

**Fakulteti i Inxhinierisë Elektrike dhe Kompjuterike**

**Universiteti i Prishtinës**

**WPScan**

Detyra 2 – Vulnerability Analysis, Siguria e Rrjetave

**Agon Hoxha**

**Përmbajtja**

[**Hyrje** 2](#_Toc532165809)

[**Përdorimi** 2](#_Toc532165810)

[**Eksperimentet** 3](#_Toc532165811)

[1. Telegrafi.com 3](#_Toc532165812)

[2. Filma24hd.cc 4](#_Toc532165813)

[3. Podujevapress.com 5](#_Toc532165814)

[4. Kutia.net 6](#_Toc532165815)

[5. Rtv21.tv 7](#_Toc532165816)

[6. Kpopmp3.net 8](#_Toc532165817)

[**Përfundimi** 9](#_Toc532165818)

[**Referencat** 9](#_Toc532165819)

**Figurat**

[Figura 1. Logoja e WPScan 2](file:///C:\Users\agoni\Desktop\NS-G13-2.docx#_Toc532165820)

[Figura 2. Lista e plugins 3](file:///C:\Users\agoni\Desktop\NS-G13-2.docx#_Toc532165821)

[Figura 3. Një nga vulnerable themes 3](file:///C:\Users\agoni\Desktop\NS-G13-2.docx#_Toc532165822)

[Figura 4. Theme aktualisht në përdorim 3](file:///C:\Users\agoni\Desktop\NS-G13-2.docx#_Toc532165823)

[Figura 5. Detajet e skanimit dhe resurseve të përdorura 3](file:///C:\Users\agoni\Desktop\NS-G13-2.docx#_Toc532165824)

[Figura 6. Përdoruesit e identifikuar 4](file:///C:\Users\agoni\Desktop\NS-G13-2.docx#_Toc532165825)

[Figura 7. Tentimi për brute-force attack 4](file:///C:\Users\agoni\Desktop\NS-G13-2.docx#_Toc532165826)

[Figura 8. Vulnerable Plugin në podujevapress.com 5](file:///C:\Users\agoni\Desktop\NS-G13-2.docx#_Toc532165827)

[Figura 9. Informata rreth vulnerability të gjetur 5](file:///C:\Users\agoni\Desktop\NS-G13-2.docx#_Toc532165828)

[Figura 10. Plugini vulnerable wordpress-seo në kutia.nët 6](file:///C:\Users\agoni\Desktop\NS-G13-2.docx#_Toc532165829)

[Figura 11. Përdoruesit në kutia.nët 6](file:///C:\Users\agoni\Desktop\NS-G13-2.docx#_Toc532165830)

[Figura 12. Vulnerabilities në krahasim me versionin aktual 7](file:///C:\Users\agoni\Desktop\NS-G13-2.docx#_Toc532165831)

[Figura 13.Plugin vulnerable gjithashtu i gjetur 7](file:///C:\Users\agoni\Desktop\NS-G13-2.docx#_Toc532165832)

[Figura 14. Dy vulnerable plugins në kpopmp3.net 8](file:///C:\Users\agoni\Desktop\NS-G13-2.docx#_Toc532165833)

[Figura 15. Një plugin me 10 vulnerabilities të ndryshme 8](file:///C:\Users\agoni\Desktop\NS-G13-2.docx#_Toc532165834)

# **Hyrje**

 WPScan (shkurt për WordPress Scan) është vegël e përfshirë në Kali Linux e bërë veqanërisht për gjetje të vulnerabilities të faqëve të konstruktuara me anë të WordPress. Pasi që WordPress është CMS (Contënt Management Systëm) më i përdorur në botë, na jep të kuptojmë se është vegël që ka aplikim tëjet të madh.

Figura 1. Logoja e WPScan

Gjersa funksioni primar është gjetja e vulnerabilities, paraqitja e detajeve rreth tyre, të dhëna ndihmëse, dhe linqë relevantë, skanimi nuk është e vetmja gjë që mund të bëj. WPScan ka mundësi të përdoret edhe për brute-force sulme. Pra, gjersa është vegël për analiz dhe skanim, është gjithashtu edhe vegël sulmi. Idealisht, do duhej të përdorej që faqet që ne i bëjmë të sigurohemi se janë të sigurta, mund të përdoret edhe për qëllime jo aq të mira, si tentim të marrjes nën kontroll të faqës.

Krijuar nga ethicalhack3r, erwan\_lr dhe FireFart, dhe sponzorizuar nga sucari.net, në gjuhën programuese Ruby, dhe me cURL si bazë, që është njëkohësisht librari dhe vegël për transferim të të dhënave me anë të protokoleve të ndryshme (FILE, FTP, FTPS, HTTP, HTTPS, IMAP, IMAPS, etj). Funksionon në qdo sistëm opërativ në të cilin funksionojn programet e gjuhës programuese Ruby, që do të thotë se përpos që funksionon në Windows, MacOS, po ashtu edhe në shumicën e distribucionëve të Linux.

Në vazhdim, do të tregojmë rreth përdorimit të kësaj vegle, si dhe të shfaqim disa ekspërimente. Nga to, do mund të arrijme në një konkluzion rreth vyeshmërisë dhe përdoshmërisë të kësaj vegle.

# **Përdorimi**

Gjersa WPScan mund të përdoret në shumicen e sistëmeve opërative modernë, përdorimi do fokusohet në Kali Linux. E cekim ketë pasi që komandat ndryshojnë paksa ndërmjet sistëmeve të ndryshme.

Struktura e komandave për WPScan ngjan me shumë vegla tjera në përdorim:  
**wpscan [--specifikimet] [vlerat]**. Dy specifikimet me të rëndësishme dhe përdorura është **--url** vlerë e të cilës është linku i faqës që dëshirojmë të e analizojmë, dhe **--enumerate** vlerë e të ciles është se qka dëshirojmë të analizojmë. Vlerat më të zakonshme të përdorura të enumerate janë:

1. **vp** (për analizim të vulnerable plugins),
2. **vt** (për analizim të vulnerable themes), dhe
3. **u** (për analizim të përdorueseve).

Pra një komande legjitime do ishtë **wpscan --url telegrafi.com --enumerate vt,vp,u**. Do e skanoj faqën telegrafi.com dhe do tentoj të gjej plugins dhe themes që janë vulnerable, si dhe do tentoj të gjej përdoruesit. Përdoruesit gjenden prej RSS feed, si dhe prej listës të përdorueseve të ruajtur.

Specifikim tjetër ndër më të zakonshem për përdorim është ai që na mundëson tëntimin për qasje në websitë përmes brute-force sulmeve: **--passwords** [lokacioni i listës të passwordeve]. Shembull,  
**wpscan --url telegrafi.com --passwords /root/pass.txt**. Mund të përdoret edhe specifikimi **-U** me **–passwords** që të limitohet tentimi i brute-force sulmit në vetëm një përdorues, që do dukej si: **wpscan --url telegrafi.com --passwords /root/pass.txt -U admin**. Me këtë komand do fokusohemi vetëm në tentim qasje në përdoruesin e admin të faqës. Mund të specifikojmë edhe disa përdorues. Përndryshe, nëse nuk specifikohet përdoruesi, listën e fjalëkalimeve do tëntoj t’e aplikoj në tërë listën e përdoruesëve.

# **Eksperimentet**

## Telegrafi.com

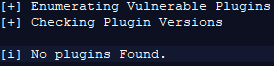
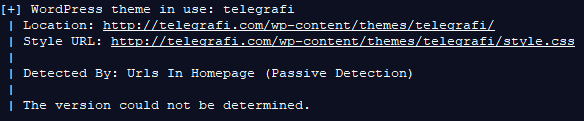
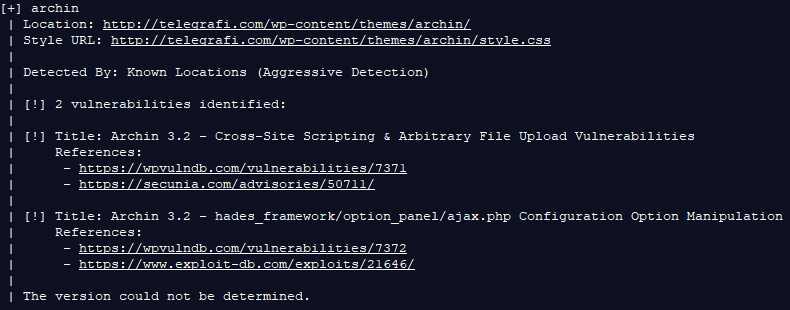
Në ketë rast, ekzekutojmë **wpscan --url telegrafi.com --enumerate vp,vt**.  
Pas ekzekutimit, fillon analiza që mund të zgjas disa sekonda deri disa minuta, varsisht prej shpejtësisë tonë të internetit. Në rast të faqës telegrafi, na shfaqet theme që janë duke e përdorur – në ketë rast, theme e bërë veqanërisht, me emrin ‘telegrafi’. Gjen se nuk ka asnjë vulnerable plugin – në fakt, nuk ka asnjë plugin të WordPress në përdorim. Gjithashtu tenton të gjej edhe themes që i ka të ruajtura.

Figura 2. Lista e plugins

Në rast të telegrafi, i kanë të ruajtura një numër tejet të madh të themes – 288 të tilla. Prej të cilave, qdo njëra konsiderohet si vulnerable, dhe figuron si 1, apo me shumë, vulnerabilities.

Figura 3. Një nga vulnerable themes

Figura 4. Theme aktualisht në përdorim

Mirëpo, kjo është një mori të rastëve false-positive. Edhe pse si rezultat në bazë të WPScan, mund të konkludojmë se kjo faqë ka mbi 288 vulnerabilities, ai konkludim në fakt nuk do ishte i saktë ngase nuk ka asnjë vulnerability. Një theme duhet të jetë në përdorim që të mund të e shfrytëzojme në ndonjë mënyrë atë vulnerability. Asnjë nga këto vulnerable themes nuk është në përdorim, ngase theme në shfrytëzim është theme e tyre.

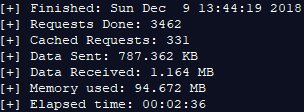
Në fund të skanimit, na njofton rreth kohes që i është duhur për të e kryer, numrin e kerkesave të dërguara, trafikun (dërgim dhe pranim), si dhe sasinë e memories tonë të përdorur. Pavarësisht prej 288 “vulnerabilities”, faqja mund të konsiderohet si e sigurtë.

Figura 5. Detajet e skanimit dhe resurseve të përdorura

## Filma24hd.cc

Ndryshe nga telegrafi.com, këtu do shfrytëzojmë edhe enumerimin tjetër – të shohim se kush janë përdoruesit, kush ka qasje për ndryshim të faqës. Për t’e arritur ketë, komanda merr formën **wpscan --url filma24hd.cc --enumerate vp,vt,u**.

Në rezultat, vërejmë se ngjajshëm si telegrafi, ka një theme paksa të specializuar me emrin filma2 dhe jo një nga default themes që vin se bashku me WordPress. Ndryshe nga telegrafi, ka plugins të WordPress në përdorim, por asnjë që është vulnerable.

 Tani, vjen pjesa që ndryshon – kemi një list të përdorueseve.

Përdoruesit me gjasa janë:

* filma24hd
* filma12admin
* The0c

Kurse tjerat janë false-positives të fituara për shkak se janë marrur nga RSS feed. Në anën tjetër, Xhoni Ferizaj mund të jetë një person që ka qasje si postues, apo është emri i vertetë i ndonjërit prej përdorueseve të cekur. False positive e quditme është emri i filmit Keep Watching që shfaqët si emër përdoruesi.

Figura 6. Përdoruesit e identifikuar

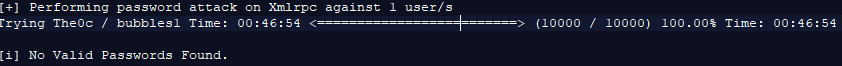
Me **wpscan --url filma24hd.cc --passwords /root/10.txt -U The0c**, tentojmë të bëjmë brute-force përdoruesin The0c. 10.txt është një file që përmban 10,000 fjalekalimet më të zakonshme në botë. Mirëpo pasi që kjo list është e fokusuar në gjuhën Angleze, ajo nuk ka mjaftueshëm efekt për gjuhën Shqipe, dhe sulmi jonë deshton pas 10,000 tentimeve për fjalëkalime të ndryshme.

Figura 7. Tentimi për brute-force attack

Siq do pritej, pasi që është duhur të tëntohen 10,000 fjalëkalime të ndryshme, është duhur gati një orë që të përfundoj sulmi. Mirëpo, ishte pa sukses.

Gjersa nuk ka vulnerable plugins, apo vulnerable themes, nuk mund të themi se është faqja e sigurtë pasi që nuk ka kurrfare mekanizëm kundër brute-force, si do ishtë ndonjë CloudFlare mbrojtje që do ndalte tentimet. Në të njëjtën kohë, gjersa brute-force është e vetmja mundesi për tentime sulmi, siguria e faqës është në nivel po thuajse të mjaftueshëm.

## Podujevapress.com

Figura 8. Vulnerable Plugin në podujevapress.com

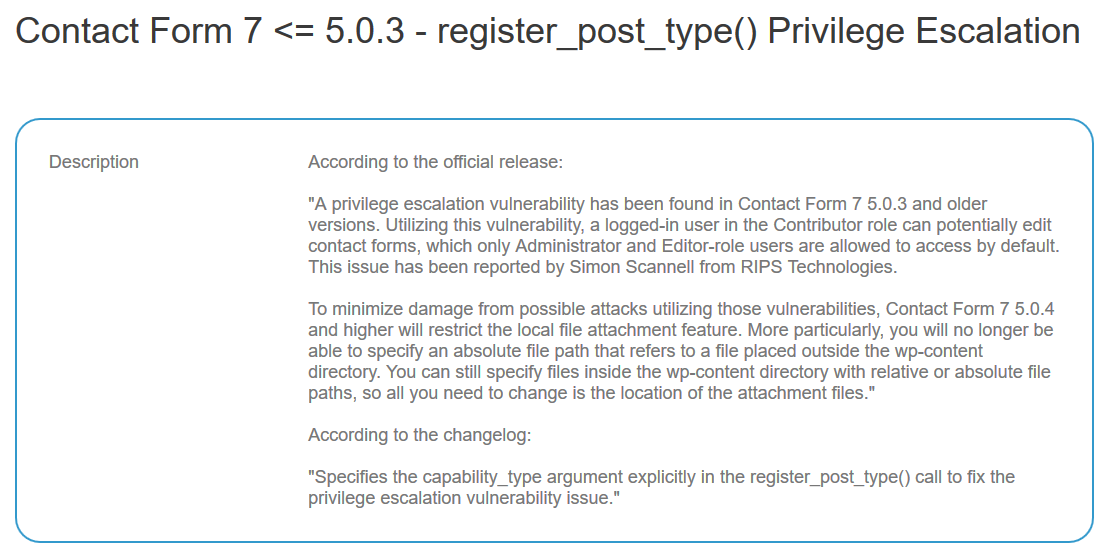
Do vazhdojmë me një faqë që ka një vulnerability në plugin që e përdorë. Me anë të komandës, **wpscan --url podujevapress.com –enumerate vt,vp,u**, gjejmë plugins dhe themes që janë vulnerable, si dhe përdoruesit, siq është cekur më herët. Podujevapress.com shihet se ka një plugin, contact-form-7, që është me version më të ulët (5.0.2) se sa versioni i tanishëm (5.0.5), dhe si i tillë, ka disa vrima në siguri që lejojn eskalim të priviligjeve. Sapo që vegla të gjejë një plugin që është vulnerable, na jep linqe me informata rreth asaj vulnerability.

Figura 9. Informata rreth vulnerability të gjetur

## Kutia.net

Kutia.net është një rast që duhet t’i kushtojmë paksa me shumë vëmendje. Ky website i përketë një kompanie që shërben si WordPress Consulting – krijojnë dhe mirëmbajnë faqe që konstruktohen me WordPress. Do pritej që kjo faqë të jetë komplet me versionet e fundit, dhe pa asnjë vulnerability, mirëpo... kjo nuk është se qka është gjetur.

Ngjajshëm me podujevapress.com, contact-form-7 është version me i vjetër se sa ai aktual, dhe në fakt edhe me i vjetër se sa versioni prezent në Podujevapress.com.

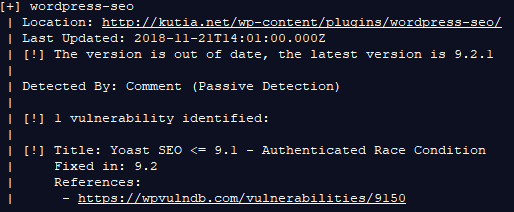
Ngjajshem me rtv21.tv, wordpress-seo është version me i vjetër. Në kutia.nët është prezent wordpress-seo versioni 7.6.1, kurse ai aktual është 9.2.1. Me vonë, në eksperimentin e fundit (faqja kpopmp3.net), do diskutohet rreth kësaj – është një plugin vulnerable me emrin wp-super-cache. Gjersa versioni i fundit i wp-super-cache është 1.6.4, versioni prezent në ketë faqë është me i ulët se 1.3. Kjo është në fakt tejet qështje serioze, siq do shpjegohet më vonë.

Figura 10. Plugini vulnerable wordpress-seo në kutia.nët

Kjo është një shenjë jo e mirë për qfarëdo konsumatori që më parë do dëshironte t’e dinte se sa mund të ju besohet kompanisë në fjale. Nëse faqja e tyre nuk është mjaftueshëm e sigurtë, atëherë një konsumator do ishte me drejtë i brengosur për të i kontraktuar kompaninë e tillë që t’ia bëjnë një faqë me WordPress. Në vend që të ishtë një ndër faqët me të sigurta, me më se pakti, apo fare vulnerability, ka një numer të madh të tyre (12), dhe mjaft serioze.

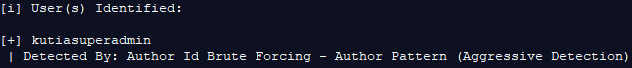
Gjithashtu edhe mund të gjejmë emrat e përdorueseve që kanë qasje për postim, apo kontroll mbi këtë faqë. Prap, një gjë e tillë do mund të pamundësohej, dhe një kompani që pretendon të jetë eksperte rreth qështjeve të WordPress nuk do duhej të kishtë asnjë vrime të tillë në siguri. Vlen të ceket se edhe gjatë testimit për brute-force sulme, nuk kishte ndonjë gjë që pengonte sulmin, sikur që është hasur në disa faqë tjera me siguri më të lartë.

Figura 11. Përdoruesit në kutia.nët

## Rtv21.tv

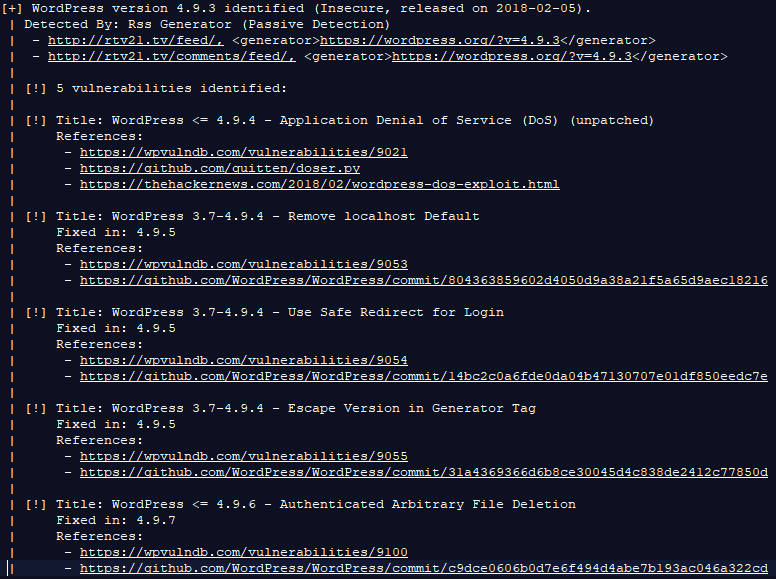
Gjetjet në rtv21.tv dallojnë paksa nga gjetjet e mëparshme. Si edhe në rastet paraprake, kemi plugins që janë vulnerable, dhe kemi arritur të gjejmë usernames të personave që kanë qasje për postim apo menaxhim, mirëpo është gjetur edhe diqka shumë më alarmante.

Figura 12. Vulnerabilities në krahasim me versionin aktual

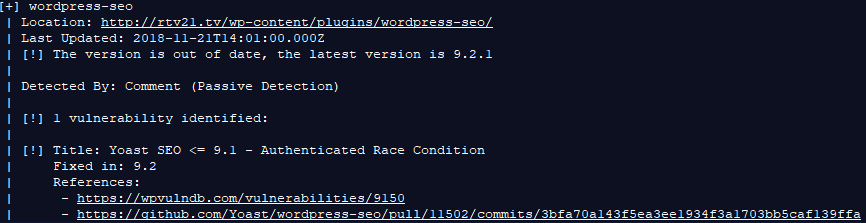
 Versioni i WordPress në përdorim në këtë faqë, është i vjetër për përafersisht 10 muaj. Në përdorim është versioni 4.9.3, gjersa versioni i tanishëm është 4.9.8 apo së fundi, është si kandidat për lansim versioni 5.0. Versioni i tillë, në krahasim me versionin e fundit, i ka pesë vulnerabilities të ndryshme.

Figura 13.Plugin vulnerable gjithashtu i gjetur

Me më pak rëndësi, por gjithashtu tejet serioz, është po një plugin që është gjetur se është vulnerable. Fjala është për wordpress-seo, që ngjajshëm me komplet WordPress në ketë faqe, është version i vjetër në krahasim me atë aktual. Pasi që informohemi nga linqet referencuese, e shohim se kjo vulnerability do mundësonte eskalim të privilegjeve – më saktësisht, personat që janë në rol si SEO Manager, mund të arrijnë të marrin privilegjet e njëjta si përdoruesi admin. Pra, gjersa dikush është vetëm i autorizuar të rregulloj paksa kërkimet dhe rezultatet e atyre kërkimeve, do jetë në gjendje që të e bëj vetvetën administrator të faqës.

Kjo jo vetëm që do mund të bëhej potencialisht problem intern i kompanisë, është qështje që e zgjeron listën e caqëve sulmuese. Le të kemi një sulmues që dëshiron të arrij kontroll mbi tërë faqën. Në rast të tille, zakonisht do interesohej më së shumti në përdoruesin admin. Përdoruesit e tjerë do i interesonin, por krahasuar me përdoruesin admin, rëndësia e tyre do ishtë shumë më e vogël. Përdoruesit e tjerë kanë qasje të limituar dhe nuk do mund t’i siguronin kontroll total mbi faqën. Mirëpo, për shkak të kesaj vulnerability, sulmuesi do e dinte që qdo person që ka rolin e SEO Manager do mund t’i siguronte ekuivalentë qasje me përdoruesin admin dhe kështu, rritet numri i caqëve të mundshme që mund të arrinin në të njëjtin rezultat. Për sulmuesin, gjasat për sukses rritën, sidomos kur SEO nuk do kenë të njetën mbrojtje sikur admin.

## Kpopmp3.net

Faqe jo Shqiptare, apo me përdorim të madh. Vetëm është marrur si shembull i një faqeje me një mori të vulnerabilities të ndryshme, apo si shembull i një gjendje tejet të keqe të një faqeje.

Siq shihet nga përshkrimi i vulnerabilities, dhe pas konsultimit me referencat e cekura, e shohim se shumica e tyre kanë të bëjnë me cross-site scripting (XSS) sulme.

Figura 14. Dy vulnerable plugins në kpopmp3.net

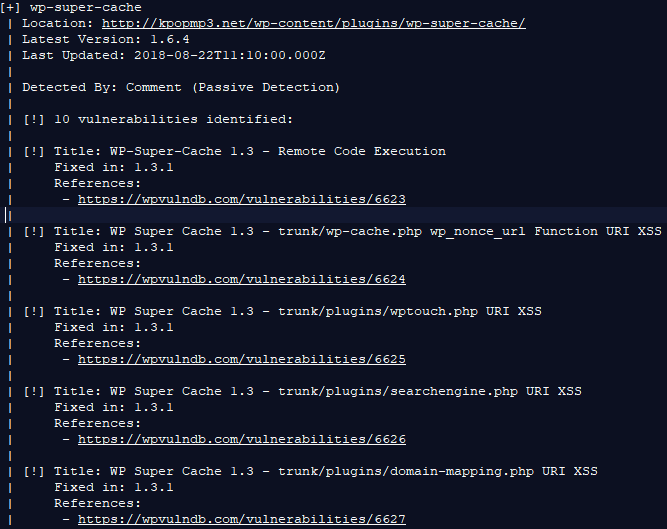
Gjithashtu ka disa që janë në lidhje me insertim të objektëve, dhe thuajse më së keqi, për ekzekutim të kodit nga distanca. Kjo faqe lirisht mund të konsiderohet totalisht e pasigurtë, dhe me nevoj të madhe për përditësim. Nga ana tjetër, mjaftojnë 3 përditësime të vogla, që të rregullohen 12 vulnerabilities mjaft serioze dhe të arrihet një gjendje e sigurtë.

Figura 15. Një plugin me 10 vulnerabilities të ndryshme

# **Përfundimi**

Pa dyshim, është një vegël që na ndihmon në caktimin e planeve dhe sulmeve të ardhshme, mirëpo edhe pse është vegël për analize të vulnerabilities, ngjan shumë me veglat për information gathering. Gjithashtu, në të njëjtën kohe, mund të përdoret për sulme të thjeshta të brute-force, pra ngjan edhe me vegël për sulme të web applications.

Këto gjëra janë qka e veqojnë dhe e rrisin përdorimin e kësaj vegle, sidomos në një epok të webit ku shumica e websitëve krijohen si të gatshme me anë të WordPress, dhe jo manualisht. Kjo ka anën pozitive të lehtësisë, por edhe anën negative të vulnerabilities të mundshme. WordPress është mjaft e mirëmbajtur nga një komunitet tejet i madh dhe ka siguri të mjaftueshme, mirëpo siq është parë shumë herë në këtë dokument, ky nivel i sigurisë mund të pritet vetëm dhe vetëm nëse qdo gjë në lidhje me WordPress është në versionin e fundit, duke përfshire plugins, themes dhe gjithsesi, vet WordPress. Qdo gjësend që mbetët pa u bërë update, paraqet vektore sulmi.

Një gjë që nuk është shfaqur mjaft përgjatë këtij dokumenti është mundësia e WPScan për të bërë brute-force sulme për qasje. Kjo është për arsye se të gjitha kanë dështuar, dhe nuk kanë pasur ndonjë rezultat të veqant që vlen të përmendet. Arsyeja se pse ka dështuar mund të jetë e llojllojshme. Personalisht, mendoj që është për shkak të listës të fjalëkalimeve që është përdorur. Gjatë sulmeve, është përdorur lista e 10,000 fjalekalimeve më të zakonshme. Mirëpo shumica e fjalëve në atë list janë të bazuara në fjale të gjuhës Angleze, kurse këtu është tentuar të sulmohen faqe ku fjalëkalimi caktohet nga njërez që përdorin ndoshta ekskluzivisht gjuhën Shqipe.

Besoj që ka nevoj për një list të tillë me fjalëkalime të zakonshme të bazuara në gjuhën Shqipe – mendoj se do ishtë ndihmë e pentesters Shqiptar dhe do kishim një vlersim shumë me realist të gjendjes të sigurisë në faqet Shqiptare.

# **Referencat**

<https://wpvulndb.com/> - Databaza përshkruese për qdo vulnerability të gjetur deri me sot në lidhje me wordpress

[https://github.com/wpscantëam/wpscan/](https://github.com/wpscanteam/wpscan/) - GitHub faqja e projektit të WPScan

<https://wpscan.org/> - Website i WPScan

<https://wordpress.org/> - Faqja e WordPress

<https://github.com/danielmiessler/SecLists/> - Lista të fjalekalimeve më të përdorura