

Co je Credential stuffing

Poslední aktualizace 29 dubna, 2026

Credential stuffing je typ kybernetického útoku, při kterém útočník zkouší uniklé přihlašovací údaje (uživatelské jméno a heslo) z jednoho webu na dalších službách. Útok spoléhá na to, že mnoho lidí používá stejné heslo na více webech. Pokud dojde k úniku [databáze](#) z jedné služby, mohou být stejné údaje zneužity i jinde. Credential stuffing je dnes jedním z nejčastějších útoků na přihlašovací formuláře.

Jak Credential stuffing funguje

Útočník nejprve získá databázi uniklých přihlašovacích údajů, například z veřejně dostupného úniku dat. Poté pomocí automatizovaných nástrojů:

- zkouší kombinace e-mailu a hesla na jiných webech
- testuje tisíce přihlášení během krátké doby
- vyhodnocuje, kde se podařilo přihlásit

Útok je plně automatizovaný a probíhá ve velkém měřítku.

Credential stuffing bývá často zaměňován s [Brute force](#), jedná se ale o rozdílné útoky.

- **Brute force** zkouší různé kombinace hesel k jednomu účtu
- **Credential stuffing** používá skutečné uniklé kombinace e-mail + heslo

Credential stuffing je efektivnější, protože pracuje s reálně používanými údaji.

Co může Credential stuffing způsobit

Úspěšný útok může vést k:

- převzetí uživatelského účtu
- krádeži osobních údajů
- zneužití platebních údajů
- rozesílání [spamu](#) z kompromitovaného účtu
- poškození reputace služby

U e-shopů nebo zákaznických portálů může mít i finanční dopady.

Jak se proti Credential stuffing bránit

Ochrana vyžaduje kombinaci technických opatření i práce s uživateli. Mezi základní ochranné mechanismy patří:

- [dvoufaktorové ověřování](#)
- [rate limiting](#) přihlašovacích pokusů
- detekce podezřelého chování
- blokace [IP adres](#) při nadměrném počtu pokusů
- kontrola hesel proti známým únikům databází

Důležité je také edukovat uživatele, aby nepoužívali stejné heslo na více službách.