Detection of the Security Vulnerabilities in Web Applications

Marius POPA
Economic Informatics Department,
Academy of Economic Studies, Bucharest, Romania
marius.popa@ase.ro

The contemporary organizations develop business processes in a very complex environment. The IT&C technologies are used by organizations to improve their competitive advantages. But, the IT&C technologies are not perfect. They are developed in an iterative process and their quality is the result of the lifecycle activities. The audit and evaluation processes are required by the increased complexity of the business processes supported by IT&C technologies. In order to organize and develop a high-quality audit process, the evaluation team must analyze the risks, threats and vulnerabilities of the information system. The paper highlights the security vulnerabilities in web applications and the processes of their detection. The web applications are used as IT&C tools to support the distributed information processes. They are a major component of the distributed information systems. The audit and evaluation processes are carried out in accordance with the international standards developed for information system security assurance.
Keywords: *security, vulnerability, web application, audit.*

1 Information Systems

A *system* represents a set of dependent elements forming a single unitary entity. A particular type of system is the *economic* one which defines economic components and mechanisms such as a company, an industry, a field of the national economy and so on. Even the national and worldwide economies can be seen at a global economic level as being complex economic systems [16].

An economic system receives an *input* of production factors. This input is processed and an *output* is provided in the shape of products and services provided to the market. The accurate transformation of the *input* into *output* is made by a *feedback loop*, figure 1.

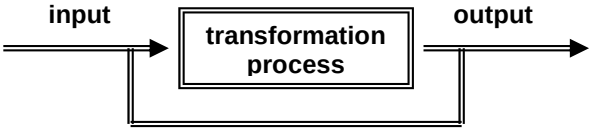

Fig. 1. Economic System

The transformation process takes place into a dynamic way that makes the system to progress according with to a specific route. The state of the system describes the system degree of evolution.

A system can be defined by the following elements:

- inputs;
- outputs;
- transformation process;
- system structure and its state.

A complex economic system is made by the following components, figure 2:

- decision system;
- operating system;
- information system.

The *decision system* is composed by specialists that are using specific methods and techniques to plan, forecast, decide, organize, coordinate and control the operating system functioning in order to successfully achieve its goals.

The *operating system* represents the technical and functional mechanisms together with the human, material and financial resources used to achieve the objectives determined by the decisions transmitted from the decision system level.

In [4] many definitions of the informational system and the informatics system are presented:
- *informational system* represents the dynamic side of the managerial system, making the link between the leading system and the leaded system inside the firm, and also between the firm and the business environment; the information system allows comprehension of the past and present situation of the organization, and the forecasts of its evolution, contributing at the objectives elaboration and fulfill; throughout the system, it is obtained the necessary information for conceiving and implementation of the decision, and also the one necessary for the company system to adapt to the internal and external changes;
- *the informational system* represents an ordered aggregate of information related to the activity, to the resources utilization and to the performances of organization, allowing optimization of the business administration;
- *the economics informational system* is an aggregate technical-organizational to conceive and obtain the necessary information for decision fundament in the economic activities management;
- *the informatics system* is part of the informational system that utilize automatic methods and means for data collecting, transmission, storage and processing, also for information capitalization in the organization management process;
- *the informatics system* is any combination of work practices, information, people and information technology, organized in order to fulfill the organization purpose;
- *the informatics system* is an application of the information and communication technology which responds to a defined need;
- *the informatics system* is a system that utilize formalized procedures in order to provide the right information to all the management levels and to all the function levels, the information is based on internal and external sources in order to allow the decisions for planning, leadership and activity control, to be taken quick and effective;
- *the informatics system* includes people, computer, application and interaction between them, within an environment which includes the working space, physical, social and the organizational medium;
- *the informatics system* is an aggregate of automatic means for information collection, production, storage, transmission and dissemination.

The *information system* resides in all the informational flows and circuits and all the methods, techniques used to process the data needed by the decision system. The information system is the middle layer between the decision and information systems and the communication between these layers is made in all possible directions. Thus, the information system is processing and transmitting data from the decision to the operating system. Also, it records, processes and transmits the information from the operating system to the decision one.

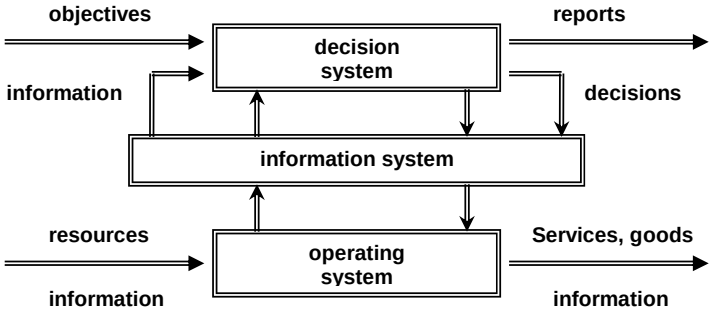

Fig. 2. The components of an economic system

We can conclude that the information system manages all the information existing at economic system level by using specific methods and techniques.

The *information technology system* is a component of the information system that is in charge with collecting, processing, transmitting, storing and presenting the data by using computing systems. In other words, it is responsible for automatic processing of the data by using various methods and techniques.
The resources involved by an information technology system can be divided into the following groups:
- the activity that is subject of the system and the primary data from inside;
- the methods and techniques used to develop the IT system;
- the hardware that is implicated in collecting, processing, transmitting, storing and presenting the final results;
- the software applications are responsible for the efficient use of the hardware resources by finding the solutions for the specific problems;
- the human resources are very important for the health of the system.
The automatic data processing covers the collecting, transmitting, processing and storing operations:
- *collecting data* – takes place at the location where the primary data are generated. All the collected elements are stored in a proper manner to be used to automatic processing;
- *processing data* – the primary data are transformed into final results by following a predefined sequence of operations adapted to the user requirements, hardware specifications and processing technique.
- *transmitting data* – from the primary locations to the automatic processing systems. Also, it is responsible for delivering the final results to the consumers;
- *storing data* – is responsible for data archiving on specific medium in order to be possible to access and process the content in the future.
In our days, the computer networks are extensively used as hardware support and the database management systems are widely exploited as the software component of the IT system. The rapid growth of the Internet made possible the use of the distributed database systems to manage the resources inside large organizations.
The information systems are complex structures and they suppose the development of the following activities in order to accomplish them [7]:
- allocation of important financial resources;
- complex and stable team building formed by analysts, designers, code programmers and personnel;
- objective establishment;
- definition of a strategy for development, exploitation and maintenance;
- acquisition of equipments, tools necessary for processing, connections and external flow development;
- human resource training for a correct and efficient system use.
An information system is a system, automated or manual, that comprises people, machines, and/or methods organized to collect, process, transmit, and disseminate data that represent user information [19].
Other statement defines the information system as any telecommunications and computer related equipment, interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware [2].
In computer security, an information system is described by the following objects:
- repositories, which hold data permanent or temporarily;
- interfaces, which exchange information with the non-digital world;
- channels, which connect repositories;
- services, which provide value;
- messages, which carries a meaning.
The repositories, interfaces and channels represent the structure, and the services and messages represent the behavior of the information systems.
In [7], the information system is defined as a set of hardware and software components interconnected in networks, the organizational and administrative framework in which these components are working. The interconnection of these components is made on two le-

vels:
- the physical one – it supposes the connection through different devices of the equipments in order to build the system;
- the functional one – it is made on the software level as to assure the system functionality through software modules collaboration.

The objective for the development and implementation of an information system is to process, to transfer and to store the information.

An information system includes hardware, software, information, data, applications, communications, and people. The security assurance of the information system assumes the development of engineering activities for information system security as follows:
- discovering the information protection needs;
- definition the system security requirements;
- design system security architecture;
- development the detailed security design;
- applying the system security;
- assessment the information protection effectiveness.

A special kind of information system is Enterprise Resource Planning – ERP. An ERP is a back office system that uses various software and hardware computer components in order to integrate in a single unified system all processes and data of a company. Due to these facts, an ERP system provides benefits in terms of standardization and lower maintenance costs and it does not need at all external interfaces between components, [15].

All the components of an ERP system are using a single database used to store data and run queries for all the applications. In our days, the monolithic ERP systems from the beginning become oriented on components using different architectures.

In software engineering, the web application is a software application that is accessed through a web browser application over a computer network such as Internet or Intranet. The web application is coded in a language understood by the web browser application such as HTML, Java, JavaScript, ASP, PHP etc.

There are some projects developed to document and avoid the security problems of the web applications. Such projects are WASC – Web Application Security Consortium and OWASP – Open Web Application Security Project. Specialized software for detecting security problems in web application is web application security scanner. This kind of software is an automated tool to check web applications for security problems.

The aim of the information system security compliance is to assure protection of the physical and logical components and of the data stored in system towards the threats that exploit the vulnerabilities of the system, [17].

2. Security Vulnerabilities

Information systems are complex constructions developed for resolving of the problems in companies and resulted from the business relationships with third parties: clients, suppliers and partners.

The audit is the process through which a person or a group of persons, independent and qualified, called auditor, makes an objective evaluation of the informatics system, usually in relation with a standard or a proposed objective. Also we have the internal audit process by which it is ensured a continuous conformity with the internal standards, [3], [5], [6], [8].

During an audit mission of an informatics system the most frequent operations are: verifications, evaluation and testing of the informational means, thus [3]:
- risk identification and evaluation in the system;
- control evaluation and testing in the system;
- physical verification and evaluation of the informational environment;
- verification and evaluation of the informatics system administration;
- verification and evaluation of informatics applications;
- verification and evaluation of the computers network security;
- verification and evaluation of the disaster and recovery plans and procedures and the business continuity plans and procedures;

- data integrity testing.

In [7], [9], [18], [10], [11], [12], the informatics audit is presented as a broad domain which includes all the auditing activities for: specifications, projects, software, databases, specific processes from the life cycle of a program, of an informatics application, of a management informatics system and of a portal of maximum complexity, associated to a virtual organization.

The informatics system audit developed as result of technological system penetration in the most part of financial and accounting operations. At the beginning, it was about a copying of the manual operations, the inputs and outputs being audited. The next achievements in technological systems, programming languages, programming techniques and data management systems determined o big change regarding the conception. Thus, the auditing is made through computer.

The security of web applications is compromised when web applications are targeted to sensitive customer and business data. In many cases, organization management levels decided to purchase and deploy software that did not meet the security requirement.

All organizations are exposed to risk from insecure web application if they deploy application running in Internet. A weak web application security results from a significant control deficiency of compliance with laws, regulations and policies applicable to the organization and its data.

The security vulnerabilities of the web applications are classified in the following categories [1], [14]:

- Cross Site Scripting (XSS);
- Injection Flaws;
- Malicious File Execution;
- Insecure Direct Object Reference;
- Cross Site Request Forgery (CSRF);
- Information Leakage and Improper Error Handling;
- Broken Authentication and Session Management;
- Insecure Cryptographic Storage;
- Insecure Communications;
- Failure to Restrict URL Access;
- Application Runtime Configuration;
- Buffer Overflows/Native Code;
- Web Services;
- Malicious Code;
- Custom Cookies/Hidden Fields.

The most common tools for application security environment in an organization are:

- Web Application Firewalls (WAF);
- Web Application Scanners (WAS);
- Source Code Analyzers (SCA).

The organization can use each tool to eliminate the security threats to data through applications. Each organization can mix the above tools to address the critical threats in the way in which it has sense for business processes.

Cross Site Scripting (XSS). It is the most predominant attacks against web applications. It is relatively easy to implement. The browser application executes client-side scripting code controlled by the attacker. The goal of a XSS attack is to hijack the user's application session and/or perform a phishing attack.

Injection Flaws. It is one of the predominant attacks carried on against web applications. The web application takes in data and treats this data as a form of code. The attacker "injects" his malicious code when data is passed to web application. The malicious code is executed and the attacker achieves his aim. The aim is to obtain or destructs the private data.

There are many types of injection flaws. One of the most common is *SQL injection*. SQL injection is a technique to inject SQL commands in the input fields by the attacker. If the web application allows user controllable input and does not validate then that application is vulnerable to some king of injection. If the SQL commands "injected" in the input fields by the attacker are executed by web application then the attacker can get information to tune his attack and finally to access private data stored in database.

XML injection is becoming more prevalent with the increased use of Web Services. This technique consists of query XML documents provided by XPath and XQuery. The technique is the same with SQL injection, being more difficult to automatically discover it.

LDAP – Lightweight Directory Access Pro-

tocol is used for account management, authentication and authorization. *LDAP injection* is a technique for use the invalidated data in the construction of LDAP queries/filter.
For instance, if a web application uses the following search filter, [14]:

```
searchfilter="(cn="+user+")"
```

which it is instantiated by a HTTP request:

```
http://www.testldapinjection.com/ldapsea
rch?user=Popa
```

If the value *Popa* is replaced with a **"*"**, then the request will look like:

```
http://www.testldapinjection.com/ldapsea
rch?user=*
```

and the filter is becoming:

```
searchfilter="(cn=*)"
```

Another form of flaws injection is *command injection*. It is one of the serious types of injection vulnerabilities. The attacker can run arbitrary system commands, having an elevated privilege level. The success of an attack is difficult to determine because the feedback to the user has a low level.
AJAX injection is a new type of attack. The vulnerability is given by the tendency to store more sensitive data on the client size. So, this data and functionality is accessible to the malicious users.

Malicious File Execution. It is a very common pattern to attack PHP applications. The attacker can upload the malicious content that will be executed by the hosting application. The web server can be caused to run arbitrary code controlled by the attacker by changing the hidden fields from the PHP expressions.
For instance, a common vulnerable construct is:

```
include $_REQUEST['filename'];
```

The above construct can be used to access local file server.
Another form of the attack is, [1]:

```
<?php include($hidden_user_skin).
       "skins"."php"); ?>
```

in which the attacker can modify the hidden field *$hidden_user_skin* to be an URL that will exploit that vulnerability.
Insecure Direct Object Reference. The data are exposed if the application exposes access to the internal object handles. The attacker can directly refer the object. For instance, this vulnerability is detected when the database exposes the primary keys.
There are many applications that expose their internal object to the users. For instance, if the web application permits to input filenames or paths then the attacker can jump out of application's directory and he can access other resources [14]:

```
<select name="language"><option value="fr">Français</option></select>
…
require_once ($_REQUEST['language'])."lang.php");
```

Using a string like **"../../../../etc/passwd%00"**, the attacker can access any file on server's file system.
Cross Site Request Forgery (CSRF). It is based on an application's trust of a client. For instance, the victim computer logs in a new account and without logging out visits a malicious site. This site can take over the trust relationship between the victim computer and trusted account. Whenever the victim computer visits the malicious site, the access to trusted account can be performed by malicious site. Thus, the malicious site can send requests instead of victim computer.
For instance, the following tag [14]:

```
<img
src="http://www.example.com/logout.php">
```

will generate a request to log out the victim.
The attacks against an on-line banking application process requests like:

```
<img src="http://www.testCSRF.com/transfer.do?frmAcct=document.form.
frmAcct& toAcct=535363&toSWIFTid=414112&amount=5000.00">
```

Information Leakage and Improper Error Handling. It is a big issue known and understood by many organizations. An error message can give the attacker the information needed for refining the attack. The automated tools cannot detect this vulnerability. The vulnerability can be remediated through source code analysis.

For instance, in Computer Associates eSCC and eTrust Audit the remote attackers can read or delete files, or can execute replay attacks. The vulnerabilities consist of:

- Discover the web server path on Windows platform;
- Read and delete arbitrary files from the host server with the permission of the service account;
- Execute external replay attacks.

Broken Authentication and Session Management. These may lead to severe vulnerabilities such as session hijack and privilege escalation. In web application, the user can access the application area of another one with a higher privilege level if the second one is not validated through the session.

In the main authentication, the flaws are weak regarding functions like logout, password management, timeout, remember me, secret question and account update. For instance, a server can store LDAP credentials in a path which has insecure permissions and any local user can get the credentials.

Insecure Cryptographic Storage. The sensitive data can be stored cryptographically. Serious information disclosure appears due the weak data encryption routine or a routine against organization policy.

To protect the sensitive information in web applications, it must do a reliable encryption process based on the following characteristics:

- Reasonable and appropriate encryption;
- Strong encryption algorithms;
- Only the absolutely and necessary information;
- Public methods that have not open vulnerabilities;
- Unnecessary data never store.

Insecure Communications. The sensitive data transmitting can be done in clear or encrypted. The web application vulnerability appears when data are not encrypted. OWASP refers to the use SSL to encrypt sensitive data between the web browser and web application running on server.

For instance, some applications that use Web Services do not require HTTPS. This fact allows the remote users to obtain sensitive information by sniffing the unencrypted HTTP traffic.

Failure to Restrict URL Access. The access to some pages of the web application is filtered through authorization to the protected links. Users performing manual attempts can pass the filter. Thus, a presentation layer authorization is not enough, and a programmatic business layer authorization layer must be implemented.

For instance, an attacker can access the admin file when the folder restrictions are implemented badly. The attack request may be:

```
https://[SERVER URL]/admin/admin.html
```

when the attacker know the possible structure of the web application:

```
[WEB ROOT]
   /admin
      admin.html
   /products
   /sales
   ...
   index.html
   login.html
   ...
```

and he follows the following standards:

```
/admin/[index.html | index.jsp | index.asp | index.php]
 /backup/
 /logs/
 /vulnerable.cgi
```

Application Runtime Configuration. An improper configuration for the runtime environment can lead to many serious risks. The risks can be internal or external runtime environment.

Buffer Overflows/Native Code. The vulnerability appears when today's web applications interface with systems developed in older programming languages. The older systems crash because they have not the mechanisms implemented in newer web application. The buffer overflow has the same style with flaws injection.

Web Services. The vulnerabilities of the web application due to web services are the result of moving to SOA – Service Oriented Architecture.

Malicious Code. There are two classes of malicious code:

- Dead, hidden or debugging code that can be used as malicious code;
- Code intentionally inserted into application to get malicious outcome.

Source code analyzers identify malicious code.

Custom Cookies/Hidden Fields. They are a common occurrence in all major web applications. The risk is that the cookies are stored on client side and the malicious user can manipulate these data. The state or control information supposes to use the hidden fields.

The vulnerability classes described above are presented in [1].

The level of organizational risk is reduced by analyzing the source code of web applications for the most common security vulnerabilities. Also, the costs to patch and fix vulnerabilities are significantly reduced when the application is deployed [13].

The web vulnerabilities are classified in:

- Coding errors – input validation, unbounded parameters and encoding;
- Design flaws – security model, improper logging, error handling and unsupported APIs.

The web applications perform actions based on user requests. The application accepts and returns data to the user. Such kind of distributed architecture does web application vulnerable to attacks caused by insertion and invalidated input.

Malicious input can be inserted into URLs, query strings, headers, cookies, form fields and hidden fields which are interpreted by server application. As result, the attacker can obtain sensitive information, modify data in databases or he can crash the application.

Validation attacks regard the following issues [13]:

- Invalidated source of input: URL parameters, form fields, cookies, HTTP headers, database queries;
- Use of invalidated input: invalidated user request passed to the server-side application;
- Invalidated output streams: malicious content passed back to the user.

Regarding the design flaws, the vulnerabilities are the result of improper implementation of the following issues [13]:

- Flawed authorization and access control: improper use of access control and its defining in formal policy;
- Flawed authorization and session management: weak, exposed or unencrypted credentials for authentication;
- Native code and buffer overflows: security risks introduced by another programming languages;
- Dynamic code: use of dynamic libraries by malicious code;
- Weak encryption: non-standard cryptography and poor entropy or randomness;
- Application configuration: access to configuration details, property files or XML data;
- Denial of service: extraneous exit calls;
- Network communications: CORBA, servlets, email, RMI – Remote Method Invocation;
- Unsupported application interfaces: applications that call directly the lower level application interfaces;
- Improper administrative and exception handling: improper error messages provide critical information to the attacker: stack traces, database dumps, error codes.

Application security is a critical component of the security practice in any organization. The access to the critical resources of an or-

ganization is controlled by software. In order to evaluate the application security, it must use the three kinds of tools to get information from system: Web Application Firewalls, Web Application Scanners and Source Code Analyzers. These tools are used in evaluation and testing the vulnerabilities in different mixes depending to class of vulnerability.

3. Conclusions

In the Knowledge Society, the organizations use Information Technology to process their information in order to accomplish better their mission. The audit process development plays a critical role to assure a high level of information system quality.

The organizations want to carry out audit processes because they need to assure a high level of the information systems, to know what and where are their vulnerabilities, to develop security policies and risk management plans and to implement measures with positive effects on their information systems. The audit results must correct some aspects concerning the information systems security.

Detection of the security vulnerabilities in an information system based on web application is a critical activity to give the confidence in that system and, also, to assure a high-level quality of the system to prevent the system crashes and sensitive data theft. If the vulnerabilities are exploited by external users, this thing may cause big loses for all partners that use the information system.

References

[1] R. Berg, "The Right Tool for the Right Job: An Application Security Tools Report Card", in *An Ounce Security Topics White Paper*, 2008

[2] S. Buchanan and F. Gibb, "The information audit: an integrated strategic approach", *International Journal of Information Management*, 18(1), 1998, pp. 29 – 47

[3] S. Capisizu, "Modele şi tehnici de realizare a auditului informației economice", *ASE Bucharest*, 2006, PhD Thesis

[4] S. Capisizu, G. Noşca and M. Popa, "Informatics Audit", in *The 37th International Scientific Symposium of METRA*, Military Equipment and Technologies Research Agency, Bucharest, May 25 – 26, 2006

[5] S. Capisizu, G. Noşca and M. Popa, "The Informatics Audit – Basic Concepts", in *Information Systems & Operations Management*, March 1-2, 2006, Universul Juridic Publishing House Bucharest, pp. 350 – 357

[6] I. Ivan, C. Boja and M. Popa, "The Informatics Audit Development Strategy", in *Information Systems and Operations Management*, Bucharest, November 29 – 30, 2004, Editura Print Grup, pp. 279 – 285

[7] I. Ivan, G. Noşca and S. Capisizu, *Auditul sistemelor informatice*, ASE Printing House, Bucharest, 2005

[8] I. Ivan, M. Popa, G. Noşca and S. Capisizu, "Data Audit for SMEs", *Information Systems & Operations Management*, Bucharest, March 1-2, 2006, Universul Juridic Publishing House Bucharest, pp. 306 – 315

[9] I. Ivan, M. Popa and S. Capisizu, "Quality Management through Informatics Audit", in *Proceedings of the 6th International Economic Symposium*, Transilvania University of Braşov, May 19-20, 2006

[10] J. Kramer, *The CISA Prep Guide: Mastering the Certified Information Systems Auditor Exam*, Wiley Publishing Inc., 2003

[11] R.K. Mautz and H.A. Sharaf, *The Philosophy of Auditing*, American Accounting Association, 1996

[12] M. Mazer, "Auditing Databases for Compliance and Risk Management", in *A Supplement to DM Review—SQL Server Executive*, March 2006, pp. 18 – 19

[13] Ounce Labs, "The Dirty Dozen: The Top Web Application Vulnerabilities and How to Hunt Them Down at the Source", in *A Security Topics White Paper*, 2008

[14] http://www.owasp.org/index.php/Top_10_2007

[15] M. Popa and F. Alecu, "ERP Informatics System Audit", in *Knowledge*

Management – Projects, Systems and Technologies, vol. II *Reinforcement and Extension of Universities & Business Community Partnerships in the Knowledge Era*, Bucharest, November 9 – 10, 2006, pp. 109 – 116

[16] M. Popa, F. Alecu and C. Amancei, "Characteristics of the Audit Process for Information Systems", in *The Proceedings of the International Conference Competitiveness and European Integration – Business Information Systems & Collaborative Support Systems in Business*, Cluj-Napoca, October 26 – 27, 2007, Risoprint Printing House, Cluj-Napoca, pp. 295 – 299

[17] M. Popa and M. Doinea, "Audit Characteristics for Information System Security", in *The Proceedings of the Eight ternational Conference on Informatics in Economy*, Academy of Economic Studies of Bucharest, May 17-18, 2007, pp. 938 – 943

[18] M. Popa, M. Florescu and C. Bodea, "Information System Quality Evaluation Based on Audit Processes", in *Proceedings of the 2008 International Conference of Information Engineering*, Imperial College London, London, Great Britain, July 2 – 4, 2008, Newswood Limited, International Association of Engineers, 2008, pp. 494 - 496

[19] http://en.wikipedia.org/wiki/Information_systems

Marius POPA has graduated the Faculty of Cybernetics, Statistics and Economic Informatics in 2002. He holds a PhD diploma in Economic Cybernetics and Statistics. He joined the staff of Academy of Economic Studies, teaching assistant in 2002 and senior lecturer in 2006. Currently, he is lecturer in Economic Informatics field and branches within Department of Economic Informatics at faculty of Cybernetics, Statistics and Economic Informatics from Academy of Economic Studies. He is the author and co-author of 6 books and over 100 articles in journal and proceedings of national and international conferences, symposiums, workshops in the fields of data quality, software quality, informatics security, collaborative information systems, IT project management, software engineering. From 2009, he is a member of the editorial team for the *Informatica Economică Journal* and between 2003 and 2008 he was a member of the editorial team for the journal *Economic Computation and Economic Cybernetics Studies and Research.*