Content Management Systems hacking probabilities for Admin Access with Google Dorking and database code injection for web content security

Ajay Kumar Phulre
(Computer Science and engineering)
LNCT University
Bhopal,India
aphulre@gmail.com

Megha Kamble
(Computer Science and engineering)
LNCT University
Bhopal,India
meghak@lnct.ac.in

Sunil Phulre
(Computer Science and engineering)
LNCT University
Bhopal,India
s_phulre@yahoo.com

Abstract—.

CMS provides a user-friendly environment for the person who has not even more technical web development skills .digital content creation, modification, and publish content facility provides for website management and preparation by the content management system. There are many tools open-source and commercial Available that are categorized in CMS like WordPress, Drupal, Magento, Joomla. Most of the web developers use these cms applications for their attractive features, and this popularity attracts illegal, unauthorized activity by hackers.CMS provides the facility to upload web themes and plugins, and these freely available applications have a lot of vulnerabilities.

These vulnerabilities highlight the importance for developers to practice security by design and for administrators to adopt security hygiene to reduce their website's attack surface. Regularly update of the content management system on the basis of previously found vulnerabilities and analysis scan plugin database store. Disable and delete outdated old vulnerable plugins and themes.

Keywords— vulnerabilities, google dorking ,website security, cyber security, Content Management Systems .

I. INTRODUCTION

The content management system (CMS) is an open-source tool to manage web content and publish. Its provide facility to structure digital data in the form of uses of many themes as well as plugins provide user friendly environment for person who has not even more technical web development skills .digital content creation, modification and publish content facility provides for website management and preparation by it .there are many tools open-source or commercial tools implemented that are categorized in CMS like WordPress,Drupal ,Magento,Joomla. These all applications have different features in term of plugins, themes, and programming languages they are supported, for example, WordPress support PHP.

Million times Downloading of plugins and themes as per the report published by W3Techs clearly shows the popularity of these CMS applications.

CMS Advantages and Disadvantages as per Security Perspective. The critical feature of CMS systems is that they provide standard requirements for different content as per project requirements.

II. LITERATURE SURVEY

The various researcher gives their opinion in the area of web content security, application security threats. The main problem, according to the researcher, needs to awareness for facing challenges javascript execution environments [1], require third party contents regular audits of inclusion contents in web applications. Those are also some of the core CMS related security issues.

However, increasing the growth of vulnerable content included web pages and freely available CMS plugins for distributing malicious code through web pages is the adoption of techniques for detection threats of web security. So researchers in propose of publishing content structure used to give and find information about vulnerabilities present in websites for security perspective[2].Many researchers focus on webpage testing, searching for malicious code, and vulnerabilities. Also, focus on some testing applications and tools for identifying harmful code present and security threats [3], [4], and various solutions give by a researcher comparing these testing tools on behalf of their results and outcomes [6].However, there is a lack of research on vulnerabilities present in CMS used websites and application security issues [7]. Compared most popular CMS WordPress, Joomla, and Drupal by their performance in terms of security threats, available themes, and plugins [8].Also, most of the researcher focuses on the vulnerabilities testing for various CMS [9].Another topic is freely available plugins and themes quality and available features.[11][10] . We can conclude that there is no recent research in the area of CMS security that analyzes responses of various communities and organizations involved when the vulnerability is discovered. [12]This research also covers the analysis of all other relevant major security factors with an analysis of the latest statistics that are of relevance to the overall security of CMS..

III. CMS COMMON VULNERABILITIES DETECTION

CMS gains popularity with the following features

· CMS provides easy installation for the person who has not even sufficient technical knowledge.
· Users can easily manage and prepare content.
· Most of the CMS components can be used immediately, such as Forum, questionnaire, etc.
· Easily granted user permissions on material.
· The latest features can be added without any technical skills.

CMS also has some security issues

Due to its manageability, easy installation, and user-friendly environment features, it is widely used by many major companies. That attracts the attention of attackers

Common security issues in the content management system are

Authorized licensed use limited to: University of New South Wales. Downloaded on September 26,2020 at 14:04:49 UTC from IEEE Xplore. Restrictions apply.

1.Default configuration usage.
2. patches issued by Content Management Systems.
3. There are some vulnerabilities when plugins installed by 3rd party.
4. Lack of security awareness in administrators.

There are many online paid/unpaid monitoring and detection tools available for the content management system. Vulnerabilities are finding tools for Joomla, WordPress, Drupal, which are used more often in Content Management Systems, for example, Wpscan for WordPress and Joomscan for Joomla applications.

WordPress Vulnerabilities Scanner

Wpscan is an open-source tool designed to collect information and identify security vulnerabilities in WordPress websites. The project developed with Ruby is updated regularly so that it can detect recent vulnerabilities. It also provides additional information, such as references and weaknesses [13]. Wpscan result obtained are as follows:

1.vulnerability detailed statements in context Plugin, theme, and version.
2. Username related enumeration.
3. Timthumb enumeration.
4 Information for password brute force. [13]

JoomScan for scanning vulnerabilities of CMS Joomla

JoomScan is available as an open-source application tool by developers. It usages the Perl programming language for collecting related information and proper identifying vulnerabilities for Joomla project websites. The following information can find with Joomscan.

1. Vulnerability detection of associated themes and used plugins
2. Also, Detect Firewall for Joomla
3. Detection of Version for Joomla
4. Exploit information for vulnerabilities [24].

IV. CMS Hacking Probabilities for Admin Access

With just client benefits, the unauthorized, illegal person gets full administrative power to access the client account. This is sufficient to edit or manipulate programmer code according to their goal. With taking all framework control remotely, to adjust malicious code in the program. Since most of the antivirus programs can control procedures to actualize code in the procedures, the programmer regularly updates and use more hidden techniques. Since the records of most corporate clients are area accounts, the space verification furnishes the client with access to the complete access of the site content.

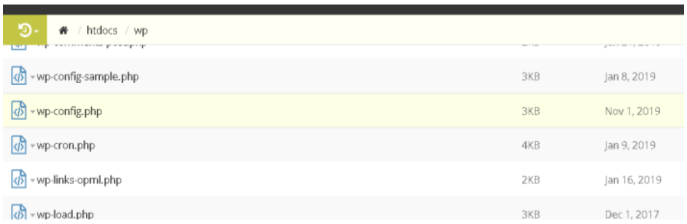
This entrance is regularly given naturally with no extra confirmation of the username and secret word. Thus, if the tainted client approaches the corporate database, aggressors can undoubtedly exploit it. For our situation, by utilizing the python code, we can change the secret organization key to get access to the entire substance of the site. There are codes available in python called Python Exploit.

Most sensitive files of Wordpress CMS

Wordpress CMS includes some sensitive file containing administrative, Database information related to web project these files are (i) Wp-config and (ii) Wp-users

(i) wp-config.php file

Stored in storage hosting account control panel stored in htdocs wp folder.Wp-config.php file contains CMS database related information which contains information of database name, DB user name DB password.



/ htdocs / wp

wp-config-sample.php	3KB	Jan 8, 2019
wp-config.php	3KB	Nov 1, 2019
wp-cron.php	4KB	Jan 9, 2019
wp-links-opml.php	2KB	Jan 16, 2019
wp-load.php	3KB	Dec 1, 2017

Pic .4.1 Wp-config.php file stored in WP/htdocs

Wp-config.php file contains the configuration of :

-Mysql settings
-Secret Keys
-ABSPATH
-Database table prefix

/** The name of the database for WordPress

*/ define('DB_NAME', 'epiz_24462049_w5**');

/** MySQL database username

*/ define('DB_USER', '244620**_1');

/** MySQL database password */

define('DB_PASSWORD', '4[pSU9v**@');

/** MySQL hostname

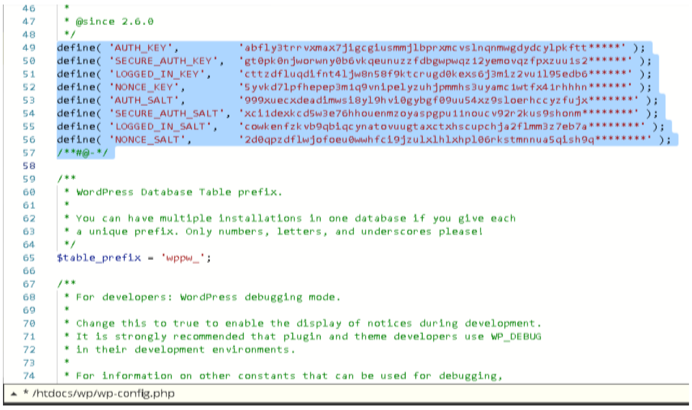
*/define('DB_HOST', 'sql108.byetclu***r.com');

/** 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', '');



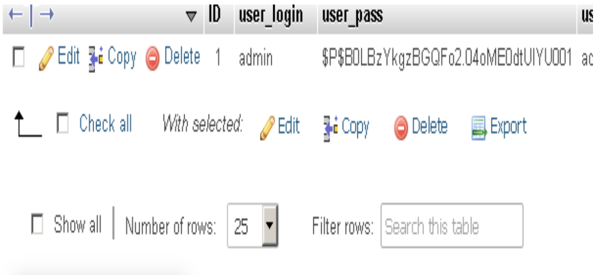
```
 *
 * @since 2.6.0
 */
define( 'AUTH_KEY',         'abfly3trrvxmax7jigcgiusmmjlbprxmcvslnqnmwgdydcylpkftt*****' );
define( 'SECURE_AUTH_KEY',  'gt0pk0njworwny0b6vkqeunuzzfdbgwpwqz12yemovqzfpxzuu1s2******' );
define( 'LOGGED_IN_KEY',    'cttzdfluqdifnt4ljw8n58f9ktcrugd0kexs6j3miz2vu1l95edb6******' );
define( 'NONCE_KEY',        '5yvkd7lpfhepep3m1q9vnipelyzuhjpmmhs3uyamc1wtfx41rhhhn******' );
define( 'AUTH_SALT',        '999xuecxdeadimwsi8yl9hvi0gybgf09uu54xz9sloerhccyzfujx*******' );
define( 'SECURE_AUTH_SALT', 'xci1dexkcd5w3e76hhouenmzoyaspgpu11noucv92r2kus9shonm********' );
define( 'LOGGED_IN_SALT',   'cowkenfzkvb9qbiqcynatovuugtaxctxhscupchja2flmm3z7eb7a********' );
define( 'NONCE_SALT',       '2d0qpzdflwjofoeu0wwhfci9jzulxlhlxhpl06rkstmnnua5qish9q********' );
/**#@-*/

/**
 * WordPress Database Table prefix.
 *
 * You can have multiple installations in one database if you give each
 * a unique prefix. Only numbers, letters, and underscores please!
 */
$table_prefix = 'wppw_';

/**
 * For developers: WordPress debugging mode.
 *
 * Change this to true to enable the display of notices during development.
 * It is strongly recommended that plugin and theme developers use WP_DEBUG
 * in their development environments.
 *
 * For information on other constants that can be used for debugging,
```

* /htdocs/wp/wp-config.php

Pic.4.2. Secure Keys in Wp-config.php

Authorized licensed use limited to: University of New South Wales. Downloaded on September 26,2020 at 14:04:49 UTC from IEEE Xplore. Restrictions apply.

(ii) wp-users.php
This is the second sensitive file is Wp-users.php which contains all administrative login information about WordPress admin (stored in PHPMyAdmin SQL database structure) which is provide all the information about the admin username and password and attached email id also .but password hashed form displayed here & we cannot log in with a hashed form of password.



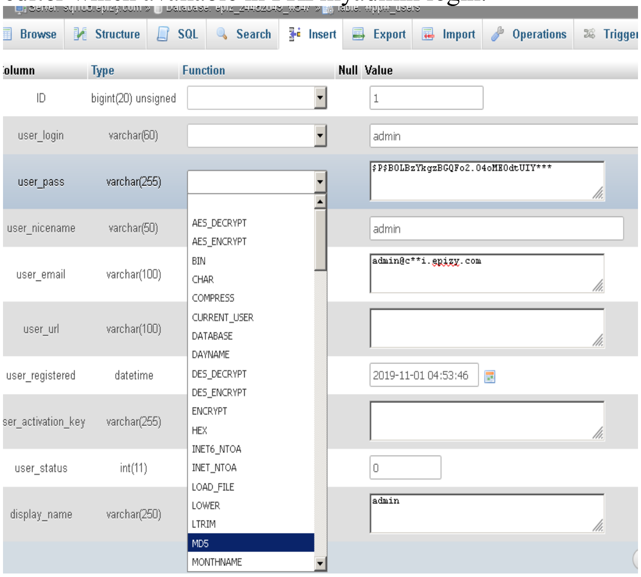
← | →	ID	user_login	user_pass	us
□ Edit Copy Delete	1	admin	PB0LBzYkgzBGQFo2.04oMEOdtUIYU001	ac

□ Check all With selected: Edit Copy Delete Export

□ Show all | Number of rows: 25 Filter rows: Search this table

Pic.4.3 Wp-pwusers file

If a hacker finds these files which are containing information about the database and admin login password related data, then they can use it for their own use or perform illegal activities PHPMyAdmin can open with control panel where all WordPress files available they can also edit from default editor which available in PHPmyadmin login.



olumn	Type	Function	Null	Value
ID	bigint(20) unsigned			1
user_login	varchar(60)			admin
user_pass	varchar(255)			PB0LBzYkgzBGQFo2.04oMEOdtUIY***
user_nicename	varchar(50)			admin
user_email	varchar(100)			admin@c**i.epizy.com
user_url	varchar(100)			
user_registered	datetime			2019-11-01 04:53:46
ser_activation_key	varchar(255)			
user_status	int(11)			0
display_name	varchar(250)			admin

Pic.4.4 Editing of Wp-pwusers file

Changing the process of admin password with the database without using forget password option.

Admin user name and password stored in wp-users.php file .as we have seen in the above picture, click for edit wppwuser.php file open it password available over here in the form of hash we cannot change it directly .but can change it after hashed of MD5 file generation as shown in the pic.

V. Vulnerabilities with Google Dorking

Google Dorking is a searching technique where we can search private website-related information with the help of using tag intitle & inurl to exploit any website if the website is vulnerable. Most of the websites designed by CMS is susceptible.

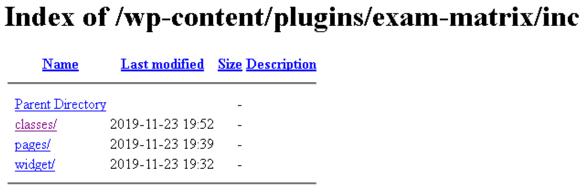
Google Dorking helps to find wp-config.php & wp-users.php files most of the hackers use Google Dorking technique for finding these files for hack vulnerable WordPress website. If the website developer set accessibility of Phpmyadmin, then we can open it after entering it after domain like cdgi.epi***.com/wp/PHPMyAdmin. Otherwise, Phpmyadmin login also supports this user id password finding with wp-config.php files. WordPress Users Knows that the default directory for storing plugins, themes, stylesheets are Wp-content directory. If the setting of permission for the wp-content directory set wrong by the user. Then wp-content can be visible. Directory indexing permission setting is essential for the content management system users. For example the Google Dork

"index of" inurl:wp-content/".

Allow searching website where wp-content directory exposed.

"inurl:"/wp-content/plugins/wp-eexamsystem/".

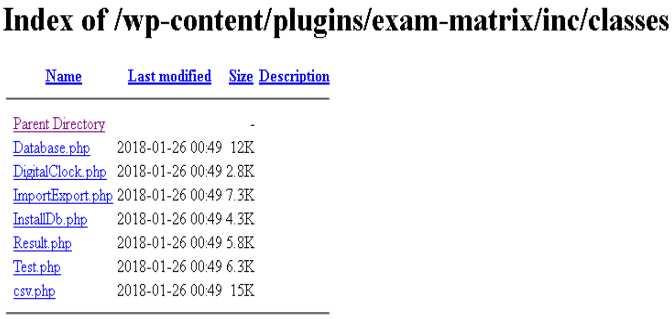
This Dork is used for allows us to search wp-content directory for search plugins.



Index of /wp-content/plugins/exam-matrix/inc

Name	Last modified	Size	Description
Parent Directory		-	
classes/	2019-11-23 19:52	-	
pages/	2019-11-23 19:39	-	
widget/	2019-11-23 19:32	-	

Pic :5.1 Example of Google Darking for plugins



Index of /wp-content/plugins/exam-matrix/inc/classes

Name	Last modified	Size	Description
Parent Directory		-	
Database.php	2018-01-26 00:49	12K	
DigitalClock.php	2018-01-26 00:49	2.8K	
ImportExport.php	2018-01-26 00:49	7.3K	
InstallDb.php	2018-01-26 00:49	4.3K	
Result.php	2018-01-26 00:49	5.8K	
Test.php	2018-01-26 00:49	6.3K	
csv.php	2018-01-26 00:49	15K	

Pic:5.2 Directory Index finding from Darking

There are many online tools available for WordPress website scanning popular tool is wpscan with the help of wp-scan scan vulnerabilities of any website. Like we can find private database directory information from where these sensitive files available, if we find the path of the database, then we can use Google Dorking for finding these files or type after domain directory path we can download manually also.

How wp-users.php file use for changing the password if available password in the form of hashed PHPMyAdmin database.

After opening the wp-users.php file in the PHPMyAdmin edit, this file password is hashed then generally hackers used online available hash code generator and can replace it with

Authorized licensed use limited to: University of New South Wales. Downloaded on September 26,2020 at 14:04:49 UTC from IEEE Xplore. Restrictions apply.

pervious hash code and save it .successfully admin password changed by hackers.

VI. WordPress SQL code Injection

We all know about popularity and uses of WordPress its vulnerable with freely available theme and plugins but most of the web hosting aware about it and doing some good practice for web security measures to avoid such kind of hacking .but at the same time its not easy task for secure all risks security solution. The Most frequently used activity done hackers are code injections via SQL it's not easy to find you are a victim of code injection question is that what is SQL code injection.

Database Injections

Unauthorized person injecting code on your web project without your permission is not an uncommon task. Hackers are frequently used pushing rogue code insertion for getting unauthorized access to the database for harming your webpage. Its all effect on web security.

WordPress content stores

Word press provides the database for store files in the form of a MySql database.WordPress website using the standard Data Base Management System. SQL query generated by word press whenever required. PHP SQL provides query oriented mechanism for storing and fetching content from the database. Including all operations like content modification (adding, deleting, or changing the database itself). However, unauthorized persons not required to enter in the database; there are many ways to inject code in the database by a hacker.

Code injection into a WordPress SQL database

Hackers can enter in your web page with the help of user input block like Forms it may be login form, contact form sign up box even from the search bar. The main problem with these form are in many instances, there are many submission received by the database. The addition of a rogue program code with this submission and code is received by the SQL database. Hacker tries to enter these rouge SQL codes .for example, there is some validation in login form means response received only in particular format like telephone number XXX_XXX_XXXX if you leave as free form unauthorized person can easily use for code injection.

VII. Conclusion

Analyzing Content management system security issues with common vulnerabilities detection and available online tool for central scanning part of the research includes sensitive files of CMS and hacking probabilities for admin access, WordPress vulnerabilities with Google Darking for exploiting WordPress website. Analyzing SQL code injection, Web analyzing responses, and actions of various parties involved in the example of content management systems security vulnerability, we managed to propose improvements that could lead to better and more organized management of security community responses in case of discovered vulnerabilities. We managed to suggest improvements that could lead to better and more organized control of security actions of various parties involved in the example of WordPress security vulnerability we managed to propose improvements that could lead to better and more organized management of security community responses in case of discovered vulnerabilities.

References

[1] Patil, S., Hare Hunting in the Wild Web: A Study of Web Security Threats and Solutions. (IRJET) Volume: 03 Issue: 08 | Aug-2016.

[2] Canfora, G. and C.A. Visaggio, A set of features to detect web security threats. Journal of Computer Virology and Hacking Techniques, 2016. 12(4): p. 243-261.

[3] Costa Nunes, P.J., J. Fonseca, and M. Vieira. phpSAFE: A Security Analysis Tool for OOP Web Application Plugins. in Dependable Systems and Networks (DSN), 2015 45th Annual IEEE/IFIP International Conference on. 2015. IEEE.

[4] Jensen, T., et al., Thaps: automated vulnerability scanning of php applications, in Secure IT Systems. 2012, Springer. p. 31-46.

[5] Sethi, S. and V. Singhal. ICTS2016-SS27-07: A Peek into Web Applications Security. in Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies. 2016. ACM

[6] Pistoia, M. and O. Tripp, Testing WEB Applications For Security Vulnerabilities With Metarequests. 2016, Google Patents.

[7] Patel, S.K., V.R. Rathod, and J.B. Prajapati. Comparative analysis of web security in open source content management system. in Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on. 2013. IEEE.

[8] Onishi, A., Security and Performance, in Pro WordPress Theme Development. 2013, Springer. p. 297-332.

[9] Mansfield-Devine, S., Taking responsibility for security. Computer Fraud & Security, 2015. 2015(12): p. 15-18.

[10] Coelho Martins da Fonseca, J.C. and M.P. Amorim Vieira. A Practical Experience on the Impact of Plugins in Web Security. in Reliable Distributed Systems (SRDS), 2014 IEEE 33rd International Symposium on. 2014. IEEE.

[11] Koskinen, T., P. Ihantola, and V. Karavirta. Quality of WordPress plug-ins: an overview of security and user ratings. in Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom). 2012. IEEE.

[12] Jerković, H., P. Vranešić, and S. Dadić. Securing web content and services in open source content management systems. in Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2016 39th International Convention on. 2016. IEEE.

[13] https://wpshout.com/wordpress-xss-attack/

[14] "Multi-layer Software Configuration: Empirical Study on Wordpress" Mohammed Sayagh, Bram Adams Polytechnique Montreal, Canada 2015.

[15] S. Zhang and M. D. Ernst, "Which configuration option should I change?" in Proceedings of the 36th International Conference on Software Engineering, ser. ICSE 2014. ACM, 2014, pp. 152–163.

[16] https://www.url-encode-decode.com/base64-encode-decode/

[17] Žolt Namestovski*, Márta Takács* *, Branka Arsović* SISY 2012 • Supporting Traditional Educational Process with E-Learning Tools IEEE 10th Jubilee International Symposium on Intelligent Systems and Informatics • September 20-22, 2012, Subotica, Serbia.

[18] Dhaval R Gandhi; Nehal N Shah Published in: "Comparative analysis for hardware circuit architecture of Wallace tree multiplier" 2013 International Conference on Intelligent Systems and Signal Processing (ISSP) Date Added to IEEE Xplore: 10 June 201.

[19] Cosmin A. Conțu ;Eduard C. Popovici ; Octavian Fratu ; Mădălina G. Berceanu "Security issues in most popular content management

Authorized licensed use limited to: University of New South Wales. Downloaded on September 26,2020 at 14:04:49 UTC from IEEE Xplore. Restrictions apply.

systems"2016 International Conference on Communications (COMM) INSPEC Accession Number: 16196383 DOI: 10.1109/ICComm.2016.7528327 Publisher: IEEE Conference Location: Bucharest, Romania 2016.

[20] Hrvoje Jerkovic, Branko Sinkovic, International Journal of Economics and Management Systems "Vulnerability analysis of most popular open source Content Management Systems with focus on WordPress and proposed integration of artificial intelligence cyber security features" http://www.iaras.org/iaras/journals/ijems 2017.

[21] https://www.wpwhitesecurity.com/how-to-tell-wordpress-blog-website-hacked/ ,https://www.wpwhitesecurity.com/online-wordpress-backup-services-ultimate-wordpress-backup-solution/,https://www.wpwhitesecurity.com/wordpress-backup-blueprints-manual-backup/

[22] https://wpshout.com/wordpress-xss-attack.

[23] https://hackingvision.com/2017/04/14/google-dorks-list-2017-sqli/

[24] https://github.com/rsrdesarrollo/joomscan-owasp

Authorized licensed use limited to: University of New South Wales. Downloaded on September 26,2020 at 14:04:49 UTC from IEEE Xplore. Restrictions apply.