Zraniteľnosti druhého rádu vo webových aplikáciách

AUTOR: OLEH SOVA

VEDÚCI PRÁCE: RNDR. JUDR. PAVOL SOKOL

KONZULTANT PRÁCE: MGR. TERÉZIA MEZEŠOVÁ

Motivácia práce

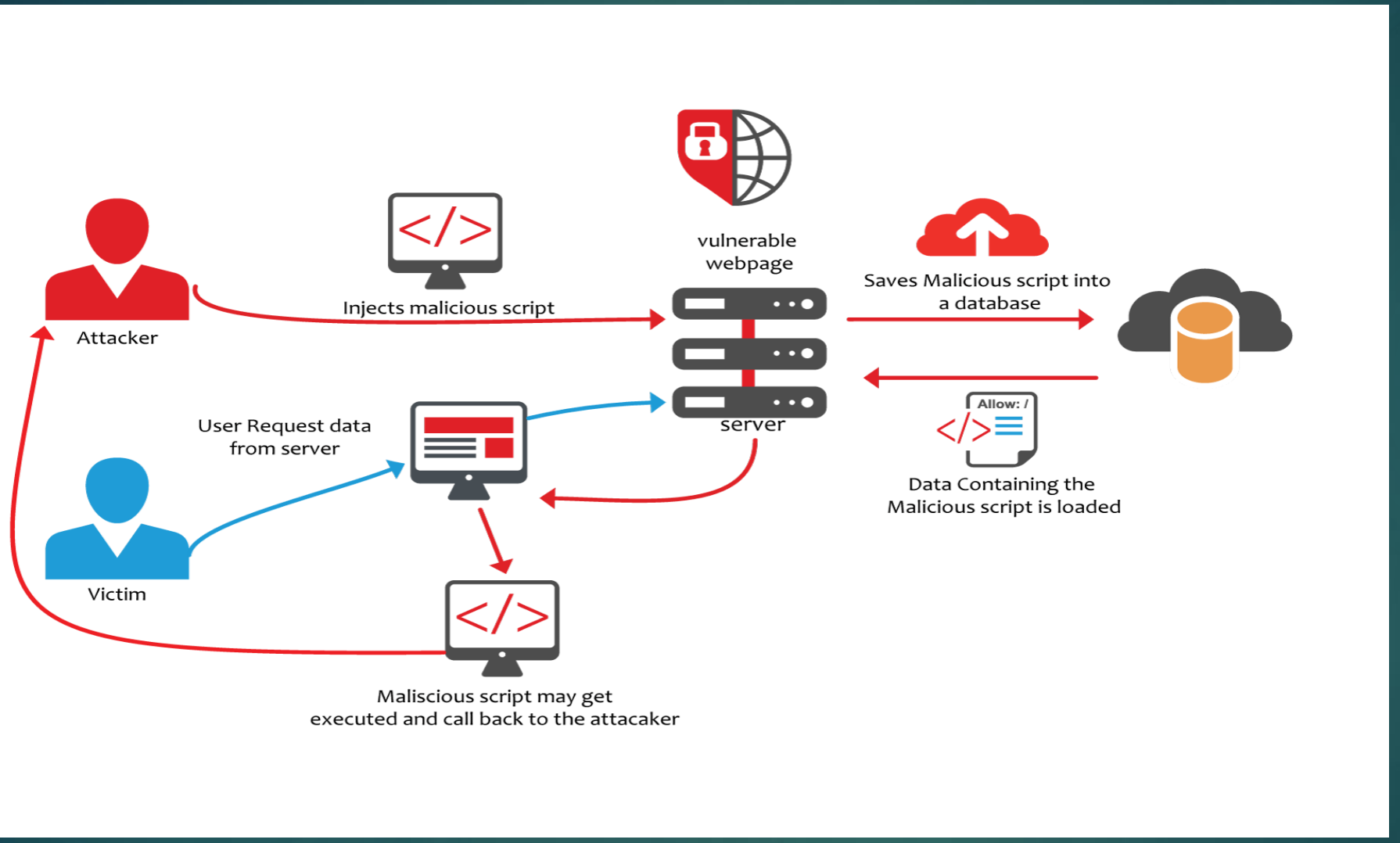
Webové aplikácie vytvorené v posledných rokoch (od jednostránkových až po multifunkčné aplikácie) získali veľkú popularitu v akejkoľvek sfére ľudskej činnosti. Táto rastúca popularita robí z webových aplikácií ciele pre mnohé typy útokov (napríklad: XSS, SQLi, DOS). Rastúci počet útokov vedie k vývoju výskumu v oblasti bezpečnosti webových aplikácií.

Takéto štúdie v zásade dokazujú pôvod zraniteľností v zdrojovom kóde a jeho štruktúre, a poukazujú na potrebu používať automatické nástroje na overovanie kódu, aby sa minimalizoval výskyt zraniteľností.

Zraniteľnosti druhého rádu vznikajú vtedy, keď aplikácia ukladá vstup do databázy bez overenia voči škodlivým príkazom a potom sa z databázy zobrazí používateľom stránky, alebo použije pri vnútornej operácií.

Jednou z takých zraniteľností je stored cross-site scripting (XSS). (ilustrácia zobrazené na ďalšom snímku)

Stored Cross-Site Scripting



Link pre obrázku

Stored Cross-Site Scripting

Útočník (hacker) nahrá škodlivý skript na aplikačný server, ktorý sa uloží do databázy (aplikácia ho považuje za štandardný vstup od užívateľa). Pri následných požiadavkách servera na databázu, databáza bude serveru vracať dáta obsahujúce tento škodlivý skript. Používateľ (obeť) tak pri kontakte s aplikáciou prijíma na svojom zariadení dáta, ktoré sú napadnuté alebo infikované škodlivým skriptom.

Potom útočník môže v závislosti od toho, na čo bol navrhnutý skript, získať kontrolu na dátami obete, alebo nad zariadením

Ciele práce

1. Analyzovať zraniteľnosti druhého rádu vo webových aplikáciách a možnosti ich detekcie.
2. Analyzovať a porovnať aktuálne prístupy k detekcii zraniteľností druhého rádu vo webových aplikáciách.
3. Návrh, implementácia a otestovanie nástroja pre testovanie zraniteľností druhého rádu pre webové aplikácie vytvorené v jazyku Javascript.

Postup práce

- analýza zraniteľností druhého rádu;
- vývoj automatizovaného systému na kontrolu štruktúry kódu, respektíve implementácia modulu pre existujúci systém na kontrolu zdrojových kódov v jazyku JavaScript;
- overiť účinnosť systému.

Literatúra

- 1) DAHSE, Johannes; HOLZ, Thorsten. Static Detection of Second-Order Vulnerabilities in Web Applications. In: USENIX Security Symposium. 2014. p. 989-1003.
- 2) OLIVO, Oswaldo; DILLIG, Isil; LIN, Calvin. Detecting and exploiting second order denial-of-service vulnerabilities in web applications. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015. p. 616-628.
- 3) MUELLER, John Paul. Security for Web Developers: Using JavaScript, HTML, and CSS. " O'Reilly Media, Inc.", 2015
- 4) BOULANGER, Jean-Louis (ed.). Static analysis of software: The abstract interpretation. John Wiley & Sons, 2013
- 5) SCHOLTE, T., ROBERTSON, W., BALZAROTTI, D., AND KIRDA, E. An Empirical Analysis of Input Validation Mechanisms in Web Applications and Languages. In ACM Symposium On Applied Computing (SAC) (2012).

Ďakujem za pozornosť!