Posudek oponenta diplomové práce

Autor/autorka práce: **Jan Froněk**

Název práce: **Security in EEG/ERP Portal**

Cílem práce je identifikovat slabá místa stávajícího EEG/ERP portálu a navrhnout a implementovat opatření, která by posílila ochranu aktuálního systému.

Autor nejdříve seznamuje čtenáře s EEG/ERP portálem. Dále je provedena analýza existujících bezpečnostních rizik se zaměřením na možnosti zabezpečení webových aplikací. Dále autor prostudoval stávající bezpečnostní řešení EEG/ERP portálu, identifikoval jeho slabá místa a realizoval vhodné bezpečnostní řešení.

Kvalita řešení a dosažených výsledků

Bezpečnostní rizika spolu s návodem, jak daný problém řešit jsou popsána celkem vyčerpávajícím způsobem. Dále je dobře popsáno zabezpečení EEG/ERP portálu. Volba navrhovaných bezpečnostních opatření je dostatečně zdůvodněna. Realizovaná opatření jsou pro portál vhodná.

Drobné připomínky:

- V sekci 3.3 uvádíte pravidla pro bezpečnou autentizaci. Chybí zde základní požadavek na heslo, což je jeho minimální délka. Doporučil bych doplnit toto omezení do aktuálního systému.
- V sekci 4.3 je uvedeno, že jsou hesla ukládána v podobě otisku (angl. hash). Není ale již uvedeno, jaká hašovací funkce je použita a zda se tato funkce považuje za bezpečnou.
- Vzhledem k tomu, že portál běží ve sdíleném prostředí, kde může kdykoli významně narůst zátěž, výkonnostní testy v sekci 5.5.5 nejsou příliš relevantní.

Formální úroveň

Průvodní dokument (65 stran + přílohy) je v angličtině a je vytvořen v systému LaTeX, což řadím mezi klady předkládané práce. Práce má logickou přehlednou strukturu a je snadné práci číst. Dokument je na slušné jazykové úrovni. Kladně hodnotím vytvořený přehled zkratek, který čtenáři usnadní orientaci v práci samotné. Bylo by ještě vhodné doplnit přehled tabulek a obrázků. Mám následující připomínku formálního charakteru: doporučil bych zestručnění některých částí práce, např. sekce 3.5.1, sekce 3.7 - obsahuje pouhý jeden odstavec relevantních informací k dané problematice, informace v prvním odst. sekce 5.5 byly již uvedeny dříve, atd.

Práce s literaturou

Použitá literatura (celkem 26 publikací) je nad rámec běžné diplomové práce. Pasáže, kde student čerpal z literatury, jsou jasně vyznačeny odkazem.

Splnění zadání

Zadání bylo splněno ve všech bodech. Autor nad rámec zadání realizoval zabezpečený elektronický obchod.

Dotazy:

1. V práci chybí popis jednoho základního bezpečnostního rizika a to přetečení bufferu na zásobníku. Vysvětlete tento bezpečnostní problém a zdůvodněte, proč toto riziko v práci neuvažujete.
2. Dále by bylo vhodné portál otestovat pomocí penetračních testů. Toto ale v práci provedeno nebylo, z jakého důvodu?
3. Z jakého důvodu jste se rozhodl implementovat el. obchod?

Navrhuji hodnocení známkou **výborně** a práci doporučuji k obhajobě.

V Plzni 4.6.2013

SOUHLASÍ S ORIGINÁLEM

Západočeská univerzita v Plzni
Fakulta aplikovaných věd
Katedra informatiky a výpočetní techniky

Ing. Pavel Král, Ph.D.