

**Web Application Security**

**Aplikační bezpečnost**

Jiří Martinů, 2023

## Background

- **Aplikační bezpečnost je stále ještě na počátku vývoje.**
- **Tradiční týmy vývojářů, provozovatelů, samostatných vývojářů dobře nerozumí rizikům spojeným s aplikační bezpečností nebo je podceňují.**
- **Pravdou je, že zajištění kvalitní bezpečnosti webových aplikací není vždy snadnou nebo levnou záležitostí.**
- **Zajištění bezpečnosti je často kompromisem – zpřístupnění vs. omezení.**

## Cíle při zajištění aplikační bezpečnosti (AB)

- **Určení/zjištění možných zranitelností s ohledem na AB**
- **Monitorování/detekce pokusů o útok**
- **Vývoj plánu pro stav ohrožení**

- 
- **Přidělení priority specifickým interním projektům AB**
  - **Proaktivní zvyšování povědomí o možných hrozbách**
  - **Modelování hrozeb (Threat Modeling - TM) a diagramy datových toků (Data Flow Diagrams – DFDs)**
  - **Manuální revize kódů (externím odborníkem)**
  - **Atd.**

# Zjištění možných zranitelností

- Automatizovaný přístup
  - Výběr automatizovaného nástroje hodnotícího AP, který nejlépe spolupracuje s vašimi technologiemi webových aplikací.
  - Zajištění VŠECH hrozeb, kterým může být webová aplikace vystavena.
  - Vložení analytických nástrojů a obranných mechanismů přímo do zdrojových kódů webové aplikace.
- Manuální přístup
  - Slouží pro doplnění automatizovaného přístupu při posuzování možných hrozeb.
  - Ruční nastavení specifických požadavků s ohledem na zajištění funkce i zabezpečení.
  - Integrace manuálního i automatizovaného hodnocení kódů/zranitelností do životního cyklu vývoje.

# Nástroje pro nalezení zranitelností

## Web Application Security Assessment vendors

- AppScan - Watchfire ([www.watchfire.com](http://www.watchfire.com))
- Core Impact - Core Security ([www.coresecurity.com](http://www.coresecurity.com))
- Hailstorm - Cenzic ([www.cenzic.com](http://www.cenzic.com))
- NTOSpider - NT OBJECTives ([www.ntobjectives.com](http://www.ntobjectives.com))
- WebInspect - SPI Dynamics ([www.spydynamics.com](http://www.spydynamics.com))
- WhiteHat Sentinel - WhiteHat Security ([www.whitehatsec.com](http://www.whitehatsec.com))

## Analýza statických kódů

- Fortify - Fortify Software ([www.fortifysoftware.com](http://www.fortifysoftware.com))
- Ounce - Ounce Labs ([www.ouncelabs.com](http://www.ouncelabs.com))
- Veracode – ([www.veracode.com](http://www.veracode.com))

## Druhy nejčastějších útoků

- XSS – Cross-Site Scripting
- SQL Injection
- DOS
- DDOS

# XSS – Cross-Site Scripting

- metoda narušení WWW stránek využitím bezpečnostních chyb ve skriptech (především neošetřené vstupy)
- využití i na statických stránkách
- jde o neošetřené přenesení proměnné z URL adresy do javascriptu
- Např.:

```
<SCRIPT>
```

```
var pos=document.URL.indexOf("jmeno=")+6;
```

```
document.write("Ahoj "+document.URL.substring(pos,document.URL.length));
```

```
</SCRIPT>
```

- Příklad na stránku: <http://blablabla.cz/stranka.html?jmeno=Jirka>
-

## SQL Injection

- technika napadení databázové vrstvy programu vsunutím (odtud „**injection**“) kódu přes neošetřený vstup a vykonání vlastního pozměňujícího poškozujícího **SQL** příkazu (dotazu DELETE, UPDATE, ALTER atp.)



## DOS – Denial of Service

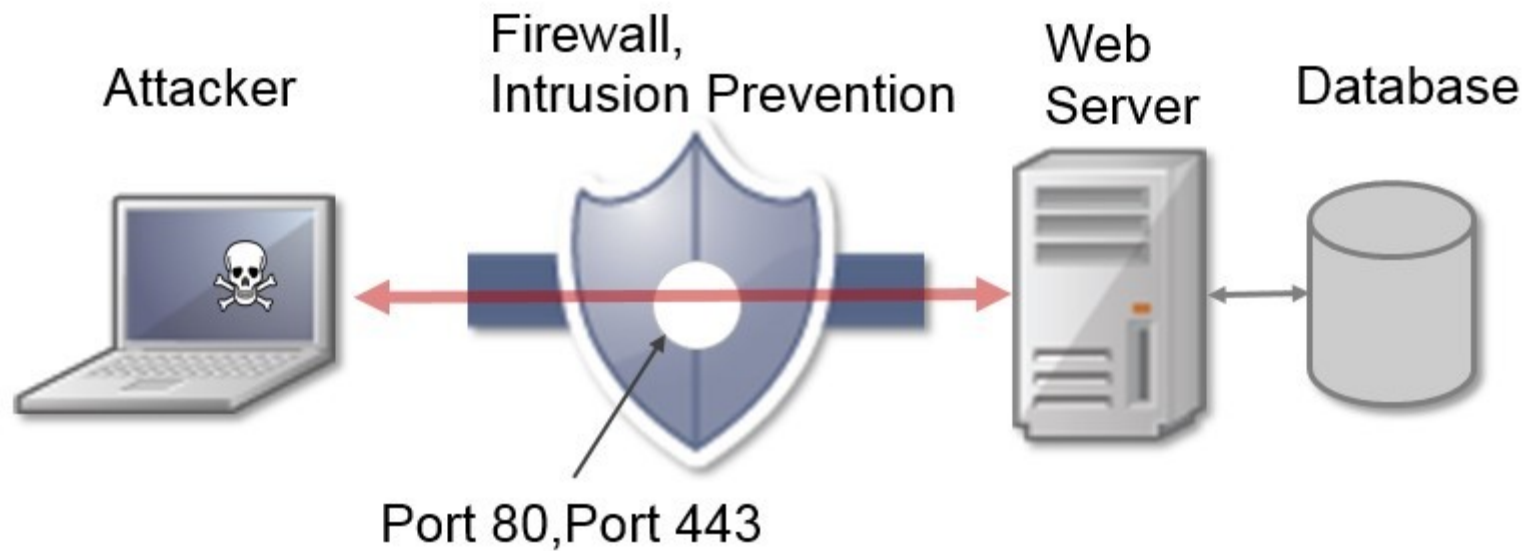
- typ útoku na internetové služby nebo stránky, jehož cílem je cílovou službu znefunkčnit a znepřístupnit ostatním uživatelům;
- může k tomu dojít přehlcením požadavky či využitím nějaké [chyby](#), která sice útočnickovi neumožní službu ovládnout, ale umožní ji rozbít.

## DDOS – Distrubuted Denial of Service

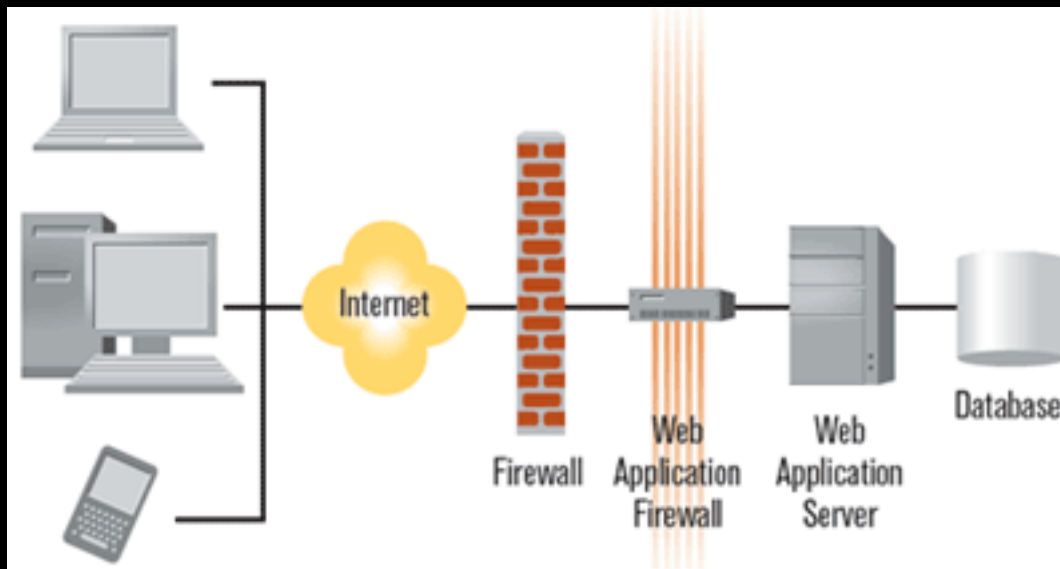
- typ útoku na internetové služby nebo stránky, jehož cílem je cílovou službu znefunkčnit a znepřístupnit ostatním uživatelům;
- může k tomu dojít přehlcením požadavky či využitím nějaké [chyby](#), která sice útočnickovi neumožní službu ovládnout, ale umožní ji rozbít.
- podtyp útoku DoS, při kterém je pro přehlcení cílové služby požadavky využito velké množství rozptýlených počítačů.

## Co je Web Application Firewall (WAF)?

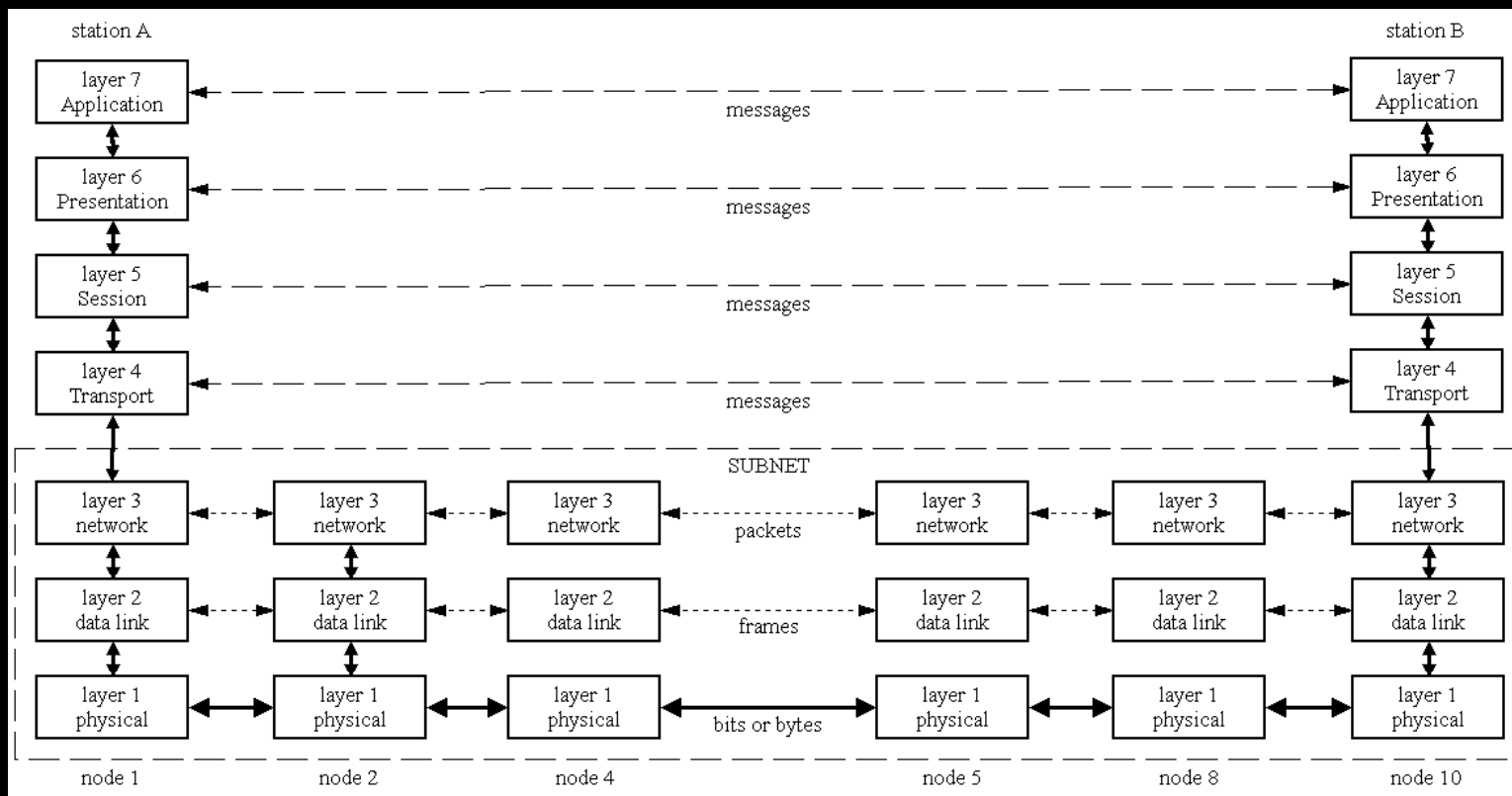
- Hlídá vrstvu webové aplikace (vrstva 7) a pracuje na ní
- Podobá se tradičnímu síťovému firewallu (vrstva 4)
- Nejedná se však o firewall
- Chová se spíše jako brána, než jako firewall
- Nejedná se však ani o bránu 😊
- U tradičního zabezpečení na síťové vrstvě – nelze chránit před tím, co není vidět...



Útok na webovou aplikaci



Umístění WAF v tradiční architektuře



Tradiční zabezpečení síťové vrstvy je vůči útokům na aplikační vrstvě slepé

## Doporučeno

- [https://www.owasp.org/index.php/Main\\_Page](https://www.owasp.org/index.php/Main_Page)
- <https://xss-game.appspot.com/>