

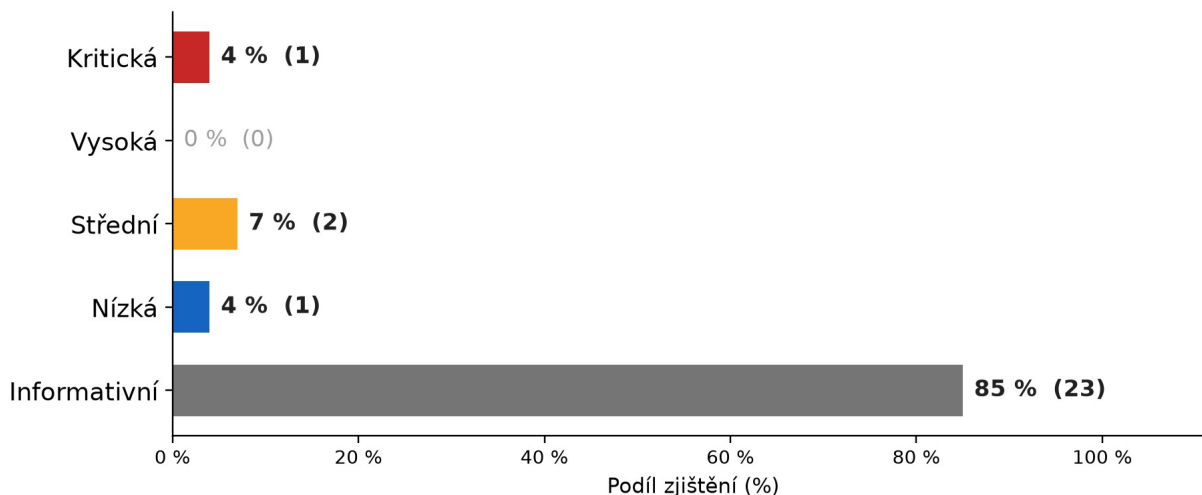
Toto je váš report z této stránky.

Skenovaná stránka: example-customer-1.cz (anonymizovaná ukázka)

Datum skenu: od 12. 1. 2026 14:46:54 do 12. 1. 2026 14:48:00 (SEČ)

Počet požadavků doložených v záznamu skenu: 13 (12 webových a 1 DNS) ¹

Ukázkový report vytvořený z anonymizovaných veřejných dat; slouží pouze ke kontrole vzhledu a obsahu šablony.



Rozdělení nalezených zjištění podle závažnosti (v %). Závažnost uvádí skener; naše doporučené pořadí oprav je níže.

Celkem nalezeno: 27 zjištění.

Toto je to, co jsme našli, shrnuto pro vás.

1. Hlavní výsledky jednoduše

Prověřili jsme veřejně dostupnou část vašeho webu. Sken našel celkem **27 zjištění: 1 kritické, 2 střední, 1 nízké a 23 informativních** (drobnosti a údaje o tom, z čeho je web postaven).

Dvě věci stojí za okamžitou pozornost:

- **Do správy webu se dá přihlásit výchozím jménem a heslem.** Je to jako nechat klíč od domu pod rohožkou: kdokoli, kdo to zkusí, se dostane dovnitř.
- **Web veřejně ukazuje soubory, které návštěvníci vidět nemají** – nastavení zdrojového kódu, popis toho, jak je server sestaven, a stránku s podrobnostmi o serveru. Je to jako nechat plány domu v poštovní schránce: samy o sobě nic neotevřou, ale útočníkovi ušetří spoustu práce.

Dobrá zpráva: nic z toho nevyžaduje velkou investici, většinou jde o změnu hesla a smazání nebo zablokování několika souborů.

Sken běžel přes nešifrované spojení (adresa začínající http://, port 80). Hesla a přihlašovací cookies tak mohou být na cestě mezi návštěvníkem a webem čitelná pro třetí osoby. Chybějící zabezpečení spojení vidíme i u cookies a v chybějících hlavičkách (viz níže).

2. Co je nejrizikovější a co to znamená v praxi

- **Výchozí přihlášení (kritické; přihlašovací formulář správy, `dvwa-default-login`)**. Útočník se může přihlásit, měnit obsah, číst data nebo web zneužít. Přihlašovací údaje, které se skenu podařilo použít, v reportu z bezpečnostních důvodů neuvádíme.
- **Veřejná konfigurace zdrojového kódu a popis serveru (střední; veřejné soubory, `git-config`, `dockerfile-hidden-disclosure`)**. Prozrazují, kde je kód uložený a jak je server nastaven. Útočník díky tomu snáz hledá slabá místa.
- **Veřejná diagnostická stránka serveru (nízké podle skeneru, u nás střední; `phpinfo-files`)**. Ukazuje verze programů, cesty k souborům na serveru i interní adresy v počítačové síti. Hodnoty zde záměrně neuvádíme.
- **Přihlašovací cookies bez ochrany (informativní, u nás střední; odpovědi serveru, `cookies-without-httponly`, `cookies-without-secure`, `missing-cookie-samesite-strict`)**. Kdo cookie získá, může se vydávat za přihlášeného uživatele.
- **Drobnosti (nízké/informativní)**. Veřejné soubory .gitignore a README.md, chybějící bezpečnostní hlavičky, viditelné verze softwaru.

3. Citlivé údaje, které sken zachytil (hodnoty z bezpečnostních důvodů neuvádíme)

Při skenu jsme narazili na následující citlivé údaje. **Konkrétní hodnoty záměrně neuvádíme**, ale víte, že riziko existuje, a níže najdete, co s tím.

Co sken zachytil	Kde to bylo vidět (oblast)	Detekováno šablonou	Proč to vadí	Co dělat	Priorita
Fungující výchozí přihlašovací údaje (jméno a heslo)	přihlašovací formulář správy webu	dvwa-default-login	Kdokoli je může použít k přihlášení	Heslo ihned změnit, zrušit výchozí účet, omezit přístup ke správě	Kritická
Aktivní přihlašovací (session) cookies	odpovědi serveru na úvodní a přihlašovací stránce (19 z 27 zaznamenaných odpovědí)	cookies-without-httponly, cookies-without-secure, missing-cookie-samesite-strict	Kdo cookie získá, může se vydávat za přihlášeného	Zneplatnit (vynutit nové přihlášení), zapnout příznaky HttpOnly, Secure a SameSite, přejít na HTTPS	Střední
Ochranný (CSRF) token	přihlašovací formulář a odpověď na přihlášení	dvwa-default-login (token je vidět v záznamu tohoto přihlášení)	Token má chránit formulář před podvrženými požadavky; ve veřejné odpovědi mu to ztěžuje	Ověřit, že se token po každém použití obnovuje a váže na uživatele	Nízká
Interní cesty na serveru a konfigurace PHP	veřejná diagnostická stránka serveru a dva veřejně dostupné soubory v kořeni webu (popis sestavení a úvodní dokumentace)	dockerfile-hidden-disclosure, phpinfo-files, readme-md	Prozrazují uspořádání serveru	Diagnostickou stránku smazat, oba soubory zablokovat, vypnout podrobná chybová hlášení	Střední
Interní IP adresy (soukromá síť)	veřejná diagnostická stránka serveru	phpinfo-files	Odhalují strukturu sítě za webem	Stránku smazat nebo omezit na správce	Střední
Adresa zdrojového repozitáře	veřejně dostupný konfigurační soubor správy verzí v kořeni webu	git-config	Ukazuje, kde se kód nachází, a usnadňuje jeho stažení	Zablokovat přístup ke složce správy verzí, odstranit ji z veřejné části webu	Střední
Kontaktní e-mail třetí strany (součást licenčního textu PHP)	veřejná diagnostická stránka serveru	phpinfo-files	Sám o sobě nebezpečný není, ale potvrzuje, že stránka vypisuje interní texty	Odstranit se spolu s diagnostickou stránkou	Nízká

4. Co opravit – podle priority

Pořadí	Priorita	Co	Co s tím
1	Kritická	Výchozí přihlašovací údaje fungují (přihlašovací formulář správy, dvwa-default-login)	Změnit heslo na dlouhé a jedinečné, zrušit výchozí účet, zapnout omezení neúspěšných pokusů nebo dvoufázové ověření.
2	Střední	Veřejný konfigurační soubor správy verzí a popis sestavení serveru (veřejné soubory, git-config, dockerfile-hidden-disclosure)	Zablokovat přístup na úrovni webového serveru nebo soubory z veřejné části webu odstranit.
3	Střední	Veřejná diagnostická stránka serveru (phpinfo-files)	Smazat soubor, případně omezit přístup jen pro správce.
4	Střední	Session cookies bez ochrany (odpovědi serveru; cookies-without-httponly, cookies-without-secure, missing-cookie-samesite-strict) a nešifrované spojení	Zapnout HTTPS (certifikát) a přesměrování z http na https, nastavit cookies s příznaky HttpOnly, Secure, SameSite; zneplatnit stávající relace.
5	Nízká	CSRF token v přihlašovacím formuláři (dvwa-default-login)	Zkontrolovat obnovování tokenů po každém použití.
6	Nízká	.gitignore a README.md veřejně dostupné (exposed-gitignore, readme-md)	Smazat nebo zablokovat.
7	Nízká	11 chybějících bezpečnostních hlaviček (např. HSTS, Content-Security-Policy, X-Frame-Options; http-missing-security-headers)	Doplnit v nastavení webového serveru; typicky jednorázová úprava konfigurace.
8	Informativní	Viditelné verze Apache a PHP; robots.txt zakazuje celý web vyhledávačům	Verze v hlavičkách skrýt. Zakazuje-li robots.txt celý web záměrně, je to v pořádku; jinak se web ve vyhledávačích neobjeví.

Pořadí vychází z toho, jak snadno lze zjištění zneužít a jak vážné by to bylo. Závažnost v grafu je ta, kterou uvádí skener; u phpinfo a cookies jsme priority zvýšili kvůli citlivým údajům, které prozrazují.

5. Srovnání s minulým měsícem

UKÁZKOVÁ DATA – NEJDE O SKUTEČNÝ MINULÝ SKEN. Minulý měsíc je uměle vytvořen z týchž anonymizovaných dat: tři nálezy z aktuálního skenu jsme odebrali (v ukázce tedy vyjdou jako „nové“), dva nálezy z jiného veřejného vzorku jsme přidali (v ukázce vyjdou jako „opravené“). Slouží jen k předvedení struktury této části reportu.

Předchozí sken (ukázka): 12. 12. 2025 14:46:54 – 12. 12. 2025 14:48:12 (SEČ), 26 zjištění. Aktuální sken: 27 zjištění.

Zjištění	Oblast / šablona	Závažnost	Minule	Nyní	Stav
Výchozí přihlašovací údaje fungují	citlivé: přihlašovací formulář správy; dvwa-default-login	Kritická	ano	ano	stále otevřené
Veřejně dostupná konfigurace zdrojového kódu (/ .git/config)	citlivé: veřejný soubor v kořeni webu; git-config	Střední	ano	ano	stále otevřené
Veřejně dostupný popis sestavení serveru (soubor Dockerfile)	citlivé: veřejný soubor v kořeni webu; dockerfile-hidden-disclosure	Střední	–	ano	nové
Veřejná stránka s podrobnostmi o serveru (phpinfo)	citlivé: veřejná diagnostická stránka serveru; phpinfo-files	Nízká	ano	ano	stále otevřené
Přihlašovací (session) cookies	citlivé: odpovědi serveru na úvodní	Informativní	ano	ano	stále otevřené

bez ochrany	a přihlašovací stránce; cookies-without-httponly, cookies-without-secure, missing-cookie-samesite-strict				
Ochranný (CSRF) token viditelný v komunikaci	citlivé: přihlašovací formulář; dvwa-default-login	Nízká	ano	ano	stále otevřené
Veřejně dostupný soubor .gitignore	veřejný soubor v kořeni webu; exposed-gitignore	Informativní	-	ano	nové
Veřejně dostupný soubor README.md	citlivé: veřejný soubor v kořeni webu (interní cesty); readme-md	Informativní	-	ano	nové
Chybějící bezpečnostní hlavičky	odpověď serveru na úvodní stránce; http-missing-security-headers	Informativní	ano	ano	stále otevřené - beze změny (11 → 11)
Dostupná instalační stránka phpMyAdmin	instalační stránka správy databáze; phpmyadmin-setup	Střední	ano	-	opraveno
Databázový server (MySQL) dostupný zvenku	citlivé: databázový port serveru; mysql-native-password-bruteforce	Informativní	ano	-	opraveno
robots.txt zakazuje vyhledávačům celý web	veřejný soubor robots.txt; robots-txt-endpoint	Informativní	ano	ano	stále otevřené
Viditelné verze použitého softwaru (Apache, PHP)	odpověď serveru na úvodní stránce; apache-detect, php-detect	Informativní	ano	ano	stále otevřené

Shrnutí srovnání (ukázka): opraveno 2, nově 3, stále otevřených 8.

Zlepšilo se to, nebo ne? Celkově bez zlepšení (mírné zhoršení). Kritické zjištění (výchozí přihlášení) je stále otevřené, citlivé údaje (označené v tabulce „citlivé“: cookies, token, interní cesty a IP adresy) rovněž. Nově přibyl veřejný soubor s popisem sestavení serveru (dockerfile-hidden-disclosure) a veřejný README.md, které prozrazují interní cesty; opraveno je citlivé zjištění o dostupném databázovém portu (mysql-native-password-bruteforce). Opraveny jsou dvě starší věci, ale přibyl tři nové. Počty podle závažnosti, minule → nyní: kritická 1 → 1, střední 2 → 2, nízká 1 → 1, informativní 22 → 23.

¹ **Jak jsme počet požadavků určili.** Soubor od skeneru obsahuje jen nálezy, ne seznam všech odeslaných požadavků, takže celkový počet (včetně kontrol, které nic nenašly) v datech není a nebudeme ho vymýšlet. Uvedené číslo 13 je počet různých požadavků zaznamenaných u nálezu: 12 webových (HTTP) a 1 DNS dotaz. Dvě kontroly cookies používají hlavičky již získané odpovědi a nové požadavky nepřidávají; 11 nálezu o hlavičkách pochází z jediného požadavku. Skutečný počet je tedy minimálně 13. Šablony skeneru, které nález vytvořily (17), mohou podle svých metadat poslat nejvýše 47 požadavků. V ostrém provozu budeme celkový počet ukládat přímo ze skeneru.