ELEKTRONSKO POSLOVANJE

školska 2024/2025 godina

Vežba 14: Bezbednost sajta i pravna usklađenost

Bezbednost i pravna usklađenost su ključni temelji ozbiljnog e-trgovinskog sajta. Kada radite sa sistemima kao što je WooCommerce, neophodno je da zaštitite osetljive podatke korisnika, sprečite zloupotrebe i obezbedite usklađenost sa zakonima poput GDPR-a (Opšta uredba o zaštiti podataka) u EU ili Zakonom o zaštiti podataka o ličnosti u Srbiji.

Pravilna implementacija tehničkih i zakonskih mera doprinosi:

- zaštiti ličnih i finansijskih podataka korisnika,
- jačanju poverenja kupaca u vašu online prodavnicu,
- smanjenju rizika od kazni i sudskih sporova.

1. Osnovne mere zaštite podataka

WooCommerce sajtovi često obrađuju podatke kao što su ime i prezime, adresa stanovanja, broj telefona, email, podaci o porudžbinama, pa čak i brojevi kartica (ako se koristi lokalno procesiranje). Zato je neophodno primeniti sledeće mere:

• Redovno ažuriranje sistema

Ažuriranje WooCommerce plugin-a, kao i svih dodataka i tema je prva linija odbrane. Stare verzije sadrže poznate bezbednosne rupe koje hakeri lako mogu iskoristiti.

• Instalacija sigurnosnih dodataka

Sigurnosni dodaci pomažu u automatskom nadzoru, blokiranju zlonamernih pokušaja pristupa i skeniranju fajlova:

- **Wordfence Security** – nudi zaštitu u realnom vremenu, firewall, skeniranje na malware, i blokiranje IP adresa sa sumnjivim aktivnostima.
- **iThemes Security** – pruža dodatnu zaštitu: dvofaktorsku autentifikaciju, detekciju promena u fajlovima, zaštitu od brute-force napada i druge bezbednosne alate.

• Ograničenje korisničkih uloga

Nikada ne dodeljujte administrativna prava korisnicima koji ne moraju da ih imaju. WooCommerce automatski dodeljuje "Customer" ulogu za kupce, što je dovoljno da vide svoje porudžbine bez pristupa podešavanjima sajta.

• Sakrivanje i zaštita administratorske stranice

Pristup stranici /wp-admin i login formi treba dodatno zaštititi:

- Sakrijte default putanju ka administraciji pomoću plugina kao *WPS Hide Login*.
- Aktivirajte **CAPTCHA** na login formi da sprečite utomatizovane brute-force napade.

• Sigurnosni sertifikat (SSL)

Obavezno je koristiti **HTTPS protokol** i validan SSL sertifikat kako bi svi podaci bili kriptovani prilikom prenosa između korisnika i servera.

---

2. Instalacija SSL sertifikata

Za WooCommerce prodavnicu, **SSL sertifikat je obavezan**, jer se putem sajta šalju osetljive informacije kao što su podaci o kartici (čak i ako koristi treću stranu za plaćanje).

Instalacija SSL sertifikata se može obaviti preko besplatne usluge kao što je **Let's Encrypt** (dostupna kod većine hosting provajdera), ili putem plaćenih sertifikata koji nude dodatne nivoe validacije (DV, OV, EV).

Nakon uspešne instalacije, u WordPress kontrolnoj tabli idite na:
Settings > General i zamenite URL-ove sajta i WordPress instalacije iz http:// u https://.

Preporučuje se da se instalira i plugin **Really Simple SSL**, koji automatski preusmerava saobraćaj na HTTPS i rešava probleme sa mešanim sadržajem (mixed content).

WooCommerce podešavanja:

U okviru WooCommerce podešavanja (WooCommerce > Settings > Advanced), potrebno je omogućiti opciju “Force secure checkout” kako bi koraci kupovine koristili HTTPS vezu.

Ova opcija dodatno osigurava da se svi podaci koje korisnik unosi tokom porudžbine (adresa, kontakt, kartica) šalju kroz enkriptovani kanal.

💡 **Zašto je važno:**

- **Povećava poverenje korisnika** – Posetioci sajta vide zeleni katanac u adresnoj liniji, što im uliva sigurnost pri kupovini.
- **Zaštita komunikacije** – Podaci između korisnika i sajta su kriptovani, što štiti od prisluškivanja i manipulacije.
- **SEO prednost** – Google favorizuje HTTPS sajtove, pa može doprineti boljoj poziciji u pretrazi.

---

3. GDPR politika privatnosti

WooCommerce omogućava jednostavnu implementaciju **GDPR politike privatnosti**, čime se obezbeđuje poštovanje prava korisnika u vezi sa obradom ličnih podataka.

Kreiranjem stranice **"Politika privatnosti"** (Privacy Policy) preko Pages > Add New, moguće je koristiti unapred pripremljeni WordPress šablon koji uključuje osnovne smernice za transparentnost.

U WooCommerce > Settings > Accounts & Privacy, mogu se precizno podesiti opcije kao:

- **Saglasnost korisnika pri registraciji**, uz dodatne informacije o načinu obrade podataka.
- **Automatsko brisanje ličnih podataka** korisnika nakon definisanog vremenskog perioda (npr. neaktivnosti).

Korišćenjem dodataka kao što su:

- **WP GDPR Compliance -** pruža prikupljanje i evidentiranje saglasnosti korisnika.
- **Complianz -** automatski generiše GDPR, CCPA i ostale pravne dokumente i omogućava prikaz kolačić banera i upravljanje saglasnostima.

🔐 **Važno:** Ovi alati ne samo da pomažu u usklađivanju sa zakonodavstvom, već i demonstriraju ozbiljnost sajta kada je u pitanju privatnost korisnika, što povećava kredibilitet i poverenje kod kupaca.

---

4. Pravila o kolačićima (Cookies Policy)

WooCommerce i razni dodaci koriste kolačiće za čuvanje podataka o korpi, sesijama, analitici i marketingu.

Potrebno je:

- Instalirati dodatak kao što je **CookieYes | GDPR Cookie Consent**, koji:
  - Prikazuje baner o kolačićima.
  - Omogućava korisniku da prihvati ili odbije određene kategorije kolačića.
  - Evidentira korisničku saglasnost (što je zakonski obavezno).
- Na stranici sajta prikazati politiku o kolačićima sa informacijama o:
  - Vrsti kolačića,
  - Svrsi i
  - Rokovima čuvanja.

---

5. Uslovi korišćenja (Terms of Service)

Za WooCommerce prodavnice, uslovi korišćenja definišu pravila o kupovini, dostavi, reklamacijama i odgovornostima. Preporučuje se:

- Kreirati stranicu “Uslovi korišćenja” i povezati je sa **Checkout** procesom.
- U **WooCommerce > Settings > Accounts & Privacy**, uključiti opciju da korisnik mora čekirati da prihvata uslove pre kupovine.
- Uslovi mogu da sadrže:
  - Opšte informacije o prodavnici,
  - Način plaćanja i isporuke,
  - Pravo na povraćaj i reklamaciju,
  - Nadležnost u slučaju spora.

⚖️ Jasno definisani uslovi štite i kupca i prodavca u slučaju nesporazuma ili pritužbi.

6. Alati za automatski backup sajta

WooCommerce prodavnice se često ažuriraju (npr. dodavanje novih proizvoda, obrada porudžbina, registracije korisnika), pa je **redovan backup ključan** za zaštitu podataka i kontinuitet poslovanja u slučaju grešaka, hakovanja ili tehničkih problema.

Preporučeni dodaci za automatski backup:

- **UpdraftPlus** – jedan od najpopularnijih besplatnih dodataka koji omogućava automatsko pravljenje rezervnih kopija fajlova i baze podataka. Pruža opcije za zakazivanje i jednostavno vraćanje sajta.
- **Jetpack Backup** (ranije VaultPress) – plaćeno rešenje koje omogućava **real-time backup** sa mogućnošću trenutno vraćanja sajta na prethodno stanje jednim klikom.

Backup se može automatski čuvati na različitim mestima:

- **Google Drive** – jednostavna integracija i besplatan prostor do određenog limita.
- **Dropbox** – popularan za deljenje i čuvanje podataka u cloud okruženju.
- **Amazon S3** – idealan za veće prodavnice zbog velike pouzdanosti i fleksibilnosti
- **Lokalni server** – rezervna kopija se čuva na istom serveru gde je i sajt, ali se preporučuje kombinovati s cloud skladištem za veću sigurnost.

📌 **Preporuka:** Pre bilo koje veće izmene na sajtu (npr. ažuriranja WooCommerce-a, WordPressa, dodavanje novog plugina ili teme), **uvek ručno napravite rezervnu kopiju**, kako biste mogli brzo vratiti prethodno stanje u slučaju nepredviđenih problema.

Korisni linkovi:

https://quadlayers.com/add-privacy-policy-for-woocommerce/

https://wpdesk.net/blog/woocommerce-gdpr-checkout/

https://cdn.websitepolicies.com/wp-content/uploads/2017/07/7-Key-Components-Every-Privacy-Policy-Should-Include.png