SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE
Fakulta informatiky a informačných technológií
Odbor: Počítačové inžinierstvo

Penetračné testovanie

Tímový projekt – posudok k implementácii konkurenčného tímu 22

Tím č. 17: Bc. Rami Al Beyrouti
Bc. Martin Blesák
Bc. Peter Daniš
Bc. Martin Močol
Bc. Peter Štuller

0. Úvod

Predkladaný dokument obsahuje posudok vypracovaný na náš konkurenčný tím (tím č. 22). Posudok sa zaoberá hlavne implementačnou časťou integračného prostredia. Vychádza z dokumentácie, ktorú odovzdal konkurenčný tím, a samotného produktu v podobe integračného nástroja, ktorého funkčnosť nám konkurenčný tím prezentoval.

1. Návrh integračného prostredia

V návrhu sa tím sústredil na splnenie požiadaviek kladených na integračné prostredie. Hlavne možnosť rozširovať množinu testov. Ich prvoradým cieľom bolo vytvoriť integračné prostredie a nie integrovať veľkú množinu testov.

Prostredie rozdelili na 5 základných častí: testovacie skripty, testovacie jadro, knižnica pre komunikáciu s jadrom, báza znalostí a užívateľské rozhranie. Modulárne rozdelenie prostredia hodnotíme veľmi pozitívne z funkčného (ľahké pridávanie funkčnosti, prípadne zmena funkčnosti niektorej časti) a z bezpečnostného hľadiska.

2. Implementácia integračného prostredia

V úvode dokumentácie k implementácii je stručne a prehľadne uvedené fungovanie systému, čo umožňuje utvorenie si globálneho pohľadu na systém ešte predtým, ako sa budú jednotlivé časti detailnejšie popisovať.

Kladne hodnotíme aj prehľadne spracovaný dátový model.

Výhrady máme k ďalším častiam dokumentácie k implementácii. Tieto by mali obsahovať hlavne popis jednotlivých častí, vysvetlenie princípu a funkčnosti. Autori sa však zamerali aj na uvádzanie zdrojových kódov rôznych častí (napríklad testov). Podľa nás je miesto pre zdrojové kódy na elektronickom médiu. V dokumentácii by mali byť len fragmenty zdrojového kódu, ktoré vysvetľujú jednotlivé použité princípy prípadne techniky.

Autori neuviedli konkrétne parametre, pri ktorých sa systém testoval. Hlavne verzie použitej databázy postgresql, webového servera apache a predovšetkým skriptovacieho jazyka PHP. Zároveň by mali byť uvedené aj verzie týchto programov (okrem testovaných), na ktorých je možné systém prevádzkovať.

Dokumentácia neobsahuje popis testovania systému.

Hlavný démon, ktorý vykonáva jednotlivé testy beží s právami administrátora. To je nutné pri vykonávaní niektorých testov, ktoré z bezpečnostného hľadiska nepovolia svoje spustenie bežnému užívateľovi operačného systému. Démon však nie je sieťovou službou. Komunikuje len s databázou a pomocou knižnice s testami. Preto démon nie je taký zraniteľný, čo je pozitívum pre bezpečnosť systému.

Démon takisto zabezpečuje automatické vykonanie testu, prípadne paralelné vykonávanie viacerých testov. Užívateľ môže skontrolovať neskôr výsledky testov, ktoré sú takisto archivované pre ďalšie analyzovanie.

Tím by mal uvážiť postup na pridávanie testov. V súčasnej podobe ide len o pridanie hotového testu (skriptu) do databázy. Nie je však určené s akým nástrojom bude test pracovať. Testy, ktoré vytvorili autori využívajú len nástroj nmap. Nie sú integrované žiadne iné testy.

Kladne hodnotíme prehľadné a užívateľsky príjemné rozhranie pre spúšťanie testov a prezeranie ich výsledkov.

Z ďalšej dokumentácie chýba systémová príručka k integračnému prostrediu, hlavne postup inštalácie a už spomínané nároky (verzie jednotlivých programov).

3. Zrhutie

V predchádzajúcej časti sme uviedli niekoľko nedostatkov práce. Treba však povedať, že systém predstavuje funkčné integračné prostredie pre penetračné testy a to bolo cieľom tohto projektu.

Celkovo hodnotíme prácu pozitívne, hlavne modulárny návrh, ktorý umožní jej ľahké rozširovanie v budúcnosti.