DEPISTAREA VULNERABILITĂȚII BAZELOR DE DATE ALE APLICAȚIILOR WEB UTILIZÂND TEHNICA SQL-INJECTION

BULDUMAC Oleg

Universitatea Tehnică a Moldovei

Abstract: *Această lucrare descrie una dintre cele mai populare tehnici de depistare a vulnerabilităților a bazelor de date cu ajutorul unor instrucțiuni speciale SQL care din careva motive nu sunt filtrare de către serverul HTTP.*

Sunt metodele de atac precum și metodele de intrare în panoul de administrare. Având datele de intrare în panoul de administrare cu ușurință se dobândește și accesul la întregul server.

Cuvinte cheie: *SQL, SQL Injection, Union, PHP, CMS, HTTP, Web Soft*

1. Introducere

Internetul în ultimii ani se dezvoltă cu pași rapizi, unde tot mai multe persoane devin pasionate de tehnologiile informaționale.

Creând aplicațiile WEB în grabă, fără a atrage o minimă atenție la partea ce ține de securitate, tinerii "pasionați de IT" nu-și dau seama în ce pericol își pun aplicațiile când le încarcă pe vreun server la care are acces toată populația conectată la plasa marelui păianjen ce poartă numele de "Internet".

2. SQL-injectarea datelor personale

Datele personale, și totodată, confidențiale, mereu a fost și vor fi ținta principală pentru persoanele care se ocupă de spargerea ilegală a sistemelor informaționale și urmăresc ca scop furtul bazei de date.

La ziua de azi, orice aplicație practic nu poate exista fără o bază de date in care se salvează diverse tipuri de date, de care are nevoie însăși aplicația.

Aici și apare noțiunea de SQL-Injection, tehnica care manipulează într-un mod ascuns cu baza de date fără a avea careva drepturi de administrare.

Vorbind simplu, SQL-Injection este un tip de atac asupra bazei de date, care permite efectuarea unor acțiuni, de care nu s-a planificat de către dezvoltatorul softului.

3. Tipurile de atac SQL: manual și automat

Atacurile SQL-injection se pot efectua atât în mod manual, cit și în mod automat folosind așa tipuri de instrumente ca SQLMap. Aceasta devine posibil daca dezvoltatorul de program din neatenție nu a filtrat datele de intrare de la utilizatori.

Datele de intrare sunt acele date, care se transmit serverului prin metodele protocolului HTTP: GET și POST.

Cel mai des, vulnerabilitățile se găsesc în aplicațiile dezvoltate în limbajul de programare PHP.

4. Rolul CMS-urlilor și framework-urilor moderne

CMS-urile gigante ca WordPress, Joomla, Magento, Opencart reduc posibilitățile de atac de tip SQL-Injection la minimum, deoarece pentru conectarea și interogarea bazei de date dezvoltatorul de soft folosește funcții speciale ale CMS-ului utilizat și nu direct al limbajului PHP.

Dar totuși, în extensiile(bibliotecile) dezvoltate de către utilizatorii externi se întâlnesc vulnerabilități lăsate din neatenție sau cu vreun anumit scop, ca de exemplu, se lasă special un "backdoor".

5. Minimizarea și înlăturarea vulnerabilităților SQL

Pentru înlăturarea vulnerabilităților există funcții anumite care ecraneaza simbolurile speciale si wildcard-urile.

Dezvoltatorii profesioniști de soft sugerează să se atragă o atenție cit mai mare la partea programului dezvoltat unde se lucrează cu datele transmise de către utilizatori.

În nici un caz nu trebuie de să se considere că utilizatorii nu sunt din auditoriul experților domeniului IT și că scopul lor nu este de a împiedica funcționarea aplicației.

Recomandări împotriva atacurilor SQL:

- Folosiți cu încredere funcția mysql_real_escape_string;
- Mai puteți pune o funcție să verifice **metodele HTTP** (GET, POST, COOKIE) și să vă alerteze prin e-mail în caz că găsesc cuvinte de genul: "union select","order by","/**/" si multe altele legate de limbajul SQL;
- Nu afișați niciodată erorile când site-ul este atacat;
- Să nu aveți niciodată încredere în vizitatori.

6. Diagrama celor mai populare tehnici de atac a aplicațiilor WEB

În diagrama din figura 1 se arată în procente cele mai răspândite metode de atac a aplicațiilor WEB.

SQL-Injection este pe al doilea loc cu 17.5% ce demonstrează utilizarea eficientă a acestei tehnici de atac.

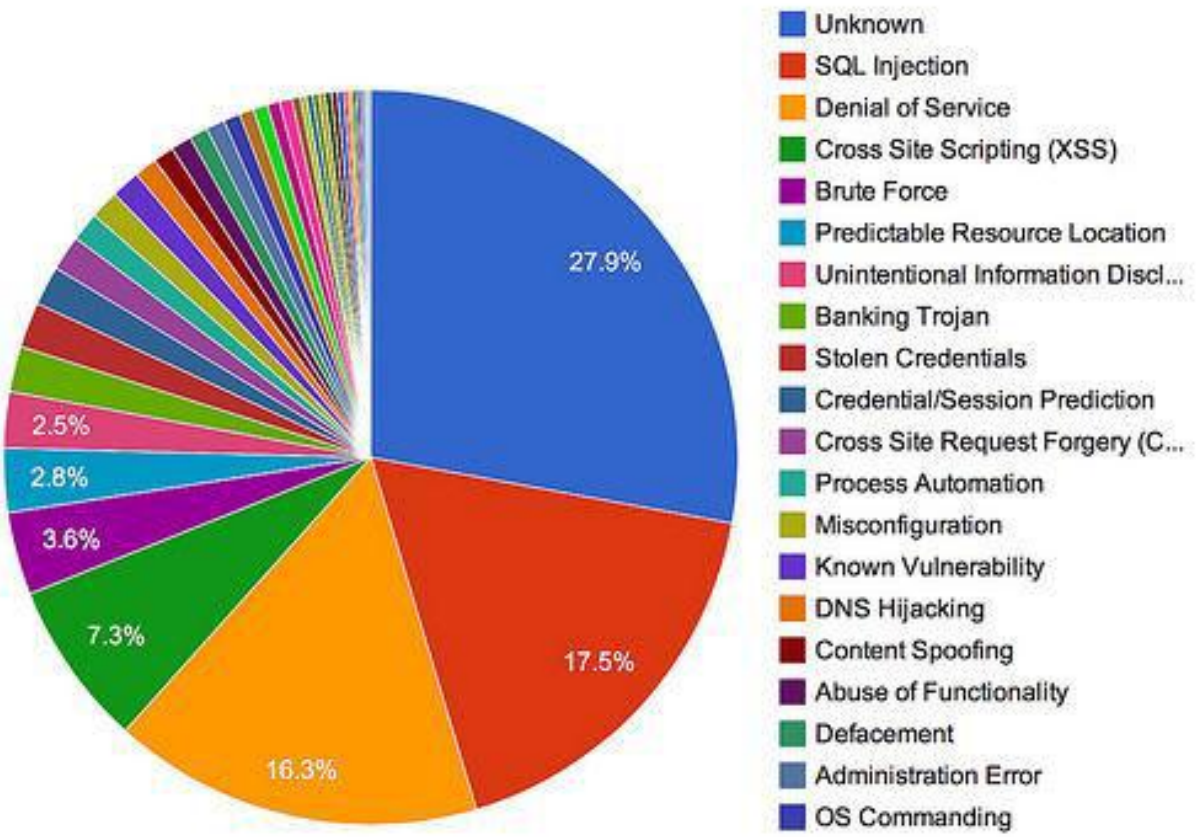

Fig.1. Diagrama celor mai des folosite instrumente de atac

Dar, totuși, presupunem că baza de date este vulnerabilă și atacul s-a efectuat cu succes. Datele deja cu siguranță au fost extrase și salvate pe calculatorul persoanei ce a efectuat atacul.

Din acest moment este nevoie de a apela organele competente și de a începe modificarea datelor bazei de date în așa fel, ca atacantul să nu aibă nici un acces ulterior.

Concluzii

Este evident că un atacator trebuie să posede cel puțin careva cunoștințe în privința arhitecturii bazei de date pentru a desfășura un atac cu succes. Obținerea acestei informații este deseori foarte simplă.

Spre exemplu, dacă o bază de date face parte dintr-un pachet software cu sursă deschisă (open-source), sau disponibilă publicului larg, cu o instalare implicită, această informație este absolut deschisă și disponibilă tuturor.

Această informație poate, de asemenea, să fie divulgată de un cod-sursă închis - chiar dacă este codificat, camuflat sau compilat - și chiar de propriul dumneavoastră cod prin afișarea mesajelor de eroare.

Alte metode includ utilizarea numelor răspândite pentru tabele și coloane. Spre exemplu, un formular de login care utilizează un tabel 'users' cu denumirile coloanelor 'id', 'username' și 'password'.

Securitatea și integritatea aplicației mereu trebuie să fie pusă pe primul plan de către dezvoltatorii de WEB-soft.

Bibliografie

1. Wikipedia. SQL Injection. [Interactiv] [Citat: 17.11.2016]. https://en.wikipedia.org/wiki/SQL_injection.
2. Veracode. SQL Injection Cheat Sheet and Tutorial. [Interactiv] [Citat: 17.11.2016]. https://www.veracode.com/security/sql-injection
3. W3schools. SQL Injection. [Interactiv] [Citat: 18.11.2016]. http://www.w3schools.com/sql/sql_injection.asp
4. Exploit-DB. Full SQL Injection Tutorial (MySQL). [Interactiv] [Citat: 18.11.2016]. https://www.exploit-db.com/papers/13045/
5. Acunetix. What is SQL Injection (SQLi) and How to Fix It. [Ineractiv] [Citat: 19.11.2016. http://www.acunetix.com/websitesecurity/sql-injection/
6. Netsparker. What is SQL Injection and How to Detect It. [Interactiv] [Citat: 19.11.2016]. https://www.netsparker.com/web-vulnerability-scanner/vulnerability-security-checks-index/sql-injection/
7. Owasp. The Open Web Application Security Project, [Interactiv] [Citat: 18.11.2016]. https://www.owasp.org/index.php/SQL_Injection