Web Applications Assessment Tools: Comparison and Discussion

Mohamad Swead[1], Dr. Muhammad Mazen Almustafa[2]

[1]Department of web sciences, Syrian Virtual University
E-Mail: Mohamad_68263@svuonline.org
[2]Department of web sciences, Syrian Virtual University
E-Mail: t_mmustafa@svuonline.org

Abstract— *Recently web applications have proliferated rapidly, with the world increasingly dependent on financial transactions, purchasing, billing, education, medicine, and many more. But the security of these applications is worrying because it directly affects the end-user. Therefore, it is necessary to detect security vulnerabilities in those applications that may cause significant user problems. Most commonly used approach to detect those vulnerabilities are assessments tools like web scanners.*

This paper will focus on usage of these web scanners and their related methodology to detect the various vulnerabilities in web applications and then compare these scanners depending on results.

Keywords— ***Web scanner, SQL Injection, XSS, Vulnerability, Assessment.***

I. INTRODUCTION

One of the common misconceptions regarding information security that they are related to computer information! However, information security relates to all aspects of information processing, transfer and storage, whether through electronic or paper-based means.

From the very beginning of the emergence of technology and computers, and throughout their growth period, information security has been a difficult challenge. The concept of information security is broad but can be shortened by blocking access to information and protecting data from unauthorized access.

The security features of Web applications are very similar to the security features of other software systems in terms of data confidentiality and integrity as well as the period in which the application remains available for use.

The security features of Web applications are very similar to the security features of other software systems in terms of data confidentiality and integrity as well as the period in which the application remains available for use. There are still many security gaps in web applications as developers often try to add many functions to their applications, which requires the writing of many codes that increase the likelihood of the emergence of coding errors and thus increase the chances of security vulnerabilities that are used to attack Web applications and steal data or stop the web application for example.

Detecting or evaluating security vulnerabilities in particular applications aims to identify weaknesses in those applications in order to protect them from bad usage by those who aim to harm those applications either by targeting the availability of those applications or by stealing certain critical information. Through this proactive approach, application developers can identify and overcome vulnerabilities before anyone else knows or even before they are released to users.

II. WEB APPLICATION ASSESSMENT TOOLS

Web application security assessment tools are divided into several categories, including analysis of source code (White Box), web application scanners (Black Box), database scanners and other miscellaneous tools. The most common security tools used to evaluate Web applications are the analysis of source codes as well as Web application scanners which we will focus on and test some of these tools in this paper. [1]

Source code analysis (White Box) shows good results in detecting security vulnerabilities in web applications, but are useful only if the source code for those applications is available, making this method limited.

Web application scanners (black box), which simulates attacks on web applications in order to get the gaps and threats in those applications, these tools usually have some problems related to performance, speed and accuracy.

III. WEB APPLICATION SECURITY PROJECT (OWASP)

As a result of the increasing the importance of application security, an open source and non-profit organization focused on the security of web applications emerged by clarifying the most important gaps, statistics and other important issues in this area (OWASP).

OWASP was founded on December 1, 2001 and was established as a non-profit charity in the United States on April 21, 2004 to ensure support and continued work. OWASP is an open source community dedicated to enabling organizations to develop and operate applications that can be trusted and provide all documents and forums free of charge to anyone who wishes to improve application security. [1]

OWASP focuses on providing a higher level of security for online applications by identifying vulnerabilities in which applications may be vulnerable and which, if exploited by attackers, could result in a loss of security and confidentiality or a complete disruption of the application. For example, security vulnerabilities may exist in a particular application because of a query or query for unreliable data, or by the possibility of breaking authentication and session management. In addition, cross-site scripting XSS is another security vulnerability that is added to the list of vulnerabilities that threaten Web applications where an attacker injects malicious scripts into web pages. Another security vulnerability is SQL injection, in which the attacker injects SQL instruction into the application database through the same interface, making the attacker able to review important data or even modify the database. [1]

IV. VULNERABILITY SCANNERS

In this section, we will sort out some of web applications scanner (Black Box):

A. SecuBat

SecuBat is an open source tool developed by a group of researchers at the university of Vienna, based on black box approach by crawling and scanning the Web application for security vulnerabilities. This tool targets four main vulnerabilities; SQL injection, simple reflected XSS, encoded reflected XSS and Form-Redirecting XSS. [2]

i) SecuBat components

This scanner consists of three main components;

- Crawling module: Collecting information about targeted web application.
- Attack module: lunching series of attacks towards targeted website depending on crawling results.
- Analysis module: analysis results of previous stage in order to specify vulnerabilities in targeted web application. [2]

ii) Implementation

SecuBat has been implemented using Windows Forms .NET application in C#. In order to maintain a flexible and open design, a general and modular structure has been used, which, as we mentioned earlier, consists of several modules (crawling, attack, analysis), which can be called separately.

In terms of performance, Secure Bat was able to launch 15 to 20 attacks at the same time without forming a burden on the processor of the computer from which the attack is launched.

The following figure illustrates the attack architecture followed by Secure Bat [2]

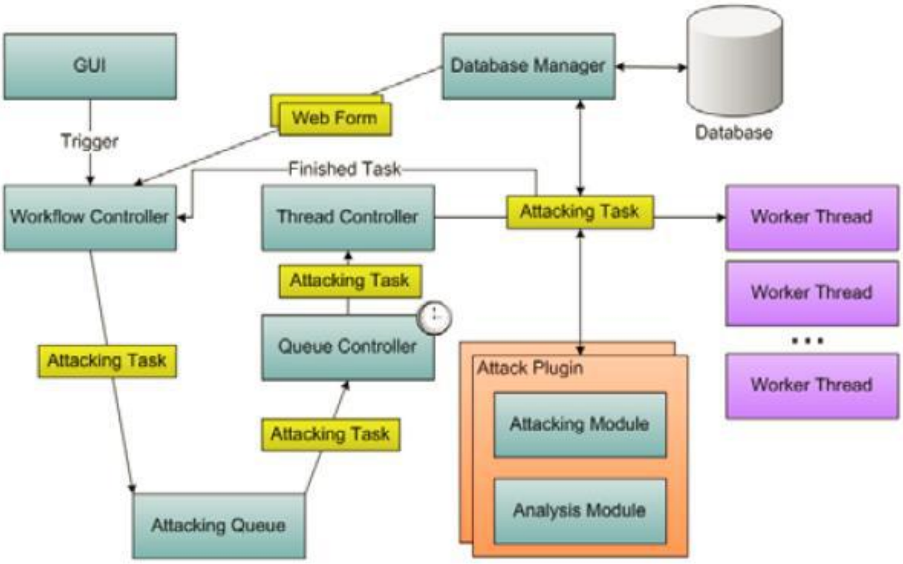
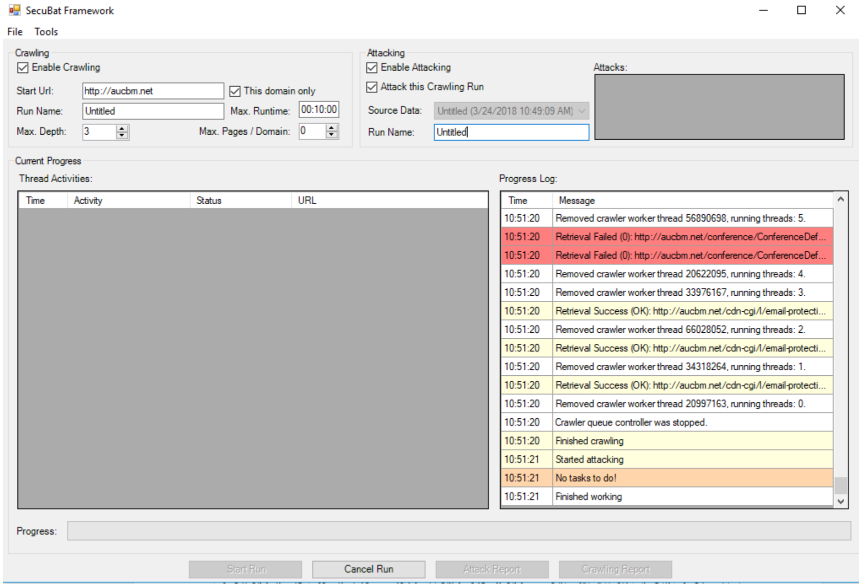


Fig.1: SecBat Architecture

iii) Results

We have install this tool in order to test it and here are the results;

- Tool has an easy interface to use as appears in below figure;



☑ Enable Crawling

Start Url: http://aucbm.net ☑ This domain only

Run Name: Untitled Max. Runtime: 00:10:00

Max. Depth: 3 Max. Pages / Domain: 0

☑ Enable Attacking

☑ Attack this Crawling Run

Source Data: Untitled (3/24/2018 10:49:09 AM)

Run Name: Untitled

```
Time      Message
10:51:20  Removed crawler worker thread 56890698, running threads: 5.
10:51:20  Retrieval Failed (0): http://aucbm.net/conference/ConferenceDef...
10:51:20  Retrieval Failed (0): http://aucbm.net/conference/ConferenceDef...
10:51:20  Removed crawler worker thread 20622095, running threads: 4.
10:51:20  Removed crawler worker thread 33976167, running threads: 3.
10:51:20  Retrieval Success (OK): http://aucbm.net/cdn-cgi/l/email-protecti...
10:51:20  Removed crawler worker thread 66028052, running threads: 2.
10:51:20  Retrieval Success (OK): http://aucbm.net/cdn-cgi/l/email-protecti...
10:51:20  Removed crawler worker thread 34318264, running threads: 1.
10:51:20  Retrieval Success (OK): http://aucbm.net/cdn-cgi/l/email-protecti...
10:51:20  Removed crawler worker thread 20997163, running threads: 0.
10:51:20  Crawler queue controller was stopped.
10:51:20  Finished crawling
10:51:21  Started attacking
10:51:21  No tasks to do!
10:51:21  Finished working
```

Fig.2: SecBat GUI

- Tool is very limited
- We weren't able to crawl on more than a URL at a time
- We weren't able to launch an attack where tool became non-responsive and needs to be restarted
- Very limited in reporting if you wish to use units of

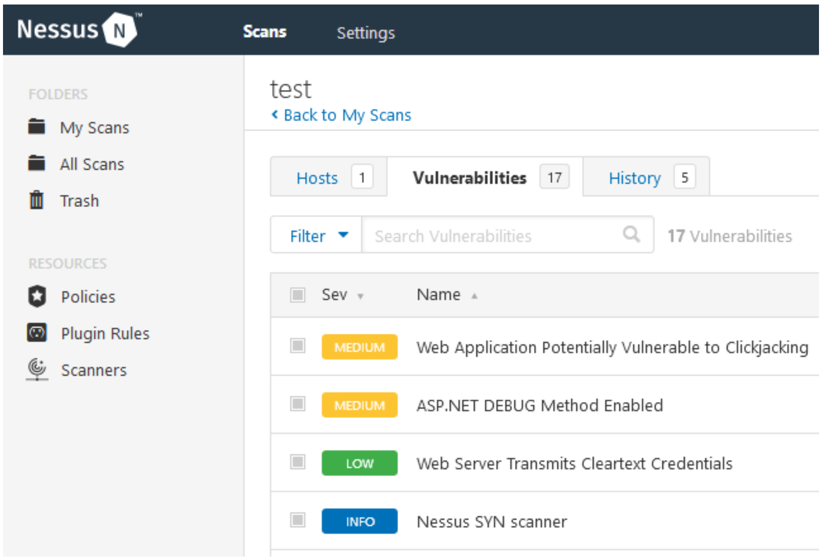
B. Nessus

Nessus is a vulnerability scanner developed by Tenable network security which cares about IT vulnerability management. [3] Multiple scanning can be launched at a time by crawling and detecting vulnerabilities in web applications, then categorize these vulnerabilities depending on its severity as the following; Critical, High, Medium, Low, Info. This tool uses Client-Server model where the session is controlled by user and the test runs on server. In order to use this tool, you need to buy a license, however trial version is provided.

Once scan is completed results can be shown in two different ways depending on host or on vulnerability type and results can be exported as HTML, PDF or CSV. [3]

We have installed trial version for testing purpose and after testing more than 50 URL we have come with below results;

- User interface as below figure



Sev	Name
MEDIUM	Web Application Potentially Vulnerable to Clickjacking
MEDIUM	ASP.NET DEBUG Method Enabled
LOW	Web Server Transmits Cleartext Credentials
INFO	Nessus SYN scanner

Fig.3: Nessus Web Interface

-

Configuration of targeted host is somehow easy to use with a lot of options where we can choose whether we want to scan host for open ports or just for web applications vulnerabilities.

- Generated report is providing description for all vulnerabilities occurred in scanning.
- Crawling doesn't show any information about targeted host like used technologies (ASP, PHP, ...) or server type (Apache, IIS, ...).
- We can scan full network subnet such as 192.168.1.0/24

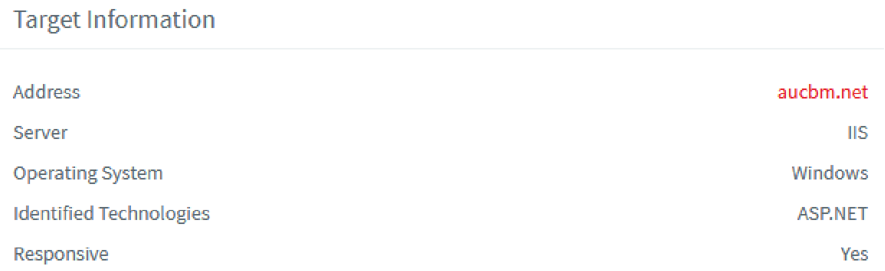
C. ACUNETIX

ACUNETIX is company which have developed tools to scan, analyze and mitigate web applications and websites. This tool mainly focuses on web related attacks such as SQL injection, XSS and more than 3000 type of vulnerabilities. [4]

It automatically crawls targeted web application and performs black box techniques. It works depending on three main criteria includes;

- Target specification: ACUNETIX checks targets and collect information regarding web technologies used, web server type (APACHE, IIS ...) and then response with proper filtering tests.

The figure below shows targeted URL specifications



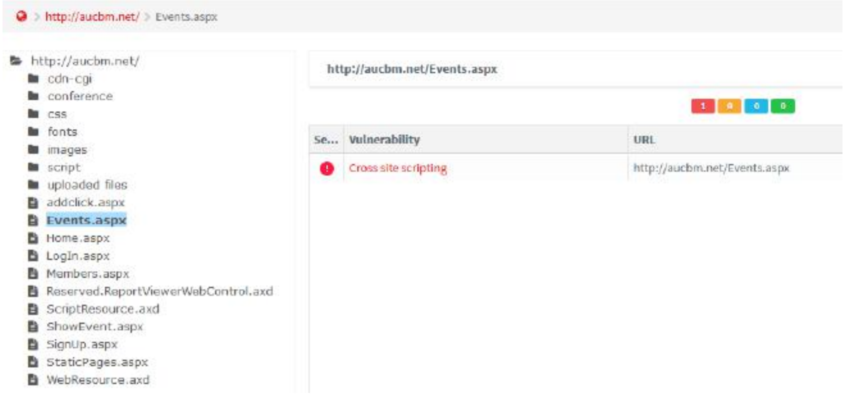
Target Information

Address	aucbm.net
Server	IIS
Operating System	Windows
Identified Technologies	ASP.NET
Responsive	Yes

Fig.4: ACUNTIX target specifications

- Site crawling and structure mapping: First the index file is located by URL, then specifying contained links, forms, input fields and client side scripts that build a list of directories and files inside the web application.

The figure below shows site structure



http://aucbm.net/ > Events.aspx

- http://aucbm.net/
  - cdn-cgi
  - conference
  - css
  - fonts
  - images
  - script
  - uploaded files
  - addclick.aspx
  - Events.aspx
  - Home.aspx
  - LogIn.aspx
  - Members.aspx
  - Reserved.ReportViewerWebControl.axd
  - ScriptResource.axd
  - ShowEvent.aspx
  - SignUp.aspx
  - StaticPages.aspx
  - WebResource.axd

http://aucbm.net/Events.aspx

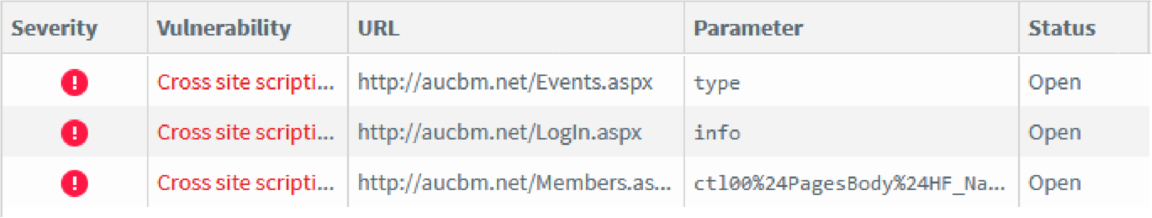
1 0 0 0

Se...	Vulnerability	URL
●	Cross site scripting	http://aucbm.net/Events.aspx

Fig.5: ACUNTIX targeted site structure

- Pattern analysis: This process is executed against targeted URL in order to detect any available threats or vulnerabilities.

The figure below shows discovered vulnerabilities



Severity	Vulnerability	URL	Parameter	Status
●	Cross site scripti...	http://aucbm.net/Events.aspx	type	Open
●	Cross site scripti...	http://aucbm.net/LogIn.aspx	info	Open
●	Cross site scripti...	http://aucbm.net/Members.as...	ctl00%24PagesBody%24HF_Na...	Open

Fig.6: ACUNTIX Discovered vulnerabilities

D. Tools Comparison

We have tried during our research to test main web scanners tools and we have come with below results on the basis of the vulnerabilities these tools detect.

Table 1: Vulnerabilities based comparison

Vulnerabilities	ACUNETIX	Nessus	Secure BAT
SQL Injection	√	√	√
Cross site Scripting	√	√	√
Improper Error Management	√	√	
Remote Code Execution	√	√	
Rogue Servers		√	

In the following table, we will find comparison on different bases such (Ease of use, response time, reporting)

Table.2: Performance based comparison.

Function	ACUNETIX	Nessus	Secure BAT
Ease of use	Very good	Fair	Good
Response time	Good	Weak	Good
Reporting	Very good	Good	Weak

V. CONCLUSION

Many kinds of techniques can be used to list the vulnerabilities present in web applications. Assessment of these vulnerabilities represents a significant role in securing business environment. No one tool can detect all kinds of vulnerabilities or providing easy environment to manage or even building different kinds or reports that supported by graphs.

In this research, we have focused on providing test bed to test different kinds of tools in order to show their capabilities and compare between it. There was another tool that we couldn't test it due to some limitation in providing proper test bed for that or due to license issue like NIKTO, BURPSUITE.

ACKNOWLEDGEMENTS

We would like to thank all people who help us especially our families.

REFERENCES

[1] OWASP, 1 October 2018. [Online]. Available: https://www.owasp.org/index.php/Main_Page.

[2] E. K. C. K. a. N. J. Stefan Kals, "SecuBat: A Web Vulnerability Scanner," International World Wide Web Conference Committee, pp. 247-256, 2006.

[3] Nessus. [Online]. Available: https://www.tenable.com/products/nessus/nessus-professional. [Accessed 1 10 2018].

[4] ACUNTIX. [Online]. Available: https://www.acunetix.com/. [Accessed 1 10 2018].

[5] C. Baojiang, L. Baolian and H. Tingting, "Reverse analysis method of static XSS defect detection technique based on database query language," in P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2014 Ninth International Conference on, 2014.