

TYPE-0 XSS PAŽEIDŽIAMUMŲ PAIEŠKA IR IŠNAUDOJIMAS

Tomas Lažauninkas

CROSS-SITE SCRIPTING TIPAI

- Stored/permanent (vis rečiau pasitaikantys)
- Reflected (vis dar gana dažnai sutinkama)
- DOM/Type-0 (randama vis daugiau)
 - Pirmą kartą paminėtas 2005 metais

DOM XSS

- XSS kurio principas pakeisti DOM struktūra savo Javascript kodo vykdymui
- Owasp aprašymas:
 - DOM Based XSS (or as it is called in some texts, “type-0 XSS”) is an XSS attack wherein the attack payload is executed as a result of modifying the DOM “environment” in the victim’s browser used by the original client side script, so that the client side code runs in an “unexpected” manner. That is, the page itself (the HTTP response that is) does not change, but the client side code contained in the page executes differently due to the malicious modifications that have occurred in the DOM environment.

DOM XSS ANATOMIJA

- **Source:** Javascript elementai, kurie gali būti kontroliuojami vartotojo
- **Filtrai:** Javascript funkcijos naudojamos keičiant tam tikrus DOM objektus
- **Sinks'ai:** potencialiai pavojingos funkcijos, kurių vykdymo eigos keitimas gali priversti prie XSS vykdymo

TRADICINIAI SOURCE'AI

- Viskas kam gali turėti įtakos vartotojas:
 - URL (document.url, document.location, window.location)
 - Referrer
 - Windows.name

TRADICINIAI SINKS'AI

- HTML modifikavimo elementai:
 - innerHTML, outerHTML, document.write
- Javascript vykdymo funkcijos
 - Eval(), execScript, function(), setTimeout()
 - iframe, script src reikšmės

TRADICINIAI FILTRAI

- (un)escape (* @ - _ + . /)
- (de)encodeURI (, / ? : @ & = + \$ #)
- Replace
- Match/test

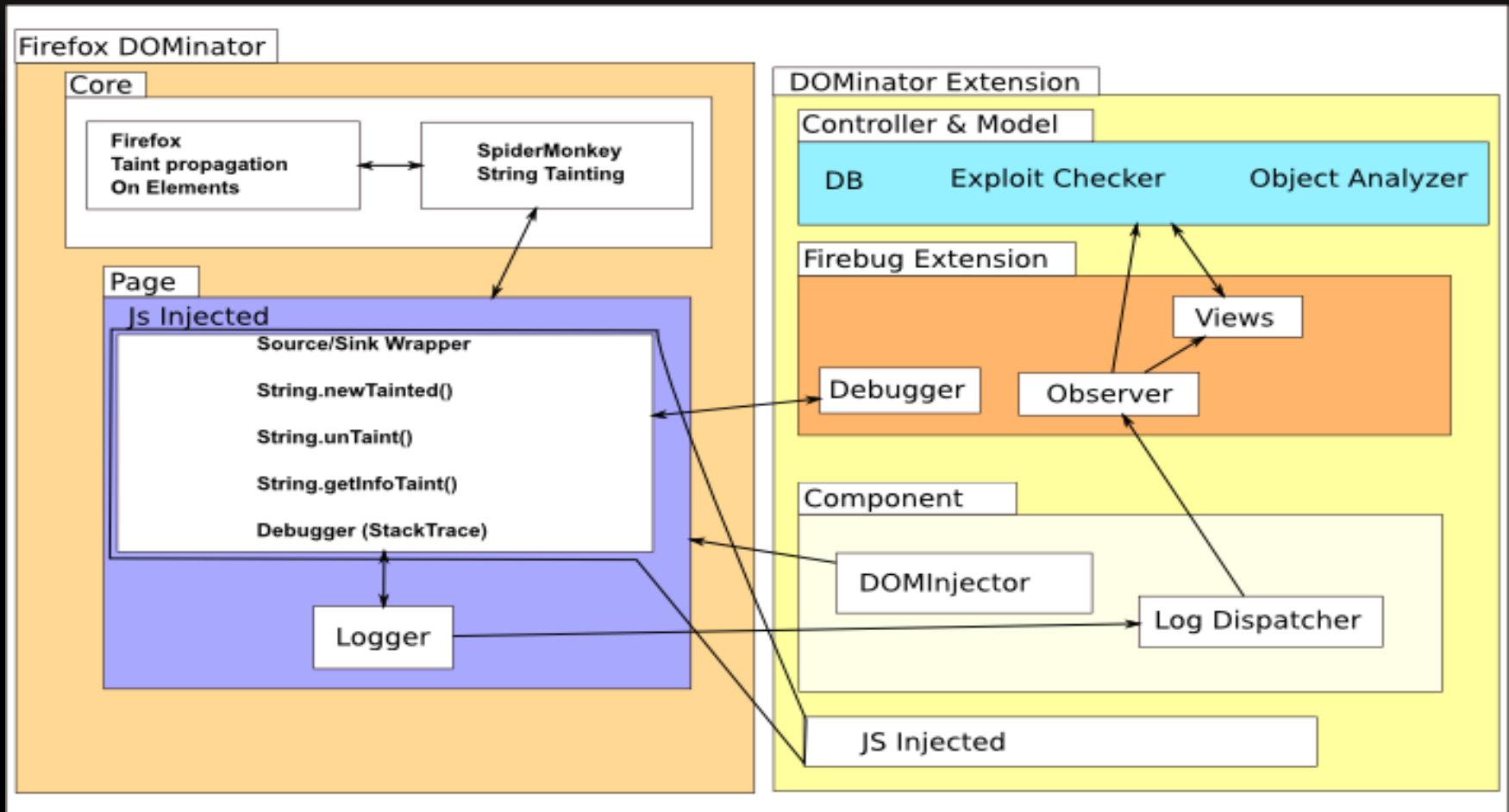
DOM XSS PAIEŠKA

- Tradicinė paieška analizuojant Javascript kodą yra gana sunki užduotis
- Neseniai išleistas runtime analizės įrankis - **DOMINATOR**

DOMINATOR

- Runtime analizės įrankis
- Modifikuota Firefox ir JS spidermonkey versija skirta sekti potencialiai pavojingų DOM vietų dinaminiam keitimui sekti

DOMINATOR STRUKTŪRA



DEMO



NUORODOS

- DOM XSS Wiki - <http://code.google.com/p/domxsswiki/>
- Dominator - <http://code.google.com/p/dominator/wiki/InstallationInstructions>
- http://dominator.googlecode.com/files/DOMinator_Control_Flow.pdf