Zabezpečení web aplikací

Radomír Orkáč, Martin Černáč

Rozdělení chyb

- Každý program je buď triviální, nebo obsahuje alespoň jednu chybu.
- Oblasti dle výskytu chyb:
  - provoz,
  - konfigurace (služby, aplikace),
  - realizace (volba software),
  - návrh (architektura řešení).

cesnet

Návrhové chyby (architektura řešení)

Návrhové chyby

- LAMP není dogma!
- Potřebuji PHP 7.2, 7.0 a 5.6 v různých konfiguracích pro různé klienty
  - Taky Perl a Python
  - A jedna aplikace potřebuje Redis
  - A jedna MongoDB
  - A jedna vyžaduje Ruby
  - A jedna …
- „Božský“ server, který umí úplně všechno
  - Aktualizace jedné komponenty rozbije závislé aplikace

cesnet

Microservices

- Reverzní proxy
- Kontejner pro každou aplikaci
- Distribuovaný systém (včetně kladů a záporů)
- Má své vlastní klady
  - Oddělení služeb a aplikací
  - Kontejner zachová stejné prostředí na více místech
  - Pomůže se škálováním a vysokou dostupností
- Má své vlastní zápory
  - Náročnější na správu a monitorování

cesnet

Realizační chyby (volba software)

Realizační chyby

- Výběr vhodného nástroje k dosažení cíle
- Hledání nástroje, ne způsobu, jak nástroj použít
- Nadměrné užívání black-box komponent
  - Nejasná interní funkce (např. iRedMail)
- Problém „standalone“ aplikací
  - Integrovaný HTTP server
  - Znovuobjevení kola a všech spojených problémů

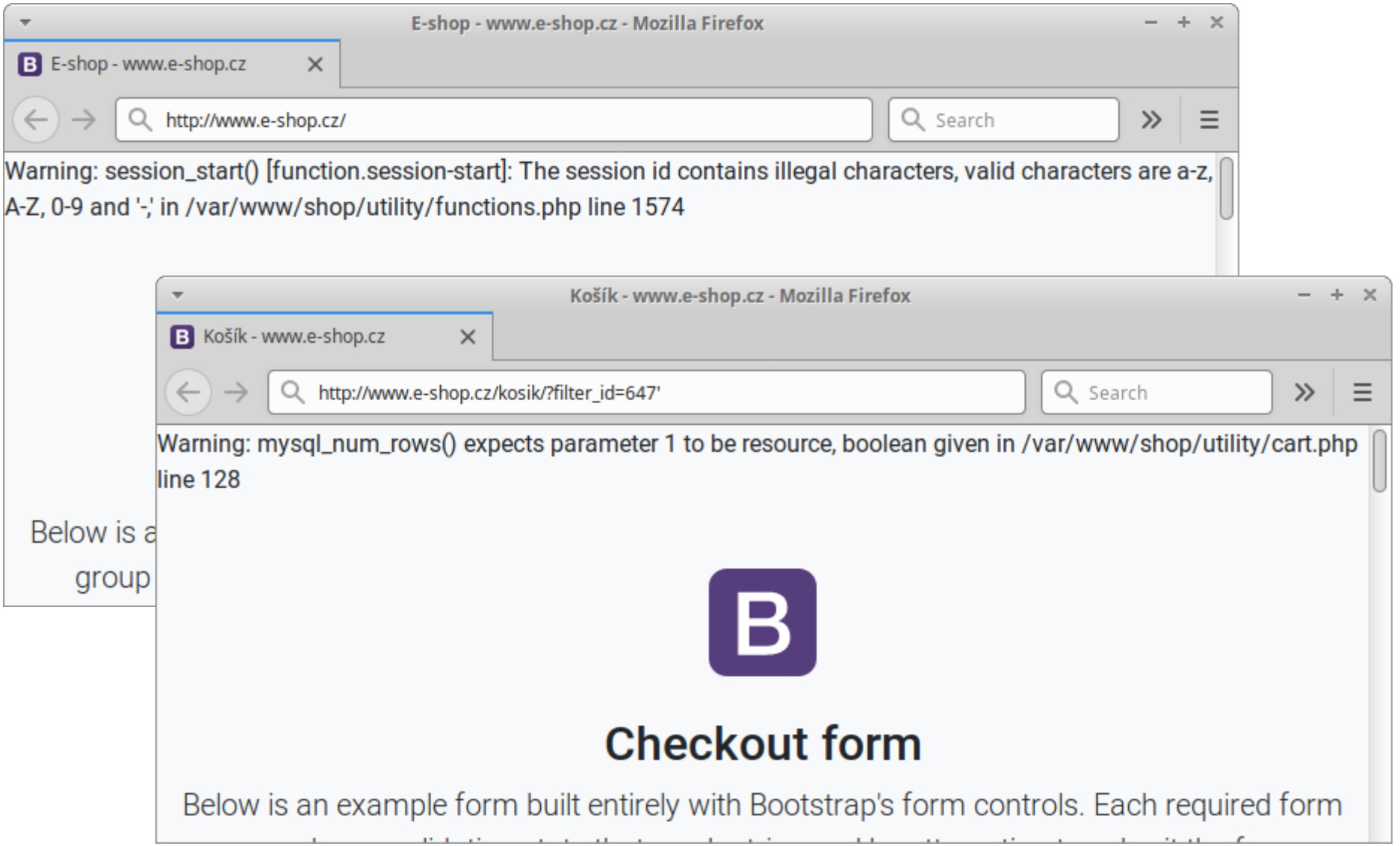
cesnet

Konfigurační chyby

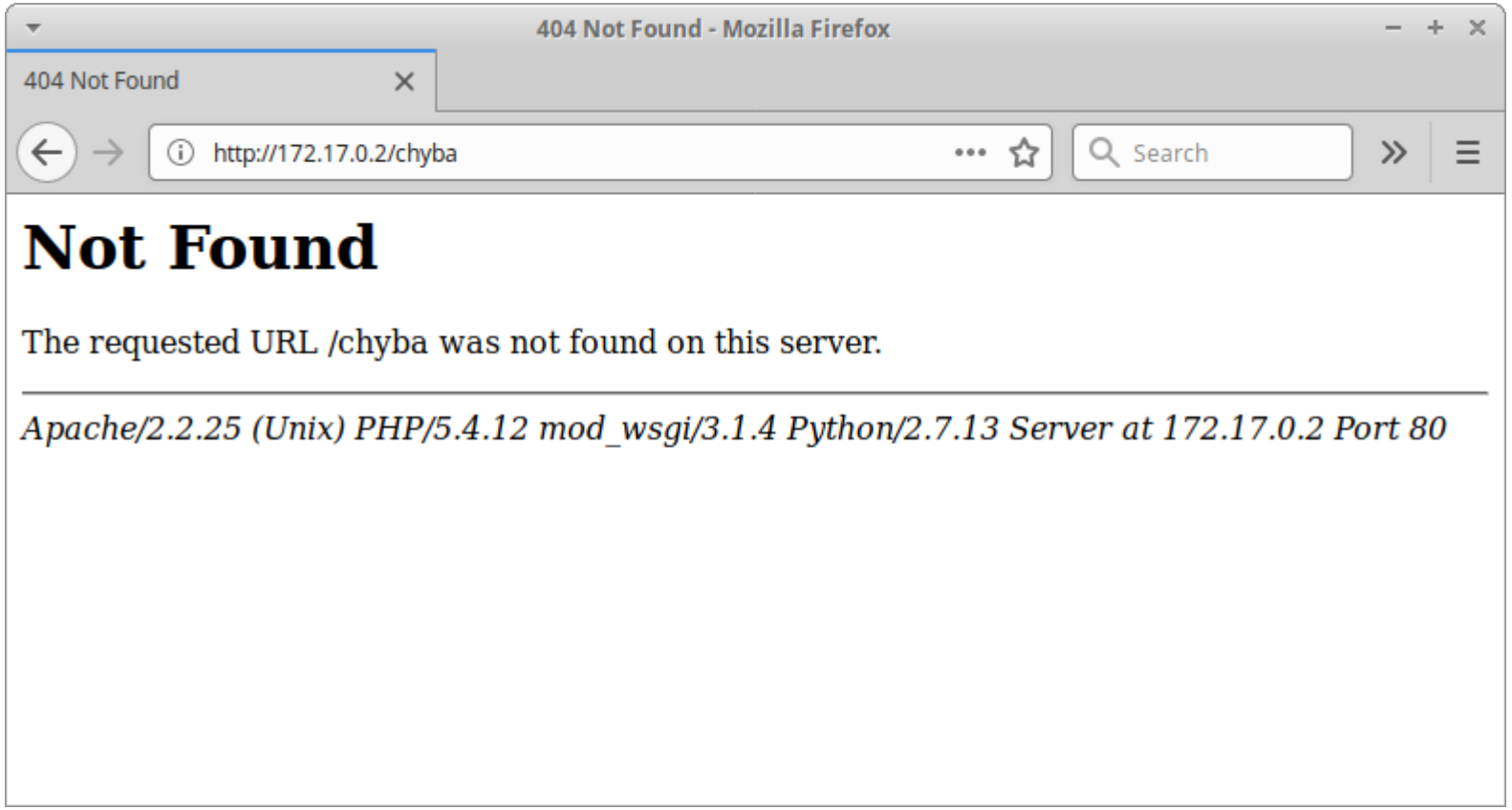
Konfigurační chyby

- Snadno detekovatelné
  - Nesprávné chování služby/aplikace
  - Dostupné kontrolní nástroje
  - Automatizace → pravidelná kontrola
- Snadno napravitelné
  - Úprava nastavení služby/aplikace

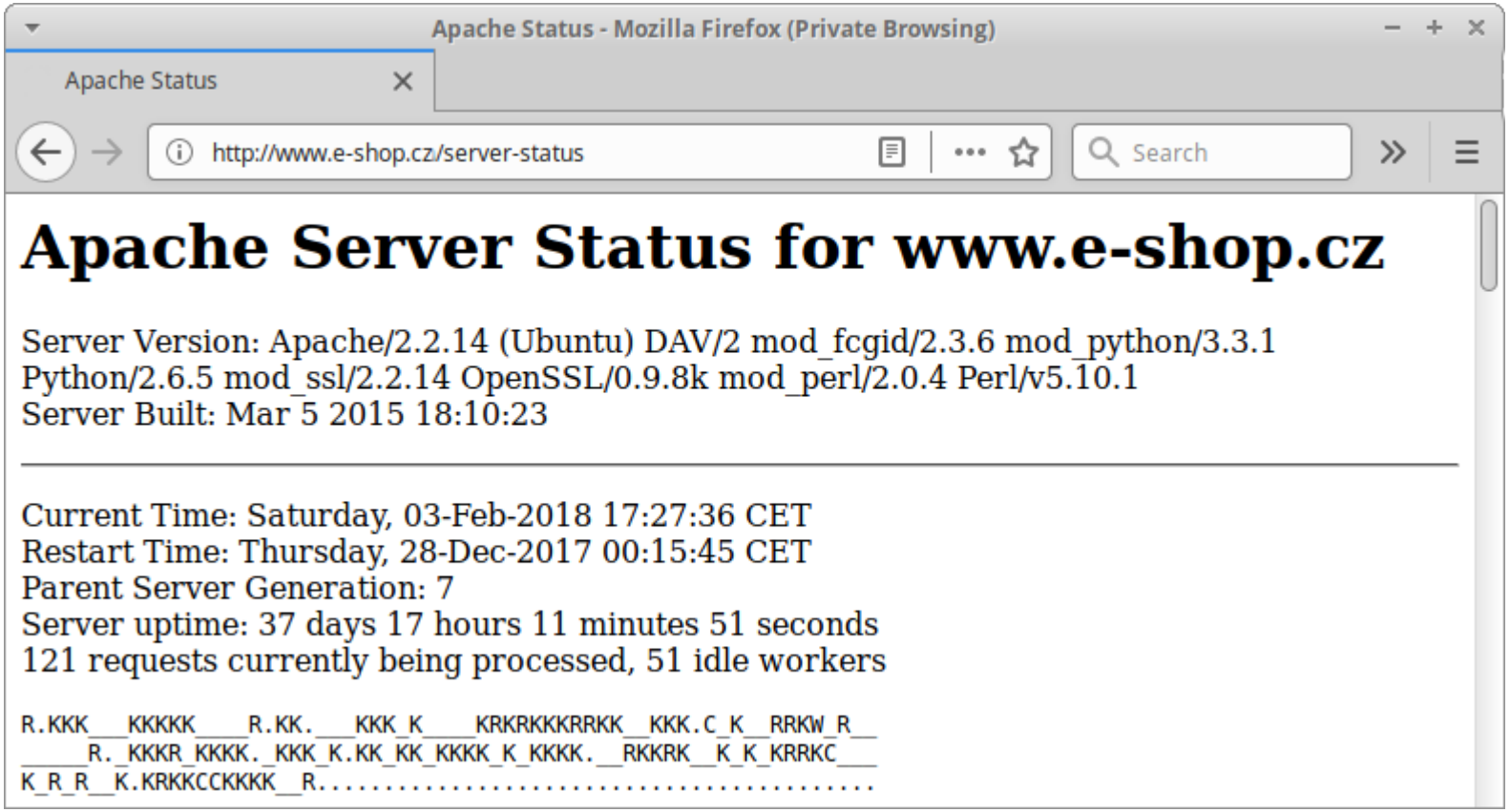
Ladění v produkci



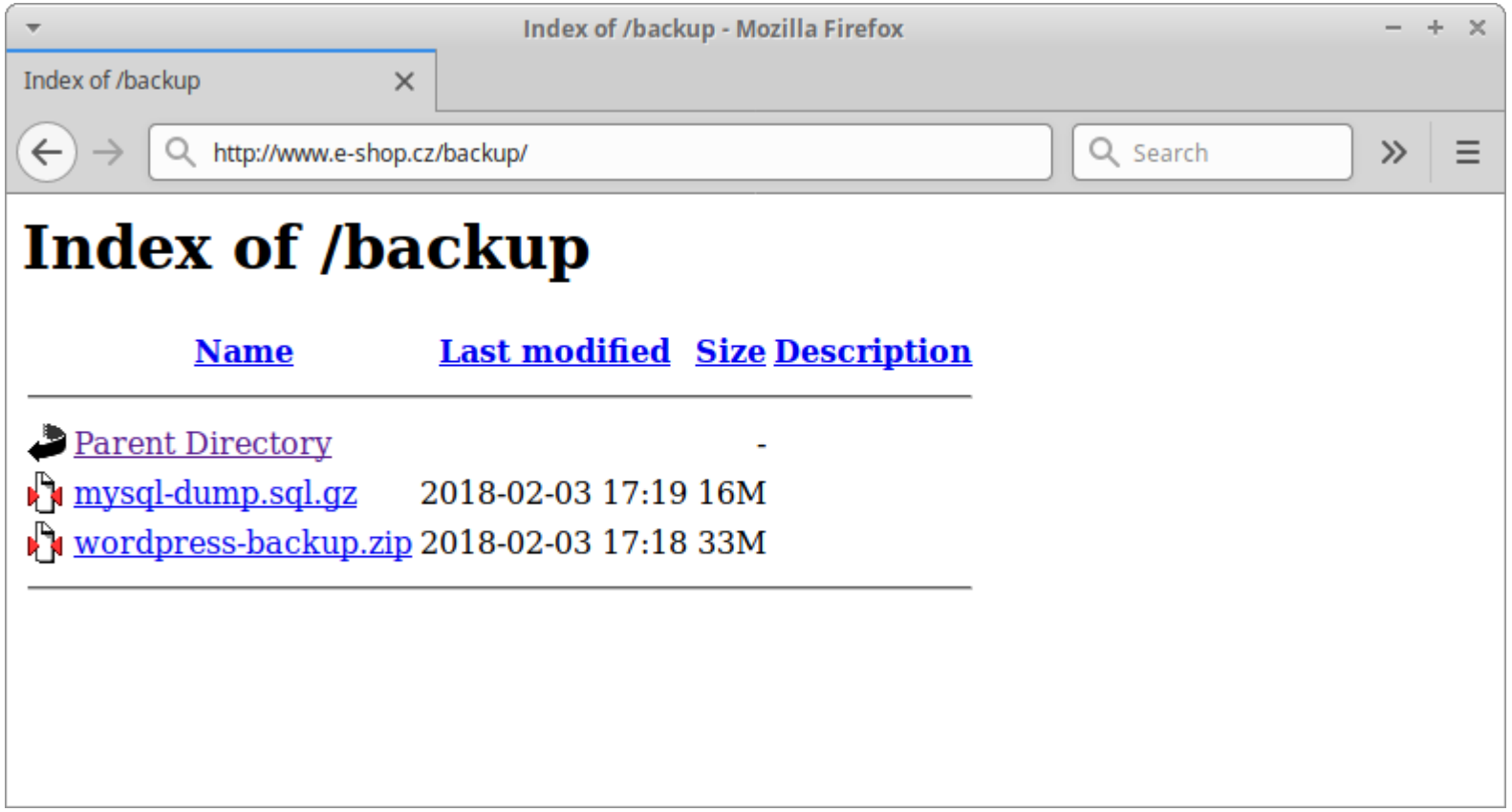
Upovídaný server



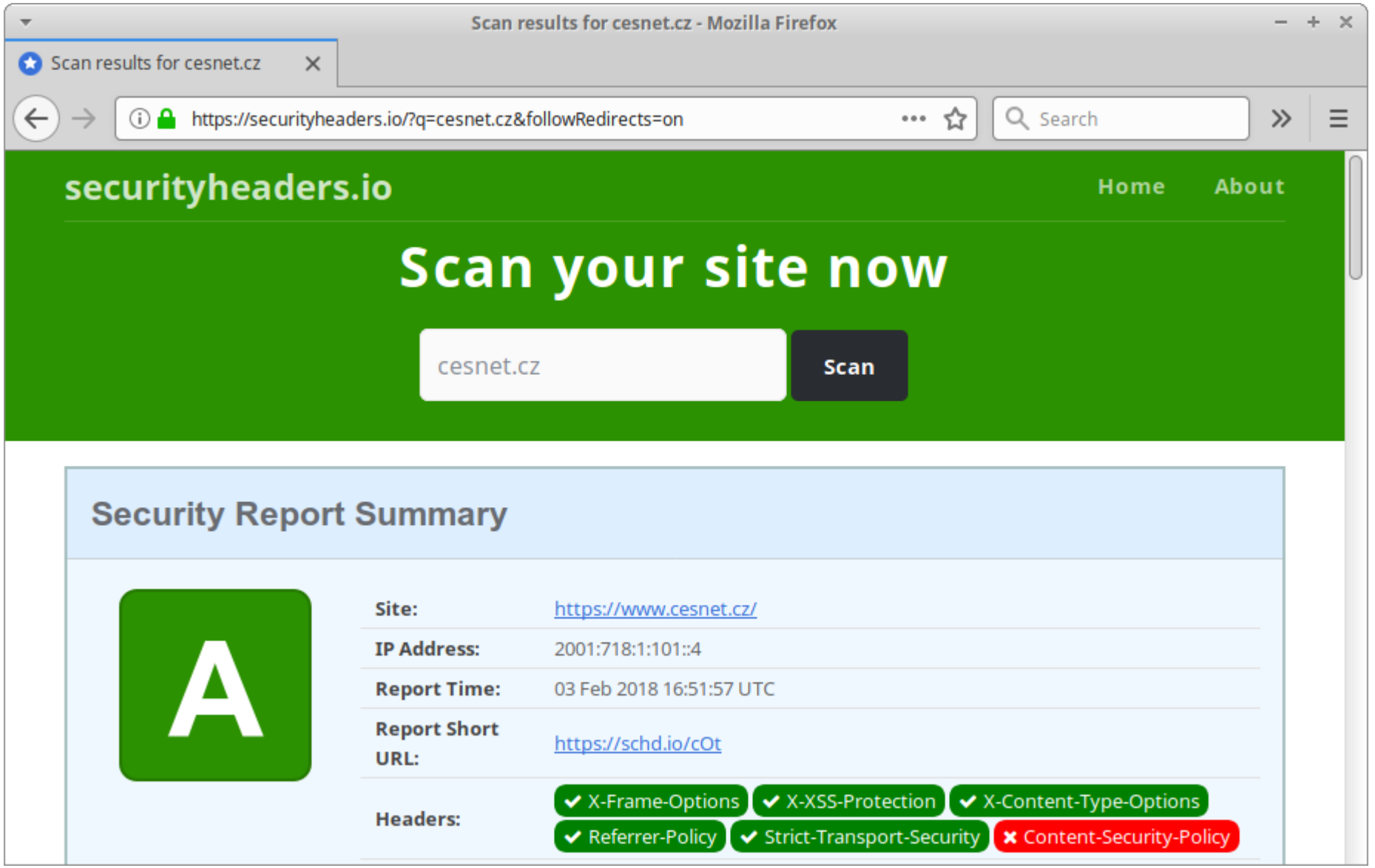
Stav serveru (mod_status)



Directory Listing



… na téma HTTP hlaviček



… na téma HTTP hlaviček

Missing Headers

Strict-Transport-Security	HTTP Strict Transport Security is an excellent feature to support on your plementation of TLS by getting the User Agent to enforce the use of HTT "strict-transport-security: max-age=31536000; includeSubDomains".
Content-Security-Policy	Content Security Policy is an effective measure to protect your site from sources of approved content, you can prevent the browser from loading
X-Frame-Options	X-Frame-Options tells the browser whether you want to allow your site t ing a browser from framing your site you can defend against attacks like value "x-frame-options: SAMEORIGIN".
X-XSS-Protection	X-XSS-Protection sets the configuration for the cross-site scripting filter b ommended value "X-XSS-Protection: 1; mode=block".
X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.

Grand Totals

A+	340,008
A	2,595,279
B	959,414
C	301,156
D	1,008,169
E	1,061,416
F	3,807,017
R	1,253,822
Total	11,326,281

… na téma HTTP hlaviček

- HTTP Strict Transport Security (HSTS)
  - Prohlížeč bude po určitou dobu načítat obsah pouze přes HTTPS
    - *Strict-Transport-Security: max-age=31536000*
    - Platnost i pro poddomény *„includeSubDomains“*

… na téma HTTP hlaviček

- Content Security Policy (CSP)
  - Politika „načítání“ zdrojů, jde o tzv. whitelisting zdrojů
  - HTTP hlavička - Content-Security-Policy
  - *Unsafe-inline* u direktiv *script-src* a *style-src* povolí inline skripty

Content-Security-Policy: script-src 'self' https://apis.google.com;
Content-Security-Policy: img-src 'self' https://.domena.cz;*
Content-Security-Policy: script-src 'self' 'nonce-jsdh7idsg...'
<script nonce="jsdh7idsg...">alert('1');</script>

… na téma HTTP hlaviček

- HTTP hlavička X-FRAME-OPTIONS
  - Načítaná stránka (ne)smí být zobrazena ve *frame, iframe, object.* Obrana proti tzv. clickjackingu.
  - Jsou k dispozici tři možnosti
    - SAMEORIGIN - povolení rámu na vlastním webu
    - DENY - stránka nikdy nesmí být zobrazena v rámu
    - ALLOW-FROM: http://www.domena.cz

Apache: *Header set X-Frame-Options SAMEORIGIN*
PHP: *header('X-Frame-Options: SAMEORIGIN');*

… na téma HTTP hlaviček

- HTTP hlavička X-FRAME-OPTIONS
  - Redakční systémy (Drupal, Wordpress, ...) již automaticky chrání přihlašovací formulář

Wordpress: Send X-Frame-Options for admin and login pages.
- Keywords 3.2-early removed
- Milestone changed from Future Release to 3.1
- Resolution set to fixed
- Status changed from new to closed

Drupal: Core is now protected against click-jacking by default
- Posted by Fabianx on 3 July 2015
- Introduced in branch: 8.0.x

… na téma HTTP hlaviček

Ukázka

… na téma HTTP hlaviček

- HTTP hlavička X-XSS-Protection
  - Vynutí použití XSS filtru v prohlížeči, který zabrání spuštění kódu, který „přišel“ přes URL nebo z formuláře.
  - Direktiva *mode=block* zakáže zobrazení stránky, namísto (ne)spuštění kódu.
  - Hlavička *„X-XSS-Protection: 1; mode=block“*

… na téma HTTP hlaviček

- HTTP hlavička X-Content-Type-Options
  - Ověření správnost MIME typu zdroje
  - Obrana proti zpracování HTML dokumentů jako skript nebo styl
  - Hlavička „*X-Content-Type-Options: nosniff*“
    - Zablokuje „*style*“ když MIME type není *"text/css"*
    - Zablokuje „*script*“ když MIME type není *JavaScript*

… na téma HTTP hlaviček

- HTTP hlavička Set-Cookie
  - *HttpOnly* - Přístup ke cookies bude možný pouze přes požadavek typu HTTP(S). Obrana proti přístupu ke cookies např. prostřednictvím JavaScriptu.
  - S*ecure* - Cookies se budou posílat pouze přes šifrované spojení.

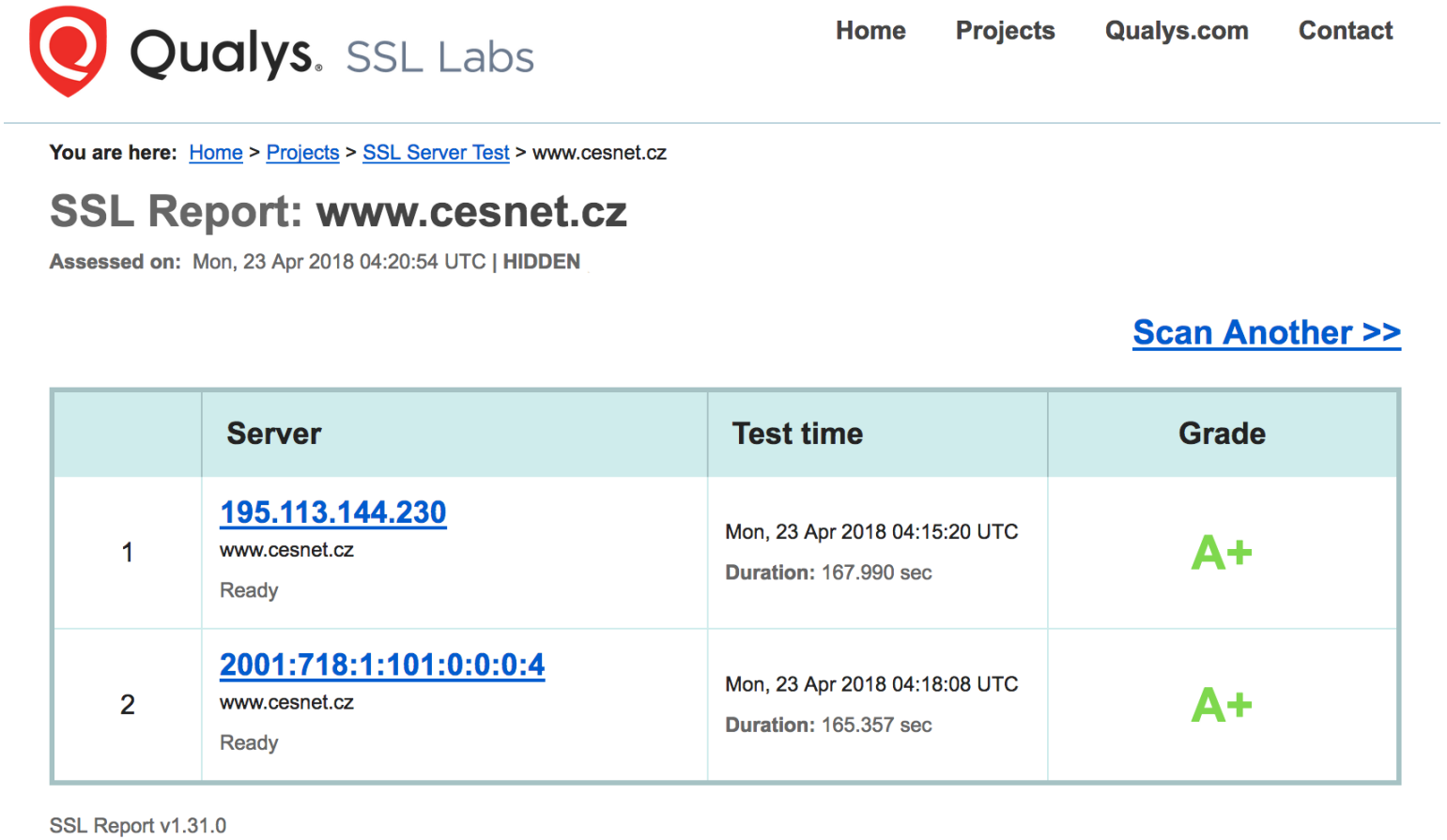
Apache: *Header always edit Set-Cookie (.*) "$1;HttpOnly;Secure"*

TLS/SSL podpora

- Základ pro bezpečí uživatelů WWW serveru
- Pouze nabízet **je málo**
  - Režim „opt-in“ nefunguje
  - Hlavička *HTTP Strict Transport Security*
- *Pouze* podporovat ***je málo***
  - Dbejte na podporované šifry (cipher suite)
  - Méně je někdy více: podpora verzí SSL a TLS
  - On-line nástroj pro kontrolu: ssllabs.com/ssltest

TLS/SSL podpora

- M. Špaček: Jak získat A+ v SSL Labs Server Testu.
- *„Když může známku A+ dostat lednička, tak můžete i vy!“*



Qualys. SSL Labs

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > www.cesnet.cz

SSL Report: www.cesnet.cz

Assessed on: Mon, 23 Apr 2018 04:20:54 UTC | **HIDDEN**

Scan Another >>

	Server	Test time	Grade
1	195.113.144.230 www.cesnet.cz Ready	Mon, 23 Apr 2018 04:15:20 UTC **Duration:** 167.990 sec	A+
2	2001:718:1:101:0:0:0:4 www.cesnet.cz Ready	Mon, 23 Apr 2018 04:18:08 UTC **Duration:** 165.357 sec	A+

SSL Report v1.31.0

Kam hlásit chyby?

- Jak získat kontakt na osobu, které by měla být nahlášena nalezená bezpečnostní chyba?
- Dostane se informace bezpečnou cestou přímo ke správnému cíli?
- Několik možností již existuje:
  - RFC2142: *abuse@, noc@, security@*
  - WHOIS
  - Web → kontakty

Kam hlásit chyby?

- Problém se pokusil vyřešit Ed Foudil návrhem standardu „A Method for Web Security Policies“.
- Jde o veřejně přístupný textový soubor security.txt, ze kterého se dozvíte koho a jak kontaktovat v případě nalezení bezpečnostního problému.

Kam hlásit chyby?

- CESNET z.s.p.o.
  - https://csirt.cesnet.cz/.well-known/security.txt

Contact: https://csirt.cesnet.cz/en/contact
Contact: mailto:certs@cesnet.cz
Encryption: https://csirt.cesnet.cz/publickey.asc
Encryption: https://pgp.mit.edu/pks/lookup?op=get&search=0xFC3F62D9F458694E
Signature: https://csirt.cesnet.cz/.well-known/security.txt.20180426.sig
Policy: https://csirt.cesnet.cz/en/vulnerability_report

Rekapitulace

- Rozdělte služby na „microservices“
- Dejte si pozor na chyby ve fázi návrhu
- Omezte upovídanost služeb
- Prověřte konfiguraci webových serverů
- Chraňte bezpečí vašich uživatelů
- Usnadněte nahlášení bezpečnostních chyb
- Prověřte snadnou dostupnost kontaktních údajů

cesnet

???

https://flab.cesnet.cz

flab@cesnet.cz