

**Sigurnosni rizici**  
***Wordpress CMS-a***

CERT.hr-PUBDOC-2021-6-402

## Sadržaj

<b>1</b>	<b>UVOD</b> .....	<b>3</b>
<b>2</b>	<b>SIGURNA INSTALACIJA I KONFIGURACIJA WORDPRESSA</b> .....	<b>4</b>
<b>3</b>	<b>SIGURNO KORIŠTENJE WORDPRESSA</b> .....	<b>9</b>
3.1	REDOVITO AŽURIRANJE <i>WORDPRESSA</i> I POVEZANOG SOFTVERA .....	9
3.2	OTEŽAVANJE/ONEMOGUČAVANJE NAPADA NA KORISNIČKE RAČUNE .....	10
3.2.1	<i>Oprezno dodjeljivanje uloga korisnicima</i> .....	11
3.2.2	<i>Prisiljavanje korisnika na postavljanje sigurne lozinke</i> .....	12
3.2.3	<i>Skrivanje stranice s obrascem za prijavu</i> .....	14
3.2.4	<i>Dvofaktorska autentifikacija</i> .....	14
3.3	SIGURNOST TEMA I DODATAKA .....	15
3.4	FAIL2BAN.....	22
3.5	ZAPISIVANJE AKTIVNOSTI U DNEVNIKE .....	23
3.6	PRIČUVNE KOPIJE .....	24
<b>4</b>	<b>ZAKLJUČAK</b> .....	<b>27</b>
<b>5</b>	<b>LITERATURA</b> .....	<b>29</b>

Ovaj dokument izradio je Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Ovaj dokument vlasništvo je Nacionalnog CERT-a. Namijenjen je javnoj objavi te se svatko smije njime koristiti i na njega se pozivati, ali isključivo u izvornom obliku, bez izmjena, uz obvezno navođenje izvora podataka. Korištenje ovog dokumenta protivno gornjim navodima povreda je autorskih prava CARNET-a, a sve navedeno u skladu je sa zakonskim odredbama Republike Hrvatske.

# 1 Uvod

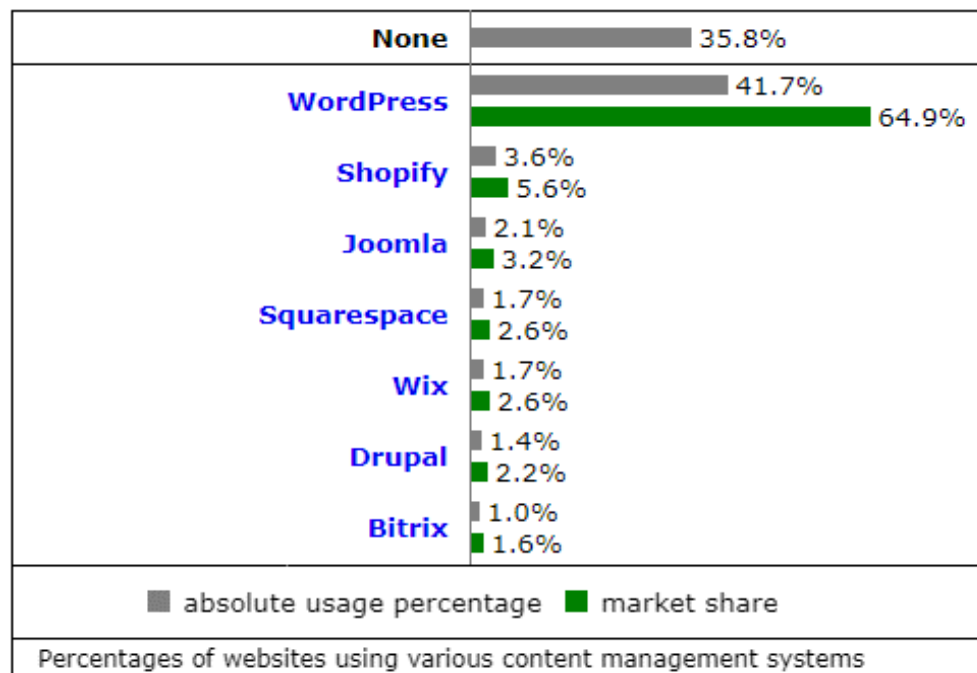
*Wordpress* je već dugo vremena najpopularniji sustav za upravljanje sadržajem (engl. *Content Management System, CMS*) na *webu*.

Karakteristike ovakvih sustava su da svojim korisnicima omogućavaju vrlo jednostavnu i brzu izradu *web* stranica i aplikacija – korisnik ne mora ovladati znanjima o tehnologijama potrebnim za izradu *web* stranice, već na jednostavnom grafičkom sučelju slaže grafičke elemente i unosi sadržaj koji želi prikazati. *Wordpress* zatim u pozadini pretvara uneseni sadržaj i odabrani dizajn stranice u HTML/CSS/JS/PHP kôd.

Čak i onaj tko nikad nije napisao niti jednu liniju HTML kôda (koji je osnova svake *web* stranice) moći će razviti i održavati stranicu izrađenu u *Wordpressu*.

Ovakvi sustavi znatno su povećali dostupnost izrade *web* stranica pojedincima i poduzećima – odjednom je svatko mogao brzo i besplatno izraditi blog ili jednostavnu *web* stranicu. Iako je nastao kao alat za blogove, već neko vrijeme je moguće izraditi i naprednije *web* aplikacije poput *online* trgovine (engl. *webshop*), *news* portala, foruma i sl.

Kao što je prikazano na slici 1, istraživanje tvrtke *W3Techs* pokazalo je da je 41.7% stranica na *webu* izrađeno u *Wordpressu* što ga čini najčešće korištenim sustavom za upravljanje sadržajem (1).



Slika 1 *Wordpress* je najkorišteniji CMS (1)

Upravo zbog svoje široke dostupnosti, *WordPress* je u zadnje vrijeme česta meta napadača i povezuje ga se s ozbiljnim napadima koji imaju drastične posljedice poput udaljenog izvršavanja kôda, otkrivanja korisničkih računa ili šifriranja poslužitelja (2) (3) (4) (5). Svrha ovog dokumenta upoznati je korisnike, prvenstveno administratore *WordPress* stranica, o najčešćim prijetnjama, napadima i mehanizmima zaštite.

## 2 Sigurna instalacija i konfiguracija *WordPressa*

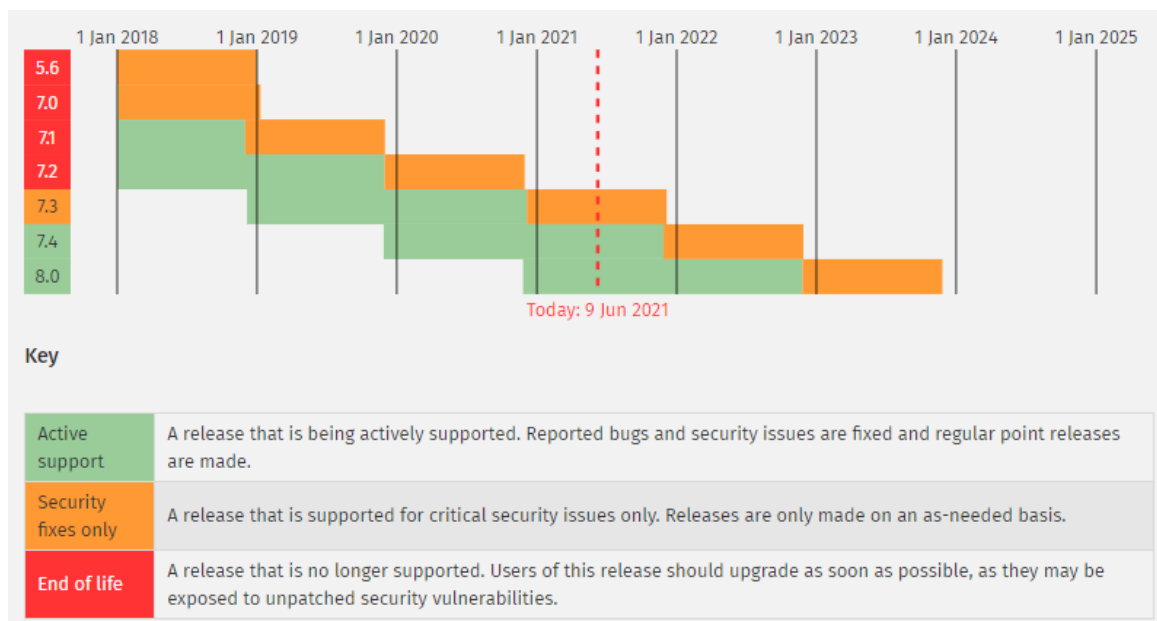
Ispravna instalacija, konfiguracija i korištenje *WordPressa* preduvjet su za minimiziranje sigurnosnih rizika i opisani su u nastavku ovog dokumenta.

Instalacija *WordPressa* vrlo je jednostavna, ali preduvjet je imati:

- instaliran, ažuriran i sigurno konfiguriran poslužiteljski softver *NGINX* ili *Apache HTTP* (više detalja o sigurnoj konfiguraciji dostupno je u dokumentu Nacionalnog CERT-a [Apache HTTP poslužitelji](#))
- instaliranu ažuriranu verziju programskog jezika PHP i
- instaliran ažurirani sustav za upravljanje bazama podataka *MySQL* ili *MariaDB*.

*Wordpress* će podržati rad i s neažuriranim/starijim inačicama nabrojanog softvera, ali to se nikako ne preporuča iz sigurnosnih razloga. Naime, nijedan softver nije savršen, već sadrži pogreške u kôdu koje mogu biti sigurnosne ranjivosti kojih ni proizvođač u trenutku objavljivanja softvera nije svjestan. Svako novo ažuriranje softvera poboljšanje je prethodnog kôda ispravljanjem tih pogrešaka i zato je bitno redovito ažurirati softver.

Dodano, bitno je pratiti pruža li proizvođač softvera održavanje, jer se inače ne može računati na sigurnosne zakrpe. Promotrimo na primjeru zašto ne bismo smjeli koristiti inačicu programskog skriptnog jezika PHP stariju od 7.3:



Slika 2 Podrška za razne verzije PHP programskog skriptnog jezika (6)

Na službenoj stranici PHP-a navedeno je da inačice 7.2, 7.1, 7.0 i 5.6 više nisu podržane i da se za njih više neće objavljivati sigurnosne zakrpe. Iako će *WordPress* podržavati korištenje PHP 7.2., treba izbjeći njegovo korištenje i čim prije se prebaciti na neku podržanu inačicu.

Instalacija će se demonstrirati na *Linux* distribuciji *Debian 10 (Buster)*, što će skupa s ostatkom potrebnog softvera činiti snažnu i popularnu LAMP arhitekturu (*Linux + Apache + MariaDB/MySQL + PHP*).

Kad je riječ o sigurnoj instalaciji softvera, obično je preporučeni način instalacije iz službenog repozitorija korištene *Linux* distribucije. Na taj način možemo biti sigurni da smo preuzeli ispravan softver iz pouzdanog izvora, a olakšano je i njegovo redovito ažuriranje.

**Neovisno o načinu instalacije *Wordpressa* i ostalog potrebnog softvera, administrator mora preuzeti odgovornost za redovito ažuriranje dostupnim sigurnosnim zakrpama (engl. *security patches*).**

Poslužiteljski softver *Apache* iz službenog repozitorija instalira se naredbama:

```
$ sudo apt update
```

```
$ sudo apt install apache2
```

Nakon toga se provjerava status i, ako *Apache* nije već automatski pokrenut, pokreće:

```
$ sudo systemctl status apache2
```

```
$ sudo systemctl start apache2
```

Tradicionalno je dio LAMP arhitekture sustav za upravljanje bazama podataka (engl. *Database Management System*) bio *MySQL*, ali u zadnje vrijeme neke distribucije *Linuxa* (poput *Debian 10*) i softversko okruženje XAMPP su se prebacile na njegovu kompatibilnu alternativu otvorenog kôda naziva *MariaDB*.

*MariaDB* je nastala od posljednje dostupne inačice otvorenog kôda *MySQL*-a (prije no što je njegov vlasnik postala tvrtka *Oracle*) i nastavila se razvijati kao zaseban proizvod. Iza njenog održavanja stoji zajednica kojoj se svatko može priključiti, tzv. *MariaDB Foundation*. Na taj način nastavljen je njegovanje ideje slobodnog i otvorenog softvera kojem svatko može pridonijeti, što je *MySQL* prestao biti jer, iako je i dalje besplatan, na njegovom razvoju sad isključivo radi tvrtka *Oracle*.

*MariaDB* instalira se naredbom:

```
$ sudo apt install mariadb-server
```

Činjenica da se *Debian* prebacio na korištenje *MariaDB* umjesto *MySQL* znači da će se *MariaDB* podrazumijevano instalirati kao sustav za upravljanje bazama podataka čak i ako se unese naredba za instalaciju *MySQL*-a:

```
$ sudo apt install mysql-server
```

*MySQL* i *MariaDB* su kompatibilni, koriste istu definiciju tablica i jedan se lako može zamijeniti drugim. Naravno, i dalje se može inzistirati na preuzimanju *MySQL*-a ako su potrebne neke njegove karakteristične funkcionalnosti.

Nakon što se instalira *MariaDB*, potrebno je poduzeti sljedeće korake kako bi se *WordPress* sigurnosno ojačao:

- ukloniti korisnika *anonymous*
- onemogućiti udaljenu prijavu za korisnika *root*
- ukloniti testnu bazu podataka naziva *test*
- ponovno učitati tablicu s informacijama o privilegijama

Na *Linux* distribucijama dostupna je skripta `mysql_secure_installation/mariadb-secure-installation` koja će automatizirano obaviti sve ovdje navedene korake i sigurno instalirati sustav za upravljanje bazama podataka *MySQL*, odnosno *MariaDB*.

Potrebno je instalirati i PHP programski jezik koji će se izvršavati na poslužitelju. Kako bi *Wordpress* uspješno funkcionirao, potrebno je, uz PHP, instalirati i još neke dodatne softverske pakete usko vezane uz PHP, takozvane ekstenzije. Npr. kako bi PHP mogao komunicirati s *MySQL/MariaDB* bazom podataka, potrebno je instalirati ekstenziju naziva `php-mysql`. Sljedećom naredbom instalirat će se svi nužni PHP softverski paketi potrebni za instalaciju i korištenje *Wordpressa*:

```
$ sudo apt install php php-mysql php-curl php-gd php-mbstring php-xml php-xmlrpc libapache2-mod-php
```

I na kraju, slijedi instalacija samog *Wordpressa*. Prije instalacije, poželjno je još jednom ponovno pokrenuti poslužiteljski softver *Apache* kako bismo bili sigurni da su sve promjene primijenjene.

Iako se može preuzeti i instalirati sa službenog repozitorija većine *Linux* distribucija, za demonstraciju ćemo prikazati instalaciju preuzimanjem arhive sa svim potrebnim datotekama za instalaciju.

Nakon što se pozicioniramo u korijensku *web* mapu `/var/www/html/`, unosimo naredbu koja će u nju preuzeti instalacijske datoteke:

```
$ sudo curl -O https://wordpress.org/latest.tar.gz
```

Preuzimanje naredbom `curl` ekvivalentno je tome da smo u *web* pregledniku posjetili navedenu *web* stranicu i preuzeli arhivu. Arhiva se zatim raspakira naredbom:

```
$ sudo tar -xvf latest.tar.gz
```

To će rezultirati novom mapom naziva *wordpress* u koju će biti raspakirane sve konfiguracijske datoteke.

Vlasništvo nad *wordpress* mapom treba dodijeliti karakterističnom korisniku `www-data` pod kojim je pokrenut i HTTP poslužiteljski softver:

```
$ sudo chown -R www-data:www-data /var/www/html/wordpress
```

Iz sigurnosnih je razloga korisno i pažljivo dodijeliti dopuštenja nad mapama i datotekama koja se nalaze u mapi *wordpress*. Primjer pametne dodjele minimuma potrebnih dopuštenja bio bi:

```
$ sudo find /var/www/html/wordpress/ -type d -exec chmod 750 {} \;
```

```
$ sudo find /var/www/html/wordpress/ -type f -exec chmod 640 {} \;
```

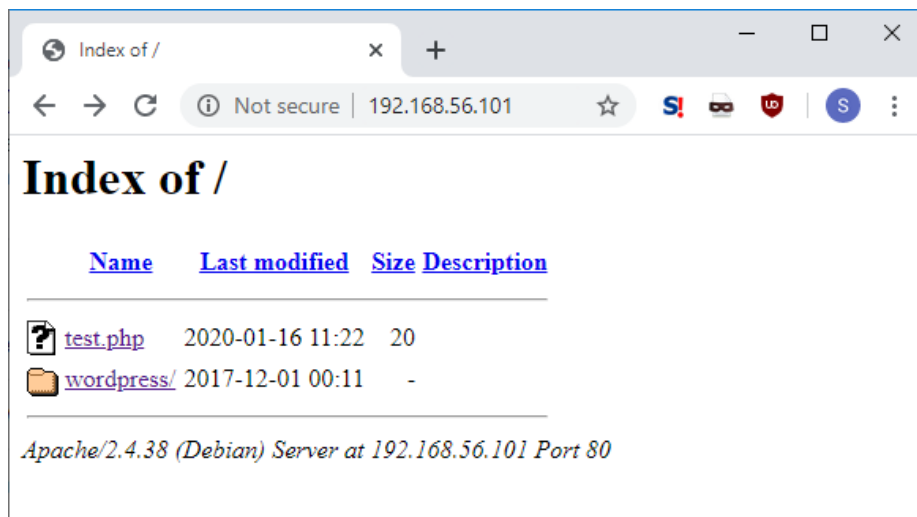
U navedenom primjeru korisnik *www-data* (koji je vlasnik mape *wordpress*) moći će pristupiti mapi *wordpress* i svim mapama unutar nje, izlistati sadržaj svake mape i preimenovati, brisati ili dodavati datoteke i direktorije u svakoj mapi. Grupa kojoj se dodijeli pravo nad mapom *wordpress* moći će samo pristupati mapama i gledati njihov sadržaj. Nijedan drugi korisnik (izuzev navedenih) nema nikakvo dopuštenje nad mapom, tj. neće im moći pristupiti.

Isto tako, kad su u pitanju datoteke, korisnik *www-data* moći će čitati i pisati u (konfiguracijske) datoteke koje se nalaze unutar mape *wordpress*, ali ih neće moći izvršiti. Grupa kojoj su dodijeljena prava nad mapom *wordpress* moći će čitati datoteke, a nitko drugi neće imati pravo pristupa datotekama.

Prije instalacije *Wordpressa*, ponovno pokrećemo *Apache*:

```
$ sudo systemctl restart apache2
```

*Wordpress* se zatim instalira putem *web* preglednika. Unosimo IP adresu ili domenu poslužitelja (ako smo instalirali *Wordpress* na isto računalo s kojega mu pristupamo, to je *localhost*). Vidljiv je izlistan sadržaj mape *var/www/html* koja je korijenski *web* direktorij. U konfiguracijskim postavkama *Apache* poslužitelja može se definirati da korijenski *web* direktorij bude *var/www/html/wordpress* i tad bismo odmah (čim bismo pristupili poslužitelju) započeli s instalacijom *Wordpressa*. U ovom slučaju prvo ćemo morati odabrati mapu *wordpress* koja je prikazana na slici 3.



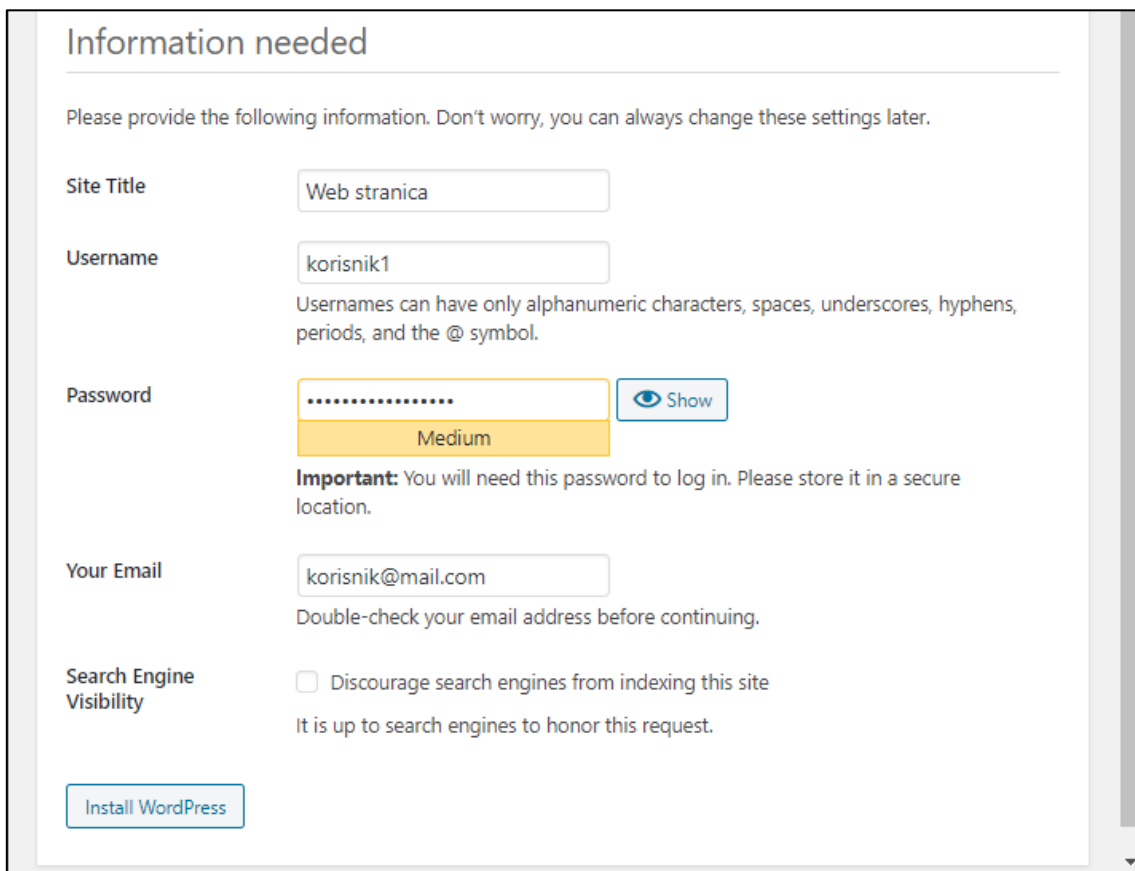
Slika 3 Sadržaj korijenskog *web* direktorija na poslužitelju

Tokom instalacije u jednom će trenutku biti potrebno unijeti korisničko ime i lozinku, kao što je prikazano na slici 4. **Kako bi se spriječila kompromitacija računala, potrebno je**

**postaviti sigurnu lozinku.** Nesigurnim lozinkama smatraju se jednostavne, česte lozinke koje napadači lako mogu pogoditi napadima uzastopnog isprobavanja lozinke (engl. *brute-force attack*) ili korištenjem nekog rječnika s popisom čestih lozinki (engl. *dictionary attack*). Kako bi se to izbjeglo, lozinka treba slijediti sljedeća pravila:

- lozinke se moraju sastojati od 10 ili više znakova,
- lozinke moraju koristiti znakove iz više različitih skupova znakova (mala slova, velika slova, brojevi, simboli),
- lozinke se ne smiju primarno sastojati od neke riječi iz rječnika, imena ili prezimena korisnika (ili varijacije), korisničkog imena, riječi vezane uz aplikaciju/poslužitelj/servis i slično (npr. `wordpress123`),
- lozinke trebaju biti jedinstvene (ne smije se koristiti ista lozinka na više mjesta),
- lozinka ne smije biti neka od općenito često korištenih lozinka; to je primjerice moguće provjeriti pomoću usluge "[Pwned Passwords](#)"

Kako bi se olakšalo korištenje jedinstvenih i sigurnih lozinki, moguće je koristiti tzv. upravitelje lozinkama (eng. *password managers*). Više informacija o upraviteljima lozinkama dostupno je u dokumentu Nacionalnog CERT-a [KeePass](#).



The image shows a screenshot of the 'Information needed' form during the WordPress installation process. The form is titled 'Information needed' and includes the following fields and instructions:

- Site Title:** A text input field containing 'Web stranica'.
- Username:** A text input field containing 'korisnik1'. Below the field, it states: 'Usernames can have only alphanumeric characters, spaces, underscores, hyphens, periods, and the @ symbol.'
- Password:** A password input field with a strength indicator showing 'Medium'. A 'Show' button is visible to the right. Below the field, it states: '**Important:** You will need this password to log in. Please store it in a secure location.'
- Your Email:** A text input field containing 'korisnik@mail.com'. Below the field, it states: 'Double-check your email address before continuing.'
- Search Engine Visibility:** A checkbox labeled 'Discourage search engines from indexing this site'. Below it, it states: 'It is up to search engines to honor this request.'

At the bottom of the form, there is a blue button labeled 'Install WordPress'.

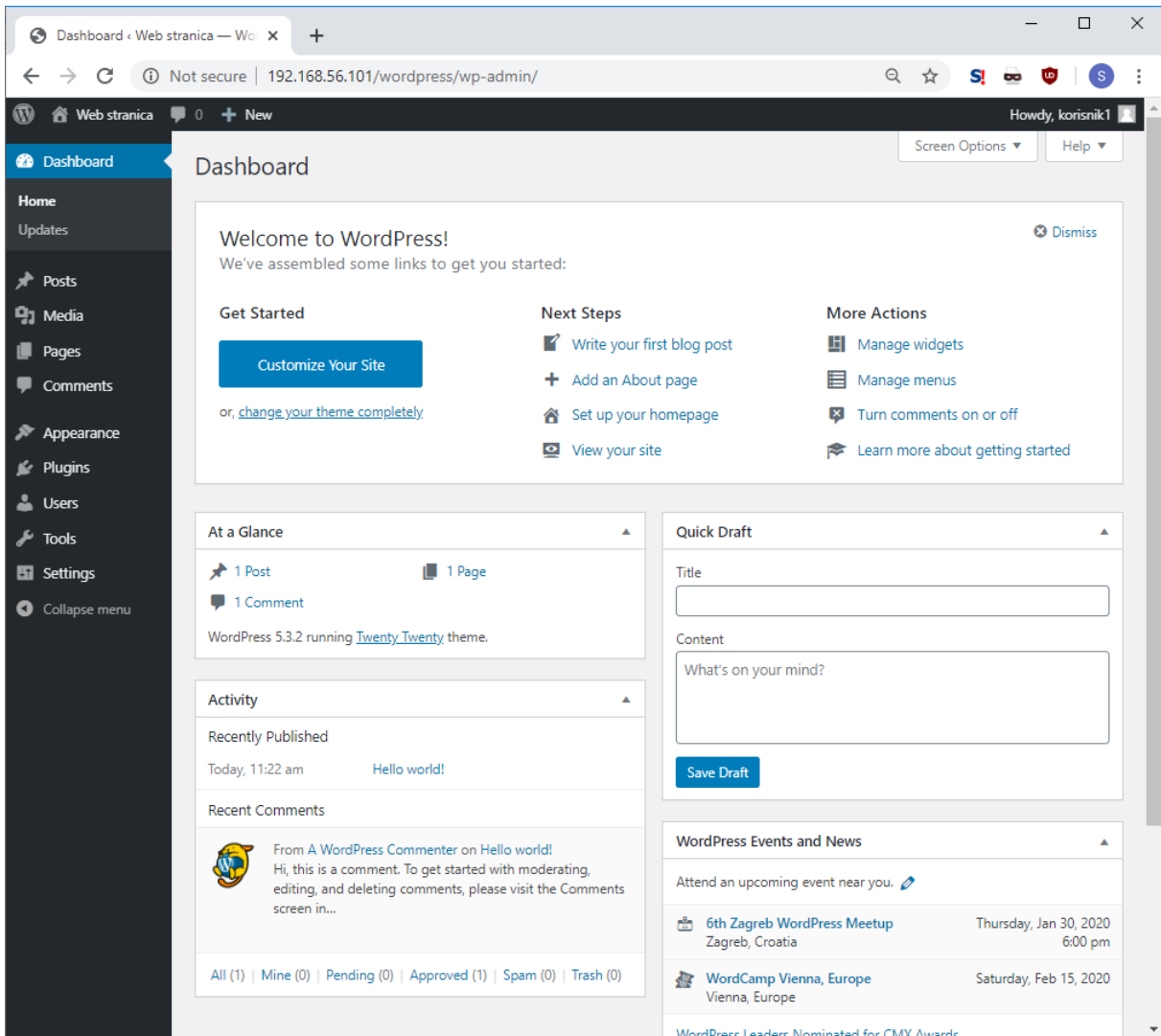
Slika 4 Popunjavanje osnovnih podataka o stranici i administratoru



### 3 Sigurno korištenje *Wordpressa*

Nakon uspješne instalacije *Wordpressa*, prijavljujemo se prethodno definiranim korisničkim imenom i lozinkom.

Nakon prijave bit ćemo preusmjereni na *Wordpressovo* upravljačko sučelje (engl. *Dashboard*) s kojeg možemo, s administratorskim ovlastima, upravljati novostvorenom *web* stranicom i njenim korisnicima (sl. 5). Tu se nalaze sve glavne funkcionalnosti i kontrole potrebne za upravljanje stranicom.



Slika 5 Upravljačko sučelje

#### 3.1 Redovito ažuriranje *Wordpressa* i povezanog softvera

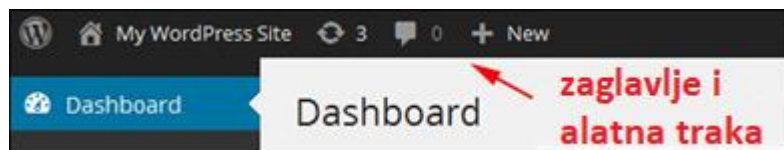
**Redovito ažuriranje *Wordpressa* i povezanog softvera (poslužiteljskog softvera, baze podataka, tema, dodataka...) vrlo je bitan korak u osiguravanju stranice.**

Naime, *WordPress*, kao i sav postojeći softver, nije savršen, već postoje pogreške u kôdu kojih proizvođač u trenutku objave softvera nije svjestan, a koje mogu biti ranjivost preko koje napadač može napasti stranicu i njene korisnike.

Iz tog razloga proizvođači softvera redovito izdaju sigurnosne zakrpe (engl. *security patches*) kojima ispravljaju pogreške, a koje bi korisnici softvera trebali čim prije instalirati i primijeniti.

Neovisno na koji način je *WordPress* instaliran (iz službenog repozitorija, preuzimanjem .zip archive...), administrator stranice mora preuzeti i ozbiljno shvatiti odgovornost njegovog redovitog ažuriranja. Isto vrijedi i za sve korištene teme (vidi 3.3) i dodatke koji su također podložni ranjivostima.

Na zaglavlju upravljačkog sučelja (sl. 6) prikazane su obavijesti o dostupnim ažuriranjima, upozorenja i obavijesti. Dostupna ažuriranja trebalo bi čim prije primijeniti.



Slika 6 Administratorska alatna traka

Informacija o trenutnoj inačici *WordPressa* u svakom trenutku vidljiva je u podnožju (engl. *footer*) stranice.



Slika 7 Podnožje upravljačkog sučelja

Iako mnogi administratori *WordPress* stranica odgađaju ažuriranje jer se boje problema s postojećim funkcionalnostima na stranici, štetu koja može nastati kao posljedica uspješnog napada može biti znatno teže sanirati.

### 3.2 Otežavanje/onemogućavanje napada na korisničke račune

Najčešći napadi na *WordPress* stranice događaju se preko ranjivih dodataka (engl. *plugins*), ali odmah za njima slijede napadi na korisničke račune.

Napadi na korisničke račune općenito su jedni od najzastupljenijih napada na web stranice. Jednom kad napadač uspješno preuzme („hakira“, „provali u“) korisnički račun nekog korisnika, može obaviti sve aktivnosti na stranici koje može i korisnik.

Preuzimanje korisničkog računa posebice je opasno kad je riječ o računima visoko privilegiranih korisnika (npr. administrator) i oni se moraju dodatno zaštititi.

Jedan uobičajen scenarij napada na *WordPress* stranicu i njene korisnike koji se oslanja na preuzimanje tuđeg korisničkog računa bio bi:

1. Administrator je postavio korisničko ime `admin` i primjerice nesigurnu lozinku `admin123` za prijavu na stranicu.
2. Napadač uspješno pogađa administratorove vjerodajnice i prijavljuje se na stranicu. Napadač sad može napraviti na stranici sve što može i administrator, tj. ima administratorske ovlasti i može ih zloupotrijebiti.
3. Napadač kompromitira dotad legitimnu stranicu dodavanjem zlonamjernog *JavaScript* kôda. Taj će kôd napasti sve korisnike koji posjete stranicu i pokušati im instalirati zlonamjerni softver na računalo.

Čak i ako bi napadač uspješno provalio u račun slabije privilegiranog korisnika (npr. *editor*), svedjedno bi mogao izazvati štetu jer bi u neku objavu mogao postaviti npr. poveznicu na zlonamjernu stranicu.

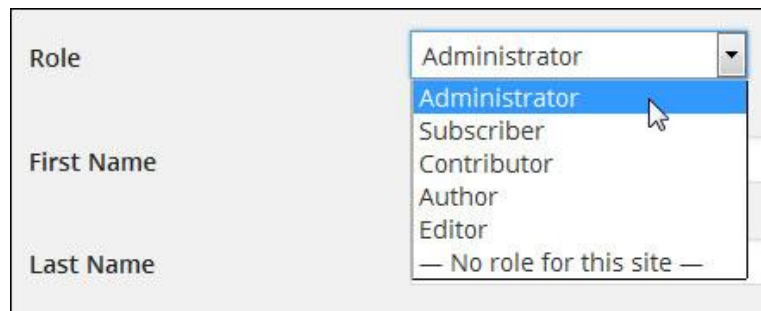
Zbog navedenih rizika bitno je dodatno osigurati korisničke račune.

### 3.2.1 Oprezno dodjeljivanje uloga korisnicima

Prilikom stvaranja novog korisnika, administrator mu može dodijeliti različite uloge (engl. *roles*) koje imaju različite razine ovlasti na stranici (sl. 8):

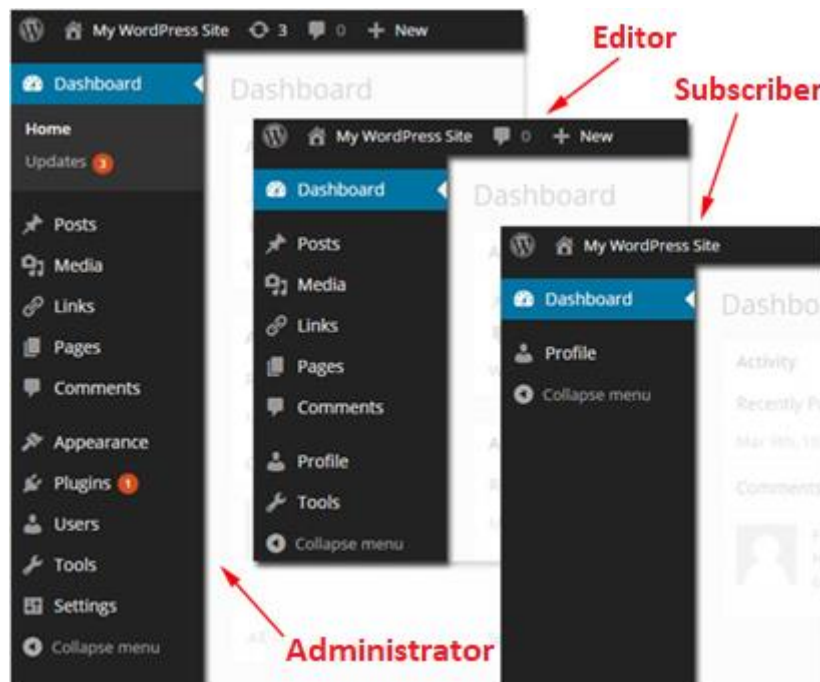
- **Administrator**
  - najveća razina ovlasti, može pristupiti svemu i koristiti sve funkcionalnosti,
- **Editor**
  - može objavljevati i uređivati sve objave na stranici (i svoje i tuđe),
- **Author**
  - može objavljevati i uređivati samo vlastite objave na stranici,
- **Contributor**
  - može uređivati vlastite objave, ali ih ne može objaviti,
- **Subscriber**
  - može samo uređivati svoj profil.

Postoji još jedna uloga koja u stvari ima najveću razinu privilegija, **super administrator**, ali ona nije obavezna i koristi se kad se upravlja s više *WordPress* stranica.



**Slika 8 Dostupne uloge s različitim razinama ovlasti na WordPress stranici**

Na slici Slika 9 prikazana je usporedba funkcionalnosti koje su dostupne administratoru, editoru i subscriberu.



Slika 9 Razlika u ponuđenim funkcionalnostima različitim vrstama korisnika

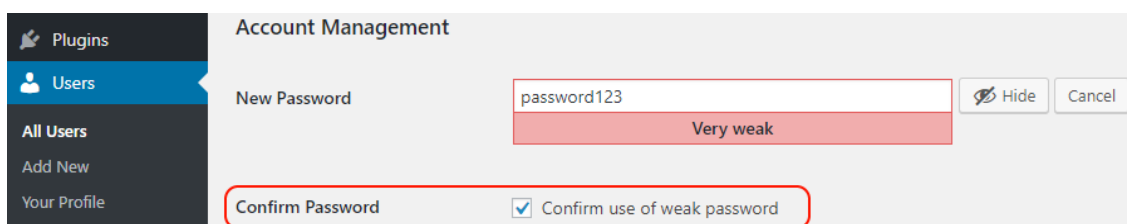
Kako bi se osigurala stranica, svakom korisniku treba dati minimalnu razinu ovlasti koja mu je potrebna za funkcionalno korištenje ili upravljanje stranicom. Pritom se korisnike, a pogotovo one u ulozi administratora, treba „prisiliti“ (engl. *enforce*) na postavljanje sigurne lozinke.

Treba izbjegavati dodjeljivanje administratorskih uloga korisnicima koji su slabije educirani o informacijskoj sigurnosti ili ih se prethodno treba educirati o mogućim napadima.

### 3.2.2 Prisiljavanje korisnika na postavljanje sigurne lozinke

Iako *WordPress* upozorava korisnika da lozinka koju postavlja postaviti nije sigurna, neće spriječiti korisnika da takvu lozinku postavi.

Prilikom instalacije *WordPresa* administrator je mogao postaviti nesigurnu lozinku, a isto tako to mogu napraviti i ostali korisnici. Korisnici mogu postaviti čak i iznimno slabe lozinke potvrđivanjem izjave „*Potvrdi korištenje slabe lozinke*“ kao što je prikazano na slici 10:



Slika 10 Korisniku je dozvoljeno postaviti iznimno slabu lozinku

S obzirom da **WordPress podrazumijevano dopušta postavljanje bilo kakve lozinke**, potrebno je instalirati neki dodatak za postavljanje politike sigurnih lozinke poput npr. *Password Policies Manager*.

Nakon instalacije dodatka, mogu se postaviti sigurnosna pravila. Kao što je prikazano na slici 11, neka od tih pravila su minimalan broj znakova, obvezno korištenje velikih/malih/brojčanih/specijalnih znakova, vrijeme nakon kojeg je potrebno promijeniti lozinku itd.

**Password Policy Manager**

**Enable Password Policies**

**Password Policies**

Passwords must be minimum  characters.

Password must contain a mix of uppercase and lowercase characters.

Password must contain numeric digits (  ).

Password must contain special characters (eg:  ).

**Password Expiration Policy**

Passwords should automatically expire in   .

*Set to 0 to disable automatic expiration.*

**Disallow old passwords on reset**

Don't allow users to use the last  passwords when they reset their password.

*The plugin will remember the last 1 password by default (minimum value: 1).*

**Slika 11 Konfiguriranje pravila za postavljanje lozinke korištenjem dodatka *Password Policies Manager***

Još neke korisne funkcionalnosti ovog dodatka su i:

- automatska izmjena lozinke svih korisnika stranice (u slučajevima kad je stranica uspješno napadnuta i brzo treba zaštititi korisničke račune). Ako se upotrijebi ova opcija, svi će korisnici na adresu e-pošte kojom su se registrirali dobiti poruku s poveznicom za ponovno postavljanje (engl. *reset*) lozinke,
- zaključavanje računa svih neaktivnih korisnika nakon određenog vremena neaktivnosti (jer bi uspješan napad i preuzimanje njihovih računa bilo vrlo teško primijetiti).

Napomena: prilikom pokušaja provaljivanja u račun, napadač mora pogoditi i korisničko ime i lozinku. Za dodatnu zaštitu, moguće je postaviti i nepredvidivo korisničko ime i time napadaču dodatno otežati pogađanje vjerodajnica, no taj bi potez mogao legitimnim

korisnicima otežati rad, pa čak i smanjiti želju da uopće koriste sustav (npr. mogli bi imati problema s pamćenjem korisničkog imena ako ono nema predvidljivi oblik).

### 3.2.3 Skrivanje stranice s obrascem za prijavu

Podrazumijevano je stranica s obrascem za prijavu (engl. *login page*) dostupna na nekoj od sljedećih putanja:

- /wp-login.php
- /login
- /wp-admin
- /admin

Jednom kad pristupi obrascu za prijavu, napadač može krenuti s napadima uzastopnim pokušajima pogađanja lozinki (engl. *brute-force attack*). Iz tog razloga, sprječavanje da se obrazac za prijavu nalazi na takvoj predvidivoj putanji može otežati napade.

Iako se to može postići konfiguracijom poslužiteljskog softvera, jednostavnije rješenje je instalirati neki od dodataka poput npr. *WPS Hide Login* kojim korisnik može promijeniti URL stranice za prijavu u bilo što drugo bez da se mora pokušati snaći među konfiguracijskim datotekama.

Postoje i dodaci za općenitu zaštitu od napada uzastopnim pokušajima pogađanja lozinki (npr. *iThemes Security*) koji će prepoznati neuobičajen broj pokušaja unosa različitih kombinacija lozinki i spriječiti napadača u daljnjem napadu.


### 3.2.4 Dvofaktorska autentifikacija

Dvofaktorska autentifikacija odnosi se na autentifikaciju ne samo lozinkom, već primjerice i jednokratnom lozinkom koja će pristići na korisnikovu adresu e-pošte ili broj mobilnog uređaja.

Pretpostavka je da napadač nema pristup korisnikovoj adresi e-pošte ili njegovom mobilnom uređaju pa čak i ako pogodi glavnu lozinku, neće moći saznati dodatnu, jednokratnu lozinku koja mu je također potrebna za prijavu.

Više informacija o dvofaktorskoj autentifikaciji nalazi se u dokumentu Nacionalnog CERT-a: „[Višefaktorska autentifikacija](#)“.

Jedan od popularnih dodataka kojima se može ostvariti dvofaktorska autentifikacija je *Two-Factor* i neke njegove mogućnosti prikazane su na slici 12:

Enabled	Primary	Name
<input checked="" type="checkbox"/>	<input type="radio"/>	Email Authentication codes will be sent to [redacted]
<input type="checkbox"/>	<input type="radio"/>	Time Based One-Time Password (Google Authenticator) Please scan the QR code or manually enter the key, then enter an authentication code from your app in order to complete setup.
		
PASWE6TVPVCCG2DTEQ6VWZTUGQWVERKJ Authentication Code: <input type="text"/> <input type="button" value="Submit"/>		
<input type="checkbox"/>	<input type="radio"/>	FIDO Universal 2nd Factor (U2F) Requires an HTTPS connection. Configure your security keys in the "Security Keys" section below.
<input type="checkbox"/>	<input type="radio"/>	Backup Verification Codes (Single Use) <input type="button" value="Generate Verification Codes"/> 0 unused codes remaining.
<input checked="" type="checkbox"/>	<input checked="" type="radio"/>	Dummy Method

Slika 12 Konfiguracija dodatka Two-Factor za dvofaktorsku autentifikaciju

### 3.3 Sigurnost tema i dodataka

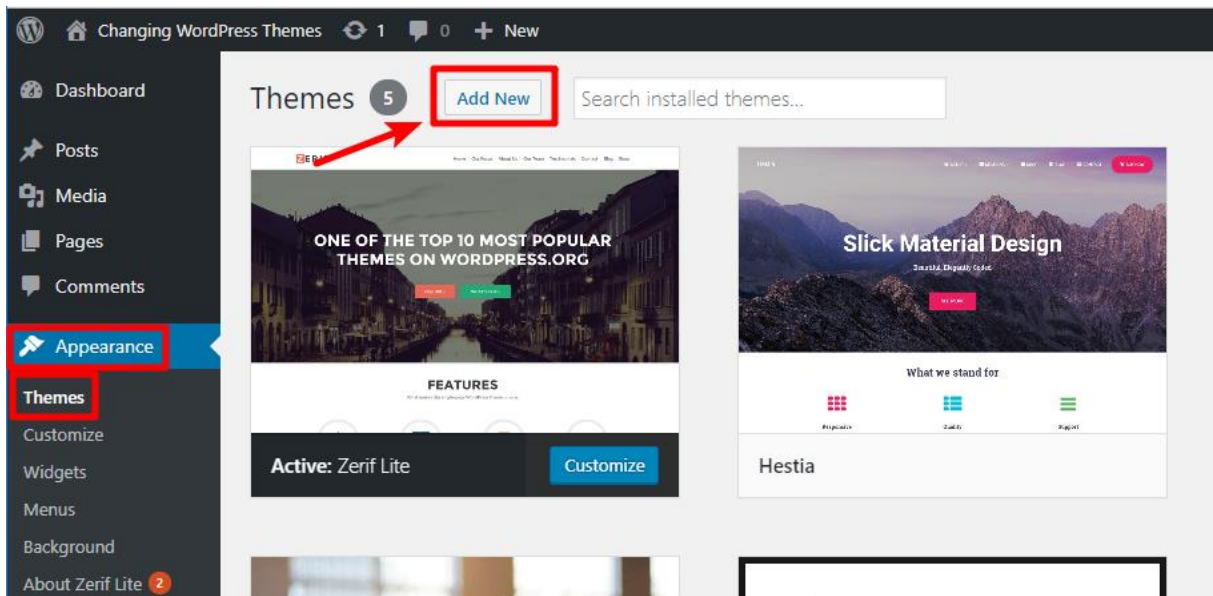
Za jednostavnu izradu, a time i popularnost stranica u *WordPressu* zaslužni su:

- **Dodaci *WordPressu*** (engl. *WordPress plugins*)  
Prava snaga *WordPressa* leži u raznim dodacima na kojima se osnovna arhitektura *WordPressa* i temelji. Za bilo koju funkcionalnost koja korisniku može pasti na pamet vjerojatno postoji dostupan dodatak kojeg je samo potrebno instalirati, jednostavno konfigurirati i može se početi koristiti. Dodacima se može ugraditi kontakt obrazac na stranicu, *web* stranica pretvoriti u *online* trgovinu, prikazivati razne statistike (npr. razvijeni su dodaci za prikaz statistika zaraženih virusom COVID-19) itd. Postoje i besplatni i komercijalni dodaci.
- **Teme** (engl. *themes*)  
Teme definiraju dizajn stranice. Postoje besplatne i komercijalne/*premium* teme. Naprednije teme s više funkcionalnosti i unikatnim dizajnom pretežito su komercijalne.

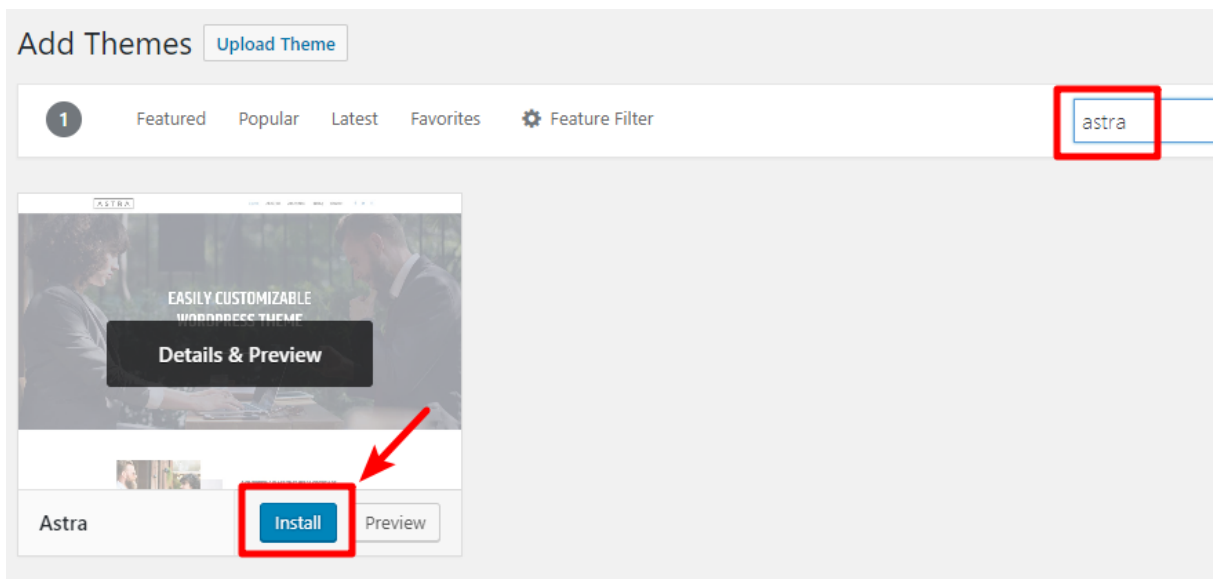
Stranicama je u početku dodijeljen generički sadržaj, tema (engl. *theme*), predložak rasporeda elemenata i nekoliko instaliranih, ali deaktiviranih dodataka.

Svi elementi stranice promjenjivi su u bilo kojem trenutku.

Odabrana tema može se promijeniti klikom na stavku „Appearance“ navigacijskog izbornika upravljačke ploče. Novu se temu može odabrati i instalirati koracima koji su prikazani na slikama 13 i 14.



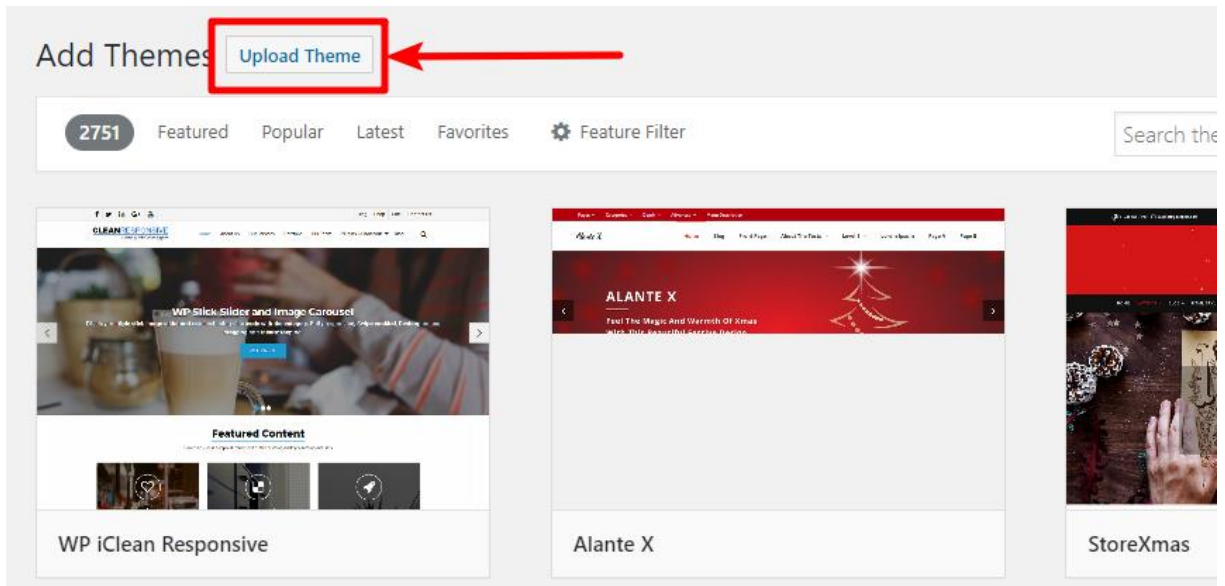
Slika 13 Dodavanje nove teme



Slika 14 Instalacija nove teme

Teme se mogu pronaći i preuzeti s raznih izvora, od WordPress repozitorija pa sve do raznih specijaliziranih stranica za teme. Ako se tema ne instalira iz WordPressovog repozitorija, njena se ZIP arhiva može učitati klikom na „Upload Theme“ kao što je prikazano na slici 15:





Slika 15 Tipka za učitavanje ZIP arhive teme

Postupak je jednak i za odabir i instalaciju dodatka.

Prilikom izbora i instalacije nove teme ili dodatka vrlo je bitno paziti da:

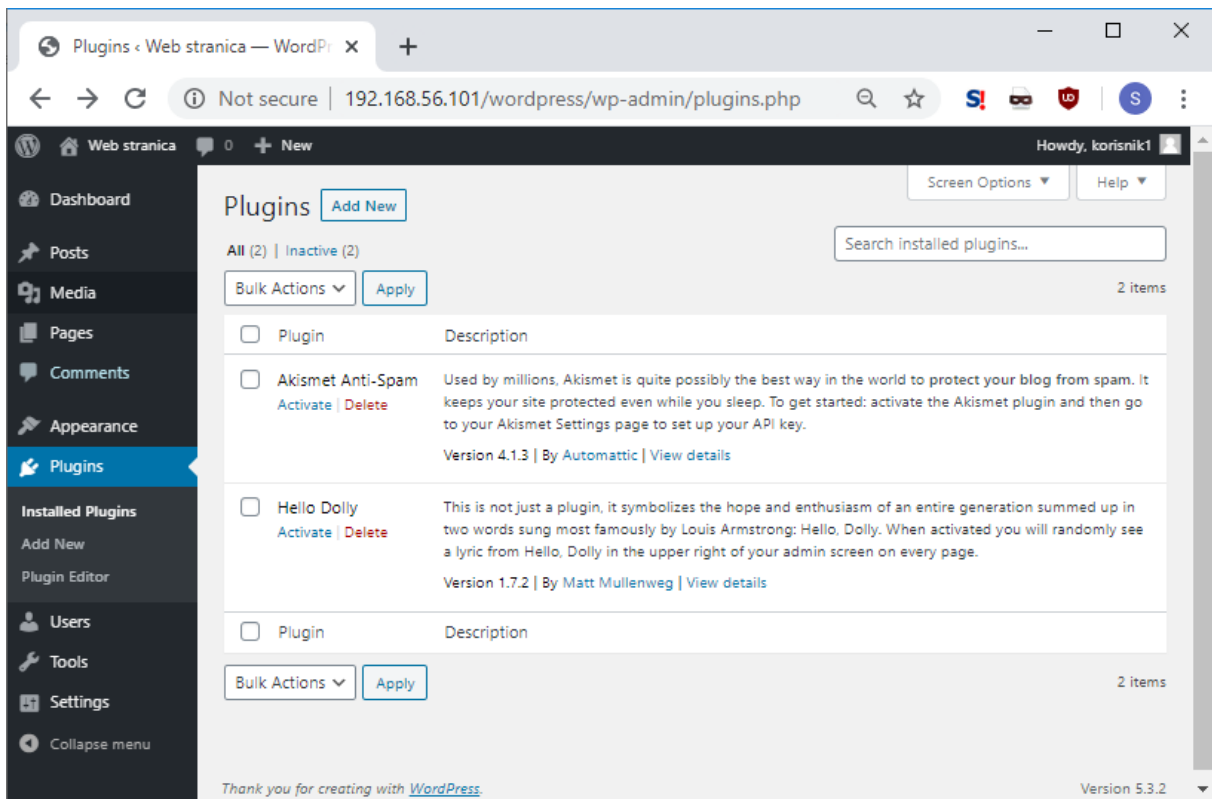
- su preuzeti s pouzdanog izvora (*WordPress*ov repozitorij ili pouzdane stranice)
- imaju podršku za održavanje i redovito se ažuriraju
- nemaju javno dostupne ranjivosti

Piratske verzije *premium* tema ili dodatka treba izbjegavati ne samo zbog povrede intelektualnog vlasništva, već i zato što su takve teme i dodaci posebno rizični budući da ne možemo vjerovati da se u njima ne nalazi neki zlonamjerni kôd ili da nisu namjerno ranjive. Prilikom preuzimanja sa službenog *WordPress*ovog repozitorija načelno možemo vjerovati korisničkim recenzijama, ali i *WordPress*ovim programerima koji su provjerili softver prije no što su dopustili njegovo postavljanje na službeni repozitorij. Kad su u pitanju piratske teme, one dolaze iz sumnjivih i nepouzdanih izvora.

Čak i ako je piratska tema sasvim dobronamjerna i legitimna, ne možemo znati hoće li se održavati. Drugim riječima, kad bismo koristili piratske verzije *WordPress* tema s neprovjerenih stranica, ne možemo biti sigurni da ta tema ne sadrži u najmanju ruku ranjivosti zbog kojih stranica na koju je instaliramo može postati žrtva raznih napada (npr. XSS, *Cross-site scripting*), a u najgorem slučaju zlonamjerni softver koji će napasti/zaraziti našu stranicu i njene korisnike.

Sve već instalirane ranjive, piratske ili teme/dodatke iz nesigurnih izvora treba deaktivirati i obrisati, a ubuduće je poželjno instalirati teme/dodatke isključivo s provjerenih izvora poput *WordPress*ovog repozitorija ili uglednih provjerenih stranica (npr. *Themeforest*, *Themeisle* itd). Zastarjele (engl. *outdated*) teme/dodatke koji više nemaju podršku i teme/dodatke koji se ne koriste također je potrebno ukloniti.

Svi instalirani dodaci mogu se vidjeti odabirom stavke „*Plugins*“ navigacijskog izbornika upravljačke ploče, a teme odabirom stavke „*Appearance*“.



Slika 16 Sučelje za upravljanje dodacima

**Ranjive teme i dodaci mogu predstavljati ranjivost preko koje napadač može napasti stranicu, njene korisnike, poslužiteljski softver, i na kraju cijelo računalo (ako *WordPress* i poslužitelj nisu sigurno konfigurirani).**

Ako nismo sigurni je li trenutna inačica *WordPressa*, dodatak ili tema koju koristimo zlonamjerna ili ranjiva, neki od načina kojima to možemo provjeriti (iako ne možemo biti u potpunost sigurni) su:

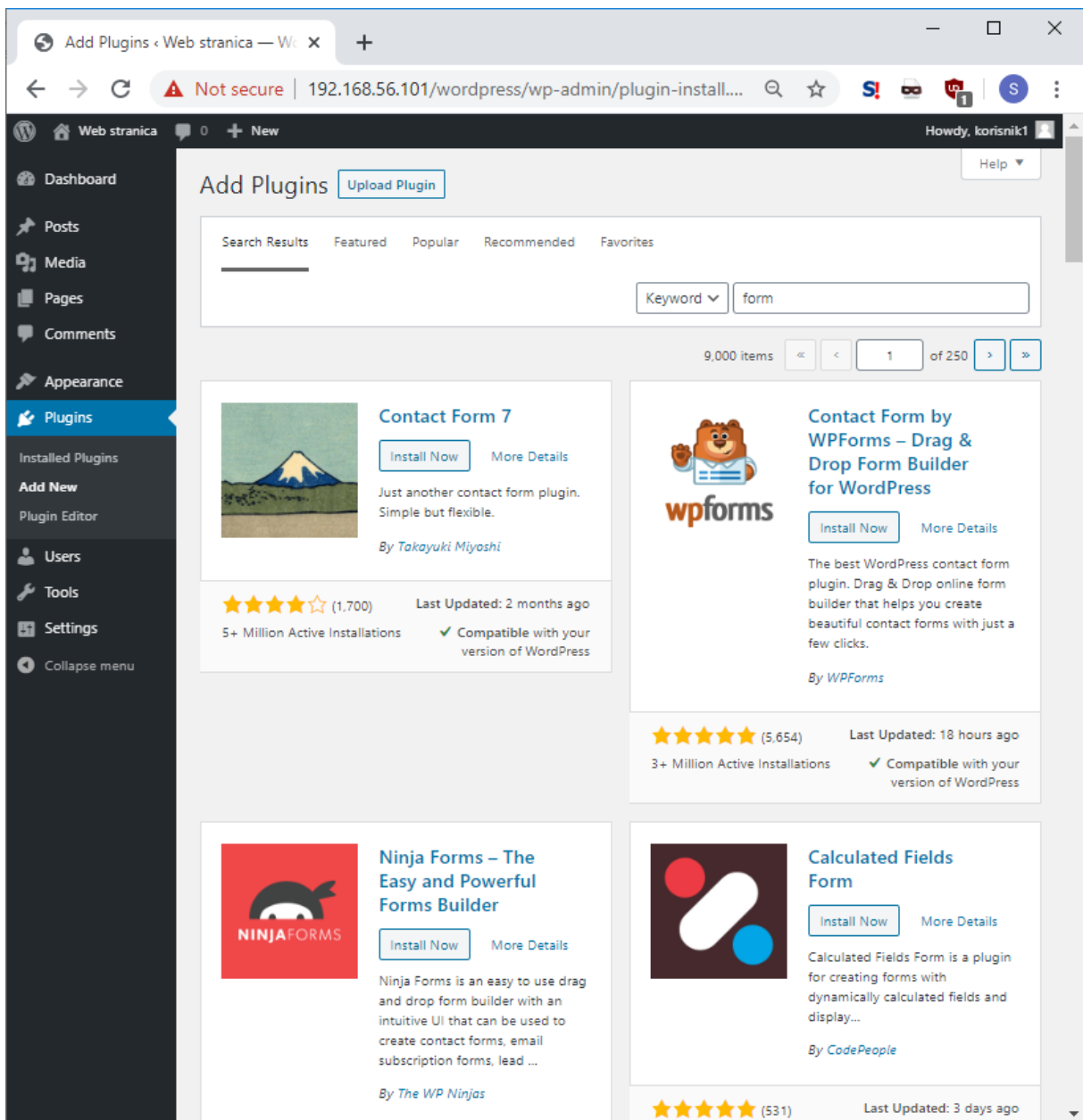
- stranica <https://www.cvedetails.com/>
  - na ovoj stranici nalazi se popis većine javno poznatih ranjivosti. Pretraživanjem pojma „*WordPress*“ možemo vidjeti trenutno javno poznate ranjivosti i njihovu kritičnost.
- stranica <https://wpvulndb.com/>
  - na ovoj stranici nalazi se popis ranjivih tema, dodataka i inačica *WordPressa*, te njihove ranjivosti. Prije korištenja određene teme ili dodataka, ovdje možemo provjeriti postoji li neka javno poznata ranjivost.
- alati za skeniranje zlonamjernog softvera na stranicama
  - za korištenje su dostupni razni alati i dodaci za skeniranje zlonamjernog softvera na *WordPress* stranicama. Ako pronađu zlonamjerni kôd, obavijestit će korisnika i ponuditi mu opciju uklanjanja zlonamjernih datoteka. Jedan primjer takvog alata je [Sucuri Security](#).

- **recenzije i komentari ostalih korisnika**

- svi pouzdani izvori s kojih možemo preuzimati teme i dodatke omogućuju korisnicima da ostave recenzije o temi ili dodatku. Češće instalirani, više recenzirani i ocijenjeni boljom ocjenom dodaci i teme se rangiraju na prva mjesta rezultata pretrage.

Iako to korisnici često izbjegavaju iz straha da će se poremetiti funkcionalnosti stranice, sve korištene teme i dodatke treba redovito ažurirati jer i naočigled sigurne teme i dodaci mogu imati ranjivosti.

Ako bismo htjeli ugraditi obrazac za kontakt (engl. *contact form*) na stranicu, možemo pretražiti dostupne dodatke u *WordPress*ovom repozitoriju klikom na stavku navigacijskog izbornika „*Plugins*“ i unosom ključne riječi „*form*“ u tražilicu.



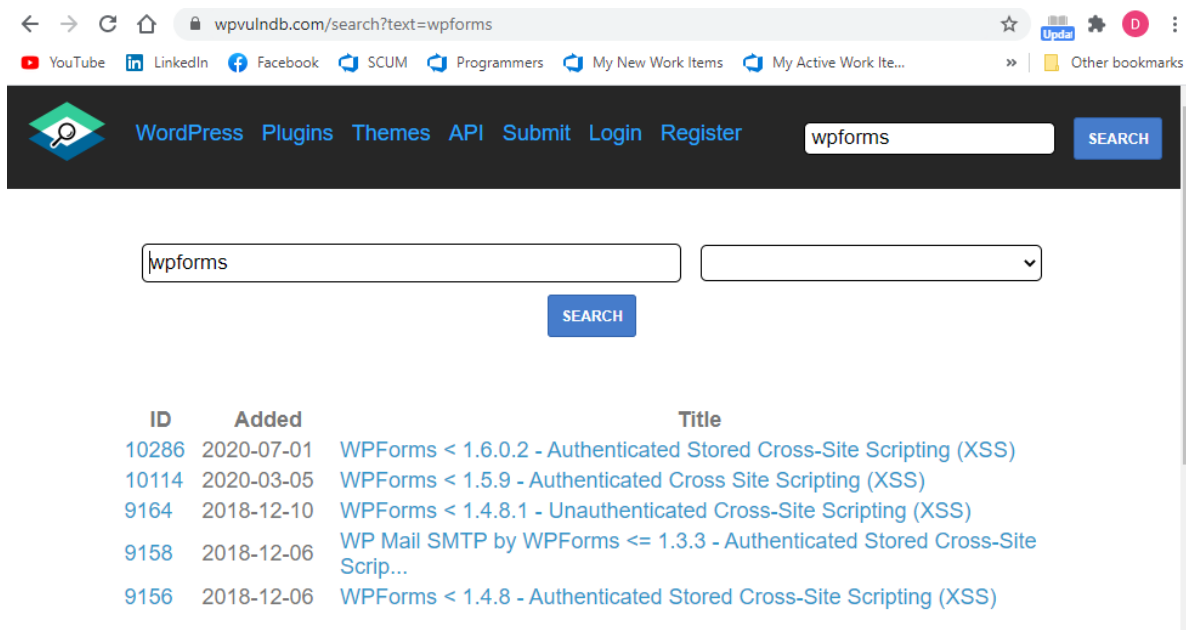
Slika 17 Rezultati pretrage dodatka za izradu obrazaca

Kao što vidimo na slici 17, postoji 9.000 rezultata pretrage, što znači da postoji velik broj dodataka povezanih s obrascima.

Dodatak naziva „*Contact Form by WPForms*“ od svih prikazanih ima najbolju ocjenu i najveći broj recenzija, a isto tako je i nedavno ažuriran (prije 18 sati) i na temelju toga bismo ga mogli smatrati pouzdanijim dodatkom u odnosu na ostale.

Dodatke koji imaju malen broj instalacija, loše ocjene ili dugo nisu ažurirani nije poželjno instalirati ako postoji bolja alternativa.

Na stranici <https://wpvulndb.com/> možemo provjeriti koje su javno poznate ranjivosti koje se odnose na dodatak *wpforms* i usporediti odnose li se na inačicu koju smo instalirali na stranicu (1.6.1).



**Slika 18 Javno poznate ranjivosti za dodatak wpforms**

Neki dodaci su čak ciljano razvijeni kao zlonamjerni dodaci koji će, ako ih administrator instalira na stranicu, napasti stranicu i/ili njene korisnike.

Jedan aktualan primjer dogodio se početkom 2020. godine (7):

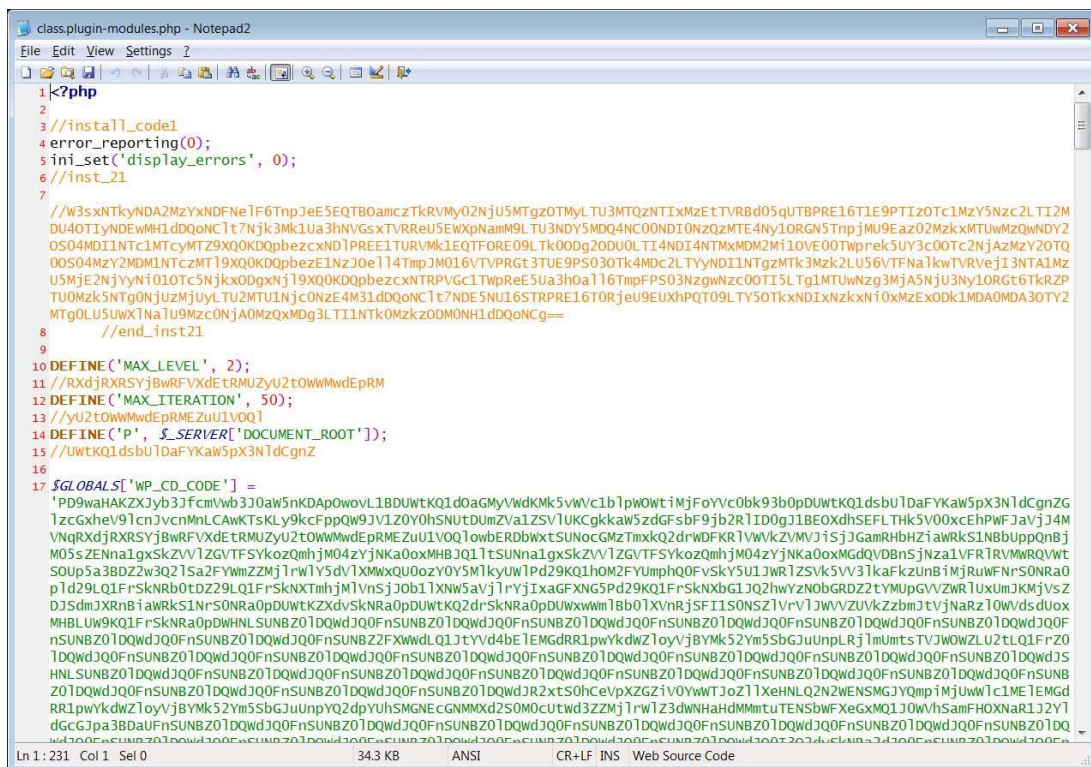
1. Usred pandemije uzrokovane virusom COVID-19 razvili su se razni dodaci koji nude grafički i numerički prikaz statistika o zaraženima (sl. 19). Ovakvi su dodaci široko korišteni, pogotovo na portalima s novostima.

**Coronavirus Statistic**

	CASES	DEATHS	RECOVERED
<b>Worldwide</b>	<b>183,805 +1,518</b>	<b>7,162 +49</b>	<b>79,980 +2,040</b>
<b>USA</b>	4,743 +80	93 +7	74 +39
<b>China</b>	80,884 +21	3,226 +13	68,869 +123
<b>Italy</b>	27,980	2,158 +123	2,749
<b>Iran</b>	14,991	853	4,996
<b>South Korea</b>	8,320 +84	81 +6	1,401
<b>Spain</b>	9,942	342	530
<b>Germany</b>	7,272 +316	17	67
<b>Franch</b>	6,653	148	12
<b>Quatar</b>	4,661	2	40

**Slika 19 Primjer prikaza statistike o širenju COVID-19 putem dodatka (8)**

2. Neki od takvih komercijalnih dodataka mogli su se kupiti na pouzdanim specijaliziranim stranicama poput npr. [envatomarketa](#). No, uskoro su se pojavile njihove besplatne piratizirane alternative.
3. Oni koji su instalirali piratizirane dodatke ubrzo su otkrili da su dodaci u stvari sadržavali datoteku `class.plugin-modules.php` (sl. 20) u kojoj se nalazio zlonamjerni kôd.



**Slika 20 Datoteka sa zlonamjernim kôdom (7)**

4. Zlonamjerni dodatak je kompromitirao dotad legitimnu stranicu dodavanjem zlonamjernog kôda u sve instalirane teme i razne PHP datoteke pohranjene na poslužitelju i na taj je način stvorio *backdoor* i preuzeo kontrolu nad stranicom.
5. Ono što je na prvi pogled izgledalo kao ušteta, pretvorilo se u katastrofu jer je dodatak napadao posjetitelje stranice zlonamjernim oglašavanjem (koje može rezultirati instalacijom zlonamjernog softvera na računalo) i preusmjeravao ih na druge stranice kako bi se tim stranicama povećala posjećenost.

### 3.4 fail2ban

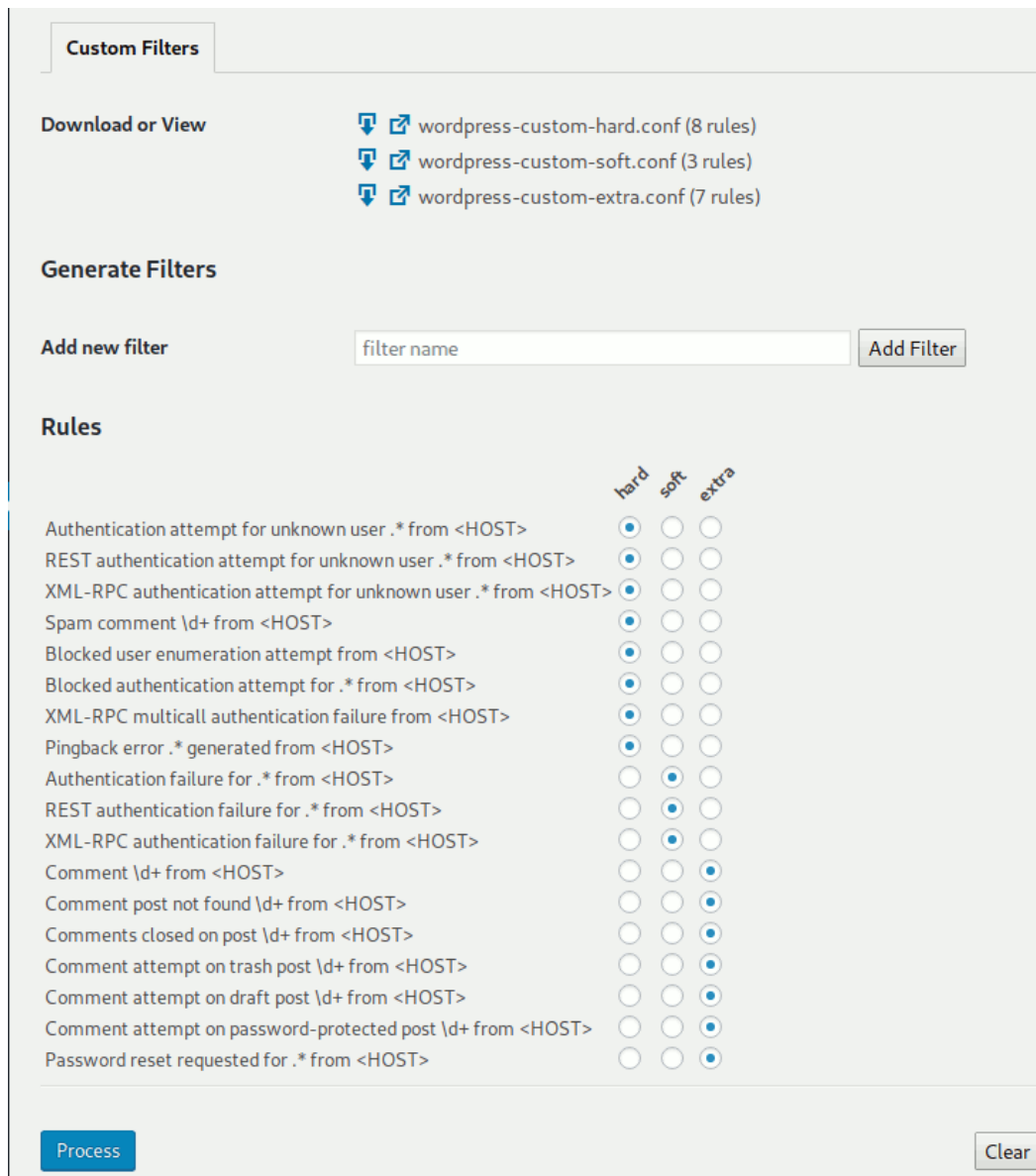
*Fail2ban* je softverski dodatak vatrozidu koji omogućuje automatsku detekciju i izolaciju određenih napada na sustav.

*Fail2ban*, jednako kao što to rade i sistemski administratori, čita dnevnik na poslužitelju te nakon određenog broja „ilegalnih“, tj. zlonamjernih radnji prilagođava pravila vatrozida kako bi izolirao i spriječio nastavak napada.

Iako je *fail2ban* namijenjen operacijskim sustavima *Linux* (i korisno ga je na njega instalirati), postoji i dodatak za *WordPress* naziva *WP fail2ban* iste namjene. Općenite informacije o *fail2banu* mogu se pronaći u dokumentu Nacionalnog CERT-a [Fail2Ban](#).

*WP fail2ban* dolazi s tri konfiguracijske datoteke – *hard*, *soft* i *extra*, a odnose se na razinu strogoće sankcije kao odgovor na nedozvoljeno ponašanje. Npr. *hard* razina će odmah blokirati daljnji pristup IP adresi s koje je nedozvoljeni zahtjev došao, a *soft* razina će dopustiti nekoliko nedozvoljenih ponašanja, ali će u jednom trenutku reagirati kad količina nedozvoljenog ponašanja prijeđe definiranu granicu (npr. 10 neuspjelih pokušaja prijave).

Na slici 21 prikazane su definirane razine sankcija za određeno nepoželjno ponašanje.



Slika 21 Primjer konfiguracije WP fail2ban dodatka (9)

### 3.5 Zapisivanje aktivnosti u dnevnik

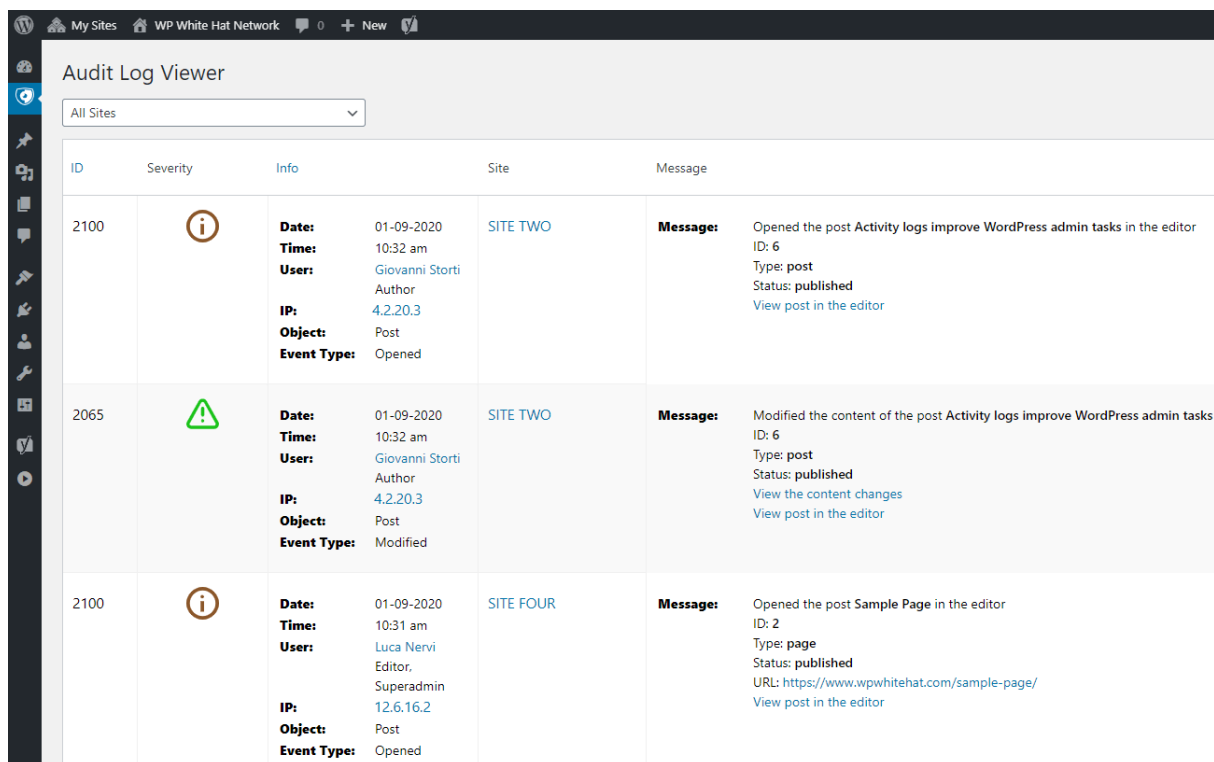
Aktivnosti koje se događaju na stranici mogu se zapisivati u dnevnik, skupa s dodatnim podacima, npr. koji je korisnik izveo koji akciju ili s kojih su se IP adresa klijenti spajali na poslužitelj. **Vođenje dnevnika olakšava kontrolu nad događajima na stranici i pomoću dnevnika se može otkriti što se dogodilo uslijed neočekivanog ponašanja stranice.**




Jedan tipičan scenarij napada u kojem bi vođenje dnevnika bilo od koristi je:

1. Napadač pokušava izvesti napad uzastopnim pokušajima pogađanja lozinke (engl. *brute-force attack*).

- U dnevnik se zapisuju sve aktivnosti pokušaja prijave. Administrator sustava uočava velik broj pokušaja prijave s različitim kombinacijama korisničkih imena i lozinki i shvaća da se dogodio/događa napad.
- Administrator može (znajući što se dogodilo) instalirati neki dodatak za zaštitu kako se napad ne bi ponovio, blokirati račun napadnutog korisnika i obavijestiti ga da mu je račun kompromitiran (ako je napadač uspio pogoditi neku kombinaciju).

Jedan primjer dodatka za zapisivanje aktivnosti u dnevnik je *WP Activity Log* koji postoji u besplatnoj i komercijalnoj (s više funkcionalnosti) inačici. Na slici 22 prikazan je dnevnik koji pregledno prikazuje obavijesti o aktivnostima na stranici:



ID	Severity	Info	Site	Message
2100		<b>Date:</b> 01-09-2020 <b>Time:</b> 10:32 am <b>User:</b> Giovanni Storti Author <b>IP:</b> 4.2.20.3 <b>Object:</b> Post <b>Event Type:</b> Opened	SITE TWO	<b>Message:</b> Opened the post Activity logs improve WordPress admin tasks in the editor ID: 6 Type: post Status: published <a href="#">View post in the editor</a>
2065		<b>Date:</b> 01-09-2020 <b>Time:</b> 10:32 am <b>User:</b> Giovanni Storti Author <b>IP:</b> 4.2.20.3 <b>Object:</b> Post <b>Event Type:</b> Modified	SITE TWO	<b>Message:</b> Modified the content of the post Activity logs improve WordPress admin tasks ID: 6 Type: post Status: published <a href="#">View the content changes</a> <a href="#">View post in the editor</a>
2100		<b>Date:</b> 01-09-2020 <b>Time:</b> 10:31 am <b>User:</b> Luca Nervi Editor, Superadmin <b>IP:</b> 12.6.16.2 <b>Object:</b> Post <b>Event Type:</b> Opened	SITE FOUR	<b>Message:</b> Opened the post Sample Page in the editor ID: 2 Type: page Status: published URL: <a href="https://www.wpwhitehat.com/sample-page/">https://www.wpwhitehat.com/sample-page/</a> <a href="#">View post in the editor</a>

Slika 22 Primjer prikaza zapisa u dnevniku (10)

### 3.6 Pričuvne kopije

Redovita izrada pričuvnih kopija trebala bi biti uobičajena praksa za svaku *web* stranicu jer se, ako nešto pođe po zlu, uvijek može vratiti na prethodno spremljeno stanje.

Dostupni su razni komercijalni i besplatni dodaci za izradu pričuvnih kopija, a među njima je trenutno najkorišteniji i najbolje ocijenjen *UpdraftPlus* koji je instaliran na više od dva milijuna *web* stranica. Postoje besplatna i komercijalna inačica (s više funkcionalnosti).

Na slici 23 prikazane su neke od postavki prilikom konfiguracije dodatka:



The screenshot shows the 'Settings' tab of the UpdraftPlus plugin interface. It is divided into several sections:

- Backup / Restore**, **Migrate / Clone**, **Settings** (active), **Advanced Tools**, and **Premium / Extensions** tabs are visible at the top.
- Files backup schedule:** Set to 'Weekly' with a dropdown arrow and 'and retain this many scheduled backups: 2'.
- Database backup schedule:** Set to 'Weekly' with a dropdown arrow and 'and retain this many scheduled backups: 2'.
- A note: 'To fix the time at which a backup should take place, (e.g. if your server is busy at day and you want to run overnight), or to configure more complex schedules, [use UpdraftPlus Premium](#)'.
- Choose your remote storage (tap on an icon to select or unselect):** A grid of storage options:
  - UpdraftPlus Vault (selected)
  - Dropbox
  - Amazon S3
  - Rackspace Cloud Files
  - Google Drive
  - Microsoft OneDrive
  - FTP
  - Microsoft Azure
  - SFTP / SCP
  - Google Cloud
  - Backblaze
  - WebDAV
  - S3-Compatible (Generic)
  - OpenStack (Swift)
  - DreamObjects
  - Email
- A note: 'You can send a backup to more than one destination with an add-on.'
- A warning: 'If you choose no remote storage, then the backups remain on the web-server. This is not recommended (unless you plan to manually copy them to your computer), as losing the web-server would mean losing both your website and the backups in one event.'
- Include in files backup:**
  - Plugins
  - Themes
  - Uploads
- Exclude these:**
- Any other directories found inside wp-content
- Exclude these:**
- A note: 'The above directories are everything, except for WordPress core itself which you can download afresh from WordPress.org. [See also the "More Files" add-on from our shop.](#)'

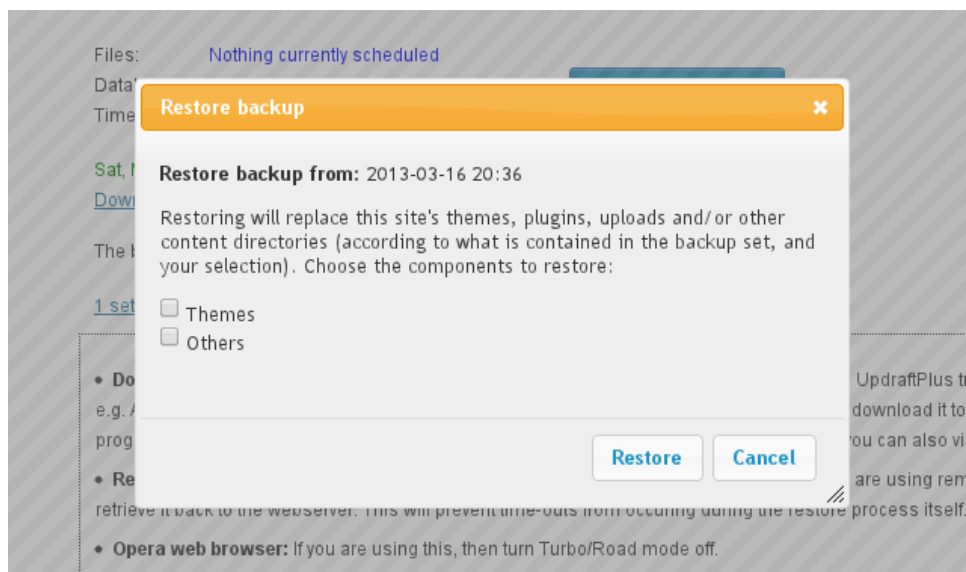
**Slika 23 Konfiguracija dodatka UpdraftPlus za izradu pričuvnih kopija**

Kao što vidimo, moguće je odabrati učestalost izrade pričuvnih kopija, lokaciju na koju će se spremati kopija i što sve treba uključiti, a što treba isključiti iz pričuvne kopije.

Kompletna pričuvna kopija stranice može se spremati na računalo ili u oblak (engl. *cloud*).

Osim izrade pričuvnih kopija, *UpdraftPlus* nudi i jednostavan oporavak sustava na stanje koje pohranjuje pričuvna kopija (engl. *restore*).

Prilikom oporavka sustava mogu se odabrati dijelovi sustava koji se žele vratiti na stanje spremljeno u pričuvnoj kopiji (sl. 24).



**Slika 24 Oporavak stranice iz pričuvne kopije (11)**

## 4 Zaključak

*WordPress* je najkorišteniji CMS i u njemu je razvijeno oko 42% svih trenutno postojećih *web* stranica. Svoju popularnost duguje jednostavnosti korištenja i brzini razvoja stranice – jednostavna stranica može se razviti u svega nekoliko sati.

Njegova se arhitektura temelji na softveru otvorenog kôda (*Apache/NGINX*, *PHP*, *MariaDB*) i mnoštvu dodataka koji pružaju razne funkcionalnosti.

Umjesto poznavanja *HTML*, *CSS*, *PHP* i *SQL* tehnologija, administrator *WordPress* stranice mora samo odabrati i instalirati potrebni dodatak. Skoro sve funkcionalnosti koje su potrebne prosječnoj *web* stranici su dostupne putem dodataka i jednostavno ih je koristiti jer su dobro dokumentirane i same navode korisnika koji sljedeći korak treba napraviti.

No, upravo popularnost i široka korištenost *WordPressa* čine ga idealnom metom za napadače, pogotovo ako se uzme u obzir da *WordPress* stranice mogu razvijati i osobe koje se slabo razumiju u *web* i sigurnost općenito.

Napadači imaju velik interes za pronaći i iskoristiti ranjivosti te neprekidno napadaju *WordPress* stranice i njihove korisnike, pri čemu se pretežito oslanjaju na:

- korištenje neažuriranih (ranjivih) inačica *WordPressa* ili povezanog softvera,
- korištenje neažuriranih, zastarjelih, zlonamjernih ili ranjivih tema ili dodataka,
- nedostatak zaštite od preuzimanja korisničkih računa (npr. *brute-force attack*)

Postoji mnoštvo korisnih dodataka koji se mogu koristiti za poboljšanje sigurnosti *WordPress* stranica i najvažnije vrste su predstavljene u ovom dokumentu.

Generalni savjeti kojih se treba pridržavati kako bi se minimizirao rizik od napada su:

- *WordPress* i pripadajući softver treba redovito ažurirati i ne koristiti inačice za koje više ne postoji podrška, tj. ne izdaju se sigurnosne zakrpe,
- Poslužiteljski softver, bazu podataka ili *WordPress* nikad ne smije pokretati *root* korisnik ili neki drugi korisnik koji može pristupiti drugim dijelovima operacijskog sustava. U tom bi slučaju napadač, ako uspije napasti *WordPress*, uspio preuzeti kontrolu nad cijelim računalom ili još nekim njegovim procesima.
- Dodaci i teme koje održava *WordPress* ili se nalaze na pouzdanim stranicama su razvijeni s najboljom namjerom, temeljito provjereni i redovito održavani. Nasuprot njima, postoje razne sumnjive teme i dodaci koji mogu biti čak namjerno razvijeni da budu ranjivi, mogu biti slabo testirani ili ih je možda razvio netko tko nije uzeo u obzir sigurnost. Takve teme i dodatke treba izbjegavati, tj. teme i dodatke treba preuzimati samo sa sigurnih izvora.
- Tvornička inačica i postavke *WordPressa* nemaju nikakvu politiku za zaštitu korisničkih računa. To je vrlo opasno ako uzmemo u obzir da je korisnicima dozvoljeno postaviti lozinke poput „lozinka123“ koje su vrlo nesigurne i napadač ih jednostavno može pogoditi. Za dodatno osiguravanje korisničkih računa mogu

se koristiti neki dodaci za postavljanje sigurnosne politike lozinki, sprječavanje napada uzastopnim pokušajima pogađanja lozinke ili dvofaktorsku autentifikaciju.

- Mogu se koristiti dodaci poput *WP fail2ban* kako bi se pratilo što se događa u sustavu i pravovremeno reagiralo na potencijalni napad.

No, uvijek treba biti spreman na činjenicu da možemo postati žrtva napada i zato je bitno redovito izrađivati pričuvene kopije (engl. *backups*) iz kojih se stranica može oporaviti i zapisivati aktivnosti u dnevnik kako bi se moglo utvrditi kako je do napada uopće došlo.

Primjenom ovih savjeta *WordPress* može postati vrlo siguran za korištenje, a čak i u slučaju napada se vrlo brzo može ponovno uspostaviti čista i sigurna verzija. Sve to može učiniti i osoba koja nije specijalizirana za računalnu sigurnost.

## 5 Literatura

1. **W3Techs**. Usage statistics of content management systems. *W3Techs*. [Mrežno] [Citirano: 9. lipnja 2021.] [https://w3techs.com/technologies/overview/content\\_management](https://w3techs.com/technologies/overview/content_management).
2. **Gatlan, Sergiu**. Critical WordPress Plugin Bug Allows Admin Logins Without Password. *Bleeping Computer*. [Mrežno] 14. siječnja 2020. [Citirano: 5. lipnja 2020.] <https://www.bleepingcomputer.com/news/security/critical-wordpress-plugin-bug-allows-admin-logins-without-password/>.
3. —. 200K sites with buggy WordPress plugin exposed to wipe attacks. *Bleeping Computer*. [Mrežno] 28. svibnja 2020. [Citirano: 5. lipnja 2020.] <https://www.bleepingcomputer.com/news/security/200k-sites-with-buggy-wordpress-plugin-exposed-to-wipe-attacks/>.
4. —. Hackers tried to steal database logins from 1.3M WordPress sites. *Bleeping Computer*. [Mrežno] 4. lipnja 2020. [Citirano: 5. lipnja 2020.] <https://www.bleepingcomputer.com/news/security/hackers-tried-to-steal-database-logins-from-13m-wordpress-sites/>.
5. —. WordPress plugin bug lets hackers create rogue admin accounts. *Bleeping Computer*. [Mrežno] 27. travnja 2020. [Citirano: 5. lipnja 2020.] <https://www.bleepingcomputer.com/news/security/wordpress-plugin-bug-lets-hackers-create-rogue-admin-accounts/>.
6. **PHP**. Supported Versions. *PHP*. [Mrežno] [Citirano: 9. lipnja 2021.] <https://www.php.net/supported-versions.php>.
7. **Abrams, Lawrence**. WordPress Malware Distributed via Pirated Coronavirus Plugins. *Bleeping Computer*. [Mrežno] 25. ožujka 2020. [Citirano: 30. srpnja 2020.] <https://www.bleepingcomputer.com/news/security/wordpress-malware-distributed-via-pirated-coronavirus-plugins/>.
8. **Elfsight**. WordPress Coronavirus Stats plugin. *Elfsight*. [Mrežno] [Citirano: 30. srpnja 2020.] <https://elfsight.com/coronavirus-stats-widget/wordpress/>.
9. **Lecklide, Charles**. WP Fail2Ban. *WP Fail2Ban*. [Mrežno] [Citirano: 30. srpnja 2020.] <https://wp-fail2ban.com/add-ons/remote-tools/>.
10. **WP White Security**. How can I change the activity log view mode? *WP White Security*. [Mrežno] [Citirano: 30. srpnja 2020.] <https://wpactivitylog.com/support/kb/change-activity-log-view-mode/>.
11. **WordPress**. UpdraftPlus WordPress Backup Plugin. *WordPress*. [Mrežno] [Citirano: 30. srpnja 2020.] <https://wordpress.org/plugins/updraftplus/>.