XSS (Cross-Site Scripting)

XSS je útok zaměřený na uživatele webové aplikace, nikoliv na server samotný. Útočník zneužívá důvěry, kterou má prohlížeč uživatele k dané webové stránce. Pokud aplikace nedostatečně filtruje vstupy od uživatelů, může útočník podvrhnout kód, který prohlížeč vykoná jako součást stránky.

Hlavním cílem XSS bývá krádež identifikačních údajů (např. cookies), přesměrování na podvodné weby nebo šíření malwaru.

Jak XSS funguje

Útok probíhá ve třech krocích:

```
1. **Vložení:** Útočník najde místo na webu, kam lze vložit text (např. vyhledávací pole, komentáře, profil). Do tohoto pole vloží skript, např.: ''<script>alert('Váš počítač je napaden!');</script>''.
2. **Uložení/Zobrazení:** Webová aplikace tento skript přijme a buď ho uloží do databáze, nebo ho ihned vypíše zpět na stránku.
3. **Exekuce:** Oběť navštíví stránku, její [[browser|prohlížeč]] interpretuje vložený kód jako legitimní instrukci od serveru a skript spustí.
```

http://googleusercontent.com/image_collection/image_retrieval/17689042437774707653

Typy XSS útoků

Typ	Popis	Nebezpečí
Stored XSS (Trvalé)	Škodlivý kód je trvale uložen na serveru (např. v komentáři pod článkem).	Nejvíce nebezpečné, zasáhne každého, kdo si stránku přečte.
Reflected XSS (Odražené)	Skript je součástí URL adresy (např. v parametru vyhledávání).	Útočník musí oběť přimět kliknout na speciálně upravený odkaz.
DOM-based XSS	Útok probíhá výhradně v prohlížeči oběti úpravou objektového modelu stránky (DOM).	Těžko detekovatelné servery, protože škodlivá data se na server vůbec nemusí poslat.

Reálné dopady útoku

- **Krádež session cookies:** Útočník pomocí skriptu přečte vaše `document.cookie` a pošle je

na svůj server. Tím může ukrást vaši aktivní relaci a přihlásit se za vás (např. do e-mailu nebo Facebooku).
- **Phishing:** Skript může upravit vzhled stránky a zobrazit falešný přihlašovací formulář, který vypadá jako součást webu.
- **Keylogging:** Škodlivý kód může sledovat stisky kláves uživatele a odesílat hesla útočníkovi.

Obrana a prevence

Zodpovědnost za ochranu před XSS leží primárně na vývojářích webových aplikací:

- **Sanitizace vstupu:** Důsledné odstraňování nebo neutralizace nebezpečných znaků (např. přeměna < na `<`) v datech přicházejících od uživatele.
- **Content Security Policy (CSP):** Bezpečnostní hlavička v HTTP odpovědi, která prohlížeči říká, ze kterých domén smí spouštět skripty. Dokáže zablokovat neschválené skripty útočníka.
- **Příznak HttpOnly:** U cookies zabraňuje JavaScriptu v přístupu k danému souboru, což znemožňuje jejich krádež přes XSS.

Související pojmy: JavaScript, Cookie, Browser, HTML, HTTP, Malware, Phishing, SQL Injection.