Ministerul Educaţiei al Republicii Moldova

Universitatea Tehnică a Moldovei

Facultatea Calculatoare Informatică şi Microelectronică

Catedra Automatică şi Tehnologii Informaţionale

**Proiect de practica**

**Aplicație pentru analiza şi depistarea a vulnerabilități-lor populare platformei CMS WordPress**

**Student:** Dumbrava V.

**Conducatorul tezei de licență:** Antohi I.

**Conducător de practica:** Bulai R.

**Chişinău 2017**

**Cuprinsul**

1. Introducerea……………………………………………………………………..,3
2. Conținutul………………………………………………………………………..4
   1. WordPress security – WPScan pentru WordPress vulnerabilitate scanner……………………………………………………………………….4
   2. WordPress și securitatea………………………………………………...8
      1. Echipa de securitate a WordPress……………………………...8
      2. Riscuri, procese și istoria securității WordPress……………….8
      3. Actualizarea automată în culise a versiunilor de Securitate……9
      4. Top 10 2013, OWASP…………………………………………9
      5. Alte riscuri de securitate și motive de îngrijorare………….…11
   3. Securitatea modulelor și temelor WordPress …………………….…...13
      1. Tema implicită………………………………………………...13

2.3.1. Depozitarele de module și teme de la WordPress.org………...13 2.3.2 Echipa de revizuire a temelor………………………………….13

2.3.3.1 O notă despre WordPress.com și securitatea WordPress ……14

2.4. Statistica……………………………………………………………….15

2.5. XSS…………………………………………………………………….16

2.5.1. Diagrama Use-Case………………………………………………….16

2.5.2 Diagrama de Activitate…………………………………………….…17

3.Concluzii………………………………………………………………………...18 4. Bibliografia…………………………………………………………………..…19

2

**1. Introducerea**

**WordPress** este o platformă de tipsursă deschisăpentru publicareablogurilor.Platforma WordPress este scrisă în limbajul PHP, folosind pentru gestionarea bazelor de date sistemul MySQL. Dispune un sistem de șabloane scrise în limbajele HTML și CSS. Avantajele majore prezentate de WordPress sunt simplitatea și numeroasele plugin-uri create de către comunitate care pot modifica funcționalitatea WordPress-ului tranformându-l în aproape orice tip de site web. De asemenea interfața poate fi schimbată foarte ușor cu ajutorul multitudinii de teme gratuite sau premium cu doar un clic.

WordPress a apărut prima dată în 2003 ca precursor al b2/cafelog, care era utilizat de 2 000 de bloguri la acea vreme.

De la începuturi și până acum, WordPress a fost etichetat în nenumărate rânduri ca fiind vulnerabil la atacuri ce vizau adăugare de conținut malițios pe blogurile sau site-urile ce foloseau această platformă. Au fost create numeroase programe automate ce căutau pe internet site-uri care foloseau această platformă și, folosindu-se de vulnerabilitățile acesteia, reușeau să introducă în conținut, fără acordul proprietarului, link-uri către site-urile celor ce foloseau aceste programe.

În ultimul timp însă, dezvoltatorii platformei au reușit să aducă WordPress într-o stare în care atacurile de acest tip sunt aproape imposibil de realizat. În momentul de față WordPress este printre cele mai sigure si mai puternice CMS-uri la ora actuală.

3

1. **Conținutul**
   1. WordPress security – WPScan pentru WordPress vulnerabilitate

scanner

WP scanare este o scanare de vulnerabilităţi pentru WordPress. Acesta este dezvoltat în Ruby. El este capabil să lista de plugin-uri utilizate şi vă va oferi vulnerabilităţi de securitate asociate. De asemenea, include un modul de forţă brută pentru a aborda interfaţa de administrare WordPress.

Este important să reţineţi că, în ceea ce priveşte majoritatea securitate şi instrumente de scanare, WPscan nu va asigura nu WordPress pentru tine. De asemenea, completarea unui control de securitate cu WPscan care nu este vizibil defecte ai nu înseamnă că WordPress este de a 100% sigur. Este o noţiune care trebuie să fie constant în minte atunci când vorbim despre securitate.

WP scanare este nativ pe distribuţii următoarele : (Windows nu este acceptată)

-BackBox Linux -Kali Linux -Pentoo

Dacă doriţi să instalaţi manual pe Debian/Ubuntu sau Fedora/CentOS, Iată premisele :

**Pe Debian :**



sudo apt-get install git ruby ruby-dev libcurl4-gnutls-dev make



git clone https://github.com/wpscanteam/wpscan.git



cd wpscan



sudo gem install bundler



bundle install --without test --path vendor/bundle

**Pe distribuţii Fedora/CentOS/RHEL :**



sudo yum install gcc ruby-devel libxml2 libxml2-devel libxslt libxslt-devel libcurl-devel



git clone https://github.com/wpscanteam/wpscan.git



cd wpscan



sudo gem install bundler && bundle install --without test



ruby wpscan.rb votrecommande ....

4

Putem folosi acum WPscan.

Înainte de orice analiză a actualiza baza de date a wp-scanare. Acest lucru este important, deoarece dacă unul decide la spre a scanda nostru WordPress cu o bază de date de vulnerabilităţi, care nu este până la data, unele vulnerabilitati de securitate legate de tema

WordPress versiunea sau versiunile de plug-in-uri de exemplu, nu ai nu va transporta, există un risc sa pierd critice pentru a asigura. Pentru a actualiza baza de date WPscan :



wpscan --update

Acum, că baza noastră de date este actualizată, putem începe să scaneze WordPress site-ul nostru :



wpscan --URL www.monsite.fr

Cu aceasta comanda va şti versiune de WordPress, numele şablonului, lista de plugin-

uri...

Atunci când aveţi un semn de exclamare roșu, acest lucru înseamnă că este important pentru a corecta eroarea. Fi actualizarea WordPress în cazul în care plugin-uri fie prin ştergerea fişierului. Majoritatea dintre noi, să fişierul "readme.html". Ştergeţi-l, acesta oferă informaţiile din versiunea WP.

Alte ordine care pot fi interesante si permite scanarea complet un blog WordPress listarea

utilizatori, plugin-uri vulnerabile, vulnerabile teme cunoscute...



wpscan --url www.monsite.fr --enumerate

Aveţi posibilitatea să rafinaţi detectarea de vulnerabilităţi prin specificarea o opţiune suplimentară de exemplu doar plugin-uri vulnerabile (-enumera vp)utilizatorii (-enumera u), … Puteţi vizualiza detalii despre opţiunile la această adresă : http://wpscan.org

Poti face un test al tău password cu următoarea comandă :



wpscan --URL www.monsite.fr --wordlist /chemindevotrelistebruteforce.txt --username votreutilisateur

5

**Exemplu:** listare versiune, thema instalata, pluginuri, vulnerabiliti cunoscute precum si userii existenti.

[root@hacklab /home/admin/tmp/lab/wpscan]#ruby wpscan.rb –url www.crystalmind.ro/wordpress –enumerate u

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| \_\_ |  |  | \_\_\_\_\_\_\_ \_\_\_\_\_ | |
| \ \ |  |  | / / | \_\_ \ / \_\_\_\_| |
| \ \ | /\ | | / /| |\_\_) | (\_\_\_ \_\_\_ \_\_ \_ \_ \_\_ | |
| \ \/ | | \/ / | | | \_\_\_/ \\_\_\_ \ / \_\_|/ \_` | '\_ \ |
| \ | /\ / | | | | | \_\_\_\_) | (\_\_| (\_| | | | | |
| \/ | | \/ | |\_| |\_\_\_\_\_/ \\_\_\_|\\_\_,\_|\_| |\_| | |

WordPress Security Scanner by the WPScan Team Version 2.8

Sponsored by Sucuri – https://sucuri.net

@\_WPScan\_, @ethicalhack3r, @erwan\_lr, pvdl, @\_FireFart\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* URL: http://www.crystalmind.ro/wordpress/
* Started: Fri Sep 25 15:47:23 2015

[!] The WordPress 'http://www.crystalmind.ro/wordpress/readme.html' file exists exposing a version number

* Interesting header: SERVER: Apache
* Interesting header: X-POWERED-BY: PHP/5.3.10-1ubuntu3.19
* XML-RPC Interface available under: http://www.crystalmind.ro/wordpress/xmlrpc.php
* WordPress version 4.3.1 identified from meta generator
* WordPress theme in use: magazine-basic – v3.0.6
* Name: magazine-basic – v3.0.6

| Latest version: 3.0.6 (up to date)

| Location: http://www.crystalmind.ro/wordpress/wp-content/themes/magazine-basic/

| Readme: http://www.crystalmind.ro/wordpress/wp-content/themes/magazine-basic/readme.txt

| Style URL: http://www.crystalmind.ro/wordpress/wp-content/themes/magazine-basic/style.css

| Theme Name: Magazine Basic

| Theme URI: https://themes.bavotasan.com/themes/magazine-basic-wordpress-theme/

| Description: Create a truly unique design with Magazine Basic, a lightweight and fully responsive HTML5 theme

…

| Author: c.bavota

| Author URI: http://bavotasan.com

[!] Title: Magazine Basic – wp-content/themes/magazine-basic/view\_artist.php id Parameter SQL Injection Reference: https://wpvulndb.com/vulnerabilities/7521

Reference: http://packetstormsecurity.com/files/118321/ Reference: http://www.securityfocus.com/bid/56664/ Reference: http://osvdb.org/show/osvdb/87838

* Enumerating plugins from passive detection …

| 7 plugins found:

* Name: addthis – v5.1.2

| Latest version: 5.1.2 (up to date)

| Location: http://www.crystalmind.ro/wordpress/wp-content/plugins/addthis/

| Readme: http://www.crystalmind.ro/wordpress/wp-content/plugins/addthis/readme.txt

[+] Name: captcha – v4.1.5

| Latest version: 4.1.5 (up to date)

| Location: http://www.crystalmind.ro/wordpress/wp-content/plugins/captcha/

| Readme: http://www.crystalmind.ro/wordpress/wp-content/plugins/captcha/readme.txt

6

* Name: fancier-author-box – v1.4 | Latest version: 1.4 (up to date)

| Location: http://www.crystalmind.ro/wordpress/wp-content/plugins/fancier-author-box/

| Readme: http://www.crystalmind.ro/wordpress/wp-content/plugins/fancier-author-box/readme.txt

* Name: mailchimp-for-wp – v2.3.12

| Latest version: 2.3.12 (up to date)

| Location: http://www.crystalmind.ro/wordpress/wp-content/plugins/mailchimp-for-wp/

| Readme: http://www.crystalmind.ro/wordpress/wp-content/plugins/mailchimp-for-wp/readme.txt

[+] Name: popup-maker – v1.3.7

| Latest version: 1.3.7 (up to date)

| Location: http://www.crystalmind.ro/wordpress/wp-content/plugins/popup-maker/

| Readme: http://www.crystalmind.ro/wordpress/wp-content/plugins/popup-maker/readme.txt

* Name: social-share-boost – v4.4 | Latest version: 4.4 (up to date)

| Location: http://www.crystalmind.ro/wordpress/wp-content/plugins/social-share-boost/

| Readme: http://www.crystalmind.ro/wordpress/wp-content/plugins/social-share-boost/readme.txt

* Name: yet-another-related-posts-plugin – v4.2.5

| Latest version: 4.2.5 (up to date)

| Location: http://www.crystalmind.ro/wordpress/wp-content/plugins/yet-another-related-posts-plugin/

| Readme: http://www.crystalmind.ro/wordpress/wp-content/plugins/yet-another-related-posts-plugin/readme.txt

* Enumerating usernames …
* Identified the following 4 user/s:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| +—-+————-+————————————————-+ | | | |  |
| | Id | Login | | | Name | | |  |
| +—-+————-+————————————————-+ | | | |  |
| | 1 | | admin1 | |  | | |  |
| | 2 | | admin2 | | Octavian, Author at Crystal Mind Academy | | | |
| | 3 | | crystalmind | Teacher, Author at Crystal Mind Academy | | | | |
| | 4 | | John | John Doe, Author at Crystal Mind Academy | | | |  |

+—-+————-+————————————————-+

* Finished: Fri Sep 25 15:48:08 2015
* Requests Done: 119
* Memory used: 75.609 MB
* Elapsed time: 00:00:45

Atentie la faptul de a nu folosi un astfel de instrument pe site-urile web care nu vă sau fără consimţământul proprietarului lor. Există mai multe alte opţiuni pentru utilizarea de WPscan, dar aici am vazut funcţionării sale globale.

Este important să ştiţi cum să lucreze WPscan şi instrumente similare pentru a înţelege că anumite reguli de securitate (şi toate) permite un sigur siguranţă 100%. Înţeleagă mai bine instrumente şi strategii de atacatori pentru a apăra mai bine.

7

2.2 Documentul alb al securității WordPress

**2.2 WordPress și securitatea**

**1.1 Echipa de securitate a WordPress**

Echipa de securitate WordPress e formată din aproximativ 25 de experți incluzând dezvoltatorii șefi și cercetătorii în securitate — aproximativ jumătate din ei angajați ai Automattic (realizatorii lui WordPress.com, prima și cea mai mare platformă de găzduire WordPress de pe web) și un număr care lucrează în domeniul securității pe web. Echipa se consultă cu cercetători de încredere renumiți și cu companii de găzduire3.

Echipa de securitate WordPress colaborează adesea cu alte echipe de securitate pentru a rezolva probleme de interdependență, cum ar fi rezolvarea vulnerabilității din interpretorul XML al PHP, folosit de API-ul XML-RPC livrat cu WordPress,

în WordPress 3.9.24. Rezolvarea acestei vulnerabilități a fost rezultatul unui efort comun al echipelor de securitate ale WordPress și Drupal.

**1.2 Riscuri, procese și istoria securității WordPress**

Echipa de securitate WordPress crede în devoalarea responsabilă prin alertarea imediată a echipei de securitate cu privire la orice potențială vulnerabilitate. Potențialele vulnerabilități de securitate pot fi semnalate echipei de securitate direct la adresa de email: security@wordpress.org5. Echipa de securitate comunică între membrii săi pe o listă privată de email și lucrează pe un Trac privat dar neînchis (*walled-off*) pentru urmărirea, testarea și rezolvarea erorilor și problemelor de securitate.

Fiecare raport de securitate este confirmat în momentul primirii și echipa lucrează să verifice vulnerabilitatea și să determine gravitatea ei. Dacă e confirmată, echipa de securitate face planificarea unei reparații (*patch*) ce poate fi asignată unei viitoare versiuni de WordPress sau poate fi imediat lansată o versiune de securitate, în funcție de gravitatea problemei.

Pentru o versiune imediată de securitate, echipa de securitate va publica o recomandare pe situl de știri WordPress.org *News*6 anunțând lansarea și detaliind modificările. În acest mesaj persoana responsabilă de descoperire va primi o recunoaștere, încurajându-se astfel pe viitor continuarea raportărilor responsabile.

Administratorii WordPress văd în panoul de control al siturilor lor o notificare de actualizare când o nouă versiune e disponibilă, iar mergând pe actualizarea manuală utilizatorii sunt redirectați la ecranul Despre WordPress care detaliază modificările. Dacă administratorii au validată actualizarea automată a noilor versiuni în culise, vor primi un email după ce actualizarea s-a terminat.

8

**1.3 Actualizarea automată în culise a versiunilor de securitate**

Începând de la versiunea 3.7, WordPress a introdus actualizarea automată în culise pentru toate versiunile minore7, cum ar fi 3.7.1 și 3.7.2. Echipa de securitate WordPress poate identifica, repara și împinge automat îmbunătățirile de securitate pentru WordPress fără ca proprietarul sitului să trebuiască să facă ceva din partea sa, actualizarea de securitate instalându-se automat.

Când este publicată o actualizare de securitate pentru versiunea curentă stabilă de WordPress, echipa nucleului va împinge de asemenea actualizările de securitate pentru toate versiunile ce sunt capabile de actualizare în culise (de la WordPress 3.7), astfel că aceste mai vechi dar încă recente versiuni de WordPress să primească și ele aceste îmbunătățiri de securitate.

Proprietarii individuali de situri pot opta pentru înlăturarea actualizărilor automate în culise printr-o simplă modificare în fișierul lor de configurare, dar păstrarea acestei funcționalități este recomandată cu tărie de echipa de bază, precum și cea de a rula ultima versiune stabilă de WordPress.

**1.4 Top 10 2013, OWASP**

Proiectul de securitate a aplicațiilor web deschise (*Open Web Application Security* *Project*, OWASP) este o comunitate internet dedicată securității aplicațiilor pentruweb. Lista Top10 OWASP8 se focalizează pe identificarea celor mai serioase riscuri de securitate ale aplicațiilor pentru un larg spectru de organizații. Cele din Top 10 sunt selectate și prioritizate printr-o combinație a estimărilor consensuale privind exploatarea, detectarea și impactul acestora.

Următoarele secțiuni pun în discuție API-urile, resursele și politicile pe care WordPress le folosește pentru a întări softul de bază dar și modulele și temele terților în fața potențialelor riscuri.

*1.4.1 A1 – Injecție*



Există un set de funcții și API-uri disponibile în WordPress pentru a-i sprijini pe dezvoltatori în a se asigura că injecția de cod neautorizat nu e posibilă, și în ai ajuta să valideze și igienizeze datele. Sunt disponibile documentații și bune

practici9 despre utilizarea acestor API-uri pentru a proteja, valida, sau igieniza datele de intrare sau ieșire în HTML, URL-uri, antete HTTP și la interacțiunea cu baza de date ori sistemul de fișiere. Administratorii pot în plus să restricționeze tipurile de fișiere ce pot fi încărcate via filtre.

*1.4.2 A2 – Autentificare defectuoasă și gestiunea sesiunilor*



Softul de bază WordPress gestionează conturile de utilizator și detaliile de autentificare cum ar fi ID-ul utilizatorului, numele și parola pe partea serverului, la

9

fel și cookie-urile de autentificare. Parolele sunt protejate în baza de date folosind tehnici standard de „sărare și întindere” *salting&stretching*. Sesiunile existente sunt distruse după deautentificare începând cu versiunea WordPress 4.0.

*1.4.3 A3 – Scripturi inter-situri (XSS)*



WordPress asigură o gamă de funcții ce pot ajuta la punerea în siguranță a datelor furnizate de utilizatori10. Utilizatorii de încredere, administratorii sau editorii într-o instalare singulară de WordPress, sau doar administratorii de situri în WordPress multi-sit, pot publica HTML sau JavaScript nefiltrat după necesități, cum ar fi în interiorul unui articol sau pagini. Ceilalți utilizatori și elementele de conținut trimise spre publicare sunt implicit filtrate pentru a fi înlăturate entitățile periculoase, folosind biblioteca KSES prin funcția wp\_kses.

Ca exemplu, echipa nucleului WordPress a observat că

funcția the\_search\_query() a fost folosită greșit de majoritatea autorilor de teme, care n-au filtrat pentru siguranță (*escaping*) rezultatul ei pentru a fi folosit în HTML. Într-o foarte rară rupere a compatibilității înapoi, ieșirea funcției a fost schimbată în WordPress 2.3 pentru a fi pre-filtrată pentru securitate (*pre-escaped*).

*1.4.4 A4 – Referință directă nesecurizată la obiect*



WordPress furnizează destul de des referințe directe către obiecte, cum ar fi identificatori numerici unici de conturi utilizator sau conținut disponibil în URL sau câmpuri de formulare. Cu toate că acești identificatori dezvăluie informații direct din sistem, elaboratul sistem de control al accesului pe care îl are WordPress împiedică cererile neautorizate.

*1.4.5 A5 – Configurarea greșită a securității*



Majoritatea operațiunilor de configurare a securității WordPress sunt limitate la un singur administrator autorizat. Setările implicite ale WordPress sunt evaluate în mod continuu la nivelul echipei de bază, și aceasta furnizează documentații și exemple de bună practică pentru a întări securitatea configurării serverelor ce rulează situri WordPress11.

*1.4.6 A6 – Expunerea datelor sensibile*



Parolele de acces ale utilizatorilor sunt „sărate și secționate” (*salted and hashed*) pe baza cadrului de tratare a parolelor din PHP-ul portabil *Portable PHP Password* *Hashing Framework*12. Sistemul de permisiuni WordPress este folosit pentru acontrola accesul la informații private cum ar fi cele de identificare a utilizatorilor, adrese de email ale comentatorilor, conținut publicat privat, etc. În WordPress 3.7, a fost inclus în softul de bază un evaluator de tărie a parolei care să ofere informații suplimentare utilizatorilor care-și stabilesc parola și sfaturi pentru a o întări.

10

WordPress are de asemenea o setare opțională de configurare pentru cerințe

HTTPS.

*1.4.7 A7 – Lipsă de control a accesului la nivel de funcții*



WordPress verifică autorizarea corespunzătoare și permisiunile pentru orice cereri de acces la nivel de funcție înainte de a fi execută acțiunea. Accesul sau vizualizarea unor URL-uri administrative, meniuri și pagini, fără autentificare corespunzătoare este integrată strâns cu sistemul de autentificare pentru a preveni accesul unor utilizatori neautorizați.

*1.4.8 A8 – Falsificare cereri inter-situri (CSRF –* Cross Site RequestForgery*)*



WordPress folosește garanți (*tokens*) criptografici, numiți nunici *nonces*13, pentru a valida intenția unor cereri de acțiuni din partea unor utilizatori autorizați pentru a asigura protecția împotriva potențialelor amenințări CSRF. WordPress oferă un API pentru generarea acestor garanți pentru crearea și verificarea temporară a unicității acestora, ei fiind limitați la un anumit utilizator, o acțiune specifică, un obiect specific, o perioadă specifică de timp și care pot fi adăugați unor formulare și URL-uri după nevoie. În plus, toți nunicii sunt invalidați la deautentificare.

*1.4.9 A9 – Folosirea componentelor cu vulnerabilități cunoscute*



Echipa de bază WordPress monitorizează îndeaproape cele câteva biblioteci incluse și cadre de lucru (*frameworks*) integrate în WordPress pentru funcționalitățile de bază. În trecut echipa de bază a contribuit la mai multe terțe componente pentru a le face mai sigure, cum a fost și actualizarea pentru repararea unei vulnerabilități inter-sit în TinyMCE în WordPress 3.5.214.

Dacă e nevoie, echipa de bază poate decide să ramifice (*fork*) sau să înlocuiască componente externe critice, cum s-a întâmplat când a fost înlocuită oficial biblioteca *SWPUpload* cu *Plupload* în 3.5.2, și când o ramificare securizată a SWFUpload a fost făcută disponibilă de echipa de securitate15 pentru acele module care au continuat să folosească pe termen scurt SWFUpload.

1. *A10 – Redirectări și trimiteri nevalidate*



Sistemul intern de autentificare și control acces al WordPress va asigura protecția împotriva încercărilor de a direcționa utilizatorii spre destinații nedorite sau redirectări automate. Această funcționalitate este de asemenea accesibilă dezvoltatorilor de module printr-un API, wp\_safe\_redirect()16.

1. **Alte riscuri de securitate și motive de îngrijorare**
   1. *Atacuri la procesarea XXE (*XML eXternal Entity*) a entităților*

11

*externe XML*



La procesarea XML, WordPress invalidează încărcarea unor entități XML personalizate pentru a preveni atât atacurile de tip Entitate externă cât și cele de tip Expansiune entitate. Dincolo de funcționalitatea de bază a PHP, WordPress nu asigură un API suplimentar de procesare XML pentru autorii de module.

*1.5.2 Atacuri SSRF (*Server Side Request Forgery*) – Cereri falsificate către server*



Cererile HTTP lansate de WordPress sunt filtrate pentru a preveni accesul la adrese IP private sau de retur (*loopback*). În plus, accesul este permis numai pe anumite porturi HTTP standard.

12

**2.3 Securitatea modulelor și temelor WordPress**

**2.3.1. Tema implicită**

WordPress are nevoie de o temă validată pentru a face conținutul vizibil în față pe sit. Tema implicită, livrată cu nucleul WordPress, (acum „*Twenty Fifteen*„) a fost revizuită viguros și testată din punctul de vedere al securității atât de echipa dezvoltatorilor de teme cât și de echipa de dezvoltare de bază.

Tema implicită poate să servească ca punct de plecare pentru dezvoltarea de teme personalizate, iar dezvoltatorii de situri pot să creeze teme copil care să includă unele personalizări dar să se bazeze pe tema implicită pentru majoritatea funcționalității și a securității. Tema implicită poate fi înlăturată cu ușurință de administrator dacă nu e necesară.

**2.3.1. Depozitarele de module și teme de la WordPress.org**

Sunt aproximativ 30.000+ de module și 2.000+ de teme listate pe situl WordPress.org. Aceste teme și module sunt înscrise pentru a fi incluse și sunt manual revizuite de voluntari înainte de a deveni disponibile în depozitar.

Includerea modulelor și temelor în depozitare nu garantează că acestea nu au vulnerabilități de securitate. Există ghiduri pentru dezvoltatorii de module pe care aceștia să le consulte înainte de la depune pentru includerea în depozitar a unui modul17, iar pe WordPress.org este disponibilă și o documentație extensivă despre cum se dezvoltă o temă WordPress18.

Fiecare modul și fiecare temă au posibilitatea de a fi dezvoltate în mod continuu de către proprietarul modulului sau temei respective, iar orice următoare reparații sau facilități adăugate pot fi încărcate în depozitar și făcute disponibile utilizatorilor ce au instalat acel modul sau temă împreună cu o descriere a modificărilor.

Administratorii de situri sunt notificați despre modulele ce trebuie să fie actualizate prin panoul de control din administrare.

Când este descoperit un modul cu vulnerabilități de către echipa de securitate WordPress, aceasta contactează autorul modulului și lucrează împreună să-l corecteze și să lanseze o nouă versiune sigură. Dacă răspunsul autorului modulului întârzie și vulnerabilitatea e severă, tema/modulul sunt scoase din directorul public, iar în unele cazuri, reparate și actualizate de către echipa de securitate.

**2.3.2 Echipa de revizuire a temelor**

Echipa de revizuire a temelor este un grup de voluntari, conduși de membri cheie consacrați ai comunității WordPress, care revizuiesc și aprobă temele depuse pentru a fi incluse în directorul oficial de teme WordPress. Echipa ține la zi ghidul oficial de revizuire a temelor19, datele unității de testare a temei20 și modulul de verificare temă21, și încearcă să angajeze și să educe comunitatea dezvoltatorilor de

13

teme WordPress cu privire la cele mai bune practici de dezvoltare. Includerea în grup e moderată de comiteri de bază ai echipei de dezvoltare WordPress.

Rolul furnizorului de găzduire web în securitatea WordPress

WordPress poate fi instalat pe o mulțime de platforme. Cu toate că nucleul software al WordPress asigură multe posibilități de a opera o aplicație web sigură, trecute în revistă în acest document, configurarea sistemului de operare și a serverului web de dedesubt care îl găzduiește este la fel de importantă pentru a menține securizate aplicațiile WordPress.

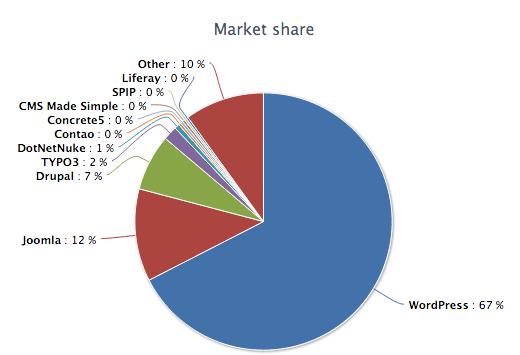
**2.3.3.1 O notă despre WordPress.com și securitatea WordPress**

WordPress.com este cea mai mare instalare WordPress la nivel global, ce aparține și este gestionată de Automattic, Inc., fondată de Matt Mullenweg, co-creatorul proiectului WordPress. WordPress.com deși rulează softul de bază WordPress, are propriile procese de securitate, de risc și de soluționare22. Acest document se referă la securitatea softului descărcat de la WordPress.org pentru o platformă auto-găzduită pe orice server din lume.

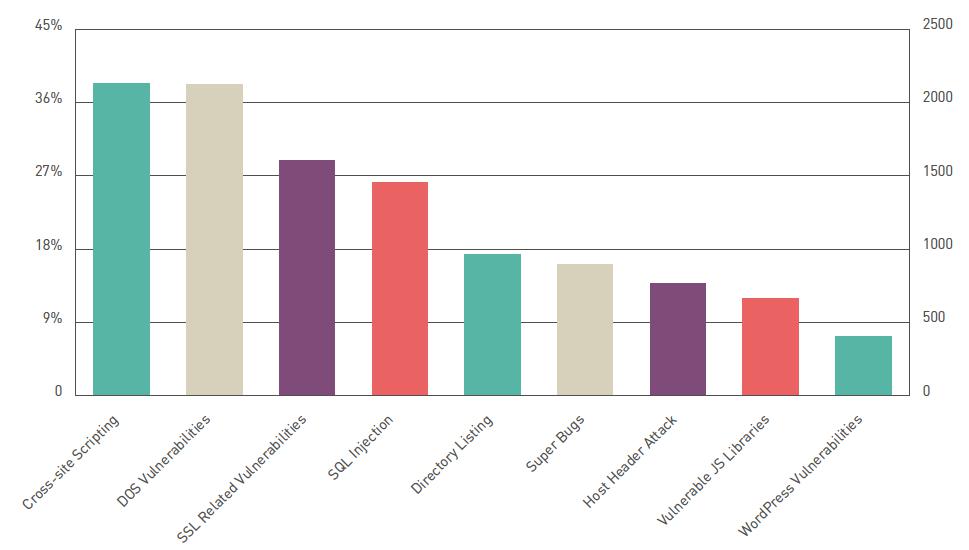
14

**2.4. Statistica**

Mai mult de 2 milioane de site-uri sunt alimentate de WordPress și care deține poziția numărul unu, cu 67% din cota de piață în CMS mondială.



Raport de vulnerabilitate recent de Acunetix arată că aproximativ 8% din vulnerabilități găsite în site-uri sunt legate de WordPress.



15

**2.5. XSS**

Cross Site Scripting (prescurtat XSS) este o vulnerabilitate web ce permite utilizatorului sa introduca un cod personal intr-o pagina web. Acest cod poate afecta ceilalti utilizatori ce vizualizeaza pagina infectata (vulnerabilitate client-side). Aceasta vulnerabilitate este periculoasa doar atunci cand codul se foloseste de prajiturele sau de sesiuni.

16

**Tehnologii**

Framework-ul Angular 2 a fost refacut complet pentru a satisface ultimele cerinte. Acum acest framework este dezvoltat fara a folosi JavaScript, ci limbajul TypeScript – mult mai util in dezvoltarea de aplicatii complexe.  
In cadrul trainingului vom discuta despre framework-ul Angular 2 si cum este folosit pentru a dezvolta aplicatii web enterprise. Cursul include informatii despre limbajele EcmaScript 2015 si TypeScript, baza de date MongoDb, NodeJS server si elementele de baza ale JavaScript packaging. Am inclus si arii ce tin de componente, directive, servicii, pipes, forms, routes dar si libraria RxJS si modul in care poate sa fie utilizata impreuna cu Angular 2. Fiecare arie are exercitii practice pentru ca participantii sa isi consolideze cunostintele.  
  
Mai mult decat atat participantii vor avea oportunitatea de a se familiariza cu utilizarea MongoDB si NodeJS server in dezvoltarea de aplicatii full stack.

17

**3. Concluzii**

În această lucrare am descris tipurile de atac asupra CMS WordPress, cum ar fi XSS și SQL Injection. Am încercat sa fac un test de penetrare asupra unui web-site folosind WPScan, avind posibilitatea de a dobindi parola de utilizator prin metoda brute-force.

Am facut o statistica despre cele mai frecvente atacuri asupra CMS WordPress. Am desenat UML diagrame (Use-Case și Activity) despre XSS atac.

18

**4. Bibliografia**

1. WPScan is a black box WordPress vulnerability scanner. [Regim de access] – https://github.com/wpscanteam/wpscan
2. SQL инъекции. Проверка, взлом, защита [Regim de access] – https://habrahabr.ru/post/130826/
3. 10 шагов для защиты вашего WordPress блога [Regim de access] – https://habrahabr.ru/post/62814/
4. Web Application Exploits [Regim de access] – https://www.exploit-db.com/webapps/
5. WordPress: небезопасен из коробки — получаем RCE с правами редактора. И еще о Google, стартапе и 1 миллиарде долларов [Regim de access] – https://habrahabr.ru/company/dsec/blog/194282/
6. Пентест WordPress своими руками [Regim de access] – https://habrahabr.ru/company/dsec/blog/196858/
7. Пентест WordPress своими руками [Regim de access] – https://habrahabr.ru/post/283210/
8. Vulners — Гугл для хакера. Как устроен лучший поисковик по уязвимостям и как им пользоваться [Regim de access] – https://habrahabr.ru/company/xakep/blog/305262/
9. https://habrahabr.ru/post/213783/ [Regim de access] – https://habrahabr.ru/company/xakep/blog/305262/

19