Cyber Security Lab

Kontrola závislostí v aplikáciách

Terézia Mézešová

Jquery » Jquery-ui » 1.11.4 : Security Vulnerabilities

Cpe Name:*cpe:/a:jquery:jquery-ui:1.11.4*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2016-7103	79		XSS	2017-03-15	2018-07-29	4.3	None	Remote	Medium	Not required	None	Partial	None

Cross-site scripting (XSS) vulnerability in jQuery UI before 1.12.0 might allow remote attackers to inject arbitrary web script or HTML via the closeText parameter of the dialog function.

Total number of vulnerabilities : **1** Page : 1 (This Page)

SME.sk Správy Služby Počasie Blogy Zľavy Komunálne voľby 2018 Viac Prihlásenie | Registrovať

SME

Sobota, 20. október, 2018 | Meniny má **Vendelín**

SME.SK POČASIE DOMOV REGIÓNY EKONOMIKA SVET KOMENTÁRE SME+ KULTÚRA ŠPORT TV AUTO TECH ŽENA ZDRAVIE BLOG MENU

Najnovšie @denniksme na Instagrame Vražda Jána Kuciaka Dobré ráno Komunálne voľby Lovíme hoaxy Rozhovory Newsletter SME.sk POST.sk

DOMOV

Hľadajú kradnuté autá: Na Slovensku sa oplatí kradnúť. Tresty sú nízke

Dvanásť žien v bazéne a úplné ticho. Tento anglický podcast vás pobaví AUDIO

SVET

Ako vypočítať vzdialenosť k hviezde? Stačí vám základná matika FOTO

Ukážte telo novinára, vyzývajú aktivisti Saudskú Arábiu

EKONOMIKA

Herný špeciál: Kedy je ťažká hra odmena a kedy je za trest

Slovensko môže zrušiť jedno- a dvojcentové mince. Ako sa zmenia účty

ŠPORT

Víťazná séria Slovana v KHL sa skončila na ľade Spartaka Moskva

Chelsea vyrovnala v šlágri proti Manchestru United v nadstavení VIDEO

Ďalšie aktuality ›

Emma Drobná: Denne som vláčila mechy so zemiakmi. Môj život nestál na Superstar

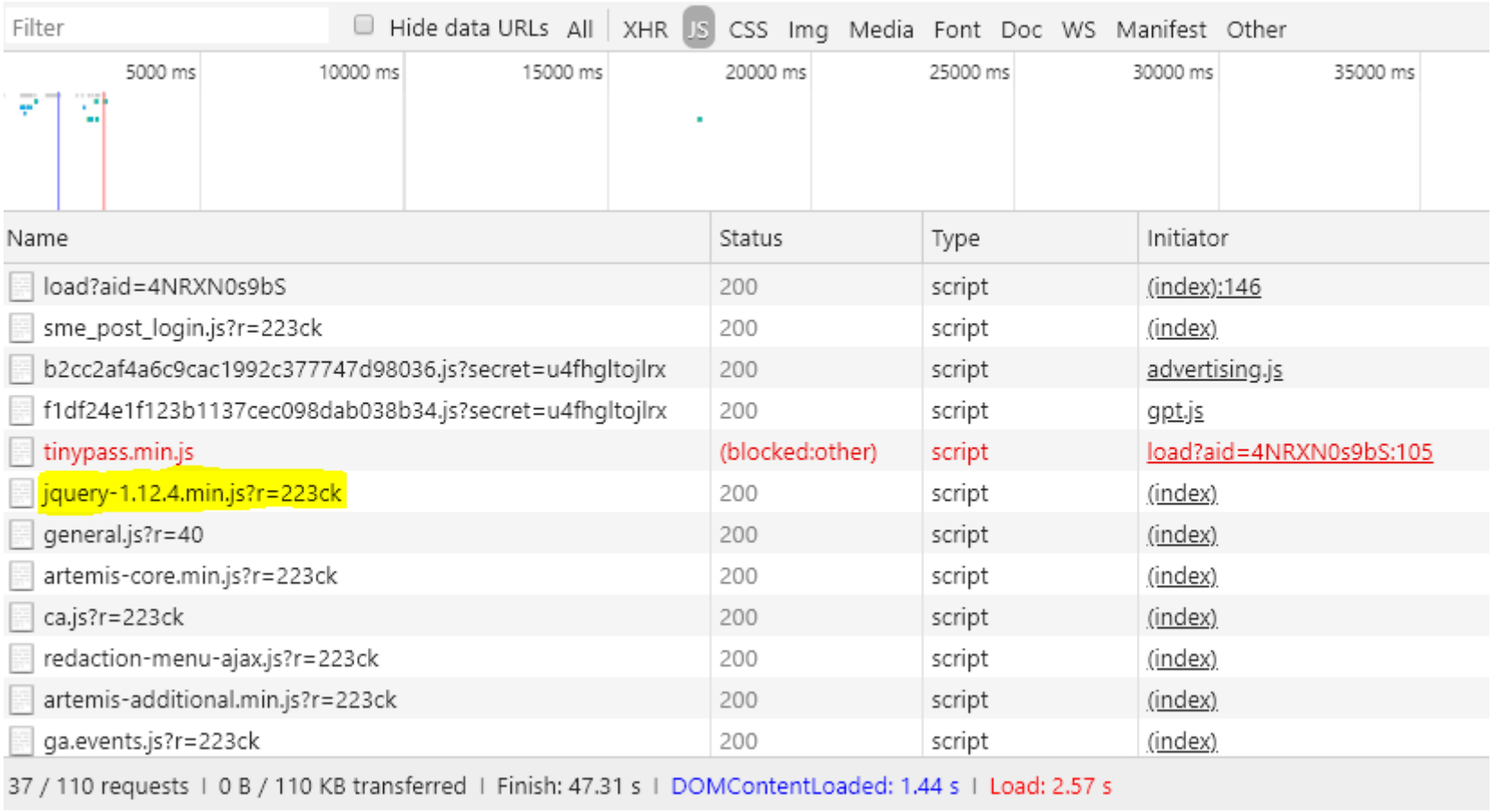
Drobná napísala najhranejšie piesne.

5

NAJČÍTANEJŠIE NA SME

4 hod | 24 hod | 7 dní | SME+ | EN

1. Triasli sa pred ním vrahovia a páchatelia sa šli radšej sami prihlásiť FOTO 12 203
2. Štát zabil novinára. Nitky vedú k princovi 7 495
3. Zámok Kunerad bol v plameňoch, požiar mal byť založený úmyselne FOTO 7 180
4. Pri samovražde muža zadržaného pre Kuciaka preverujú aj cudzie zavinenie 5 529
5. V Nitre robili rekonštrukciu nehody, pri ktorej zomrela mladá Oravčanka FOTO 5 298
6. V kluboch sú hviezdami. Na Lobotku a Škriniara reagovali aj miestne médiá VIDEO 4 622
7. Po svadbe ju vzal do bordelu. Tina Turner vydala novú knihu o svojom živote 3 423
8. Stavba diaľnice pri Košiciach pokročila. Pozrite si aktuálny stav FOTO 3 314


Filter
Hide data URLs
All
XHR
JS
CSS
Img
Media
Font
Doc
WS
Manifest
Other
5000 ms
10000 ms
15000 ms
20000 ms
25000 ms
30000 ms
35000 ms
Name
Status
Type
Initiator
load?aid=4NRXN0s9bS 200 script (index):146
sme_post_login.js?r=223ck 200 script (index)
b2cc2af4a6c9cac1992c377747d98036.js?secret=u4fhgltojlrx 200 script advertising.js
f1df24e1f123b1137cec098dab038b34.js?secret=u4fhgltojlrx 200 script gpt.js
tinypass.min.js (blocked:other) script load?aid=4NRXN0s9bS:105
jquery-1.12.4.min.js?r=223ck 200 script (index)
general.js?r=40 200 script (index)
artemis-core.min.js?r=223ck 200 script (index)
ca.js?r=223ck 200 script (index)
redaction-menu-ajax.js?r=223ck 200 script (index)
artemis-additional.min.js?r=223ck 200 script (index)
ga.events.js?r=223ck 200 script (index)
37 / 110 requests | 0 B / 110 KB transferred | Finish: 47.31 s | DOMContentLoaded: 1.44 s | Load: 2.57 s

Výber knižnice

- Funkcionalita?
- Kompatibilita s ostatnými už používanými?
- Jednoduchosť použitia?
- Licencia?

Používanie open source knižníc

priemerný počet
open source knižníc
v komerčnej aplikácii

aplikácií obsahovalo knižnice
so zraniteľnosťami

Zdroj: https://info.blackducksoftware.com/rs/872-OLS-526/images/OSSAReportFINAL.pdf

Používanie open source knižníc

1,894 days

priemerný vek nájdených zraniteľností

22.5

Priemerný počet knižníc
v 1 aplikácii

Zdroj: https://info.blackducksoftware.com/rs/872-OLS-526/images/OSSAReportFINAL.pdf

Scenáre

- IoT zariadenia so zraniteľnosťami bez možnosti aktualizácie
- Obídenie autentifikácie (slf4j - CVE-2018-8088)
- Vzdialené spustenie príkazu (struts2 - CVE-2017-5638)

Kontrola závislostí

VERACODE

Ako minimalizovať riziko?

- Získanie knižnice len z oficiálnych distribúcií
- Pravidelná kontrola používaných knižníc
- Monitoring voči novým zraniteľnostiam

US Databáza zraniteľností (NVD)

- Komplexná databáza zraniteľností
- Jedinečný CVE identifikátor zraniteľností
- Ohodnotenie CVSS
- Zoznam programov + verzií kde sa vyskytuje zraniteľnosť

Security Advisories

- RSS feed / mailing list zraniteľností a opráv + archív
- Zraniteľnosti aj bez CVE
- Seclists
- BugTraq

Retire.js

OWASP Dependency check

hands-on ukážka

Otázky?

Cyber Security Lab