

Inteligentné rozhranie pre zabezpečenie webovských aplikácií

Ing. Michal Takács

prof. Ing. Vladimír Vojtek, PhD.

Fakulta informatiky a informačných technológií,
Slovenská technická univerzita

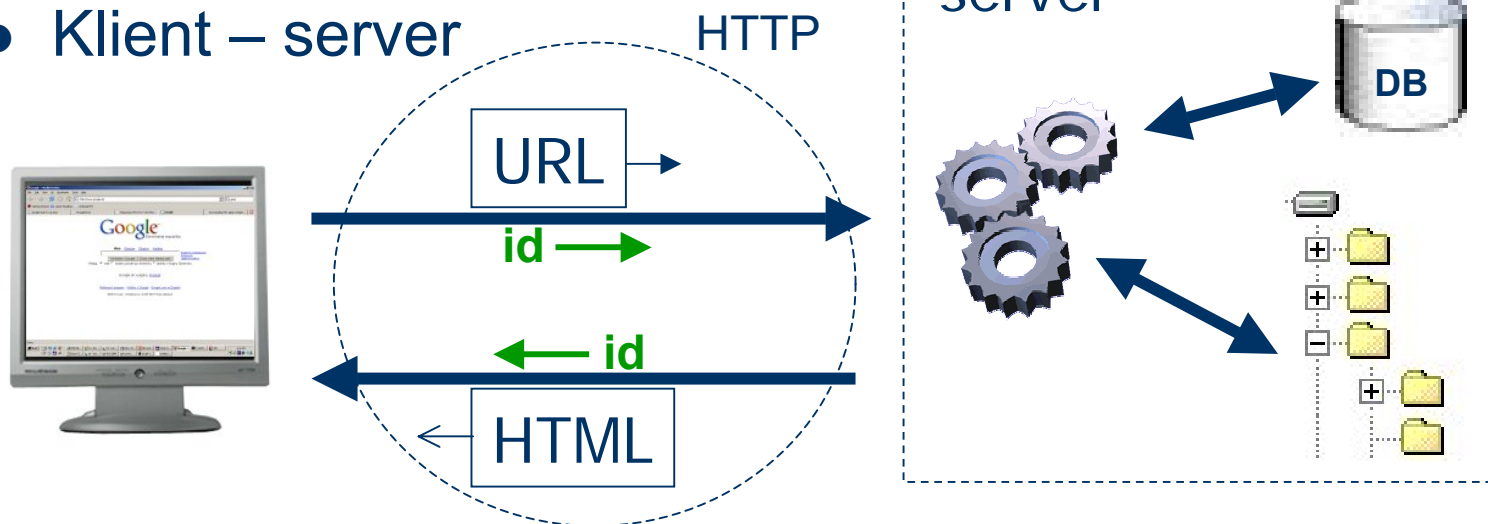
Obsah prezentácie

- **Webovské aplikácie**
 - Základné pojmy
 - Útoky
- **Návrh bezpečnostného rozhrania**
 - Existujúce riešenia, motivácii
 - Princíp ochrany
 - Konceptia riešenia
- **Experimentálne overenie**
 - Implementácia pokusného systému
 - Testovanie

Základné pojmy

Webovská aplikácia

- Klient – server



- URL: <http://meno.servera/aplikacia?param1=val1>
- Session: identifikovaná reťaz požiadaviek
- Internet → vysoká dostupnosť → „obliehanie“

Útok: overovanie a autorizácia

- Útok na kontrolu mena a hesla

- Generovanie používateľských hesiel, slovníky
- Opakované, rýchle prístupy

IP: 165.22.18.11	Heslo: alter	20:05:11.521	} 15 ms!
IP: 165.22.18.11	Heslo: atlantis	20:05:11.536	
IP: 165.22.18.11	Heslo: bogart	20:05:11.541	} 5 ms!
IP: 165.22.18.11	Heslo: carnaz	20:05:11.560	} 19 ms!

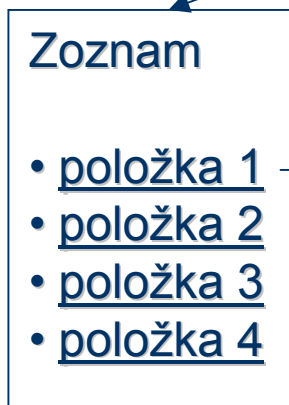
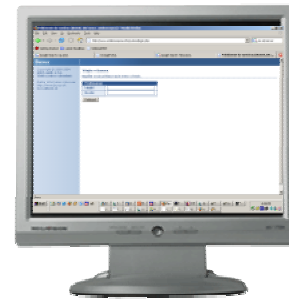
- Útok na session

- Kradnutie informácií

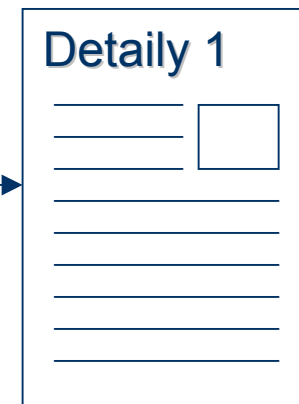
Útok: zmena URL

Význam parametrov

zobraz zoznam:
`app?action=list`



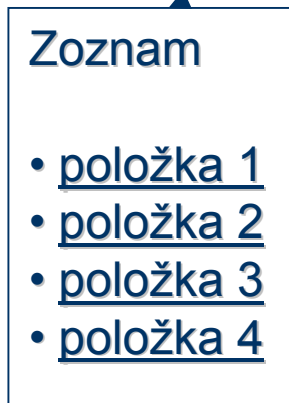
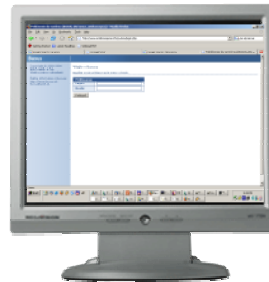
zobraz detaily 1:
`app?action=detail&id=1`



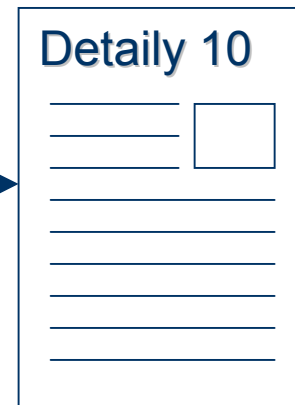
Útok: zmena URL

Jednoduché zneužitie parametrov

zobraz zoznam:
`app?action=list`



zobraz detaily 1: 
`app?action=detail&id=10`



Útok: zhubné hodnoty parametrov



- SQL injection

- Útok na databázu
- Vloženie SQL príkazov



- Cross site scripting - XSS

- Útok na iných používateľov
- Vloženie klientského skriptu (Javascript)



- Denial Of Service - DOS

- Útok na server
- Hľadanie slabín, ktoré spôsobia haváriu systému

Súčasný stav riešenia bezpečnosti

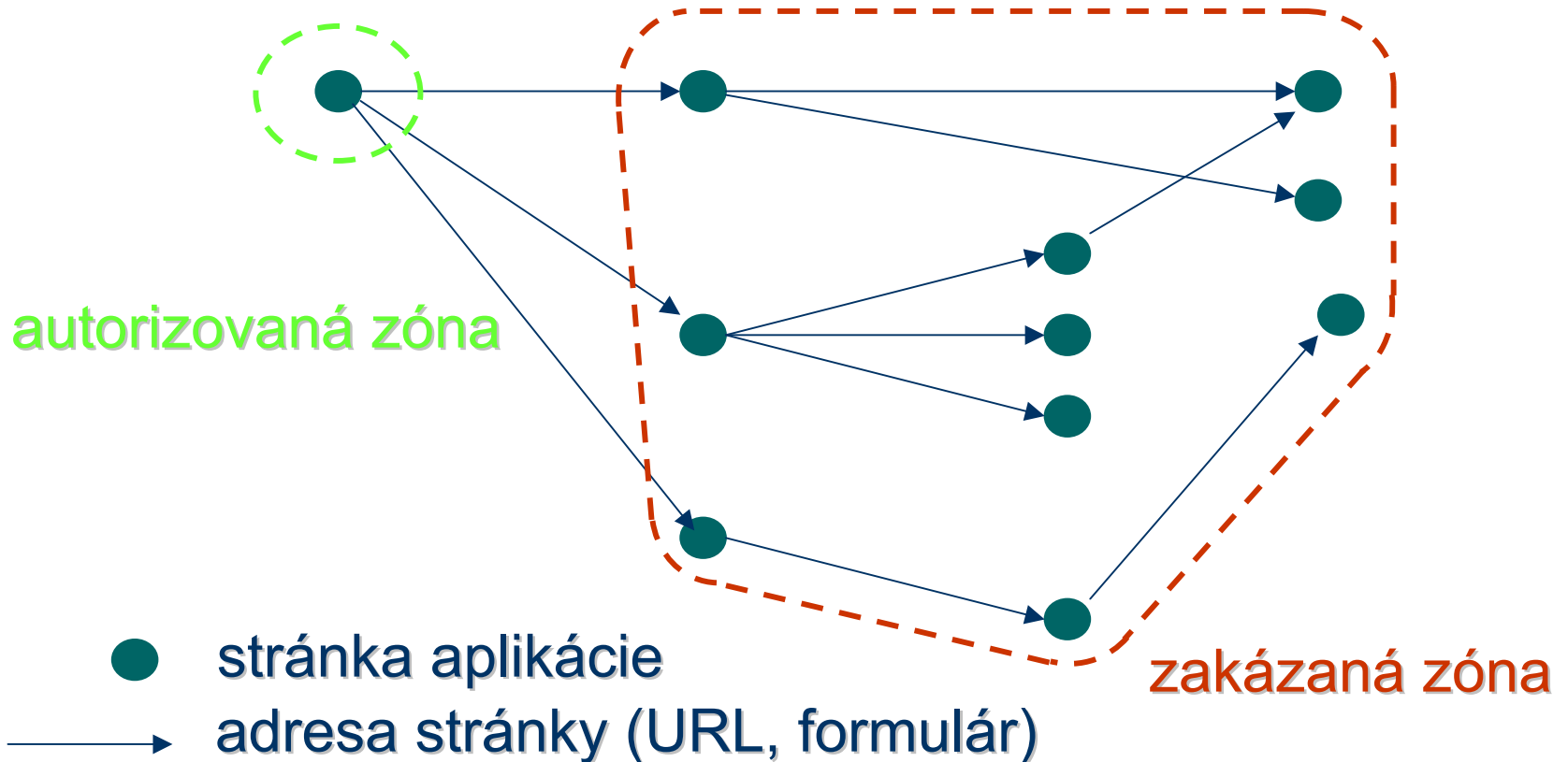
- Existujúce riešenia
 - aplikačná úroveň
 - drahé, neúplné
 - pevné filtrovanie vstupov, volaní, IDS
 - striktné, vyžadujú nastavovanie
 - nevhodné pre existujúce aplikácie
- Požiadavky
 - adaptívne, autonómne
 - ochrana existujúcich aplikácií

Návrh bezpečnostného rozhrania

- Princíp „vpust' dnu len to, čo si videl vyjsť von“
 - Analýza komunikácie
 - Hľadanie zverejňovaných URL v rámci HTML
 - Vytváranie bázy povolených adries – bezpečnostných zón
- Analýza z časového hľadiska
 - Identifikácia DOS útokov
- Analýza požiadaviek
 - SQL injection
 - XSS

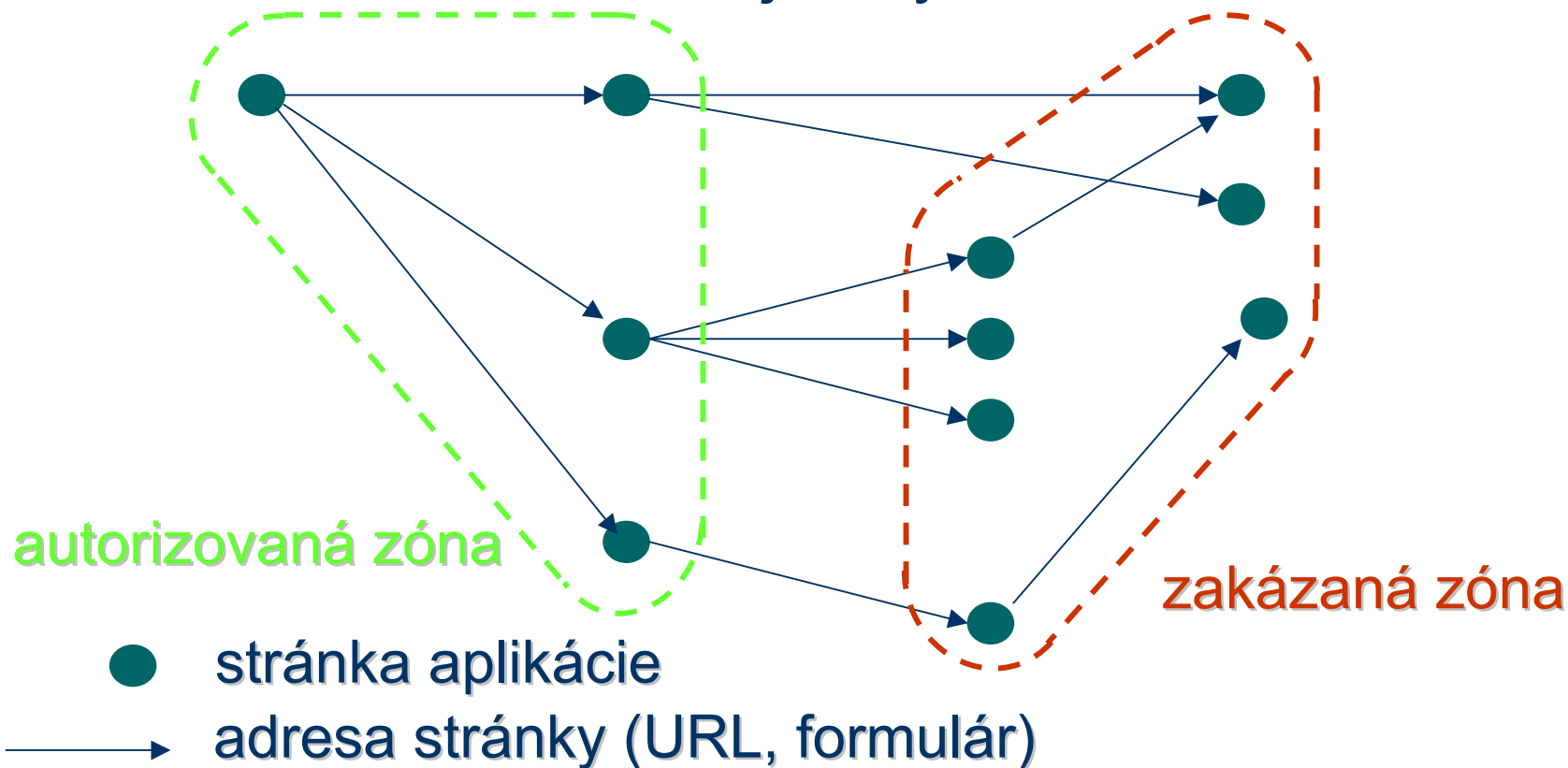
Návrh bezpečnostného rozhrania

Bezpečnostné zóny



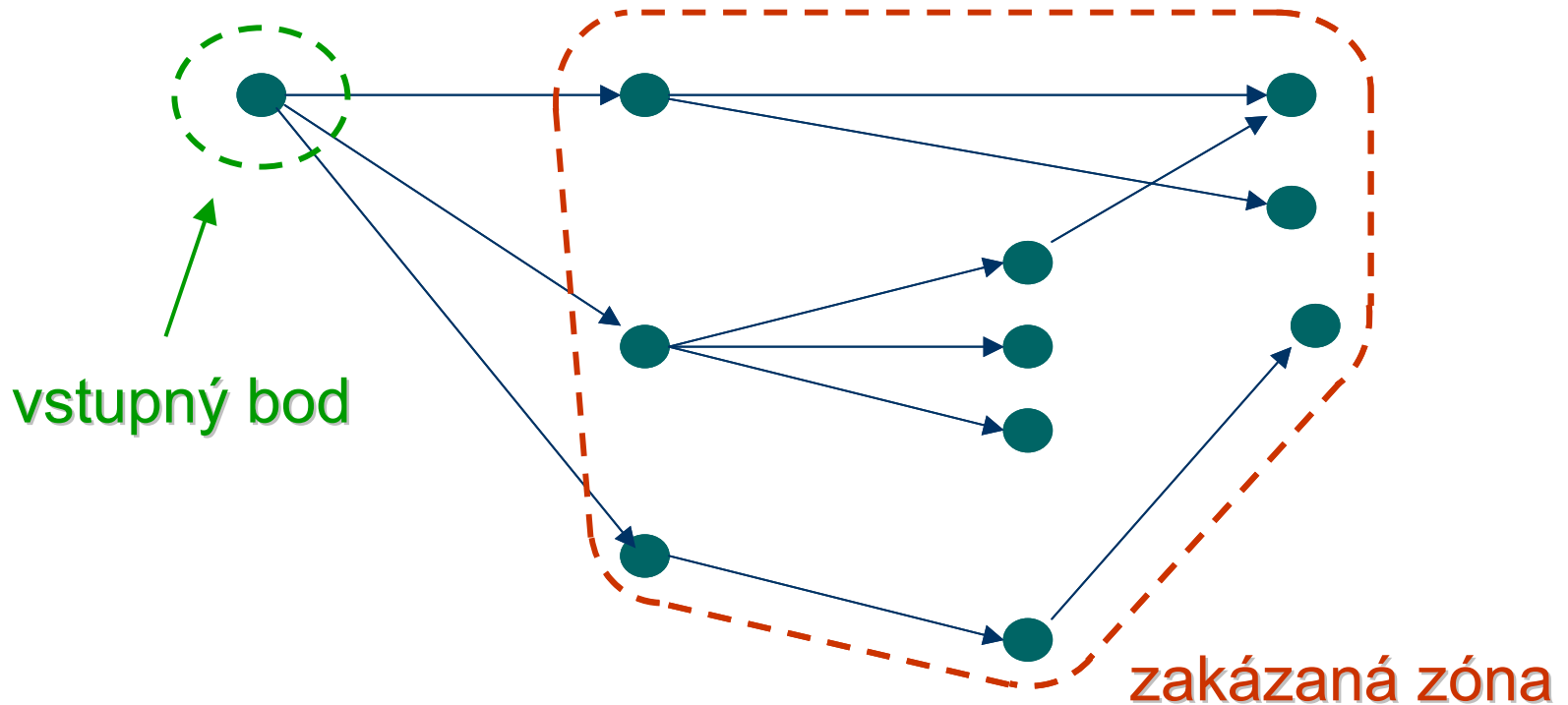
Návrh bezpečnostného rozhrania

Rozšírenie autorizovanej zóny



Návrh bezpečnostného rozhrania

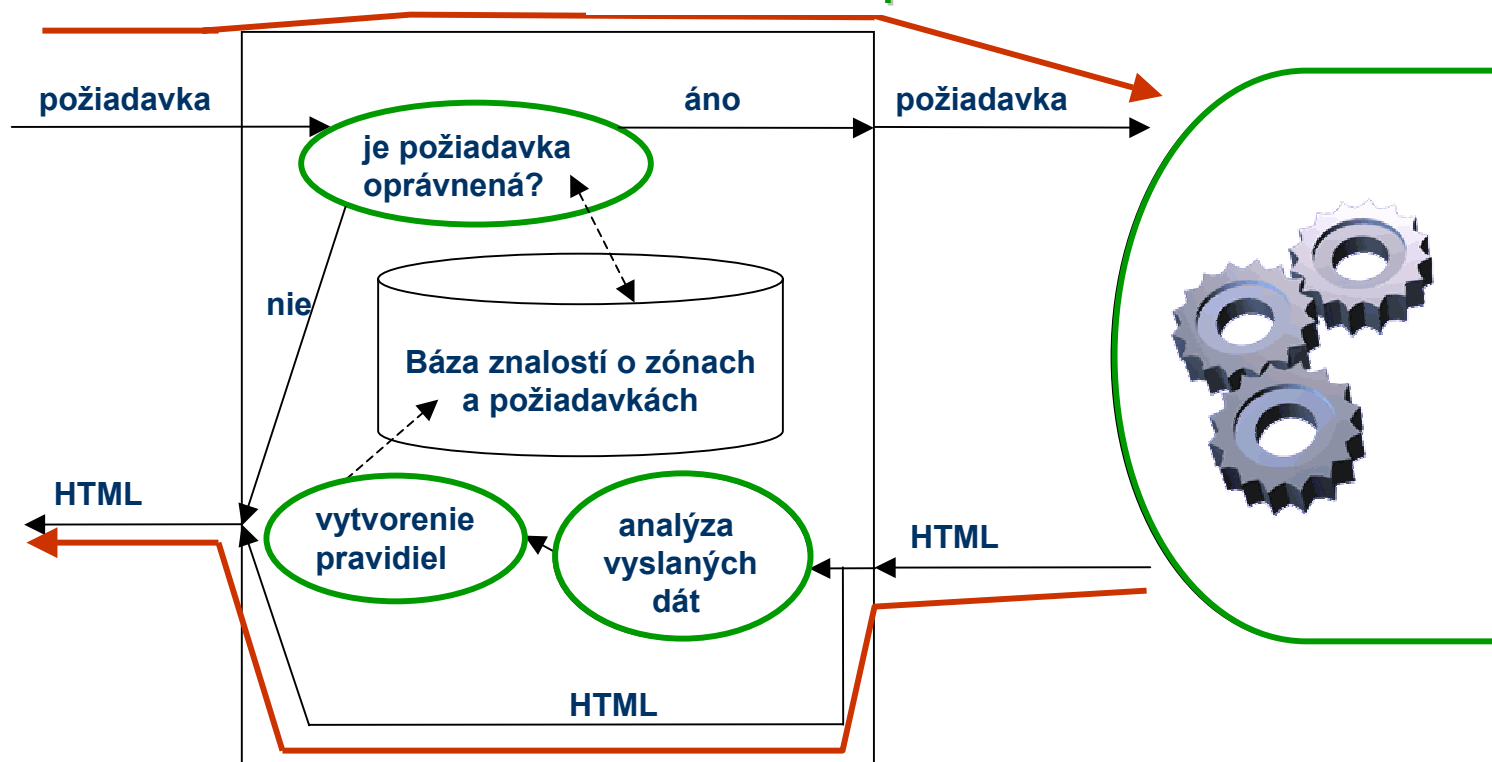
Vstupné body – riešenie úplnej reštrikcie



Návrh bezpečnostného rozhrania

Dynamika systému

so zabezpečením



Experimentálne overenie

- Implementácia pokusného systému
 - Java, Tomcat, JavaServlet Filter
- Bezpečnostné testy
 - Testy prienikov do zakázanej zóny
 - Zmeny adresy
 - Odstránenie parametrov
 - Útok hrubou silou
 - Testy zneužitia parametrov
 - XSS
 - SQL Injection

Overenie riešenia

- Výkonnostné testy
 - Dôležité pre reálnosť riešenia
 - Simulácia stredne zložitých operácií
 - Intenzívne databázové operácie
 - Konštantná výkonnostná degradácia
 - Vhodné pre ochranu náročnejších aplikácií

Zhodnotenie

- Úspešnosť navrhovanej metódy
- Principiálne nevhodné pre web services
- Výkonnostná degradácia
- Vhodné pre ochranu existujúcich a zle zabezpečených WA
- Ďalšie možné príspevky
 - Jemnejší návrh analytických častí
 - Širšia aplikácia umelej inteligencie
 - Import navigačných modelov

Ďakujem za pozornosť



Diskusia