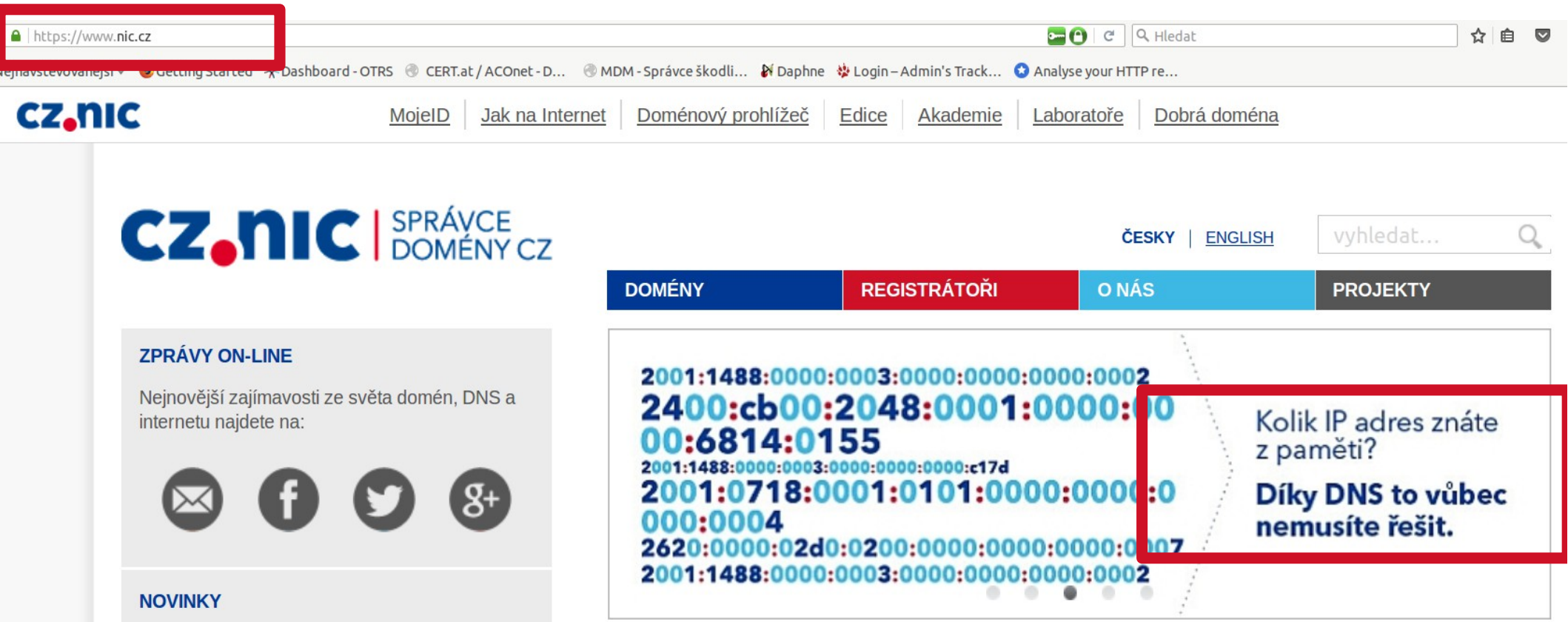
Skenerwebu

Proč si nechat otestovat webovou aplikaci?

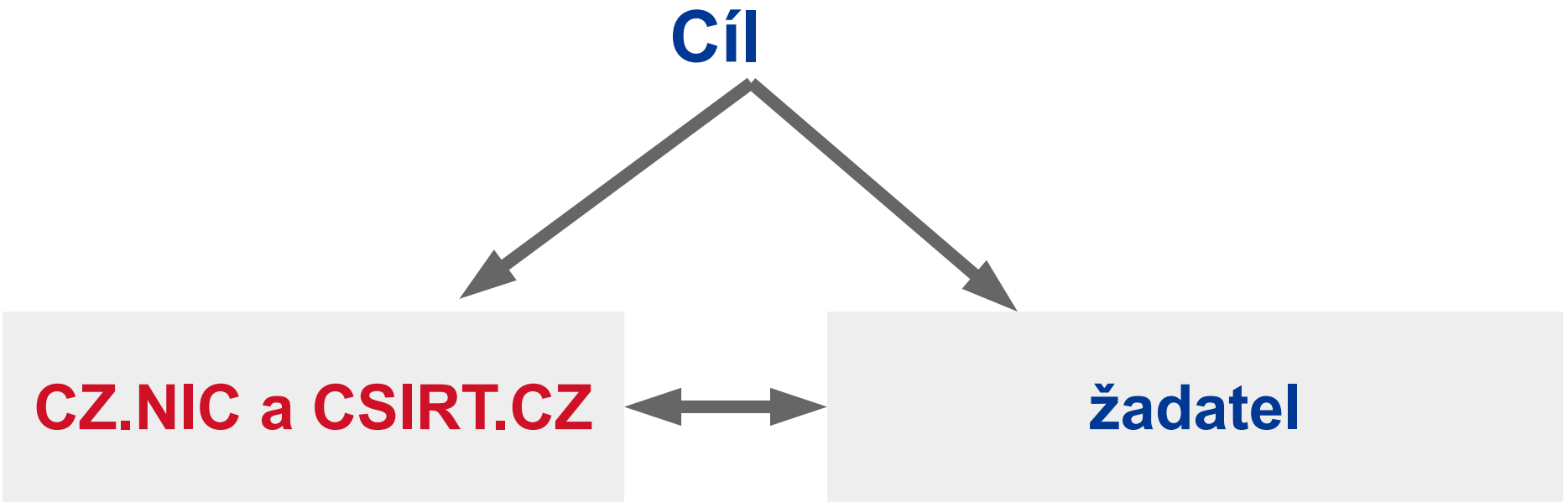
Věra Mikušová • vera.mikusova@nic.cz •
14.6.2016

CZ.NIC | SPRÁVCE DOMÉNY CZ


https://www.nic.cz
Hledat
Dashboard - OTRS
CERT.at / ACOnet - D...
MDM - Správce škodli...
Daphne
Login – Admin's Track...
Analyse your HTTP re...
cz.nic
MojeID
Jak na Internet
Doménový prohlížeč
Edice
Akademie
Laboratoře
Dobrá doména
cz.nic | SPRÁVCE DOMÉNY CZ
ČESKY | ENGLISH
vyhledat...
DOMÉNY
REGISTRÁTOŘI
O NÁS
PROJEKTY
ZPRÁVY ON-LINE
Nejnovější zajímavosti ze světa domén, DNS a internetu najdete na:
NOVINKY
2001:1488:0000:0003:0000:0000:0000:0002
2400:cb00:2048:0001:0000:0000:6814:0155
2001:1488:0000:0003:0000:0000:0000:c17d
2001:0718:0001:0101:0000:0000:0000:0004
2620:0000:02d0:0200:0000:0000:0000:0007
2001:1488:0000:0003:0000:0000:0000:0002
Kolik IP adres znáte z paměti?
Díky DNS to vůbec nemusíte řešit.

SKENER WEBU

- Sužba byla spuštěna v roce 2013
- Primárně vyvinuta pro neziskový a veřejný sektor



Motivace

- Stav zabezpečení webových aplikací
- Snaha o zlepšení situace na českém trhu
- Podpora osvěty mezi administrátory webových stránek (počítačová bezpečnost prakticky)
- Zlepšení zabezpečení veřejných služeb
- Možnost sledovat stav/trendy v oblasti webových aplikací

Objednávka

- Držitel domény
  - Validovaný účet moje ID
  - Elektronická objednávka (Česká pošta s.p., První certifikační autorita a.s., eIdentity a.s.)
    - objednavka@skenerwebu.cz
  - Písemná objednávka s úředně ověřeným podpisem

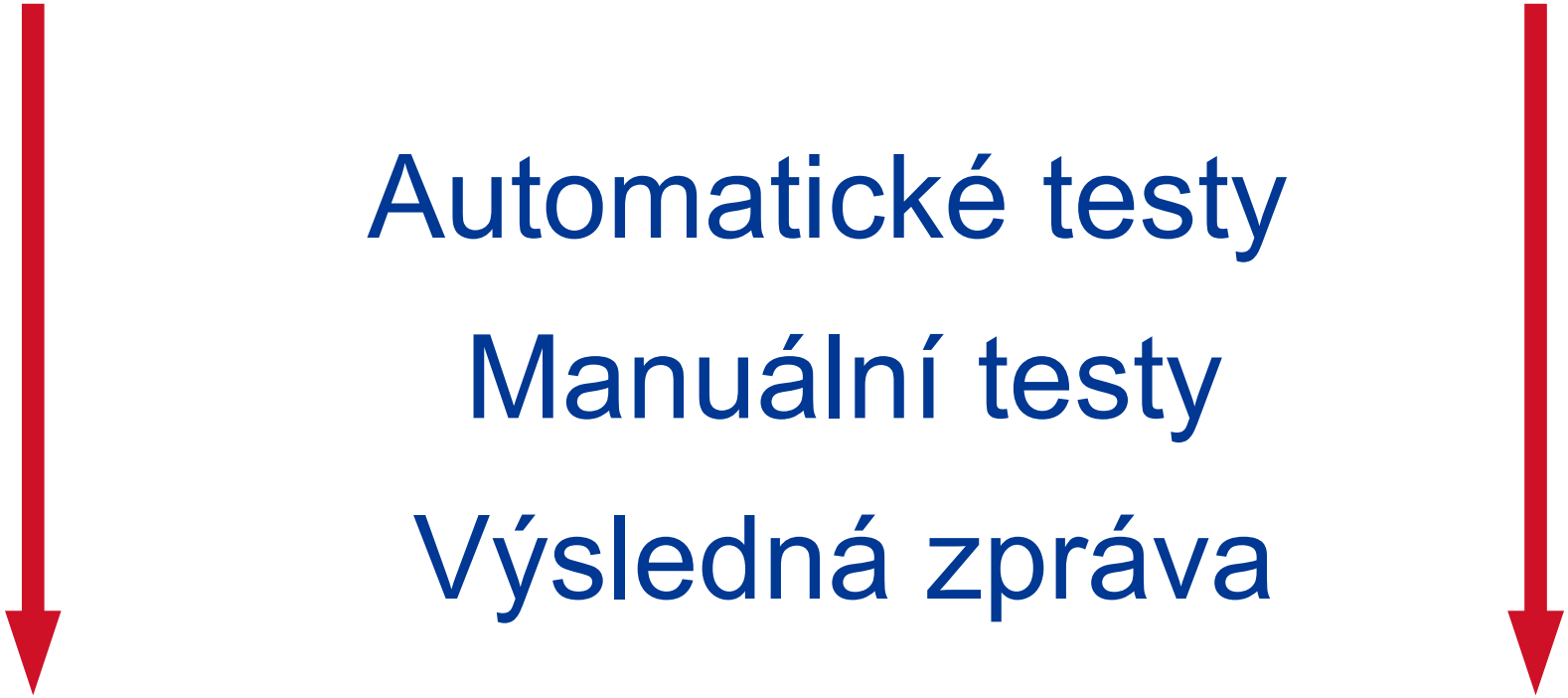
    CZ.NIC, z. s. p. o.

    Milešovská 1136/5

    130 00 P3

Jak test probíhá?

- Metodika OWASP (Open Web Application Security Project) Top 10 najčastějších zranitelností na webových aplikacích



Co zjišťujeme

- Injektování (spouštění příkazů s privilegovanými právy)
- Chybná autentizace a správa relace (převzetí identity uživatele)
- XSS (přetvoření vzhledu stránek, přesměrování uživatele na škodlivé weby)
- Nezabezpečená konfigurace (neautorizovaný přístup k některým funkcím)

Co zjišťujeme

- Expozice citlivých dat
- Cross-Site Reguest Forgery (smazání účtu či přidání záznamu)
- Použití známých zranitelných komponent
- Zbytečné informace usnadňující napadení webu
- Únik dat na internet...

Výsledná zpráva

- Rozdělení nálezů do logických částí
- Označení odhadu závažnosti nálezu (informační, nízký, střední, vysoký a kritický)
- Popis nálezu a možný technický dopad
- Detail zranitelnosti (popis kde sa nález vyskytuje URL, screenshot...)
- Doporučení k odstranění

V číslech (2015)

- 135 otestovaných webových aplikací
- Vydáno přes 1000 doporučení
- Na každém webu najdeme zhruba 10-20 nálezů

Komu službu doporučujeme

- Veřejné a státní správě
- Neziskovému sektoru
- Jako doplňkový test

-

- nudná administrativa
- delší čekací doba na testování
- nelze zahrnout více webů

+

- komplexní zpráva o zabezpečení webu
- každý nález je popsaný spolu s doporučeným řešením
- každý nález je označený možnou mírou rizika
- test je bezplatný :)

Děkuji za pozornost

Věra Mikušová • vera.mikusova@nic.cz