Bachelor's thesis errata

Topic: Security of small business e-commerce sites
Author: Karel Kohout
Supervisor: Ing. Jaromír Veber
Academic Year: 2009/2010

Note: only errors affecting readability or comprehensibility of the text have been corrected; minor typographical errors were ignored.

Format:

Location

– Corrected text –

– Wrong text –

1 Acronyms

page xiii

SQL Structured Query Language

SQL Structured Query Language.e

2 Thesis

page 4, footnote 7

It might be tempting to call the e-commerce application "the front end" and the rest (ERP, CRM) "the back end". However, such separation is not clear either.

It might be tempting to call the e-commerce application "the front end and the rest (ERP, CRM) "the back end. However, such separation is not clear either.

page 5, footnote 10

Example (but not in the SMB sector): iTunes.

Example (but in SMB sector): iTunes.

page 13

First, a basic legal framework, based on European Union's legislation ("acquis communautaire") with focus on private data protection ...

First, a basic legal framework, based on European Union's legislation ("acquis communautaire") with on focus on private data protection ...

page 16, Figure 2.3

Notice An organization must inform individuals about the purpose of collection and use of the data. It must also supply a contact information for further inquiries.

Notice An organization must inform individuals about the purpose of collection of data, use of the data. It must also supply a contact information for further inquiries.

page 21

Another view of assets is presented in ...

Another view at assets is presented in ...

page 24, subsection User authentication and accounts

After successful authentication, the user is handed a session token ...

After successful authentication, the user is handled a session token ...

page 42

... and April and results were checked at the end of April for any changes (in case of a new release, the source code was compared via *diff* utility).

... and April and results were checked at the end of April for any changes (in case of a release a new version release, the source code was compared via *diff* utility).

page 51

... but only as a few files and a regular announcement on the page (as of April, hidden bellow several other announcements) ...

... but only as a few files and an regular announcement on the page (as of April, hidden bellow several other announcements) ...

page 54

Granular permissions are non-existent – a plugin is available, but only compatible with Zen Cart up to 1.3.8.

Granular permissions are non-existent – a plugin is is available, but only compatible with Zen Cart up to 1.3.8.

page 54

However, for correct password, no delay is present, so an attacker can still guess passwords faster by considering a certain delay as an unsuccessful attempt.

However, for correct password, no delay is present, so an attacker can guess passwords by considering a certain delay as unsuccessful attempt.

page 63

E-commerce site owners are at risk of storing potentially sensitive data, ...

E-commerce site owners are in risk of storing potentially sensitive data, ...

page 66

... closed-source applications or reliability and temporariness of disclosed "security leaks").

... closed-source appliacations or reliability and temporariness of disclosed "security leaks").

3 Bibliography

[6]

Refer to [34] (duplicate).

DAFYDD STUTTARD, M. P. The Web Application Hacker's Handbook: Dis- covering and Exploiting Security Flaws. Indianapolis, US: Wiley Publishing, Inc., 2008. ISBN 978-0-470-17077-9.

[10]

EUROPEAN PARLIAMENT, C. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [on- line], January 2002. URL: `http://eur-lex.europa.eu/`

LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML, last retrieved February 21, 2010.

EUROPEAN PARLIAMENT, C. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [on- line] [online], January 2002. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML, last retrieved February 21, 2010.

[22]

KISSEL, R. Small Business Information Security: The Fundamentals (draft), NISTIR 7621 [online], October 2009. URL: http://csrc.nist.gov/publications/drafts/ir-7621/draft-nistir-7621.pdf, last retrieved June 6, 2010.

KISSEL, R. Small Business Information Security: The Fundamentals (draft) [online], October 2009.

[27]

PARLIAMENT OF THE CZECH REPUBLIC. Act 101 of April 4, 2000 on the Protection of Personal Data and on Amendment to Some Acts ("Personal Data Protec- tion Act" [online], April 2000. URL: http://ec.europa.eu/justice_home/fsj/privacy/docs/implementation/czech_republic_act_101_en.pdf, last retrieved June 5, 2010.

CZECH REPUBLIC, PARLIAMENT. Act 101 of April 4, 2000 on the Protection of Personal Data and on Amendment to Some Acts ("Personal Data Protec- tion Act" [online], April 2000. URL: http://ec.europa.eu/justice_home/fsj/privacy/docs/implementation/czech_republic_act_101_en.pdf, last retrieved June 5, 2010.