

Bezpečnost webových stránek

Přehled pro provozovatele webu bez IT vzdělání

Tento dokument je úvod do bezpečnosti webových stránek pro člověka, který si staví vlastní web a nepochází z IT oboru. Cílem není nahradit odborníka, ale dát vám slovník a orientaci: jaké útoky na weby existují, co je potřeba hlídat a testovat, a jak k tomu přistoupit, pokud web obsahuje rezervační systém nebo platební bránu. Dokument uzavírá kontrolní seznam bezpečnostního minima.

Upozornění: jde o obecný přehled. Konkrétní kroky se liší podle toho, jaký CMS, hosting nebo platební bránu použijete. U citlivých částí (platby, osobní údaje) doporučujeme na klíčová rozhodnutí přizvat odborníka nebo dodavatele, který za bezpečnost nese odpovědnost.

1. Pět klíčových zdrojů k tématu

Následující zdroje jsou standardně uznávané organizace a normy v oboru webové bezpečnosti. Doporučujeme se k nim vracet i po přečtení tohoto přehledu.

1. OWASP Top 10

Nejcitovanější seznam nejkritičtějších bezpečnostních rizik webových aplikací, který sestavuje nezisková organizace OWASP (Open Worldwide Application Security Project). Dobrý první krok pro pochopení, co útočníci nejčastěji zneužívají.

<https://owasp.org/www-project-top-ten/>

2. OWASP Web Security Testing Guide (WSTG)

Rozsáhlá praktická příručka od stejné organizace, jak se web dá systematicky testovat — od základní konfigurace přes ověřování a přihlašování až po platební a relační logiku. Vhodné spíš jako referenční příručka než čtení od začátku do konce.

<https://owasp.org/www-project-web-security-testing-guide/>

3. NÚKIB — Doporučení a Minimální bezpečnostní standard

Národní úřad pro kybernetickou a informační bezpečnost publikuje doporučení v češtině zaměřená i na menší organizace, včetně dokumentu Minimální bezpečnostní standard, který srozumitelně popisuje základní opatření.

<https://www.nukib.cz/cs/infoservis/doporuceni/>

4. PCI DSS — Payment Card Industry Data Security Standard

Pokud bude web přijímat platby kartou, tento standard definuje 12 základních požadavků na ochranu dat platebních karet. Spravuje ho PCI Security Standards Council, sdružení hlavních karetních společností (Visa, Mastercard a další).

<https://www.pcisecuritystandards.org/>

5. Mozilla — Web Security Guidelines / Observatory

Praktický, srozumitelný přehled bezpečnostních doporučení pro provozovatele webů od Mozilly, doplněný o bezplatný nástroj Mozilla Observatory, kterým lze web okamžitě otestovat a dostat konkrétní doporučení.

https://infosec.mozilla.org/guidelines/web_security a <https://developer.mozilla.org/en-US/observatory>

2. Nejčastější typy útoků na běžné weby

Útočníci většinou nejdou po „velké rybě“ — jdou po nejsnadnějším cíli. Malý web bez zabezpečení je pro ně stejně zajímavý jako velký, protože útoky se často spouští automatizovaně na tisíce webů najednou. Níže jsou nejčastější typy útoků, se kterými se běžný web může setkat.

2.1 SQL injection (vpašování databázového příkazu)

Útočník vloží do formuláře (přihlášení, vyhledávání, kontaktní formulář) speciálně sestavený text, který se místo dat vykoná jako příkaz do databáze. Výsledkem může být únik celé databáze (e-maily, hesla, objednávky) nebo její smazání. Riziko roste, pokud web nepoužívá standardní, ošetřené dotazy do databáze.

2.2 Cross-site scripting — XSS

Útočník vloží do webu (např. do komentáře, recenze, jména v rezervaci) kus kódu, který se pak spustí v prohlížeči jiných návštěvníků nebo administrátora. Může tak krást přihlašovací údaje, přesměrovávat na podvodné stránky nebo jednat jménem přihlášeného uživatele.

2.3 Broken access control — nedostatečné ověření oprávnění

Web sice ověří, že je uživatel přihlášený, ale už nekontroluje, zda smí vidět nebo měnit konkrétní záznam. Typický příklad: v URL adrese rezervace stačí změnit číslo a zobrazí se cizí rezervace nebo faktura (tzv. IDOR — Insecure Direct Object Reference).

2.4 Prolomení hesla a přihlašování

Sem patří hrubá síla (postupné zkoušení hesel), credential stuffing (zkoušení hesel unikátých z jiných služeb) a phishing zaměřený přímo na administrátora webu. Slabá hesla a chybějící dvoufaktorové ověření jsou nejčastější důvod, proč se útočník dostane do administrace.

2.5 Cross-site request forgery — CSRF

Útočník donutí přihlášeného uživatele (např. přes odkaz v e-mailu), aby nevědomky odeslal na web požadavek — třeba změnu hesla nebo e-mailu ve svém účtu — aniž by to sám zamýšlel.

2.6 Chybná konfigurace zabezpečení

Ponechané výchozí přihlašovací údaje, veřejně přístupné administrační nebo testovací rozdíly, zapnuté podrobné chybové hlášky odhalující strukturu serveru, otevřené zálohy databáze ke stažení. Toto je extrémně častá příčina úspěšných útoků, protože nevyžaduje žádnou složitou techniku — útočník jen zkouší známé cesty a nastavení.

2.7 Nebezpečné nahrávání souborů

Pokud web umožňuje nahrát soubor (fotku, přílohu, životopis) a nekontroluje jeho typ a obsah, útočník může nahrát skript, který se následně na serveru spustí, a tím převzít nad webem kontrolu.

2.8 Zranitelné a zastaralé komponenty

Web postavený na CMS (WordPress, Shoptet, PrestaShop apod.) používá desítky pluginů a knihoven. Pokud nejsou pravidelně aktualizované, útočníci zneužívají veřejně známé díry v konkrétních verzích — toto je dnes vůbec nejčastější cesta k napadení malých webů.

2.9 Phishing a sociální inženýrství

Útok necílí na technologii, ale na člověka — podvodný e-mail vydávající se za hostingovou firmu, registrátora domény nebo bankovní bránu, který má vylákat přihlašovací údaje nebo platbu.

2.10 DDoS a zahlcení serveru

Web je zahlcen velkým množstvím požadavků a stane se nedostupným. U malých webů jde méně o cílený útok, více o vedlejší efekt automatizovaných botů nebo o vydírání (zaplatte, jinak web spadne).

2.11 Man-in-the-middle a chybějící šifrování

Pokud web (nebo jeho část, například přihlášení) neběží na zabezpečeném HTTPS, data cestující mezi návštěvníkem a serverem lze na cestě odposlechnout nebo pozměnit — typicky ve veřejné Wi-Fi síti.

2.12 Ransomware a defacement

Po proniknutí na server útočník buď obsah zašifruje a požaduje výkupné, nebo web viditelně poškodí (změní úvodní stránku). Obranně proti následkům pomáhají hlavně funkční zálohy mimo server.

3. Co hlídat a testovat u běžného webu

Tato kapitola shrnuje oblasti, které má smysl pravidelně kontrolovat, i bez hlubokých technických znalostí — buď vlastníma rukama pomocí volně dostupných nástrojů, nebo formou zadání konkrétní kontroly dodavateli webu.

3.1 Aktualizace

- CMS, šablona a všechny pluginy/rozšíření jsou na nejnovější verzi.
- Nepoužívané pluginy a účty se odstraňují, ne jen deaktivují.
- Hostingová platforma (PHP, databáze) běží na verzi, kterou výrobce ještě podporuje bezpečnostními opravami.

3.2 Šifrování a certifikát (HTTPS)

- Web běží celý na HTTPS, včetně administrace a všech podstránek — ne jen úvodní stránka.
- Certifikát je platný a automaticky se obnovuje (např. Let's Encrypt).
- Testovatelné zdarma nástrojem SSL Labs (ssllabs.com/ssltest) — ukáže i chyby v konfiguraci šifrování.

3.3 Přístupy a hesla

- Každý administrátor má vlastní účet — žádné sdílené heslo.
- Dvoufaktorové ověření je zapnuté minimálně pro administraci a hosting.
- Po odchodu spolupracovníka nebo dodavatele se přístupy okamžitě ruší.

3.4 Formuláře a vstupy uživatelů

- Každé pole (jméno, e-mail, zpráva, datum) se kontroluje i na straně serveru, ne jen v prohlížeči — kontrolu v prohlížeči lze snadno obejít.
- Formuláře mají ochranu proti spamu a automatizovanému zneužití (CAPTCHA, honeypot pole, limit počtu odeslání).
- Nahrávání souborů, pokud existuje, má omezený typ a velikost souboru.

3.5 Zálohy a obnova

- Zálohy obsahu i databáze běží automaticky a pravidelně.
- Záloha je uložena mimo stejný server (jinak ji zničí stejný útok/ransomware jako originál).
- Alespoň jednou byla reálně vyzkoušena obnova ze zálohy, ne jen její existence.

3.6 Bezpečnostní hlavičky a nastavení serveru

- Nastavené hlavičky Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Strict-Transport-Security.
- Chybové stránky nezobrazují technické detaily (verze softwaru, cesty na serveru, chybové výpisy databáze).
- Adresáře serveru nejsou veřejně procházitelné (výpis souborů v prohlížeči).

3.7 Monitoring a reakce

- Existuje přehled o tom, kdo a kdy se přihlásil do administrace.
- Je nastavené upozornění na neobvyklou aktivitu (např. hromadné neúspěšné přihlášení).
- Je jasné, koho kontaktovat a co dělat, pokud se web chová podezřele.

4. Specifika: rezervační systém

Rezervační systém pracuje s osobními údaji zákazníků a s obchodně citlivými daty (kapacita, ceny, termíny), proto vyžaduje o něco přísnější kontrolu než statický web.

4.1 Co hlídat

- **Ochrana cizích rezervací:** ověřte, že po přihlášení nelze pouhou změnou čísla v adrese (např. /rezervace/1024 na /rezervace/1025) zobrazit nebo upravit rezervaci jiného zákazníka.
- **Souběžné rezervace téhož termínu:** pokud dva zákazníci kliknou na rezervaci stejného posledního volného místa ve stejnou chvíli, systém by měl obsloužit jen jednoho, ne oba (tzv. race condition, dvojí rezervace).
- **Rozsah osobních údajů:** sbírejte jen údaje, které skutečně potřebujete k vyřízení rezervace, a jasně napište, jak s nimi nakládáte (soulad s GDPR).
- **Potvrzovací odkazy a tokeny:** odkazy pro potvrzení/zrušení rezervace by měly obsahovat dostatečně dlouhý, neuhodnutelný kód, ne jen prosté pořadové číslo.
- **Omezení zneužití formuláře:** limit počtu rezervací z jedné IP adresy nebo e-mailu za krátký čas, aby šlo předejít zahlcení systému falešnými rezervacemi.

4.2 Jak to otestovat sami (základní, netechnická kontrola)

- Vytvořte si dvě testovací rezervace pod dvěma různými účty/e-maily a zkuste přes odkaz na potvrzení jedné rezervace jen změnit číslo — mělo by to selhat nebo vyžadovat přihlášení.
- Zkuste odeslat rezervační formulář vícekrát rychle po sobě a sledujte, jestli systém omezí opakované odesílání.
- Ověřte, že e-mail s potvrzením rezervace neobsahuje citlivější údaje, než je nutné (např. neposílejte v e-mailu plné číslo platební karty).

5. Specifika: platební brána

Toto je nejcitlivější část webu — spojuje se zde bezpečnost, právní odpovědnost a důvěra zákazníků. Základní pravidlo: údaje o platební kartě by neměly nikdy procházet ani se ukládat na vašem vlastním serveru.

5.1 Základní princip

Pro přijímání plateb kartou použijte certifikovanou platební bránu (např. přes banku, GoPay, Stripe, PayU, Comgate apod.), která zákazníka buď přesměruje na svou vlastní zabezpečenou stránku, nebo vloží platební formulář na váš web technologií, kde s daty karty nepřichází do styku váš server (tzv. iframe/hosted fields). Tím se většina povinností z normy PCI DSS přenáší na poskytovatele brány a vy jako provozovatel webu neneste plnou zátěž certifikace.

5.2 Přehled požadavků PCI DSS (orientačně)

- Instalace a údržba firewallu chránícího data držitelů karet.
- Nepoužívání výchozích hesel a nastavení dodavatele.
- Ochrana uložených dat držitelů karet (ideálně je vůbec neukládat).
- Šifrování přenosu dat karet přes veřejné sítě (HTTPS/TLS).
- Používání a pravidelná aktualizace antivirové ochrany.
- Vývoj a údržba bezpečných systémů a aplikací (aktualizace, testování).
- Omezení přístupu k datům karet jen na nutné minimum osob.
- Přidělení jedinečného identifikátoru každému uživateli se systémovým přístupem.
- Omezení fyzického přístupu k datům karet.
- Sledování a evidence veškerého přístupu k síti a datům karet.
- Pravidelné testování bezpečnostních systémů a procesů.
- Udržování zdokumentované bezpečnostní politiky.

Konkrétní rozsah povinností, které se vás jako provozníka webu skutečně týkají, závisí na tom, jakou variantu integrace platební brány zvolíte — to je vhodné probrat přímo s poskytovatelem brány.

5.3 Co konkrétně hlídat

- **Žádná vlastní evidence karet:** číslo karty, CVV kód ani datum platnosti se nikdy neukládají do vaší databáze, souboru ani e-mailu.
- **Zobrazení platební brány:** platební formulář by měl vizuálně i technicky jasně patřit doméně platební brány, ne vypadat jako obyčejné pole na vašem webu (kvůli důvěryhodnosti i technickým požadavkům brány).
- **HTTPS bez výjimky:** celá cesta objednávky, od košíku po potvrzení platby, běží na zabezpečeném HTTPS.
- **Testovací prostředí (sandbox):** platební brány nabízejí testovací režim se zkušebními kartami — veškeré testování plateb probíhá tam, nikdy na reálné kartě až do doby, kdy je vše hotové.
- **Potvrzení platby ze strany brány:** objednávka by se měla označit za zaplacenou až na základě potvrzení od platební brány (serverové notifikace), ne jen podle toho, že se zákazníkovi zobrazila „děkovací“ stránka — tu lze podvrhnout.

6. Jak testovat — nástroje a postup

Testování bezpečnosti nemusí hned znamenat najatého hackera. Pro začátek postačí kombinace bezplatných automatizovaných nástrojů a několika manuálních kontrol; profesionální penetrační test má smysl přidat u webu s platbami nebo většími objemy osobních údajů.

6.1 Automatizované nástroje (netechnické, zdarma)

- **Mozilla Observatory:** zadáte adresu webu a nástroj ohodnotí bezpečnostní hlavičky a nastavení, s konkrétními doporučeními k opravě.
- **SSL Labs (Qualys SSL Test):** zkontroluje kvalitu HTTPS certifikátu a šifrování, upozorní na zastaralé a nebezpečné protokoly.
- **Security Headers (securityheaders.com):** rychlá kontrola bezpečnostních HTTP hlaviček s doporučeními, jak je nastavit.
- **Have I Been Pwned:** ověří, zda se firemní e-maily/hesla neobjevily v některém z veřejně známých úniků dat.

6.2 Nástroje pro hlubší (poloautomatizované) testování

- **OWASP ZAP:** bezplatný nástroj, který automaticky projde web a hledá běžné zranitelnosti (XSS, chybějící hlavičky, zastaralé komponenty apod.) — vhodné svěřit dodavateli webu nebo IT konzultantovi, výstup vyžaduje technickou interpretaci.
- **WPScan a obdobné skenery pluginů:** pokud web běží na WordPressu nebo podobném CMS, tyto nástroje zkontrolují, zda použité pluginy neobsahují známé díry.

6.3 Manuální kontroly, které zvládnete i bez IT vzdělání

- Zkuste v adrese měnit čísla u objednávek/rezervací a sledujte, zda se nezobrazí cizí data.
- Vyzkoušejte odhlásit se a zkuste se dostat na stránky administrace přímo přes URL — mělo by vás to vždy vrátit na přihlášení.
- Zkuste zadat do formulářů neobvyklé znaky (uvozovky, znak < >) a sledujte, zda se nezobrazí chybová hláška prozrazující technické detaily.
- Zkontrolujte, že admin rozhraní a citlivé sekce nejsou dostupné bez HTTPS (zámek v adresním řádku).
- Projděte, zda web při zadání neexistující stránky nebo špatného hesla nevypisuje detailní technické chybové hlášky.

6.4 Profesionální penetrační test

Jde o cílený, ručně vedený test od specializované firmy nebo odborníka, který simuluje reálný útok, včetně logiky konkrétních funkcí (rezervace, platby, slevové kódy). Doporučuje se před spuštěním webu s platbami, po větší změně systému a pak přibližně jednou ročně. Vybírejte dodavatele s prokazatelnými referencemi, jasně definovaným rozsahem testu a písemnou zprávou s doporučeními k nápravě.

6.5 Jak často testovat

- Automatizovaná kontrola (Observatory, SSL Labs, skener pluginů) — v ideálním případě průběžně/automaticky, minimálně jednou měsíčně.

- Kontrola aktualizací CMS a pluginů — průběžně, ideálně s automatickými upozorněními.
- Manuální kontrola rezervací/přístupů — po každé větší úpravě webu.
- Penetrační test — před spuštěním platební/rezervační funkce a poté přibližně ročně.

7. Kontrolní seznam bezpečnostního minima

Barevné označení ukazuje orientační prioritu: červená — kritické, bez čeho web nemá jít do provozu; oranžová — vysoká priorita, doplnit brzy po spuštění; zelená — doporučené vylepšení.

Oblast	Opatření	Priorita
HTTPS	Celý web (včetně admin rozhraní) je dostupný pouze přes HTTPS, platný certifikát, žádný smíšený obsah (HTTP prvky na HTTPS stránce).	Kritické
Aktualizace	CMS, pluginy, šablony a knihovny jsou na aktuální verzi. Zapnuté automatické bezpečnostní aktualizace, kde to jde.	Kritické
Hesla a přístup	Silná unikátní hesla ke všem účtům (hosting, CMS, e-mail, DNS), správce hesel, dvoufaktorové ověření (2FA) na admin účtech.	Kritické
Admin rozhraní	Přihlašovací stránka administrace není veřejně inzerovaná, omezený počet pokusů o přihlášení, IP omezení nebo VPN, pokud to provoz umožňuje.	Vysoké
Zálohy	Automatické pravidelné zálohy (obsah i databáze), uložené mimo produkční server, ověřená obnovitelnost.	Kritické
Platby	Platební údaje nikdy neprocházejí vlastním serverem ani se neukládají — používá se certifikovaná platební brána (PCI DSS).	Kritické
Formuláře	Validace vstupů na straně serveru, ochrana proti spamu (CAPTCHA/honeypot), limit počtu odeslání za čas (rate limiting).	Vysoké
Rezervace	Ověření, že uživatel může vidět a měnit pouze svou rezervaci (ne cizí přes změnu ID v URL), ošetření souběžných rezervací téhož termínu.	Vysoké
Osobní údaje	Soulad se zásadami GDPR — jasné informace o zpracování, minimalizace sbíraných údajů, šifrované uložení citlivých dat.	Vysoké
HTTP hlavičky	Nastavené bezpečnostní hlavičky (Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Strict-Transport-Security).	Doporučené
Nahrávání souborů	Pokud web umožňuje nahrávat soubory (přílohy, fotky), je omezen typ a velikost souboru a soubory se neprovádí jako kód.	Vysoké
Chybové stránky	Vlastní chybové stránky (404, 500) nezobrazují technické detaily, verze softwaru ani cesty na serveru.	Doporučené
Logování	Web i hosting zaznamenávají přihlášení, změny a chyby; logy se pravidelně kontrolují nebo je nastaveno upozornění na podezřelou aktivitu.	Doporučené
Testování	Web je alespoň jednou ročně (a po každé větší změně) prověřen automatizovaným skenerem a případně penetračním testem.	Doporučené
Plán reakce	Existuje jednoduchý plán, co dělat při napadení webu (koho kontaktovat, jak obnovit ze zálohy, jak informovat zákazníky).	Vysoké

Poznámka na závěr: bezpečnost webu není jednorázový úkon, ale průběžný proces — aktualizace, zálohy a kontroly se dělají opakovaně, ne jen při spuštění webu. Pokud si u některého bodu nejste jistí, je to signál probrat ho s dodavatelem hostingu, CMS nebo platební brány, ne bod přeskočit.