V. Savchenko and O. Mnushka

Modern Secure Programming Technologies. Workshops

Ministry of Education and Science of Ukraine
National Technical University
“Kharkiv Polytechnic Institute”

Volodymyr Savchenko and Oksana Mnushka

Modern Secure Programming Technologies. Workshops

Educational and methodological guide
for university students specializing in
123 “Computer Engineering”.

Approved by
the Editorial and Publishing
Council of NTU“KhPI”,
prot. No. 2 of 27.06.2024, pos. 88.

Kharkiv
2024

UDC 004.42/.49:004.056
C11

Reviewers: *V. D. Kovalov*, Doctor of Technical Sciences, Professor, Rector of Donbas State Engineering Academy, Laureate of the State Prize of Ukraine in Science and Technology.

O. *I. Fediushyn*, Candidate of Technical Sciences, Associate Professor, Associate Professor at the Department of Information Technology Security at Kharkiv National University of Radio Electronics.

Розглянуто сучасні технології безпечного програмування, роботу з базами даних загальновідомих вразливостей програмного забезпечення, а також методи підвищення захищеності програм в умовах кіберзагроз. Містить необхідний теоретичний мінімум і завдання для індивідуальної роботи (англійською мовою).

Іл. 24. Табл. 22. Алг. 11. Ліст. 7. Бібліог. 158 назв.

Savchenko V.

C11 **Modern Secure Programming Technologies. Workshops :** Educ.-method. guide / V. Savchenko, O. Mnushka. – Kharkiv: FOP Brovin O. V., 2024. – 136 p. – In English.

ISBN 978-617-8238-76-6

The guide covers modern secure programming technologies, working with databases of known software vulnerabilities, and methods for enhancing software security in the face of cyber threats. It includes essential theoretical knowledge and exercises for independent practice.

Educational and methodological guide for university students specializing in 123 "Computer Engineering".

Fig.: 24. Tabl.: 22. Alg.: 11. List.: 7. Bibl.: 158 titles.

ISBN 978-617-8238-76-6

Table of Contents

Introduction **7**

1 *OWASP Top 10* **9**

1.1 General Theoretical Information..... 10

1.1.1 Tools..... 14

1.1.2 Methodologies and Standards..... 17

1.2 Individual Tasks..... 18

1.2.1 Example Report Template..... 18

1.3 Review Questions..... 19

References..... 19

2 **Online *CVE* Databases** **23**

2.1 General Theoretical Information..... 23

2.2 Individual Tasks..... 30

2.2.1 Example of Data Analysis..... 31

2.3 Review Questions..... 36

References..... 36

3 Phishing. Research on Phishing *URL* Databases **39**

3.1 General Theoretical Information..... 39

3.2 Individual Tasks..... 45

3.2.1 General Task..... 47

3.2.2 Individual Task 47

3.3 Review Questions..... 49

References..... 50

4 Malware Signature Identification **53**

4.1 General Theoretical Information..... 53

4.2 *YARA* Utility..... 56

4.2.1 Installing the *YARA* Utility..... 57

4.2.2 Configuring *YARA* Dependencies..... 57

4.2.3 Installing *YARA* from Source Code 58
4.2.4 Syntax and Basic Rules of *YARA* 60
4.3 Individual Tasks 69
4.3.1 *YARA* Rules with *HEX* Strings 69
4.3.2 Searching for the *"Hello, World!"* Signature 69
4.3.3 Searching for the *EICAR* Signature 70
4.4 Review Questions 71
References 72
5 Basics of Hashing **75**
5.1 General Theoretical Information 75
5.2 Simple Hashing Methods 79
5.2.1 Character Code Sum 79
5.2.2 *XOR* Hashing 80
5.2.3 Polynomial Hashing 82
5.3 Hash Tables 83
5.3.1 Non-Cryptographic Hashing in Hash Tables 84
5.3.2 Importance of Choosing a Quality Hash Function 85
5.3.3 Visualization of Key-to-Index Mapping **86**
5.4 Individual Tasks 87
5.4.1 Analysis of Hashing Algorithms 87
5.4.2 Implementation of a Standard Algorithm 88
5.5 Review Questions 88
References 89
6 One-Way Hashing in Cryptography **91**
6.1 General Theoretical Information 91
6.2 Collision Resistance and Use of Hash Functions 92
6.2.1 The *MD5* Algorithm 94
6.2.2 Steps of the *MD5* Algorithm 94
6.2.3 One-Way Hashing and Quantum Computers 98
6.3 Hash Calculation Algorithms in *OpenSSL* 99
6.4 Individual Tasks 102
6.4.1 Analysis of Hash Calculation Algorithms in *OpenSSL* 102
6.4.2 Implementation and Testing of a Message Digest Algorithm 102

6.5 Review Questions..... 103
References..... 103
7 Error Correction Codes 105
7.1 General Theoretical Information..... 105
7.1.1 Encoding Methods for Ensuring Data Integrity..... 107
7.1.2 Variant 1. Reed-Solomon Code..... 108
7.1.3 Variant 2. Cyclic Redundancy Check *(CRC)*..... 110
7.1.4 Option 3: Hamming Code (7,4)..... 111
7.2 Developing a Program for the Hamming (7,4) Error Correction Code 111
7.2.1 Libraries for Calculating *CRC16/32*, Hamming Code (7,4), and Reed-Solomon Code..... 114
7.3 Review Questions..... 116
References..... 117
8 Ensuring Data Integrity and Authenticity 119
8.1 General Theoretical Information..... 119
8.1.1 Fundamentals of *HMAC* and *DSA*..... 121
8.1.2 *HMAC*..... 122
8.1.3 Digital Signature Algorithm *(DSA)*..... 124
8.2 Qualified Electronic Signature..... 126
8.3 Central Certification Authority of Ukraine..... 128
8.4 Individual Tasks..... 129
8.4.1 Exploring *HMAC*..... 129
8.4.2 Exploring *DSA*..... 130
8.4.3 Document Signing Services..... 132
8.5 Review Questions..... 132
References..... 133