Architecture of web based intellectual vulnerability scanners for OWASP web application auditing process

S Nurmyshev, K Kozhakhemt, L Atymtayeva
Kazakh British Technical University, Tole bi 59, Almaty, Kazakhstan

*Corresponding author’s e-mail: kanik85@gmail.com, Latymtayeva@gmail.com, s.nurmyshev@gmail.com

Abstract

Now, all business applications (e-commerce, banking, blogs, web mail, etc.) are usually made as web-based systems. Increasing distinction and usage of these applications have made them more responding to attacks because they store enormous amount of sensitive user information. Traditional security mechanisms like network firewalls, intrusion detection systems, and use of encryption can protect the network, but cannot mitigate attacks targeted towards web applications. Vulnerability scanners are often used in web application security assessments, but there are few properly developed web-based vulnerability scanners, that used intellectual expert based tools. Development of intellectual web-based vulnerability scanners for OWASP security standard has high demand in security auditing area. Expert systems in vulnerability scanners can increase effectiveness and decrease a cost of OWASP auditing process.

Keywords: intellectual vulnerability scanner, expert system, OWASP auditing process

1 Introduction

Nowadays, expert systems were going to be widely used in information security auditing process [1-4]. It helps to decrease information security auditing process. Also, using of intellectual approach in OWASP security process becomes obliged, because of high complexity features in the auditing process. In recent years, increased the number of publications applied to this new trend in the field of information security, as an adaptive network security. This line consists of two major technologies - security analysis (safety assessment), and detection of attacks (intrusion detection). It is the first technology and the subject of this article.

Briefly illuminating active auditing process, we can highlight following issues; the network consists of communication channels, nodes, servers, workstations, application and system software, databases, etc. All of these elements need to be evaluated for their protection effectiveness. Security review tools and explore the network looking for "weak" place in it, analyze the results and create on their basis of various kinds of reports. In some systems, instead of "manual" intervention by the administrator found the vulnerability will be eliminated automatically (for example, System Scanner System). Here are some of the problems identified by the analysis of security systems:

- "Hatches" in the programs (back door) and programs such as "Trojan horse";
- weak passwords;
- susceptibility to penetration of unprotected systems;
- misconfiguration of firewalls, Web-servers and databases;
- etc.

Security analysis technology is an efficient method of implementing network security policies before completing its attempt to breach the outside or from inside the company in OWASP auditing process.

This is one of the aspects common to all systems of security analysis. They are designed to detect only known vulnerabilities have described them in the database, but multiple expertise of auditors can increase the effectiveness of OWASP auditing process.

2 Vulnerability scanner working process

A vulnerability scanner can assess a variety of vulnerabilities across information systems (including computers, network systems, operating systems, and software applications) that may have originated from a vendor, system administration activities, or general day-to-day user activities:

1. Vendor-originated: this includes software bugs, avoiding operating system patches, accessible services, vulnerable default configurations, and web application vulnerabilities.
2. System administration-originated: this includes inaccurate or unauthorized system configuration changes, loss of password protection policies, and so on.
3. User-originated: this includes sharing directories to unauthorized parties, failure to run virus scanning software, and malicious actions, such as carefully introducing system backdoors.

On the Figure 1 we can show a typical web application testing methodology with highlighted stages which can be partially automated with vulnerability scanners on Testing methodology [5].
3 The limitations of vulnerability scanners

The drawbacks of vulnerability scanners are:

1. Snapshot only: a vulnerability scanner can only assess "a snapshot of time" in terms of a system or network's security status [6]. Therefore, scanning needs to be conducted regularly, as new vulnerabilities can emerge, or system configuration changes can introduce new security holes.

2. Human judgement is needed: Vulnerability scanners can only report vulnerabilities according to the plug-ins installed in the scan database. They cannot determine whether the response is a false negative or a false positive. Human judgement is always needed in analysing the data after the scanning process.

3. Others: a vulnerability scanner is designed to discover known vulnerabilities only. It cannot identify other security threats, such as those related to physical, operational or procedural issues.

4 The architecture of intellectual vulnerability scanner

In general, a vulnerability scanner is made up of four main modules, namely, a Scan Engine, a Scan Database, a Report Module and a User Interface.

1. The Scan Engine executes security checks according to its installed plug-ins, identifying system information and vulnerabilities. It can scan more than one host at a time and compares the results against known vulnerabilities.

2. The Scan Database stores vulnerability information, scan results, and other data used by scanner. The number of available plug-ins, and the updating frequency of plug-ins will vary depending on the corresponding vendor. Each plug-in might contain not only the test case itself, but also a vulnerability description, a Common Vulnerabilities and Exposures (CVE) identifier, and even fixing instructions for a detected vulnerability. Scanners with an "auto-update" feature can download and install the latest set of plug-ins to the database automatically.

3. The Report Module provides different levels of reports on the scan results, such as detailed technical reports with suggested remedies for system administrators, summary reports for security managers, and high-level graph and trend reports for executives.

4. The User Interface allows the administrator to operate the scanner. It may be either a Graphical User Interface (GUI), or just a command line interface.

Most vulnerability scanners are characterized by their modular structure as explained above. However, there are also primitive scanners that are basically sets of scripts or C code exploits producing simple plain-text files as scanning results. Updates to these primitive scanners are infrequent and require manual intervention.

5 Using vulnerability scanners in OWASP auditing process

For those who are new in the web application security field; OWASP is short for Open Web Application Security Project. OWASP is a non-profit organization that raises web application security awareness. Every three years OWASP publishes the OWASP Top 10 list. The list highlights the most commonly exploited vulnerabilities and security problems found in websites and web applications.

The list as such is not the holy grail for web application security experts, but it serves as guidelines for organizations to ensure their web applications are not vulnerable to these most commonly exploited vulnerabilities and web application security issues. In fact there are many other vulnerabilities and security issues that can be found in web applications that are not listed in the OWASP Top 10 lists, and ideally all of them should be addressed with time.

6 Conclusion

Using intellectual scanners and development of knowledge base system can improve affectivity of information security auditing processing OWASP. In Addition, creating correct knowledge base of vulnerability sets in expert system of intellectual vulnerability scanners can reduce cost of auditing process.

Acknowledgments

This work is implementing at Kazakh-British Technical University under the research project “Expert systems for active audit and management of information security” funded by Ministry of Education&Science of the Republic of Kazakhstan as a part of the State Research Program “Development of the local products for Oil&Gas industry needs”.

FIGURE 1 Web application testing methodology
References


