



auditeshopu.eu

UKÁZKA – smyšlený e-shop

FUNKČNÍ AUDIT WEBU

Číslo zprávy UKZ-2026-001

Datum 28. 10. 2026

Verze v1

UKÁZKA, smyšlený e-shop.

Tento dokument je vzor výstupu auditu. E-shop „Čajovna Mlha“ ani doména **cajovna-mlha.example** neexistují. Všechny nálezy, časy, adresy a hodnoty jsou vymyšlené podle typických chyb, které na webech nacházíme.

Funkční audit webu cajovna-mlha.example

UKÁZKA, smyšlený e-shop

Web	https://www.cajovna-mlha.example (smyšlený)
Typ	e-shop s čajem a čajovým nádobím
Rozsah	objednávka, registrace, zapomenuté heslo, kontaktní formulář, pošta, cookies, dostupnost
Souhlas majitele	písemný, před začátkem auditu
Období testů	7 dní (UKÁZKA)

Zpráva má tyto části:

- Zpráva pro majitele.** Co je špatně, co to dělá se zákazníky a co opravit nejdřív.
- Nálezy podle dopadu.** Každý nález s obrázkem „takhle to vidí zákazník → po opravě“.
- Výsledky ověřovacích testů.** Co jsme vyzkoušeli a jak to dopadlo.
- Výpadky webu.** Kdy web neběžel nebo byl pomalý.
- Přehled pro správce (IT).** Přesné kroky, jak chybu zopakovat, a postup opravy.
- Doporučení dalšího postupu.**
- Co potřebujeme k dokončení.**
- Technická příloha.**

1. Zpráva pro majitele

UKÁZKA, smyšlený e-shop.

Shrnutí

Web na první pohled funguje. Při nákupu jako zákazník jsme ale našli několik míst, kde se objednávky a zákazníci ztrácejí potichu: nikdo nedostane chybovou hlášku a vy se o tom nedozvíte.

Nejvážnější je kombinace dvou chyb. Překlep v e-mailu projde bez upozornění a potvrzení objednávek z domény navíc padají do spamu. Zákazník tak často nemá žádné potvrzení a nevěří, že objednávka prošla.

Stav	Oblast	Co to znamená pro zákazníka
●	Pošta domény	Potvrzení objednávek padají do spamu nebo se nedoručí vůbec.
●	E-mail v objednávce	Překlep v adrese projde. Zákazník nedostane potvrzení a myslí si, že objednávka neprošla.
●	Košík	Košík jde rozbít: záporný počet ho smaže, písmena místo čísla dají cenu 0 Kč.
●	Výpadky	Web opakovaně vrací chybu 502, jednou nejel kolem 20 minut.
●	Roboti	Registrace a zapomenuté heslo nemají ochranu. V databázi přibývají falešné účty.
●	Formuláře	Telefon nebo PSČ s mezerou formulář odmítne. Na mobilu se ukáže písmenná klávesnice.
●	Cookies	Facebook a Seznam měří ještě před souhlasem. V liště chybí tlačítko „Odmítnout“.
●	Texty	Na webu visí staré oznámení a v patičce zmínka o EET.

● bere objednávky hned · ● bere zákazníky nebo hrozí pokuta · ● kazí dojem

Co opravit nejdřív

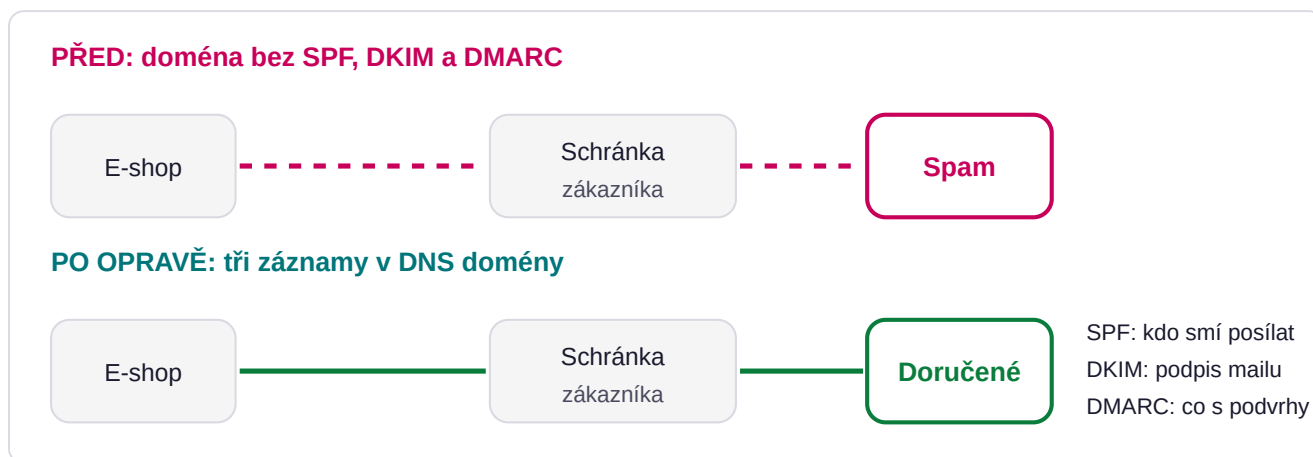
- Pošta domény (SPF, DKIM, DMARC).** Malý zásah v nastavení domény. Bez toho nemají smysl ostatní opravy kolem e-mailů.
- Kontrola e-mailu v objednávce.** Upozornit na překlep („Nemysleli jste gmail.com?“) a e-mail ověřit.
- Košík.** Povolit jen celé kladné počty a stejné zboží slučovat.
- Výpadky.** Zjistit příčinu chyb 502 u hostingu a zapnout hlídání dostupnosti.
- Ochrana proti robotům** na registraci, zapomenutém heslu a formulářích.
- Cookies.** Spouštět měření až po souhlasu a přidat „Odmítnout“.
- Formuláře a texty.** Drobnosti, ale zákazník je vidí.

2. Nálezy podle dopadu

UKÁZKA, smyšlený e-shop.

● Maily z e-shopu končí ve spamu

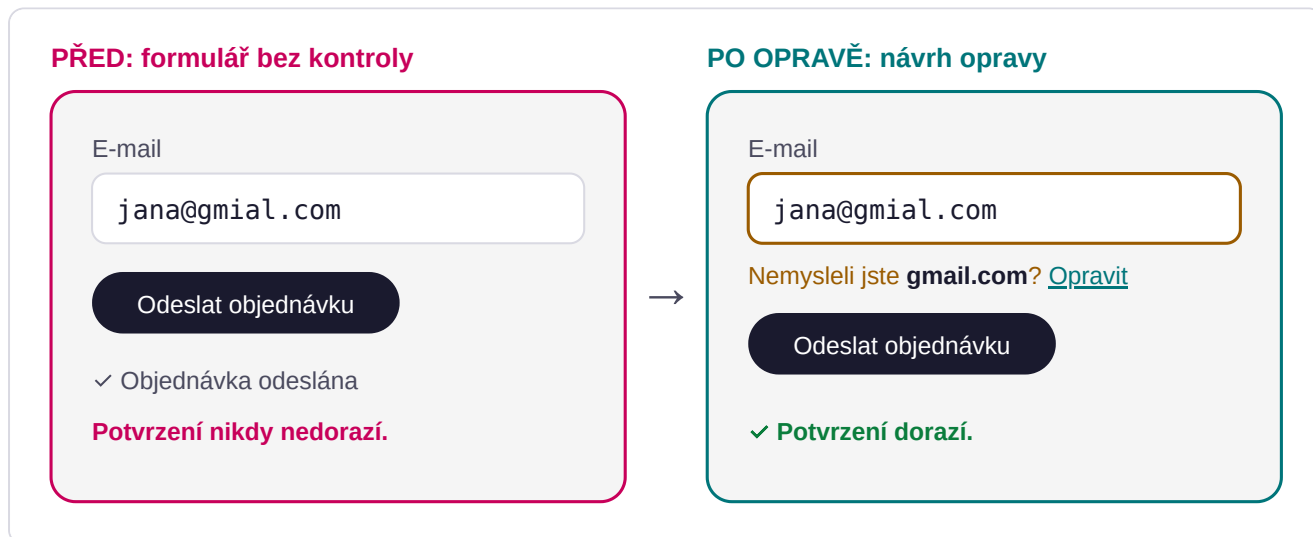
Doména nemá nastavené SPF ani DMARC a maily nejsou podepsané (DKIM). Velké schránky takovým mailům nevěří. Potvrzení objednávky, odpověď na dotaz i obnova hesla končí ve spamu.



Pošta: bez SPF, DKIM a DMARC skončí mail ve spamu

● Překlep v e-mailu projde bez upozornění

Zákazník napíše **gmial.com** místo **gmail.com** a objednávka projde. Potvrzení odejde na neexistující adresu a zákazník ho nikdy nedostane.



Překlep v e-mailu: před a po opravě

● Košík jde rozbít

Záporný počet kusů smaže celý košík. Písmena místo čísla dají cenu 0 Kč. Stejně zboží přidané dvakrát se neslučuje.

PŘED: košík přijme cokoli

Zelený čaj
-1

Košík je prázdný.

Konvička
abc

Celkem
0 Kč

→

PO OPRAVĚ

Zelený čaj
- 2 +

Méně než 1 kus nejde zadat.

Konvička
- 1 +

Stejně zboží se sečte do jednoho řádku.

Košík: před a po opravě

● Výpadky a pomalé stránky

Během sedmi dnů měření web opakovaně vracel chybu 502 a jednou nejel kolem 20 minut. Úvodní stránka se načítala 3 až 21 sekund. Podrobnosti jsou v části 4.

● Formuláře odmítají správné údaje

Telefon nebo PSČ s mezerou formulář odmítne. Zákazník to zkusí jednou, dvakrát a odejde.

PŘED: správné údaje neprojdou

Telefon

+420 777 000 000

Neplatné telefonní číslo

PSČ

110 00

Neplatné PSČ

→

PO OPRAVĚ

Telefon

+420 777 000 000
✓

PSČ

110 00
✓

Na mobilu rovnou číselná klávesnice.

Formulář: před a po opravě

● Měření před souhlasem s cookies

Facebook a Seznam měří hned po otevření stránky. Lišta nabízí jen „Přijmout vše“, odmítnout nejde.



Cookies: před a po opravě

● Roboti v registraci

Registrace a zapomenuté heslo nemají ochranu proti robotům a nová registrace nevyžaduje potvrzení e-mailu. V administraci přibývají účty s náhodnými adresami.

● Zastaralé texty

Na úvodní stránce visí oznámení o loňské vánoční dovolené. V patičce je věta o evidenci tržeb (EET).

3. Výsledky ověřovacích testů

UKÁZKA, smyšlený e-shop. Testovací objednávky byly označené jako test a majitel je stornoval.

#	Test	Postup	Očekávané	Skutečné	Výsledek
T1	Potvrzení objednávky	objednávka na schránky u Gmailu a Seznamu	potvrzení v doručené poště	Gmail: spam, Seznam: spam	chyba
T2	Překlep v e-mailu	objednávka s test@gmial.com	upozornění na překlep	projde bez upozornění	chyba
T3	Kontaktní formulář	dotaz z formuláře	dotaz dorazí majiteli	dorazí, odpověď zákazníkovi ve spamu	částečně
T4	Košík: záporný počet	počet -1	odmítnout	košík smazán	chyba
T5	Košík: nečíselný počet	počet abc	odmítnout	cena 0 Kč	chyba
T6	Košík: stejné zboží 2x	přidat stejný čaj dvakrát	1 řádek, 2 kusy	2 řádky	částečně
T7	Registrace robotem	odeslání formuláře bez prohlížeče	odmítnout	účet založen	chyba
T8	Zapomenuté heslo	20 žádostí za minutu na jednu adresu	omezit	všech 20 odešlo	chyba
T9	Telefon s mezerou	+420 777 000 000	přijmout	„Neplatné telefonní číslo“	chyba
T10	PSČ s mezerou	110 00	přijmout	„Neplatné PSČ“	chyba
T11	Cookies před souhlasem	otevření stránky, bez volby	žádné měření	Facebook, Seznam	chyba
T12	Odmítnutí cookies	hledat „Odmítnout“	tlačítko v liště	chybí	chyba
T13	Objednávka až do konce	objednávka s převodem	potvrzení + platební údaje	proběhne, potvrzení ve spamu	částečně

chyba · částečně funguje jen částečně · v pořádku v pořádku

4. Výpadky webu

UKÁZKA, smyšlený e-shop. Měřeno každou minutu po dobu 7 dní z veřejného internetu.

Den	Čas	Trvání	Co vidí zákazník
2. den	10:14–10:16	2 min	chyba 502
3. den	19:42–20:03	21 min	chyba 502
5. den	08:30–08:31	1 min	chyba 502
6. den	20:10–20:14	4 min	odezva nad 15 s

Odezva úvodní stránky: obvykle 3 až 5 s, ve večerní špičce až 21 s.

Co z toho plyne: výpadky přicházejí hlavně večer, kdy lidé nakupují nejvíc. Chyba 502 znamená, že server za webem nestíhá. Nejčastější příčiny jsou málo výkonu na hostingu, chybějící cache a zbytečná zátěž od robotů.

5. Přehled pro správce (IT)

UKÁZKA, smyšlený e-shop. Všechny adresy, hodnoty a výstupy jsou smyšlené.

ID	Závažnost	Oblast	Nález	Test
A-01	vysoká	Pošta	Chybí SPF, DMARC; DKIM nenastaven	T1, T3
A-02	vysoká	Objednávka	E-mail se nekontroluje na překlepy ani neověřuje	T2
A-03	vysoká	Košík	Záporný a nečíselný počet kusů, neslučování položek	T4-T6
A-04	vysoká	Dostupnost	Opakované 502, výpadek kolem 20 min, odezvy 3-21 s	část 4
A-05	střední	Ochrana	Registrace a zapomenuté heslo bez ochrany proti botům	T7, T8
A-06	střední	Formuláře	Telefon a PSČ s mezerou odmítnuty, chybí type="email" a type="tel"	T9, T10
A-07	střední	Cookies	Měřicí skripty před souhlasem, chybí „Odmítnout“	T11, T12
A-08	nízká	Obsah	Zastaralé oznámení, zmínka o EET v patičce	-

A-01 Pošta: chybí SPF a DMARC, DKIM není nastaven

Zjištění (DNS, UKÁZKA):

```
$ dig +short TXT cajovna-mlha.example
"google-site-verification=..."      ← SPF chybí
$ dig +short TXT _dmarc.cajovna-mlha.example
                                     ← DMARC chybí
$ dig +short TXT default._domainkey.cajovna-mlha.example
                                     ← DKIM pod běžnými selektory nenalezen
```

Oprava:

- Zjistit všechny služby, které posílají maily za doménu (e-shop, poštovní schránky, newsletter).
- Přidat jeden SPF záznam, např. **v=spf1 include:<poskytovatel> -all**.
- Zapnout DKIM u každé odesílající služby a vložit klíč do DNS.
- Přidat DMARC nejdřív v režimu sledování: **v=DMARC1; p=none; rua=mailto:<adresa pro reporty>**. Po kontrole reportů přejít na **p=quarantine**, pak **p=reject**.

Ověření: testovací mail na schránky u Gmailu a Seznamu dorazí do doručené pošty a v hlavičce je `spf=pass, dkim=pass, dmarc=pass`.

A-02 Objednávka: překlep v e-mailu projde

Kroky: vložit zboží do košíku, do pole E-mail zadat `test@gmial.com` (také `seznam.cy`, `centum.cz`, `emial.cz`), dokončit objednávku.

Oprava: u pole e-mailu nabídnout opravu známých domén („Nemysleli jste gmail.com?“), pole označit `type="email"` a `autocomplete="email"`. Nedoručitelné potvrzení (bounce) posílat i správci e-shopu.

Ověření: nabídka opravy se ukáže a po opravě potvrzení dorazí.

A-03 Košík

Oprava: validace na serveru (celé číslo, minimálně 1, rozumný strop), ne jen v prohlížeči. Pole `type="number" min="1" step="1" inputmode="numeric"`. Při přidání stejného zboží zvýšit počet u existující položky.

Ověření: testy T4–T6 projdou, i když se požadavek pošle mimo formulář.

A-04 Dostupnost a odezva

Oprava: projít s hostingem logy v časech výpadků z části 4 (PHP procesy, paměť, databáze). Zapnout cache stránek a ochranu před boty, která sníží zbytečnou zátěž. Nasadit hlídání dostupnosti s upozorněním.

Ověření: hlídání po dobu aspoň dvou týdnů bez výpadku, odezva úvodní stránky trvale nízká.

A-05 Roboti: registrace a zapomenuté heslo

Oprava: Cloudflare Turnstile (nebo jiná ochrana) na registraci, přihlášení, obnovu hesla a formuláře. Ověření e-mailu při registraci. Limit pokusů z jedné IP. Smazat falešné účty.

Ověření: automatizované odeslání formuláře bez ochranného tokenu server odmítne (T7), obnova hesla je omezená (T8).

A-06 Formuláře

Oprava: mezery a pomlčky před kontrolou odstranit, ne odmítnout. Doplnit `type="tel"`, `inputmode="numeric"` u PSČ a `autocomplete` u všech polí.

A-07 Cookies

Oprava: měřicí skripty spouštět až po souhlasu (blokování v nástroji pro souhlas nebo Consent Mode). Do lišty přidat „Odmítnout“ stejně viditelné jako „Přijmout“.

Ověření: v nástrojích prohlížeče (Síť) se před souhlasem nenačte žádný měřicí skript. Po odmítnutí také ne.

A-08 Zastaralé texty

Oprava: texty odstranit nebo aktualizovat. Oznámením nastavit datum, kdy samy zmizí.

6. Doporučení dalšího postupu

UKÁZKA, smyšlený e-shop.

Hned (tento týden)

- Nastavit SPF, DKIM a DMARC (A-01).
- Kontrola překlepu v e-mailu v objednávce (A-02).
- Opravit košík (A-03).

Do dvou týdnů

- Vyřešit s hostingem výpadky a zapnout hlídání dostupnosti (A-04).
- Ochrana proti robotům a smazání falešných účtů (A-05).
- Cookies podle pravidel (A-07).

Potom

- Formuláře a texty (A-06, A-08).
- Po opravách krátké přezkoušení testů T1–T13.
- Zvážit, jestli se současná platforma vyplatí dál opravovat, nebo jestli je výhodnější převod na jinou.

7. Co potřebujeme k dokončení

UKÁZKA, smyšlený e-shop.

Některé věci se ze zvenku ověřit nedají. K dokončení auditu potřebujeme:

- **Přístup ke správě DNS** (nebo kontakt na toho, kdo ji spravuje), abychom ověřili nastavení pošty po opravě.
- **Seznam služeb, které posílají maily za doménu** (e-shop, newsletter, účetní systém).
- **Logy serveru z časů výpadků** z části 4, od hostingu.
- **Kontakt na správce webu**, se kterým projdeme technický protokol.
- **Souhlas s druhým kolem testovacích objednávek** po opravách.

8. Technická příloha

UKÁZKA, smyšlený e-shop.

Jak jsme testovali

- Se souhlasem majitele, z běžného prohlížeče (počítač a mobil) a z příkazové řádky.
- Testovací objednávky byly označené jako test a majitel je stornoval. Testovací účty jsme po auditu smazali.
- Zátěžové testy ani útoky jsme nedělali.

Testované adresy

Stránka	Adresa (smyšlená)
Úvod	https://www.cajovna-mlha.example/
Košík	https://www.cajovna-mlha.example/kosik/
Objednávka	https://www.cajovna-mlha.example/objednavka/
Registrace	https://www.cajovna-mlha.example/registrace/
Zapomenuté heslo	https://www.cajovna-mlha.example/zapomenute-heslo/
Kontakt	https://www.cajovna-mlha.example/kontakt/

Hlavičky úvodní stránky (výňatek, UKÁZKA)

```
HTTP/2 200
server: nginx
content-type: text/html; charset=utf-8
set-cookie: PHPSESSID=...; path=/

    ← chybí strict-transport-security
    ← žádná ochrana proti botům
```

Slovníček

- **SPF:** záznam v DNS, který říká, které servery smí posílat maily za vaši doménu.
- **DKIM:** elektronický podpis mailu. Schránka podle něj pozná, že mail nikdo cestou nezměnil.
- **DMARC:** pravidlo, co má schránka udělat s mailem, který neprojde SPF ani DKIM.
- **502 Bad Gateway:** server za webem neodpověděl včas. Zákazník místo stránky vidí chybu.
- **Turnstile:** ochrana proti robotům od Cloudflare. Lidé obvykle nic nevyplňují.

Konec ukázky. UKÁZKA, smyšlený e-shop: „Čajovna Mlha“ ani [cajovna-mlha.example](https://www.cajovna-mlha.example) neexistují.