2019. [online] Disponibil la: <https://sucuri.net/reports/2019-hacked-website-report/> [Accesat 13 mai 2020].



Anexe Capitolul 2. - Testare WordPress la nivel de server

Observatory.mozilla.org. 2020. Mozilla Observatory :: Scan Results For Olivian.Ro. [online] Disponibil la: <https://observatory.mozilla.org/analyze/olivian.ro> [Accesat 8 mai 2020].

Test Scores

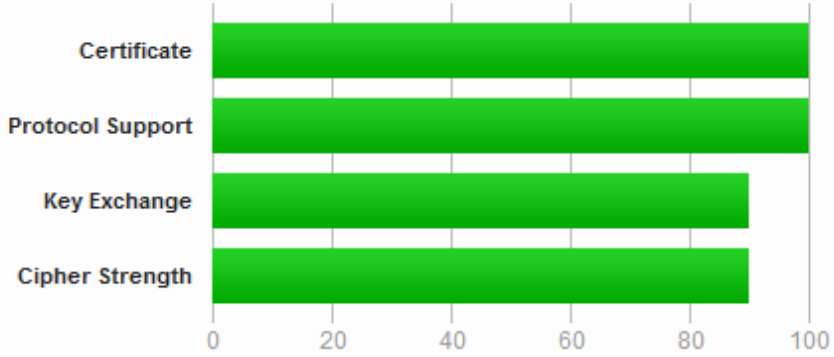
Test	Pass	Score	Reason	Info
Content Security Policy	✗	-25	Content Security Policy (CSP) header not implemented	ⓘ
Cookies	–	0	No cookies detected	ⓘ
Cross-origin Resource Sharing	✓	0	Content is not visible via cross-origin resource sharing (CORS) files or headers	ⓘ
HTTP Public Key Pinning	–	0	HTTP Public Key Pinning (HPKP) header not implemented (optional)	ⓘ
HTTP Strict Transport Security	✗	-20	HTTP Strict Transport Security (HSTS) header not implemented	ⓘ
Redirection	✓	0	Initial redirection is to HTTPS on same host, final destination is HTTPS	ⓘ
Referrer Policy	–	0	Referrer-Policy header not implemented (optional)	ⓘ
Subresource Integrity	–	0	Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin	ⓘ
X-Content-Type-Options	✗	-5	X-Content-Type-Options header not implemented	ⓘ
X-Frame-Options	✗	-20	X-Frame-Options (XFO) header not implemented	ⓘ
X-XSS-Protection	✗	-10	X-XSS-Protection header not implemented	ⓘ

Anexe Capitolul 2. - Testare WordPress la nivel de server

Ristic, I., 2020. CAA Mandated By CA/Browser Forum | Qualys Blog. [online] Qualys Blog. Disponibil la: <https://blog.qualys.com/ssllabs/2017/03/13/caa-mandated-by-cabrowser-forum> [Accesat 8 mai 2020]

Overall Rating

A



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This site works only in browsers with SNI support.

This server supports TLS 1.3.

Anexe Capitolul 3. - Testare WordPress la nivel de versiune diferită (5.0 vs. 5.4, testat comparativ)

Pentest-Tools.com. fără dată. Website Vulnerability Scanner - Online Scan For Web Vulnerabilities | Pentest-Tools.Com. [online] Disponibil la: <https://pentest-tools.com/website-vulnerability-scanning/website-scanner> [Accesat 26 April 2020].

Findings

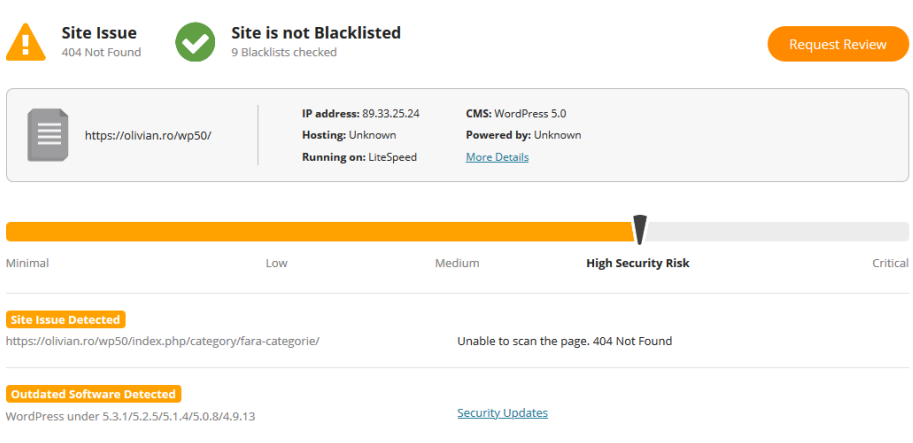
Vulnerabilities found for server-side software

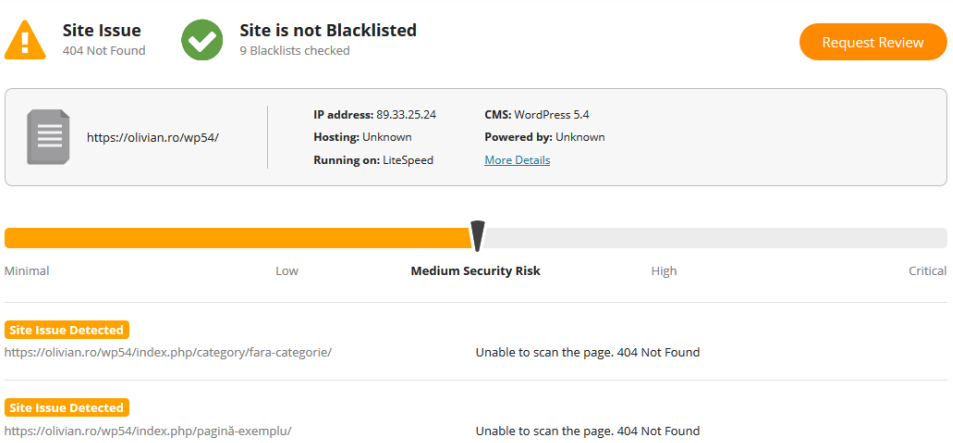
Risk Level	CVSS	CVE	Summary	Exploit	Affected software
	7.5	CVE-2018-20148	In WordPress before 4.9.9 and 5.x before 5.0.1, contributors could conduct PHP object injection attacks via crafted metadata in a wp.getMediaItem XMLRPC call. This is caused by mishandling of serialized data at phar:// URLs in the wp_get_attachment_thumb_file function in wp-includes/post.php.	N/A	WordPress 5.0
	6.8	CVE-2019-9787	WordPress before 5.1.1 does not properly filter comment content, leading to Remote Code Execution by unauthenticated users in a default configuration. This occurs because CSRF protection is mishandled, and because Search Engine Optimization of A elements is performed incorrectly, leading to XSS. The XSS results in administrative access, which allows arbitrary changes to .php files. This is related to wp-admin/includes/ajax-actions.php and wp-includes/comment.php.	N/A	WordPress 5.0
	6.5	CVE-2019-8942	WordPress before 4.9.9 and 5.x before 5.0.1 allows remote code execution because an _wp_attached_file Post Meta entry can be changed to an arbitrary string, such as one ending with a .jpg?file.php substring. An attacker with author privileges can execute arbitrary code by uploading a crafted image containing PHP code in the Exif metadata. Exploitation can leverage CVE-2019-8943.	N/A	WordPress 5.0
	5.8	CVE-2019-16220	In WordPress before 5.2.3, validation and sanitization of a URL in wp_validate_redirect in wp-includes/pluggable.php could lead to an open redirect.	N/A	WordPress 5.0
	5.5	CVE-2018-20147	In WordPress before 4.9.9 and 5.x before 5.0.1, authors could modify metadata to bypass intended restrictions on deleting files.	N/A	WordPress 5.0

› Details

Anexe Capitolul 3. - Testare WordPress la nivel de versiune diferită (5.0 vs. 5.4, testat comparativ)

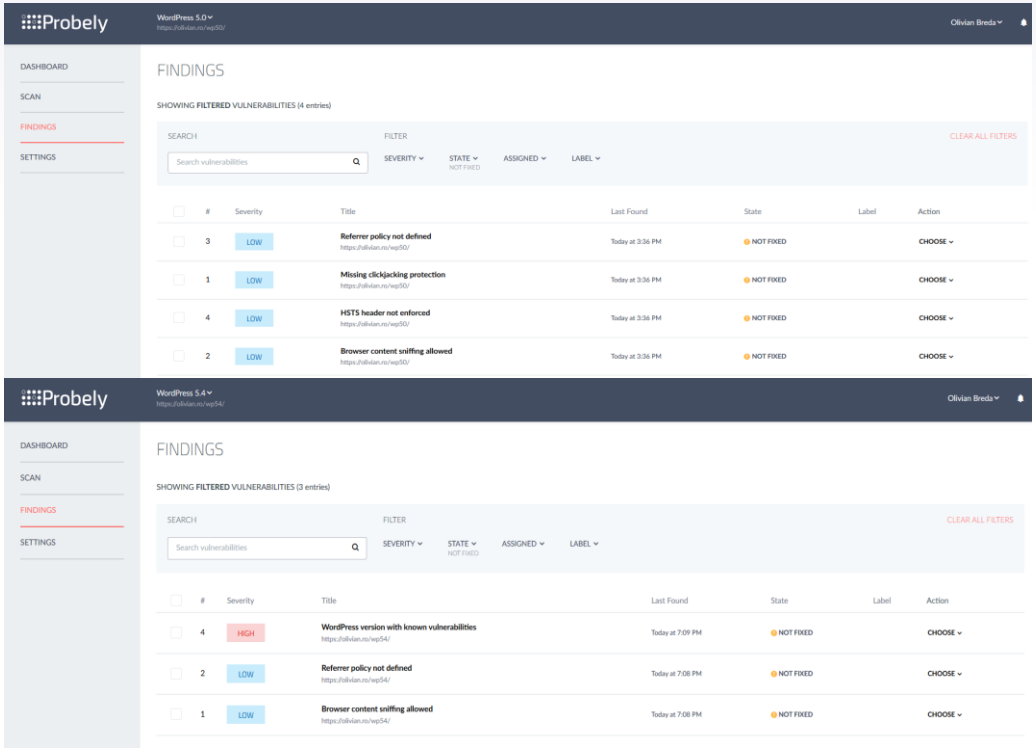
Sucuri Security. fără dată. Https://Olivian.Ro/Wp50/. [online] Disponibil la: <https://sitecheck.sucuri.net/results/https/olivian.ro/wp50/> [Accesat 17 mai 2020].
Sucuri Security. fără dată. Https://Olivian.Ro/Wp54/. [online] Disponibil la: <https://sitecheck.sucuri.net/results/https/olivian.ro/wp50/> [Accesat 17 mai 2020].





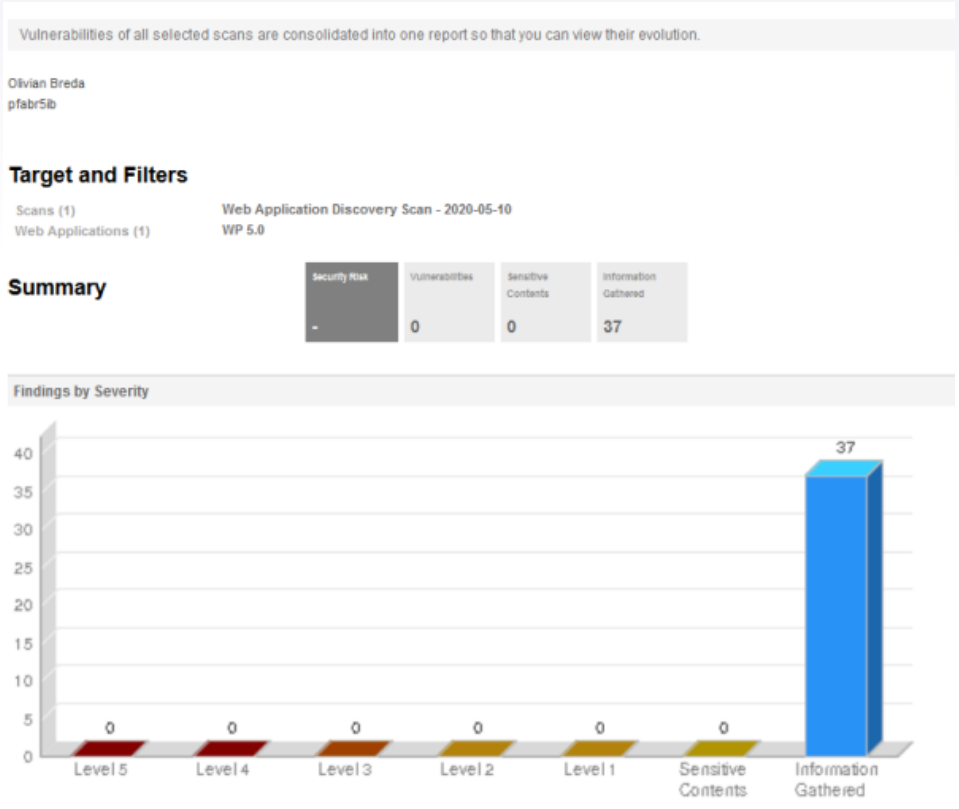
Anexe Capitolul 3. - Testare WordPress la nivel de versiune diferită (5.0 vs. 5.4, testat comparativ)

fără dată. Probely. [online] Disponibil la: <https://app.probely.com/portal/2N9Z7NHvQq3e/findings/1/filter?state=notfixed> [Accesat 17 mai 2020].
fără dată. Probely. [online] Disponibil la: <https://app.probely.com/portal/2HCuuCbULi6c/findings/1/filter?state=notfixed> [Accesat 17 mai 2020].



Anexe Capitolul 3. - Testare WordPress la nivel de versiune diferită (5.0 vs. 5.4, testat comparativ)

Qualysguard.qg2.apps.qualys.eu. fără dată. Qualys Security And Compliance Suite Login. [online] Disponibil la: <https://qualysguard.qg2.apps.qualys.eu/> [Accesat 17 mai 2020].



Capitolul 4. Potențiale soluții - cum se poate securiza WordPress?

Pluginuri dedicate:

- Adăugarea de pluginuri care pot preveni atacuri de tip DoS (denial-of-service attack);
- Alegerea unui plugin de backup corespunzător;
- Akismet Anti-Spam;
- Conditional CAPTCHA;
- Cookie Notice for GDPR & CCPA;
- Really Simple SSL;
- Protect Your Admin;
- Limit Login Attempts Reloaded;
- Simple Trackback Validation;
- Advanced noCaptcha & invisible Captcha (v2 & v3).

Capitolul 4. Potențiale soluții - cum se poate securiza WordPress?

Actualizarea completă - WordPress, pluginuri și teme - Conform statisticilor oficiale ale WordPress, 42,6% dintre utilizatori utilizează în continuare diverse versiuni mai vechi de WordPress.

Rehman, I., 2020. Top 6 Most Common Wordpress Vulnerabilities (With Fixes). [online] Website Hosting Rating. Disponibil la: https://www.websitehostingrating.com/most-common-wordpress-vulnerabilities/> [Accesat 14 mai 2020].

Capitolul 4. Potențiale soluții - cum se poate securiza WordPress?

Cu autentificarea în doi pași / cu doi factori, în afară de parolă, se va introduce, pentru logare, în mod obligatoriu un cod suplimentar într-un timp dedicat.

Chahal, P., 2020. Hardening Wordpress Security: For Beginners To Advanced. [online] TemplateToaster Blog. Disponibil la: https://blog.templatetoaster.com/hardening-wordpress-security/> [Accesat 14 mai 2020].

Concluzii

#1 Serverul olivian.ro nu este suficient de bine securizat.

#2 Notele generale în urma analizelor sunt undeva în gama "note medii".

#3 Hostingul (găzduirea) site-ului are soluții de blocare atacuri automate.

#4 Am găsit observații de securitate în plus la instanța de WordPress 5.4.

#5 Sunt numeroase lucruri teroetice utile pentru securitatea WordPress.

#6 Literatura în domeniul securității WordPress este foarte bogată.

#7 WordPress nu își propune securitate ridicată în mod implicit.

#8 De-a lungul anilor, WordPress a făcut periodic îmbunătățiri constante.

#9 WordPress, în mod implicit asigură o securitate de bază.

Bibliografie selectivă

- Dunn, I., 2018. Wordpress 5.0.1 Security Release. [online] WordPress News. Disponibil la: <https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/> [Accesat 13 mai 2020].
- HackerTarget.com. fără dată. 28 Online Vulnerability Scanners & Network Tools | Hackertarget.Com. [online] Disponibil la: <https://hackertarget.com/> [Accesat 17 mai 2020].
- Infosec Resources. 2011. 9 Easy Wordpress Security Tips: Hardening Wordpress. [online] Disponibil la: <https://resources.infosecinstitute.com/hardening-wordpress/> [Accesat 14 mai 2020].
- Król, K., 2019. Wordpress 5 Complete. Packt Publishing.
- MacDonald, M., 2014. Wordpress: The Missing Manual. 1st ed. Sebastopol: O'Reilly Media, Inc.
- Onishi, A., 2013. Pro Wordpress Theme Development. New York: Apress L.P.
- Owasp.org. fără dată. OWASP Top Ten Web Application Security Risks | OWASP. [online] Disponibil la: <https://owasp.org/www-project-top-ten/> [Accesat 12 mai 2020].
- Rehman, I., 2020. Top 6 Most Common Wordpress Vulnerabilities (With Fixes). [online] Website Hosting Rating. Disponibil la: <https://www.websitehostingrating.com/most-common-wordpress-vulnerabilities/> [Accesat 14 mai 2020].
- Sucuri. fără dată. Sucuri - Website Threat Report 2019. [online] Disponibil la: <https://sucuri.net/reports/2019-hacked-website-report/> [Accesat 13 mai 2020].
- W3techs.com. fără dată. Usage Statistics And Market Share Of Apache, mai 2020. [online] Disponibil la: <https://w3techs.com/technologies/details/ws-apache> [Accesat 8 mai 2020].

Credits

Special thanks to all the people who made and released these awesome resources for free:

- Presentation template by SlidesCarnival
- Illustrations by Sergei Tikhonov
- Photographs by Unsplash

Extra resources

Illustrations created by Sergei Tikhonov.

Free illustrations published under the MIT License. You can use them for personal and commercial projects, without the need to include attribution.

See license.

Extra resources

Illustrations created by Sergei Tikhonov.

Free illustrations published under the MIT License. You can use them for personal and commercial projects, without the need to include attribution.

See license.