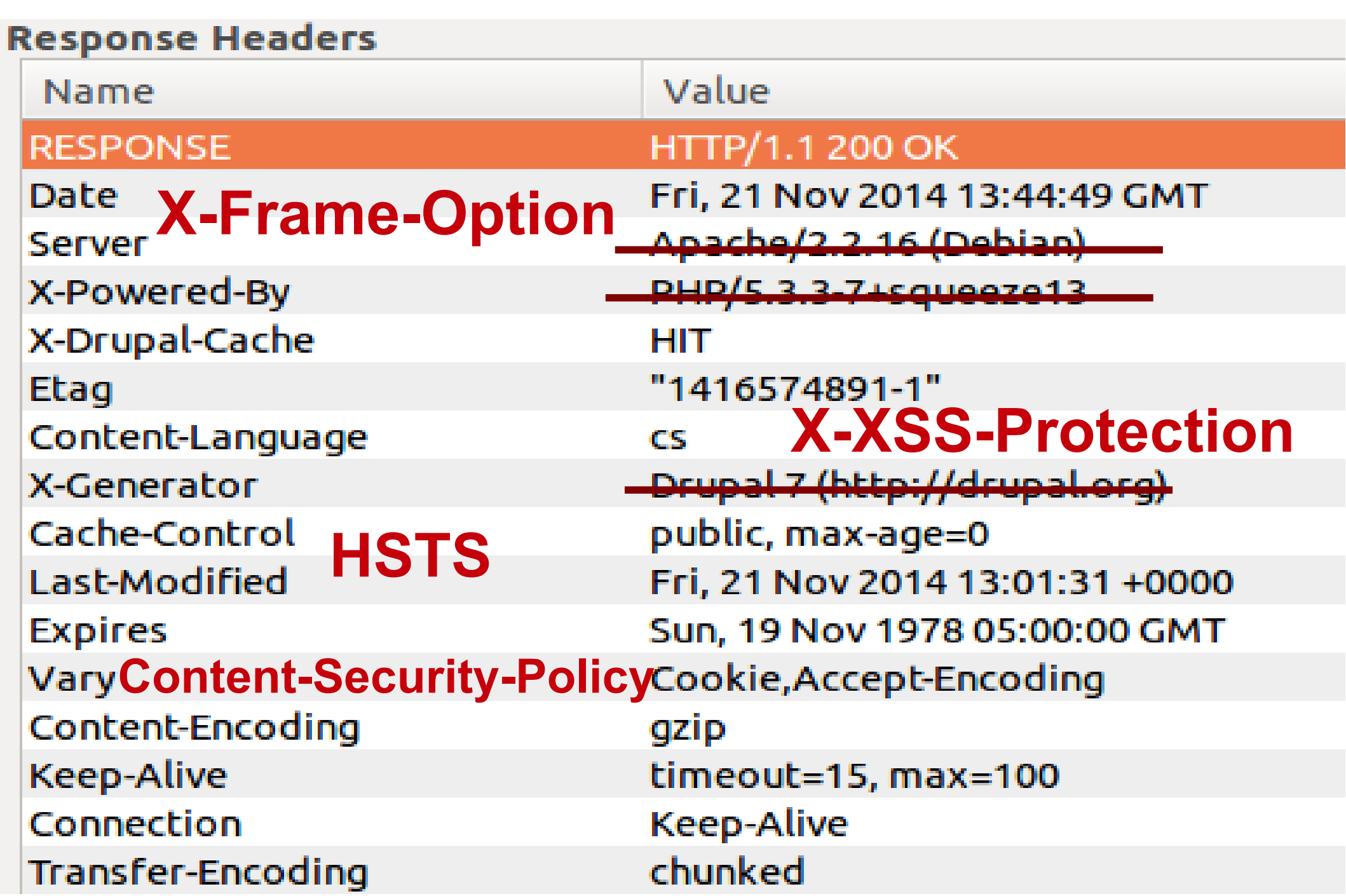
Skener webu

OWASP

Zuzana Duračinská • zuzana.duracinska@nic.cz •
29.11.2014


Response Headers
Name
Value
RESPONSE
HTTP/1.1 200 OK
Date
Fri, 21 Nov 2014 13:44:49 GMT
X-Frame-Option
Server
Apache/2.2.16 (Debian)
X-Powered-By
PHP/5.3.3-7+squeeze13
X-Drupal-Cache
HIT
Etag
"1416574891-1"
Content-Language
cs
X-XSS-Protection
X-Generator
Drupal 7 (http://drupal.org)
Cache-Control
public, max-age=0
HSTS
Last-Modified
Fri, 21 Nov 2014 13:01:31 +0000
Expires
Sun, 19 Nov 1978 05:00:00 GMT
Vary
Content-Security-Policy
Cookie,Accept-Encoding
Content-Encoding
gzip
Keep-Alive
timeout=15, max=100
Connection
Keep-Alive
Transfer-Encoding
chunked

Skener webu

- Bezplatná služba testovania webových strániek
- Spustená v auguste 2013

Záujem

Objednávka

Testovanie

Výsledná správa

...

Služba CAPTCHA Help

CAPTCHA Help se týká CAPTCHA, na který čas od času narazíme na mnoha webových stránkách - nejčastěji je požadováno opsání textu, který je zobrazen na obrázku. Avšak ouha, pokud text z obrázku nemůžete přečíst. Třeba nevidíte (nevidomí), zápasíte s písmenky (dyslektici) anebo existuje jiný důvod, který vám brání v opsání CAPTCHA kódu z obrázku. A právě pro jednotlivce, kteří nemohou CAPTCHA kód přečíst anebo reguléně opsat, vznikly služby CAPTCHA Help:

- rozšíření prohlížeče:
  - pro Chrome a Chromium.
  - pro Internet Explorer - od 28. února 2014 je k dispozici alfa verze, tj. verze, na kterou se ještě nadá spolehnout a je určena pro testování v úzkém okruhu lidí.
  - Více informací na stránce „Jak to funguje“.
- e-mailové odeslání požadavku na přečtení obrázku CAPTCHA
  - Dnes již historická alternativa k výše uvedeným doplňkům.
  - Více informací na stránce „Jak to funguje“.

CAPTCHA Help je určen pro webové uživatele se specifickými CAPTCHA potřebami. Služby, které nabízíme, poskytujeme zdarma. Odměnou nám je dobré slovo a případné dobré náměty pro zlepšení služeb.

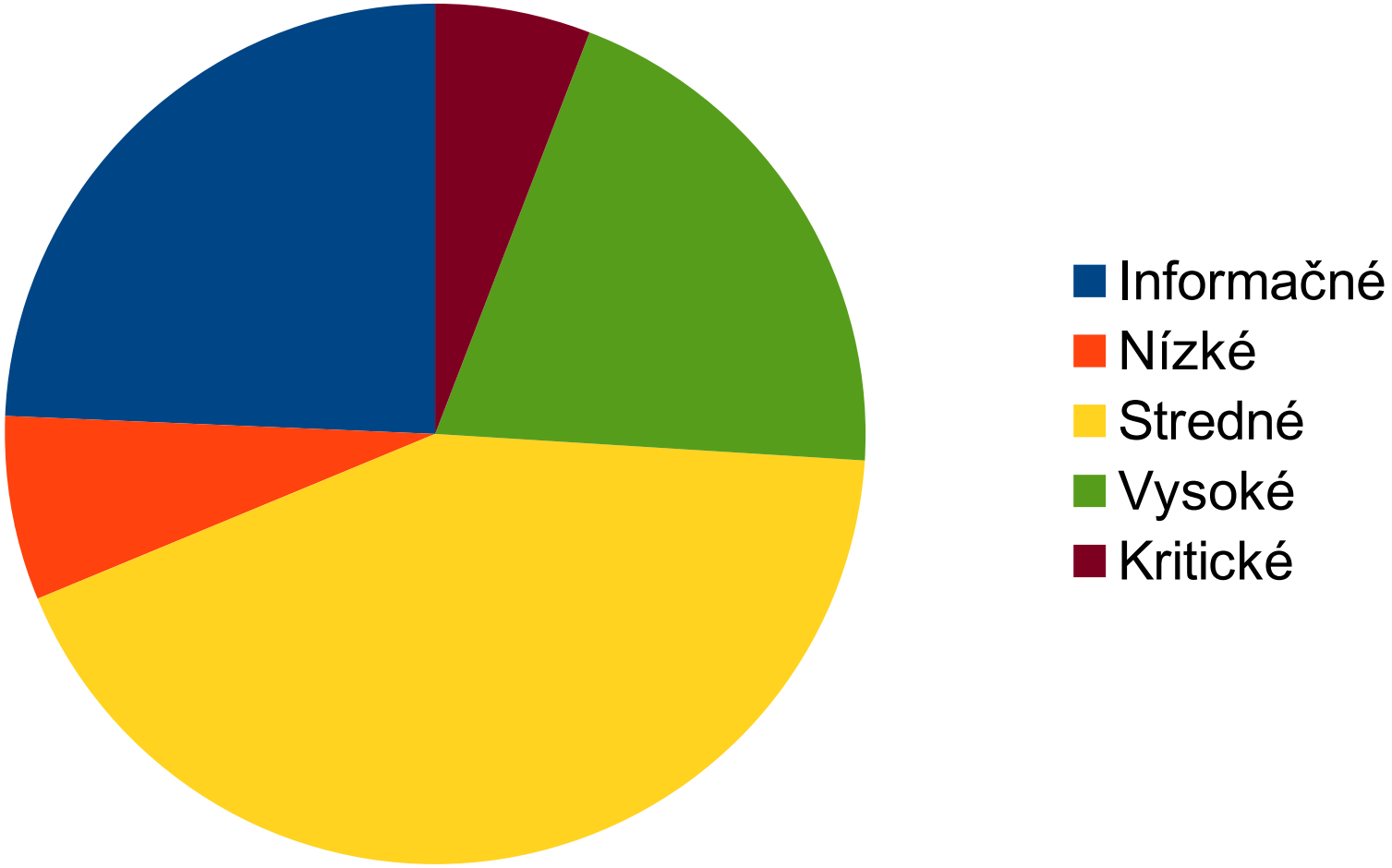
cz.nic

Čísla v prezentácií musia byť:)

- 1667
- Cca 444 626
- 673
- 32
- 130
- 1789
- 92
- **42**

- Nájdených zraniteľností
- .CZ - DNSSEC
- Zraniteľností so stredných rizikom
- Bitov má 4ková adresa
- Otestovaných domén
- Začiatok francúzskej revolúcie
- Kritických zraniteľností
- **Odpoveď na otázku života a vesmíru**

Aj graf musí byť:)



Najčastejšie chyby

- Autentizácia a správa sedenia

  - slabá politika hesiel (dĺžka hesla, spôsob zasielania hesla, spôsob zmeny hesla...)

  - prihlasovanie bez šifrovaného spojenia

  - nedostatočné nastavenie lifetime session cookie

  - absencia bezpečnostných flagov pre prácu cookies

  - verejne dostupné administrátorské rozhranie

Najčastejšie chyby

- Cross Site Scripting (stored/reflected)

  - neošetrenie vstupov v aplikácií

- Chybná konfigurácia

  - chýbajúce doplnky v hlavičkách (napr. X-Frame Options, X-XSS)

  - informácie o platformách (hlavičky, fingerprint servera...)

  - neošetrené chybové hlášky

  - citlivé informácie v URL

  - enumerácia užívateľských mien, e-mailov, adresárov

Najčastejšie chyby

- Použitie známych zraniteľností komponent
  - neaktuálne verzie používaných programov
- Ostatné
  - zobrazenie neprístupných údajov pre roboty
  - prelinkovanie s inými webmi
  - otvorené porty
  - nezabezpečený DNS
  - možné uploadovanie súboru
  - chýbajúca podpora pre IPv6

Ako výsledky zdieľame s vami?

- Blog NIC.CZ
- Sekcia Rady a návody na webe CSIRT.CZ
- Prezentácie
- Školenia
- …
- Osobne
- Nebránime sa ani iným možnostiam

OWASP

- Open Web Application Security Project
- Projekt (?) zahájený v roku 2001
- Nezisková organizácia s celosvetovou pôsobnosťou
- Zameranie na rôzne dielče časti webovej bezpečnosti

OWASP

- Cheat sheets
- ZAP (The Zed Attack Proxy)
- Development Guide
- AppSec Tutorial series...
- **OWASP Top 10**
- ...

OWASP Top 10

- 2004...2007...2010...2013
- Konsenzus 10 najkritickejších chýb v zabezpečení webových aplikácií
- Cieľom je zvýšiť povedomie o zabezpečení webových aplikácií
- CSIRT.CZ sa rozhodol pridať :)

OWASP Top 10

Během testu jsou vyhledávány především zranitelnosti, které uvádí soupis OWASP Top 10 mezinárodního projektu a komunity bezpečnostních specialistů Open Web Application Security Project (OWASP) OWASP Top 10:

A1 - Injektování (Injection)

Chyby umožňující napadení aplikace vložením kódu přes neošetřený vstup. Vkládáním kódu do neošetřeného vstupu útočník může spouštět příkazy s privilegovanými právy, k nimž by neměl mít přístup.

– Více informací o injektování

Původce hrozby	Vektor útoku	Bezpečnostní slabina		Technické dopady	Obchodní dopady
Aplikační specifikum	**Zneužitelnost snadná**	**Rozšíření běžné**	**Zjistitelnost průměrná**	**Dopad vážný**	**Aplikační / obchodní specifikum**
Vezměte v úvahu každého, kdo může posílat nedůvěryhodná data do systému,	Útočník posílá jednoduché textové příkazy, které zneužívají syntaxi cílového	Chyby typu injektování vznikají, když aplikace posílá do interpretu nedůvěryhodná data. Tyto chyby jsou velmi rozšířené, obzvláště v tzv. Legacy Code. Často		Injektování může mít za následek ztrátu nebo narušení integrity, odpovědnost	Zvažte obchodní hodnotu dotčených dat a platformy, na níž běží

A čo si urobil TY pre zabezpečenie webových aplikácií?

Zuzana Duračinská • zuzana.duracinska@nic.cz