Bezpečnosť webových aplikácií

- zuzana.duracinska@nic.cz, 21.10.2015

CZ.NIC | AKADEMIE

CZ.NIC | LABS

SKENER WEBU

captchahelp

mojeID

Tablexia

CSIRT.CZ
powered by CZ.NIC

BIRD

JAK NA INTERNET

PROJECT:TURRIS

KNOT DNS

CZ.NIC | SPRÁVCE DOMÉNY CZ

CZ.NIC z.s.p.o.

- prevádzkovanie registru doménových mien .CZ

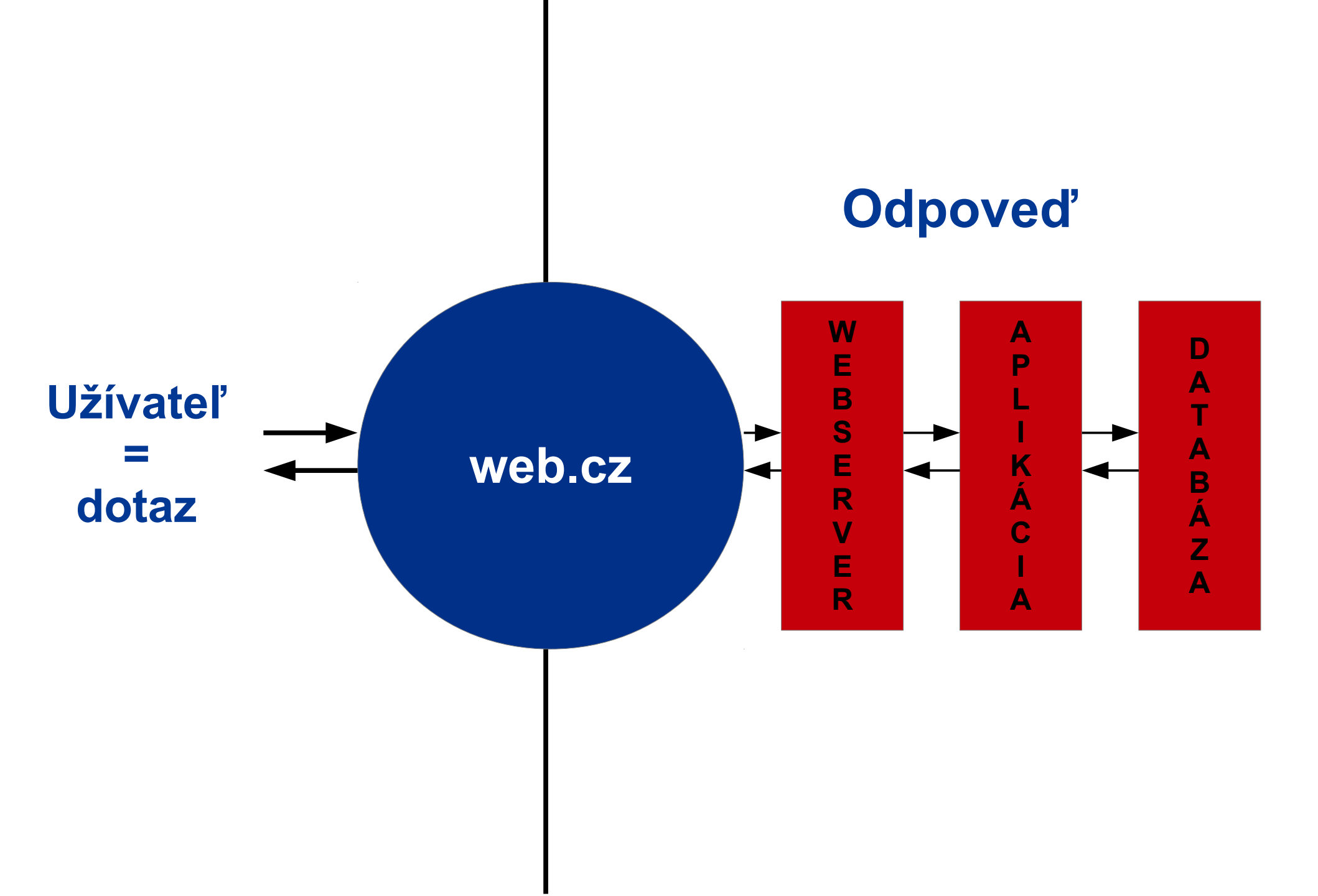
1 219 867

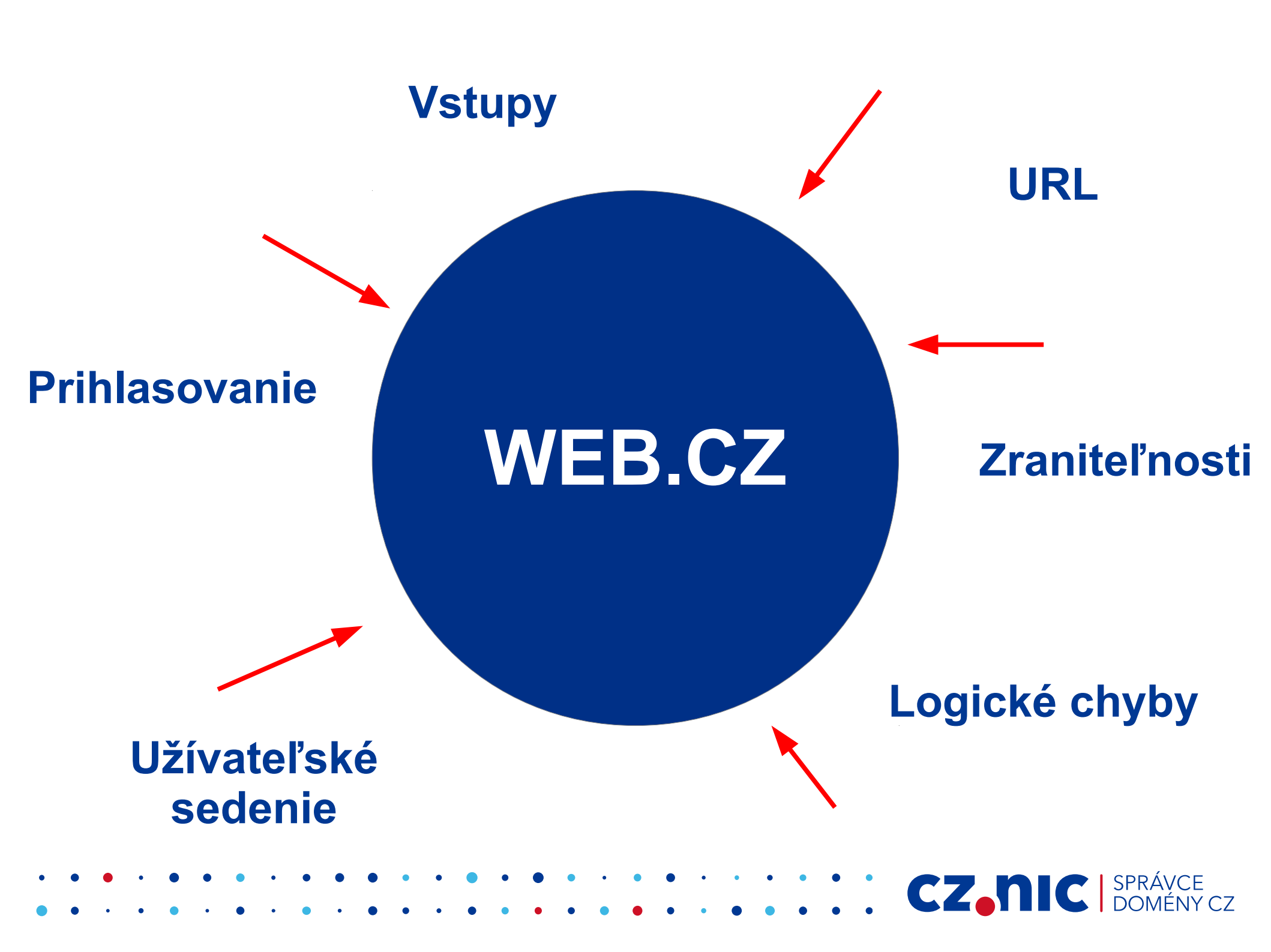
Register → ? → Držiteľ domény

Registrácia domény

- gTLD vs. ccTLD
- Zvolíme dobré doménové meno
- Zistíme, či je doména voľná
- Vyberieme si registrátora
- IPv6 

- Certifikácia registrátora 
- ? 


Odpoveď
Užívateľ
=
dotaz
web.cz
WEBSERVER
APLIKÁCIA
DATABÁZA


Vstupy
URL
Prihlasovanie
WEB.CZ
Zraniteľnosti
Logické chyby
Užívateľské sedenie

Testovanie webových aplikácií

- **Automatické**

(nikto, Nessus, nmap, wapiti, skipfish)

- **Ručné**

(kontrola vstupov, overenie nálezov z aut.testov, hľadanie logických chýb...)

*OWASP (Open Web Application Security Project)

```
User-agent: *
Disallow: /wp-admin/
Disallow: /wp-includes/
```

Automaticky
Ručne

```
User-agent: *
Disallow: /wp-admin/
Disallow: /wp-includes/
```

Čo si jako užívateľ všímať?

- Https (typ certifikátov?)
- DNSSEC
- URL
- Logiku aplikácie
- Preklikanie aplikácie
- Grafika

- Bezplatná služba
- Penetračné testovanie webových stránok
- Služba spustená v roku 08/2013
- Celkovo otestovaných približne 260 webových aplikácií
- Celkovo vydaných cez 4000 doporučení na vylepšenie
- https://www.skenerwebu.cz/

Kritické

Stredné

Nízké

Informačné

Stredné

Nízké

Not Found

The requested URL /login was not found on this server.

Apache/2.2.15 (CentOS) Server at [redacted] Port 80

Stredné

Nízké

Response Headers

Name	Value
RESPONSE	HTTP/1.1 200 OK
Date	Thu, 05 Feb 2015 14:13:28 GMT
Server	Apache
X-Powered-By	PHP/5.3.3-7+squeeze23
Cache-Control	no-cache
Keep-Alive	timeout=15, max=96
Connection	Keep-Alive
Transfer-Encoding	chunked
Content-Type	text/html; charset=UTF-8
X-Pad	avoid browser bug

Kritické

Stredné

Nízké

```
Pro aktivaci prosím navštivte následující odkaz v průběhu
následujících 24 hodin:

http://info.[redacted]

Po aktivaci se můžete přihlásit s následujícími údaji:


Uživatelské jméno: skener

Heslo: test123
```

Najčastejšie chyby

- Chýba šifrované spojenie
- Neošetrené session, cookies
- XSS :(
- Zraniteľné/neaktuálne SW
- Logika aplikácie
- Spracovávanie užívateľských údajov

- Výstup pre nás: prehľad o najčastejších chybách vo webových aplikáciach + možnosť osvety
- Výstup pre žiadateľov: výstupná správa s nálezmi, označením ich závažnosti a navrhnuté riešenie

Ďakujem za pozornosť

Zuzana Duračinská • zuzana.duracinska@nic.cz