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

Penetračné testovanie

Tímový projekt

Tím č. 3: Bc. Rami Al Beyrouti
Bc. Martin Blesák
Bc. Peter Daniš
Bc. Martin Močol
Bc. Peter Štuller

OBSAH

0. Úvod

Cieľom tohto dokumentu je priblížiť a vysvetliť riešenie zadania Tímového projektu s názvom Penetračné testovanie. Výsledkom riešenia je web aplikácia, ktorá má za úlohu prezentovať základné a aj mierne pokročilé vedomostné informácie o Penetračnom testovaní. Druhou úlohou aplikácie je zastrešovať aj integračné prostredie, ktorým bude možné uskutočňovať vybraté penetračné testy.

Dokument je rozdelený na viacero kapitol, ktoré zodpovedajú jednotlivým činnostiam nasledujúcim po sebe pri vytváraní konečného riešenia zadania.

V analýze problematiky sa pozrieme na Penetračné testovanie ako také, na jeho použitie, a na jeho dostupnosť pre ľudí, ktorí by sa ním chceli zaoberať. Tiež sa pozrieme na zdroje našej tvorby, ktoré môžeme použiť pri implementácii.

V kapitole špecifikácia si podrobnejšie opíšeme požiadavky na funkcie systému, na údaje, ktoré budeme využívať a určíme si, ako by sa mala naša aplikácia správať.

Kapitola návrh riešenia ukazuje, akým smerom by sme sa chceli vydať pri implementácii riešenia nášho problému.

Konečný produkt nášho snaženia vychádza zo všetkých týchto fáz tvorenia, preto sa snažíme splniť ich čo najvernejšie a tomuto snaženiu čo najvernejšie prispôsobiť aj tento dokument.

1. Analýza problematiky

Najprv by bolo vhodné vysvetliť, čo vlastne penetračné testovanie ako termín znamená.

Penetračné testovanie – je termín z oblasti bezpečnosti počítačových a informačných systémov, ktorým označujeme činnosť, pri ktorej sa pokúšame nájsť slabiny vlastného systému, pričom ich hľadáme formou útoku na vlastný systém. Čiže sa tvárime, ako útočník na systém a prenikáme do neho (z latinčiny penetratio – prenikanie). Samotný útok sa väčšinou uskutočňuje sadou nástrojov, ktorým sa hovorí testy.

Bolo by ešte vhodné vysvetliť niekoľko pojmov, ktoré sa bezprostredne viažu na penetračné testovanie.

Pozrieme sa aj, aké existujúce implementačné prostredia by sme mohli využiť.

1.1. Metodiky

Metodiky sú súbory pravidiel, podľa ktorých sa testy vykonávajú. Všeobecne sa dá súbor testov rozdeliť na oblasti testovania, ktoré testujú niektorú časť informačného systému organizácie. Jednotlivé oblasti sa pritom môžu prekrývať a delia sa na moduly. Jeden modul spúšťa jednu testovaciu úlohu. Výsledky testovania sa zapíšu a porovnajú s úplnou bezpečnosťou, ktorú si definuje organizácia ako požiadavku.

1.2. Existujúce nástroje vykonávajúce penetračné testovanie

Jestvuje veľmi veľa nástrojov, ktorými sa dajú uskutočniť testy. Niektoré sú komerčné, niektoré voľne šíriteľné a niektoré sú tzv. open source (ich zdrojový kód je voľne šíriteľný). Keďže máme implementovať aj integračné prostredie na spúšťanie týchto nástrojov, uznali sme za vhodné použiť open source nástroje.

Na tému penetračného testovania existuje veľmi veľa materiálov, ale väčšinou sa jedná o zahmlené informácie firiem, ktoré ponúkajú produkty z tejto oblasti. Preto je výhodnejšie zamerať sa na informácie o voľne šíriteľných nástrojoch vykonávajúcich testy.

Najprístupnejšie sa javia nástroje Nessus, S.A.T.A.N. a niektoré ďalšie.

1.3. Existujúce web rozhrania

Prvou úlohou nášho zadania je vytvoriť webovú prezentáciu informácií o penetračnom testovaní. Tu nájde vzdelaný laik prípadne odborník prehľadne spracované informácie o penetračnom testovaní od základov cez všeobecnú metodológiu penetračného testovania až po popis nástrojov a systémov slúžiacich na penetračné testy.

Nakoľko sa bude jednať hlavne o informácie, je vhodné použiť už existujúci systém správy obsahu (CMS – Content Management System, ďalej v texte len cms systém) . V tomto prípade nám odpadá práca s navrhovaním webovskej stránky a môžeme sa sústrediť hlavne na informácie v nej obsiahnuté.

CMS systémov existuje veľké množstvo, nakoľko ho chceme použiť pri našom školskom projekte, výber obmedzíme na voľne šíriteľné riešenia. Tieto sú väčšinou založené na kombinácii webového servera Apache, jazyka PHP a databázy Mysql. Umožňuje to jednoduchú správu a prenositeľnosť medzi platformami.

1.3.1. Drupal

CMS systém s otvoreným zdrojovým kódom napísaný v jazyku PHP šírený pod licenciou GPL. Umožňuje užívateľom jednoducho publikovať, spravovať a organizovať rozmanitý obsah na webovskej stránke.
Hlavné výhody:

- Jeho funkčnosť možno rozširovať mnohými modulmi.
- Používa užívateľsky prívetivé URL adresy. Využíva na to modul *mod_rewrite* z webového servera Apache. Užívateľ si môže URL adresy prispôsobiť podľa svojich potrieb. Zároveň sú tieto adresy prívetivé aj k vyhľadávacím systémom.
- Oprávnenia sa nemusia priraďovať zvlášť každému používateľovi. Stačí mu priradiť rolu v systéme a následne určovať oprávnenia jednotlivých rolí.
- Na stránke sa dá jednoducho vyhľadávať, všetok obsah je indexovaný.
- Prístup do databázy sa uskutočňuje pomocou abstrahujúcej vrstvy, ktorá zabezpečuje databázovú nezávislosť. Stačí napísať pre túto vrstvu rozhranie na konkrétnu databázu a táto sa môže používať.
- Systém má podporu mnohých jazykov.
- Systém má vlastné logovacie záznamy o všetkých aktivitách na stránke. Udržiava si štatistiky prístupov na jednotlivé časti stránky.
- Pri veľkej záťaži poskytuje možnosť vyrovnávacej pamäte pre požiadavky na databázu.
- Umožňuje vkladať obsah ako text, html ale aj ako php kód.

1.3.2. PHP-Nuke

Automatizovaný systém pre vytváranie interaktívnej webovej stránky. Administrátor má úplnú kontrolu nad celou stránkou, zároveň má k dispozícii mnoho nástrojov na jej správu. Opäť ide o systém založený na PHP. Najviac testovaná platforma pre jeho spúšťanie je OS Linux, webový server Apache, databáza Mysql.
Hlavné výhody:

- Veľká miera flexibility, používateľ si systém ľahko upraví do podoby, ktorá mu najviac vyhovuje.
- Jazyková podpora – viac ako 20 jazykov.
- Rozšíriteľný pomocou mnohých zásuvných modulov (pluginov), kde veľa z nich je súčasťou základnej inštalácie.

1.3.3. Plone

CMS systém založený na aplikačnom servery Zope. Riešenie je s otvoreným zdrojovým kódom v jazyku Python.
Hlavné výhody:

- Jazyk Python zabezpečuje dobrú platformovú prenositeľnosť.
- Objektovo orientovaný aplikačný server Zope zabezpečuje robustnosť riešenia, databázovú nezávislosť. Nie je potrebný webový server.
- Jazyk Python umožňuje v prípade vlastného rozširovania tohto systému vysokú programátorskú produktivitu.
- Preložený do asi 50 jazykov.

1.4. Nároky používateľov

Cieľom nášho snaženia je vytvoriť web aplikáciu, ktorá bude zrozumiteľná, bude obsahovať len dôležité údaje, graficky bude príjemná, k informáciám sa používateľ ľahko dostane, integrácia spúšťania testov bude nenásilná. Takéto vlastnosti by uvítali používatelia aplikácie.

2. Špecifikácia

Na každý systém sa kladú určité požiadavky, nech už tým systémom je rozsiahla databáza, operačný systém alebo web aplikácia. Preto je potrebné presne špecifikovať požiadavky aj na našu aplikáciu.

2.1. Špecifikácia funkcií systému

Funkcie nášho systému sú dané požiadavkami človeka, ktorý ho bude používať. Ten by chcel, aby bol systém (v našom prípade web aplikácia) jednoduchý na ovládanie, poskytoval mu čo najviac ľahko prístupných a dôležitých informácií podaných v uhladenej forme, a dovolil mu spustiť niektoré testy.

Zo znenia nášho zadania vyplýva, že aplikácia musí mať dve hlavné funkcie. Sú to tieto dve:

- Prezentovanie informácií o penetračnom testovaní
- Spúšťanie penetračných testov v integrovanom prostredí

Prezentačná časť bude teda obsahovať funkcie zobrazovania informácií, ich zoradenia do kapitol, vyhľadávania, otestovania znalostí v danej problematike a bude obsahovať odkazy na obsiahlejšie informácie o niektorých podoblastiach, na ktoré používateľ narazí. Celá prezentačná časť musí mať príjemné používateľské rozhranie a aj nevtieravú a harmonickú grafickú podobu.

Potrebujeme jednoduchým a prehľadným spôsobom uverejniť na stránke spísané informácie o penetračnom testovaní. Vytvoriť menu, ktoré bude umožňovať štruktúrovaný prístup k týmto informáciám. Uverejňovať na stránke text alebo html prezentáciu spolu s obrázkami a animáciami.

Integračná časť umožní spúšťanie vybratých nástrojov priamo z web aplikácie, pričom by nemala byť narušená logická, sémantická ani grafická nadväznosť na prezentačné prostredie.

2.2. Špecifikácia údajov v systéme

Údaje v systéme sú v našom prípade informácie o penetračnom testovaní. Získavame ich štúdiom materiálov, ktoré by mali byť uvedené aj v aplikácii, ak by používateľ chcel zistiť o problematike niečo viac. Údaje by mali byť do systému ľahko vkladateľné, keďže predpokladáme v tejto oblasti informačných technológií ďalší rozvoj. Oprava údajov by mala byť tiež zabezpečená, ako aj ich prípadné rušenie.

2.3. Správanie sa systému

Systém by sa mal správať ako všeobecná webová aplikácia, ktorej zameranie je poskytovať používateľovi informácie, ktoré si môže pomocou integrovaného rozhrania na spúšťanie testov aj v praxi overiť. Mal by byť teda stabilný s rýchlou odozvou, obsahujúci množstvo údajov, ktoré sú rýchlo dostupné. Podľa toho je dôležité správne si zvoliť implementačné prostredie.

3. Návrh riešenia

V tejto kapitole je rozpísaný náš návrh, ako budeme implementovať jednotlivé časti aplikácie, a ako chceme, aby výsledok nášho snaženia vyzeral. Keďže máme na starosti dva typy úloh, a to prezentačné a integračné prostredie, ich návrhy sa budú líšiť, aj keď navonok by mali pôsobiť ako jednoliaty celok.

3.1. Návrh prezentačného prostredia

Ako prvé je dobré navrhnúť prezentačné prostredie, keďže obsahuje informácie aj o integračnom prostredí. Pri jeho návrhu musíme vychádzať z už spomínaných požiadaviek. Systém je navrhovaný ako web aplikácia, keďže to udáva zadanie.

Ako prvé si musíme zvoliť implementačné prostredie, navrhnúť scenár alebo štruktúru web aplikácie, a nakoniec aj jej výzor a rozhranie s používateľom.

3.1.1. Návrh implementačného prostredia

V časti analýzy sme uviedli 3 CMS systémy, z ktorých musíme vybrať jeden najviac spĺňajúci naše požiadavky. Tieto boli stanovené v časti špecifikácie.

Každý zo systémov do istej miery spĺňa naše požiadavky, a keby sme sa nemohli slobodne rozhodnúť, hociktorý zo systémov by bol vyhovujúci. Rozhodli sme sa ale uprednostniť systém *Drupal*. Zvyšné 2 systémy sú totiž na naše použitie príliš robustné a zbytočne komplexné. Naproti nim Drupal poskytuje potrebnú funkčnosť pri zachovaní jednoduchého a intuitívneho ovládania. Zároveň je možné vyjsť z jeho hodnotenia podľa [4], kde jednoznačne dominuje spomedzi ostatných CMS systémov s otvoreným zdrojovým kódom.

3.1.2. Návrh kapitol

Rozvrhnutie stránok vo web aplikácii by sa dalo realizovať prostredníctvom kapitol. Jedna kapitola reprezentuje jednu stránku, ktorá sa objaví v prehliadači. Všetky údaje by sa dali čítať sekvenčne, alebo by sa v nich dalo pohybovať pomocou nadpisov kapitol.

Návrh kapitol vyzerá takto:

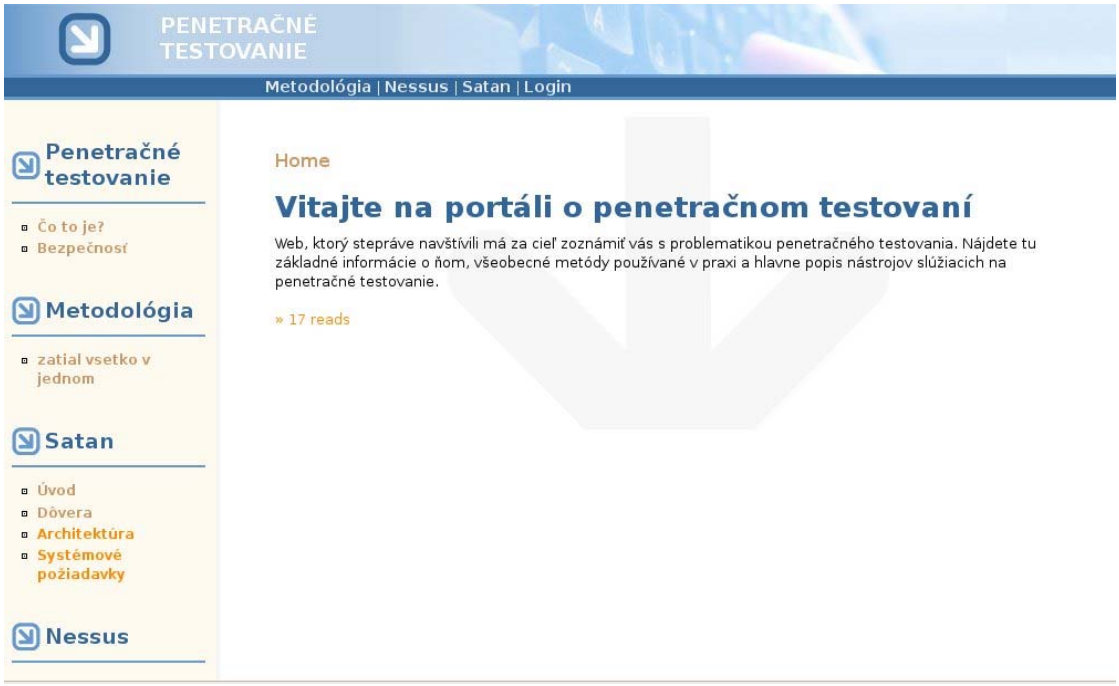
- 1.kapitola : Úvod
- 2.kapitola: Metodológie testovania
- 3. kapitola: Niektoré používané nástroje
  - 3.1.: Nessus
  - 3.2.: S.A.T.A.N.
  - 3.3.: Ďalšie nástroje
- 4. kapitola: Integrované prostredie
- 5. kapitola: Test znalostí
- 6. kapitola: Zaujímavé odkazy
- 7. kapitola: O autoroch

Každá kapitola bude naplnená údajmi v podobe článkov, integračného prostredia, testu, a odkazov. Na konci kapitoly bude možnosť plynulého prechodu na ďalšiu kapitolu.

3.1.3. Návrh rozhrania

Rozhranie webovskej prezentácie je do istej miery dané vybratým CMS systémom. Tento je možné samozrejme prispôsobovať podľa potreby. Používateľ bude mať k dispozícii prehľadne štruktúrované menu, kde každá jeho časť sa bude týkať jednej kapitoly. Návrh menu možno vidieť na obrázku č. 1.

V hornej časti vidíme linky pre rýchly prístup k jednotlivým témam, linka smeruje vždy na prvú stránku s danou témou (úvod). Na ľavej strane sa nachádza menu pre každú tému. Jednotlivé body sú zoradené podľa odporúčaného poradia čítania, každý bod môže byť štruktúrovaný do ďalších podbodov.



Obr. č. 1: Návrh rozhrania webovskej prezentácie

3.2. Návrh integračného prostredia

Integračné prostredie má za úlohu spúšťať vybrané testy a nemalo by sa vymykať designu prezentačného prostredia.

Bližšia analýza, návrh a implementácia integračného prostredia budú nasledovať v letnom semestri.

4. Literatúra

[1] - Informácie o systéme Drupal
http://drupal.org/about
http://drupal.org/node/22963
http://drupal.org/features
(posledný prístup 17.11.2005)

[2] - Informácie o systéme PHP-Nuke
http://www.phpnuke.org/modules.php?name=FAQ&myfaq=yes&id_cat=1&categories=
(posledný prístup 17.11.2005)

[3] - Informácie o systéme Plone
http://plone.org/about/plone/
(posledný prístup 17.11.2005)

[4] - Prehľad a hodnotenie CMS systémov s otvoreným kódom
http://www.opensourcecms.com/index.php?option=content&task=view&id=388&Itemid=143
(posledný prístup 17.11.2005)