INFORINO 2020

Moscow, Russia
14-17 April, 2020

Assessing Information Risks When Using Web Applications Using Fuzzy Logic

Speaker
Pavel B. Khorev
NRU “MPEI”
Moscow, Russia

Authors:

Pavel B. Khorev, Maxim I. Zheltov

National Research University “MPEI”

Moscow, Russia

IEEE

NATIONAL RESEARCH UNIVERSITY

CROC

Assessing Information Risks When Using Web Applications Using Fuzzy Logic

The development of information technology entails the emergence of various information risks associated with their use. Creating methods and tools for assessing information risks is a pressing issue of information security.

Web applications have become an integral part of information systems. Security and information risk assessment associated with web applications are necessary for the owner of almost any web resource.

Assessing Information Risks When Using Web Applications Using Fuzzy Logic

Web application vulnerability analysis software is designed to look for "weaknesses" that could lead to information security threats for users of such applications. Existing solutions generally do not have a system to assess the likelihood of a threat being implemented, nor are they able to assess the expected losses that may occur when various vulnerabilities are exploited.

Assessing Information Risks When Using Web Applications Using Fuzzy Logic

The aim of this work is to explore how to integrate vulnerability detection techniques with information risk assessment methods for web applications. To achieve the goal, the following tasks will be solved:

1. Analysis of methods for assessing information risks caused by web application vulnerabilities.
2. Designing a prototype web application vulnerability scanner that includes information risk assessment functions based on fuzzy logic.
3. Software implementation, testing and debugging of a web application vulnerability scanner prototype with information risk assessment features and the ability to customize them.

Assessing Information Risks When Using Web Applications Using Fuzzy Logic

The term "risk" means that events with negative consequences as a result of certain decisions or actions are possible or likely. According to ISO 27005:2018 the risk is usually characterized by possible events and consequences or their combination. Also risk is measure of the extent to which an organization is threatened by a particular event.

Information risk analysis refers to the process of comprehensive assessment of the security of the information system with the transition to quantitative and qualitative indicators of risks.

Assessing Information Risks When Using Web Applications Using Fuzzy Logic

There are two main groups of methods for calculating information risks. The first group determines the level of risk by assessing the degree to which a certain set of information security requirements is compliant with a certain set of requirements. The sources of requirements may be:

- Requirements and recommendations of national and international standards.
- Recommendations of software and hardware manufacturers (Microsoft, Cisco, Oracle, etc.).

Assessing Information Risks When Using Web Applications Using Fuzzy Logic

The second set of methods for assessing information security risks is based on determining the likelihood of threat implementation, the extent of the damage to their implementation and the vulnerability of the resource. The value of the damage is determined by the owner of the information resource, and the probability of the attack and the measure of the resource's vulnerability to the threat are assessed by experts.

Assessing Information Risks When Using Web Applications Using Fuzzy Logic

The proposed method of assessing information risks should eliminate the shortcomings of qualitative and quantitative methods and have the ability to adjust itself flexibly.

The fuzzy-logic risk assessment method involves determining the relationship between inputs and information risk. These relationships can be formalized by the product rules of the kind of "if ..., then ...". In addition, the fuzzy logic mechanism requires the formation of estimates of key parameters and their representation as fuzzy variables. It is necessary to take into account the many sources of information and the uncertainty of the information itself.

Assessing Information Risks When Using Web Applications Using Fuzzy Logic

Some of the parameters used to assess risks cannot be accurately measured. When assessing such parameters, a subjective component is expressed by fuzzy estimates such as "high," "low," "most preferred," etc. This parameter is described as a linguistic variable with its thermo-multiple values.

The connection of the quantitative value of a certain factor with its qualitative linguistic description is set by the so-called functions of the factor's non-fuzzy set. To simplify the task of assessing information risks, it is necessary to reduce the set of all the indicators studied to one comprehensive parameter. The value of this parameter will allow you to assess the security of the information system.

Assessing Information Risks When Using Web Applications Using Fuzzy Logic

Key web application vulnerabilities and examples of how to use them:

- SQL Injection.
- Inter-site scripting
- Cross-Site Request Forgery.
- Local file inclusion.

Assessing Information Risks When Using Web Applications Using Fuzzy Logic

Let's look at how to detect web application vulnerabilities:

- Web application security audit.
- OWASP methodology (Open Web Application Security Project).
- Using web application vulnerability scanners. Software or hardware tools that search for web application vulnerabilities that can be used, both in security audits and as a separate tool. Web vulnerability scanners can detect coding stage vulnerabilities, the web application implementation and configuration stage vulnerabilities, the website operation phase vulnerabilities.

Assessing Information Risks When Using Web Applications Using Fuzzy Logic

It is proposed to use a qualitative assessment of information risks and to use the following factors in calculations:

- Cost of resource.
- Measure of resource vulnerability to threat.
- Probability of implementing a threat.

It is also proposed to use risk assessment using a fuzzy logic apparatus. Matlab r2017a is used to build the model.

Assessing Information Risks When Using Web Applications Using Fuzzy Logic

Linguistic variables:

- "Probability of threat implementation". The term-set values include "low" (T1), "average" (T2) and "high" (T3). Media (U) determines the interval from 0 to 1. Syntax rule: what is the probability of implementing the threat?
- "Resource Cost". Term-set values include "low" (T1), "medium" (T2) and "high" (T3). Media (U) determines the interval from 0 to 1,000,000 (measured in rubles). Syntax rule: what is the cost of a resource that has vulnerability?
- "Resource vulnerability to threat". Term-set values include "minimum" (T1), "medium" (T2), "maximum" (T3). Media (U) determines the interval from 1 to 3. Syntax rule: what is the measure of resource vulnerability to threat?

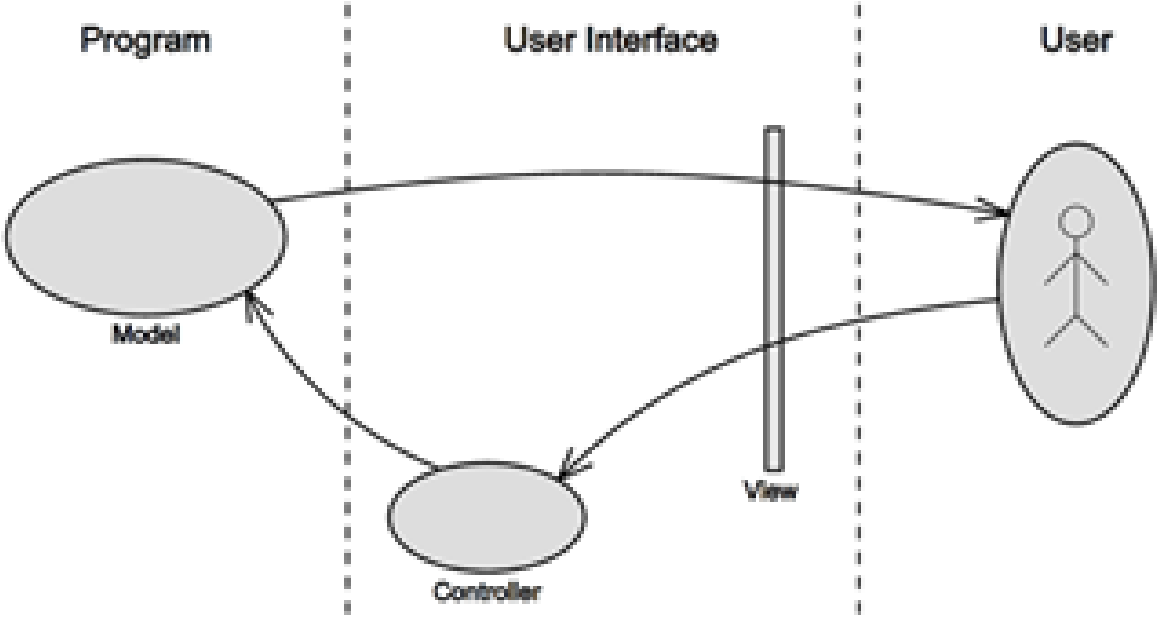
Assessing Information Risks When Using Web Applications Using Fuzzy Logic

Output variable "risk". Term-set values include "Very Low" (T1), "Low" (T2), "Medium" (T3). Media (U) determines the interval from 1 to 5. Syntax rule: risk determination.

The "if-then" rule base includes 27 rules. In program implementation, all parameters, functions and rules can be changed. Therefore, an information security specialist can approach the risk assessment of different web applications individually by changing these parameters.

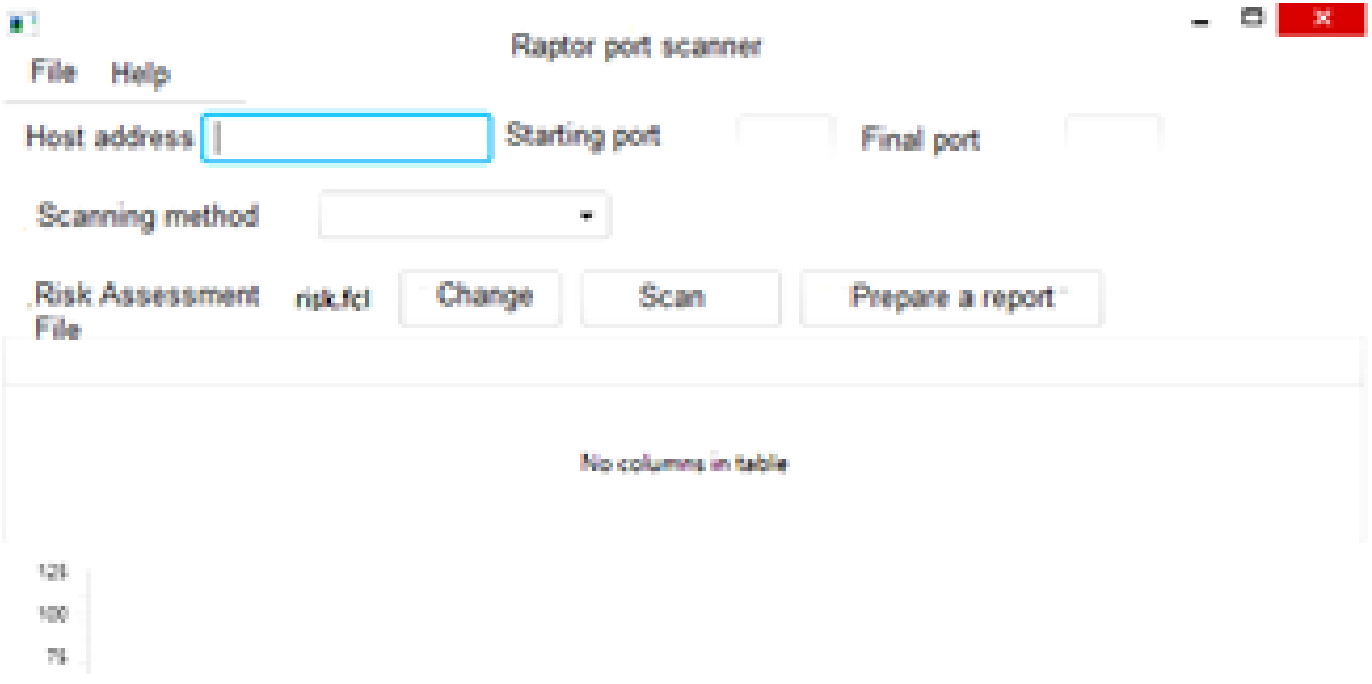
A pattern Model-View-Controller (MVC) [9] was chosen as the basis for the web application vulnerability scanner structure.

Assessing Information Risks When Using Web Applications Using Fuzzy Logic



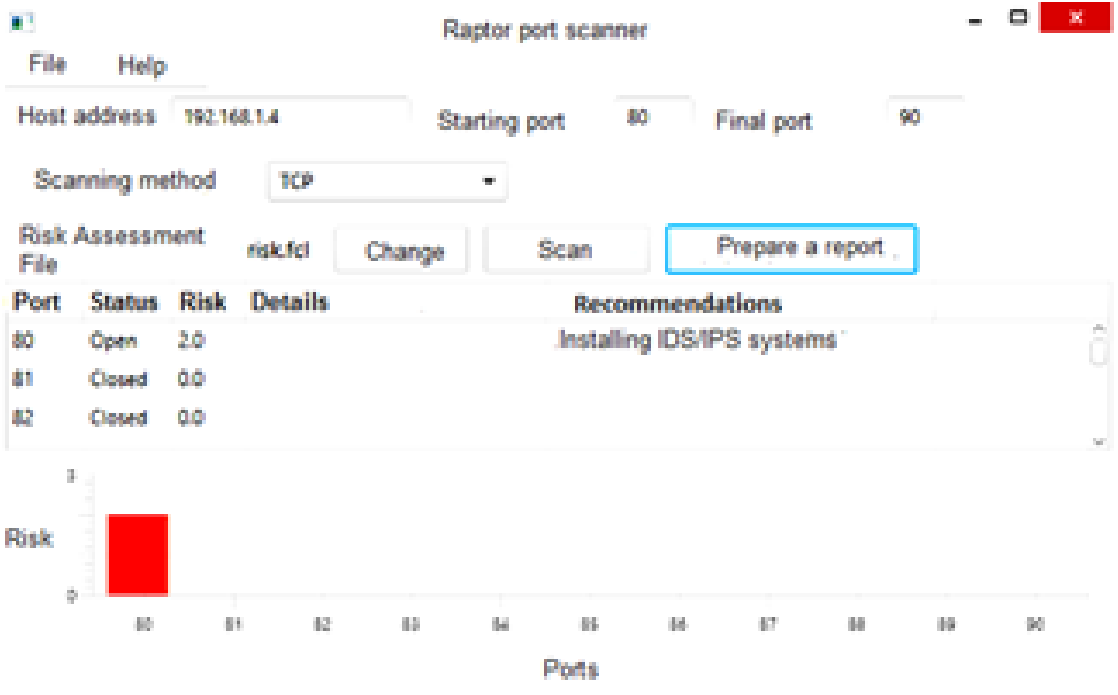
MVC scheme

Assessing Information Risks When Using Web Applications Using Fuzzy Logic



Port scanner user interface

Assessing Information Risks When Using Web Applications Using Fuzzy Logic



The result of the port scanner on the test stand

Assessing Information Risks When Using Web Applications Using Fuzzy Logic

- Java programming language was selected for implementation.
- The database was created using the PostgreSQL database management system.
- JavaFX was used to create a graphical component that allows you to create applications with a rich graphical interface.
- The jFuzzyLogic library was chosen to implement the fuzzy logic apparatus because the entire machine of fuzzy logic is encoded in the intuitive language of FCL.
- The entire fuzzy logic machine needed to assess the risks is described in a special file that has an extension .fcl.

Assessing Information Risks When Using Web Applications Using Fuzzy Logic

The work identified information security threats when using web applications and their possible vulnerabilities. Methods of assessing information risks have been analyzed. The possibilities of using methods of fuzzy logic to assess information risks in the use of web applications have been explored.

Web application vulnerability scanner have been designed, implemented and tested. The developed scanner is additionally capable of assessing information risks based on techniques of fuzzy logic. Also developed scanner has the ability to adjust flexibly.

The web application vulnerability scanner prototype presented in this work is used in a laboratory workshop at the National Research University "MPEI".

INFORINO 2020

Moscow, Russia
14-17 April, 2020

Thank you for attention!

Speaker's contacts:

Pavel B. Khorev

NRU "MPEI"
Moscow, Russia

pbkh@yandex.ru

www.appmat.ru

IEEE

NATIONAL RESEARCH UNIVERSITY

CROC