P1R4T3 SECURITY

Webshop biztonsági ellenőrzőlista

Élesítés előtt, a saját webshopban vagy tesztkörnyezetben. Idegen oldalt engedély nélkül ne próbáljon ki.

Fiókok és belépés

- [ ] Kétlépcsős azonosítás minden adminisztrátori fiókon
- [ ] Korábbi fejlesztők fiókjai törölve, nincs közös admin fiók
- [ ] Korlátozott belépési próbálkozás
- [ ] A jelszó-visszaállító link rövid ideig él, egyszer használható

Vásárlói adatok

- [ ] Az egyik fiókból nem nyitható meg a másik rendelése vagy számlája
- [ ] Számlák és rendelések belépés nélkül nem letölthetők
- [ ] Csak a szükséges adat tárolva, kártyaadat a fizetési szolgáltatónál

Rendelés és fizetés

- [ ] A fizetési visszaigazolást a szerver ellenőrzi
- [ ] Negatív vagy nulla darabszám nem fogadható el
- [ ] A kupon a korláton felül nem váltható be
- [ ] A rendelés nem véglegesíthető fizetés nélkül

Szoftver és fájlok

- [ ] Rendszer, téma, bővítmények frissítve, a nem használtak törölve
- [ ] Mentés, .env, .git, tesztfájl nem érhető el a webről
- [ ] A hibaoldal nem mutat műszaki részletet, nincs hibakereső mód

Szerver és e-mail

- [ ] HTTPS mindenhol, érvényes tanúsítvány, biztonsági fejlécek
- [ ] SPF, DKIM és DMARC beállítva
- [ ] Elkülönített, kipróbált mentés
- [ ] Naplózás és vészhelyzeti kapcsolattartó
- [ ] Ismert incidenskezelési teendők és határidők

A lista nem helyettesíti a behatolástesztet: a jogosultsági és üzleti logikai hibák kézi vizsgálatot igényelnek.
p1r4t3.hu/webes-behatolasteszt.html

Tájékoztató anyag, nem jogi tanács.