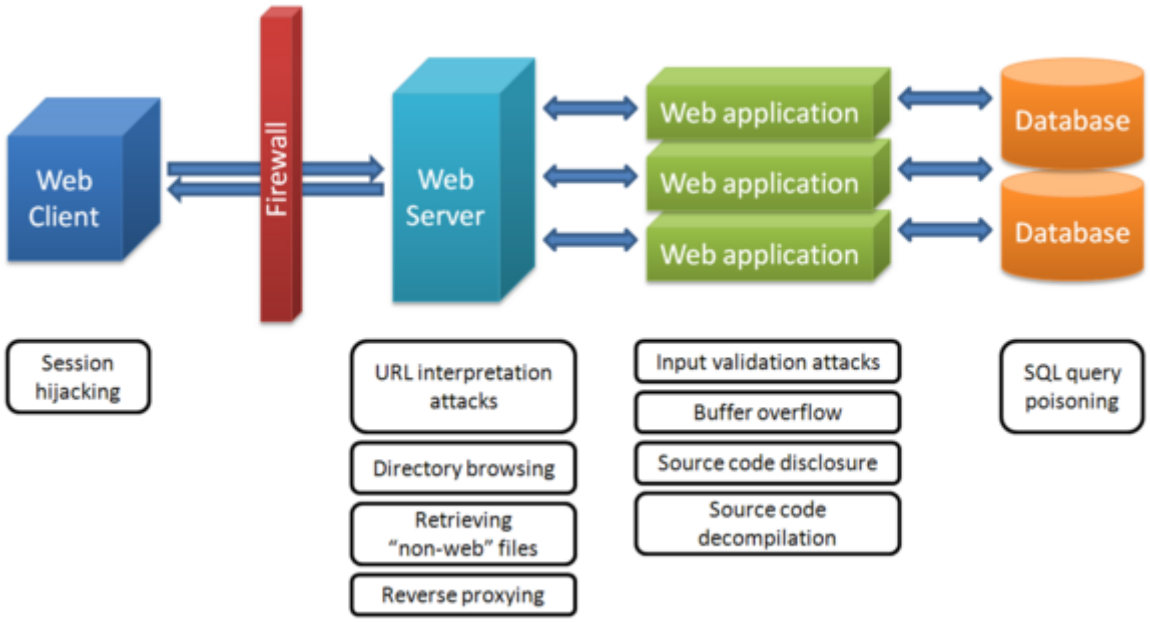
Bezpečnost webových aplikací

Z FITwiki

Obsah



Cíle útoku

- Extra informace
- Zdrojový kód libovolné soubor
- Zpřístupnění dat
- vykonání libovolného příkazu

Techniky útoků

Chybná interpretace URL

Nebezpečí

- přes speciálně zadanou URL je možné zaútočit na server

Příčiny

- Webový server nesprávně parsuje URL adresu (podstrčení bílých znaků, unicode znaky, ...)
- Chybné mapování zdrojů v konfiguraci

Řešení

- záplaty od výrobce serveru
- kontrola konfiguračních souborů

Procházení adresářů

Nebezpečí

- útočník získá seznam všech souborů, které jsou na serveru

Příčiny

- chybné nastavení serveru
- chyba serveru

Řešení

- správné nastavení (zakázat DirectoryIndex)
- záplata od výrobce serveru

Získání „non-web“ souborů

Nebezpečí

- útočník získá soubory, ke kterým by neměl mít přístup

Příčiny

- názvy souborů, které lze uhodnout
- přítomnost souborů, které by neměl být věřejně přístupné

Řešení

- zbavit se souborů
- zakázat zpracování souborů daných typů (resource mapping)

Únik zdrojových kódů

Nebezpečí

- Získání zdrojových souborů aplikace a následná analýza na bezpečnostní chyby

Příčiny

- chybná konfigurace
- chyby aplikace
- chyby serveru

Řešení

- správná konfigurace
- oprava aplikace
- záplaty od výrobce serveru

Útoky přes vstupní data

Nebezpečí

- Útok na aplikaci podstrčením neočekávaných dat

Příčiny

- nejčastější typ útoku
- kontrola dat pouze na straně klienta
- předávání dat přes skrytá pole formulářů bez jejich kontroly

Řešení

- Vstupy musí být kontrolované – rozsah hodnot, datové typy, metaznaky
- nevěřit ničemu co přijde od klienta
- před použitím vstupu jej vždy ošetřit na meta-znaky

SQL injection

Nebezpečí

- útočník provádí neoprávněné SQL příkazy

Příčiny

- vstupy používané v SQL dotazech bez ošetření
- nedostatečná validace a ošetření vstupů

Řešení

- důsledná validace a ošetření vstupu
- přístup přes mezi vrstvu, která nebezpečí vyloučí (ORM, uložené procedury)

Buffer overflow

Nebezpečí

- útočník ovlivní fungování serveru (DoS, pád aplikace, vzdálené sputění příkazů (shellcode), přepsání hodnot)

Příčiny

- slabá kontrola vstupu
- chyby v aplikaci
- chyby serveru

Řešení

- Statická analýza kódu aplikace
- robustní knihovní funkce
- jiné technologie např. .Net, Java
- Ochranné mechanismy např. StackShield

Krádež session

Nebezpečí

- útočník ukradne identitu oprávněného uživatele

Příčiny

- nezabezpečené předávání session ID (předávání přes URL - únik přes referer, předávání přes nezabezpečené cookies - únik přes XSS)
- session nejsou kontrolovány na straně serveru

Řešení

- hlídání session na straně serveru (timestamp, IP)
- změna session ID při přihlášení

Kategorie: Státnice 2011 | Bezpečnost informačních systémů

- Stránka byla naposledy editována 27. 1. 2014 v 14:47.