A Comparative Study of Pen Testing Tools

Mayur Turuvekere
Department of Computer Applications
Veermata Jijabai Technological Institute

Anala A. Pandit, PhD
Department of Computer Applications
Veermata Jijabai Technological Institute

ABSTRACT
It is a well-known fact that it is important and vital to the business to ensure data security. A business can have important information about it clients and customers, its vendors and the sales information which when put in wrong hands can be fatal for not only the business organization but also its various stakeholders. A penetration test, also known as a pen test, is a simulated cyberattack against any computer system to check for exploitable vulnerabilities. In the context of web application security, penetration testing makes a web application firewall more reliable and robust. Penetration testing tools are a part of a penetration test (Pen Test) to automate certain tasks, improve testing efficiency and discover issues that might be difficult to find using manual analysis techniques alone. There are various penetration testing tools available in the market that organizations use as per their requirement. This paper focuses on various attacks that are possible on a web application and comparison of various penetration tools to find best tools for penetration testing.

Keywords
Penetration test, web scanner, SQL injection, web vulnerabilities.

1. INTRODUCTION
Testing the security of web application is a very important thing. There are various ways of doing it. Following are the important types of testing: Black Box Penetration Testing, White Box Penetration Testing and Grey Box Testing [1]. One way to perform all types of testing is to use automatic penetration testing tools. These tools test the security by performing an attack, without malicious payload (i.e. they will not delete parts of the web application or the database it uses), against the web application that should be tested. The results of these tools shows the vulnerabilities if there are any so that they can be resolved.

The primary objective of the reported study is to evaluate various pen testing tools available and to find the best penetration-testing tool. Apart from the main objective, the quest is to find the answers to the following intermediate questions:

1. What are possible common attacks?

2. What penetration testing tools exist?

3. What vulnerabilities can these tools detect and what not?

This paper is structured as follows: Section 2 discusses on common vulnerabilities, Section 3 shows the comparison of various tools and finally Section 4 recommends the best tool based on comparison and tools recommended for specific purpose.

2. COMMON VULNERABILITIES

2.1 SQL Injection
SQL injection is a technique where an attacker executes malicious code to database and finds unauthorized ways of gaining access to the database [2]. This weakness is been used by the attacker to bypass authentication and authorization of the web application. Using SQL injection attacker can add, modify or delete the data affecting the data integrity [2].

Attackers can extract data from servers by exploiting in various ways. Common method are retrieving data based on errors, true or false conditions and timing. There are six SQL injection techniques: Boolean-based blind, time-based blind, UNION query-based, error-based, out-of-band and stacked queries [3].

Boolean-based blind*:* Sometimes, when an SQL query fails there is no visible error message on the page, making it difficult for an attacker to get information from the vulnerable application. Still there is a way to extract information. When an SQL query fails some part of web page may disappear or change or entire website can fail to load. These indications allows attackers to determine whether the input is vulnerable. Attackers can test for this by inserting a condition: https://example.com/index.php?id=1+AND+1=1. If the page loads as usual then it might be vulnerable to SQL injection. To be sure, attacker typically tries to provoke a false result using the condition https://example.com/index.php?id=1+AND+1=2. Since the condition is false page does not work as usual. This indicates that the page is vulnerable to an SQL injection. [4]

Time-based blind*:* In some cases, even though SQL query does not have any visible effect on the output, it may still be possible to extract information from the database. Hackers can determine this by instructing the database to sleep for an amount of time before responding. Hackers can use this type of code: https://example.com/index.php?id=1+AND+IF(version()+LIKE+'5%',sleep(3),false). If the page loads quickly then page is not vulnerable and if page loads slowly, it is vulnerable. [4]

Union-based is an in-band SQL injection technique that uses the UNION SQL operator to combine the results of two or more SELECT statements into a single result and then this result is returned as part of a response. [5]

Error-based is an in-band SQL injection technique that relies on errors thrown by the database to obtain the structure of the database. In some cases error-based alone is enough for an attacker to enumerate through whole database. [5]

Out-of-band techniques involve sending data directly from database server to attacker's machine. It occurs when attacker cannot use the same channel to launch attack and retrieve results. This relies on the server's ability to deliver data to the attacker for DNS or HTTP request. [5]

Stacked queries provides control to the attacker by terminating the original query and adding a new one. It is possible to modify data and call stored procedures. [6]

2.2 XPath Injection

XPath injection is similar to SQL injection. The difference is that the SQL injection attack takes place in a SQL database whereas XPath injection attack takes place in an xml file. XPath is a query language of XML file. Some websites use user-supplied information to construct an XPath query for XML data. Attacker can send intentionally malformed information to find out how the XML data is structured or access data. [7]

2.3 XSS

Cross-site scripting occurs when an attacker can input browser side script such as JavaScript, which executes when the user visits the site. An attacker can send malicious code to unsuspecting user. Browser has no way to know if the script can be trusted or not, hence, it will execute the script. Scripts can be simple as just displaying messages like alert ("XSS hack") or the attackers might use XSS to steal a user's cookie to impersonate the user on a website. [8]

2.4 Denial of Service

Denial of service attack means resources are blocked or be unavailable so that no one can access the resources. Resources become unavailable by manipulating network packets, logical or resources handling vulnerabilities. In DOS, a service receives a very large number of request due to which it may be blocked or be unavailable to normal users. Exploitation of programming vulnerability may also stop the service. [9]

2.5 Session Hijacking

The Session Hijacking attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the Web Server.

"The session token could be compromised in different ways; the most common are:

1. Predictable session token
2. Session Sniffing
3. Client side attacks
4. Man-in-the-middle attack
5. Man in the browser attack" [10]

Predictable Session token: In this attack, attacker focuses on prediction session ID that helps to bypass the authentication. Session ID values can be predicted by understanding the Session ID generation process. [11]

Session sniffing: In this, attacker uses the sniffer to capture a valid token i.e. Session ID and then gain unauthorized access. [12]

Client side attack*:* Attacker can compromise the session token by running malicious code on the client side like cross-site scripting. If an attacker sends a malicious JavaScript to the victim using a link and if the victim clicks on the link, JavaScript will run all the instructions made by the attacker. This JavaScript can contain codes like sending cookie information of current session to the attacker. [12]

Man-in-the-middle attack: intercepts a communication between two systems i.e. TCP connection between client and server. Once the connection is been, intercepted attacker can read and modify the data. The man-in-the-middle attack is very effective because of the data transfer are ASCII based. Therefore, it is possible to view and modify the data from the http protocol. [13]

Man-in-browser attack*:* It is same as Man-in-the middle attack, but in this case, Trojan horse is used. Trojan horse is been used to intercept and modify calls between application and security mechanisms. The common objective is to cause financial frauds. [14]

2.6 Heartbleed

Heartbleed bug allows the attacker to read the memory of the systems, protected by vulnerable version of OpenSSL software. The compromised secret key, which is been used to identify the service providers and encrypt the traffic, passwords of the users. This allows attackers to eavesdrop on communication and steal the data of the users.

The type of information which can be compromised are the secret keys used for our X.509 certificates, usernames and passwords, instant messages, emails and business critical documents and communication. [15]

2.7 Shellshock Bug

As some web server's deployments use bash for processing request, attackers can misuse it. Attackers can create vulnerable bash to execute arbitrary commands. This allows the attacker issue commands on the server remotely, which is also known as remote code execution.

"Many internet and network services such as web servers use environment variables to communicate with the server's operating system. Since the environment variables are not sanitized properly by Bash before being executed, the attacker can send commands to the server through HTTP requests and get them executed by the web server operating system." [16]

2.8 Cross-Site Tracing

It involves the use of Cross-site Scripting and the TRACE HTTP methods. TRACE allows the client to see what data is been received at the other end of the request and use that data for testing. So, this method can be used to steal user's cookie data via Cross-site-Scripting. [17]

Table 1. Comparison of Web Scanners

	Acunetix [20]	**Wapiti** [21]	**Arachni** [22]	**Burp Suite** [23]	**Netsparker** [24]
XSS	Y	Y	Y	Y	Y
Buffer overflow	Y				
Remote file inclusion	Y	Y	Y		Y
Local file inclusion	Y	Y		Y	Y
Command Injection	Y	Y	Y	Y	Y
Session Management	Y			Y	
XPath Injection	Y	Y	Y	Y	Y
LDAP Injection	Y	Y	Y	Y	Y
Cross Site Tracing	Y		Y		Y
Open SSL Heartbleed	Y				Y
Shellshock Bug	Y				Y
Error Based SQL Injection	Y	Y	Y	Y	Y
Blind/Time-Based SQL Injection	Y	Y	Y	Y	Y
Server Side Java Script (SSJS/NoSQL) Injection	Y		Y	Y	
Reflected Cross Site Scripting	Y	Y	Y	Y	Y
Persistent Cross Site Scripting	Y	Y		Y	Y
DOM Based Cross Site Scripting	Y		Y	Y	Y
Unrestricted File Upload	Y	Y	Y	Y	Y
Open Redirect	Y		Y	Y	Y
SMTP/IMAP/Email Injection	Y				
Server-Side Includes Injection	Y				

2.9 Local File Inclusion

It refers to an inclusion attack through which an attacker can include files on the web server by exploiting functionality that dynamically includes local files or script. Successful attack includes directory traversal and information disclosure. In Local file inclusion, an attacker can only include only local files and not remote files like in the case of Remote File Inclusion. [18]

3. COMPARISON OF TOOLS

There are various tools in the market nowadays, which can find most of the vulnerabilities. Some of the tools that are commonly used are Acunetix, Wapiti, Arachni, Burp Suite, Netsparker, Vega, sqlmap, ZAP [19]. Various tools were studied and it was found that the tools Acunetix, Wapiti, Arachni, Burp Suite and Netsparker were able to find most of the vulnerabilities. The comparison of these tools with respect to the various vulnerabilities is given in Table 1.

4. RECOMMENDED TOOLS

In website pen testing, we can have one tool to do the entire task or we can divide tools for specific purpose. We require tools for

1. Scanning Vulnerabilities
2. Capturing packets and extracting data from network
3. Penetration of database/storage [2]

As per the comparison table, it clearly states that Acunetix can find highest number of vulnerabilities. Therefore, Acunetix is a preferred tool to do the entire task. Combination of tools for various task can also give good results, as some tools are very good for specific purpose.

4.1 Recommended Tool for Scanning Vulnerabilities - Acunetix

Acunetix web scanner is a testing tool that audits web applications by checking for various vulnerabilities**.** Acunetix uses acusensor technology, which allows finding more vulnerabilities compared to traditional web scanners. It also shows where exactly in the code the vulnerability lies.

Acunetix alerts the user of web configuration problems, which can expose internal application details. For e.g. if custom errors are enabled in .net then it can expose sensitive application details to a malicious user.

Acusensor technology intercepts all web applications input and build a list of all combinations of input and test them. It can detect more SQL injection vulnerabilities than before. [25]

Acunetix features DeepScan Technology, which allows the scanner to robustly test any application. At the heart of DeepScan, is a fully automated web browser that can understand and interact with complex web technologies such as AJAX, SOAP/WSDL, SOAP/WCF, REST/WADL, XML, JSON, Google Web Toolkit (GWT) and CRUD operations just like a regular browser would.

This allows Acunetix to test web applications just as though it is running inside of a user's browser, allowing the scanner to seamlessly interact with complex controls just as a user would, significantly increasing the scanner's coverage of the web application. [26]

"Acunetix achieved the highest WIVET score of 94%. WIVET (Web Input Vector Extractor Teaser) is a project that measures how well a scanner is able to crawl an application, and how well can it locate input vectors by presenting a collection of challengers that contain links, parameters and input delivery methods that the crawling process should locate and extract." [27]

Table 2. WIVET Score of Web Application Scanner [27]

Rank	Detection Accuracy	Vulnerability Scanner
1	94%	Acunetix
2	91%	Netsparker
3	44%	Wapiti
4	19%	Arachni
5	16%	Burp Suite Professional

4.2 Recommended Tool for Capturing Packets – Burp Suite

It not only provides basic functionalities like proxy server, scanner and intruder but also provides advanced options like spider, a repeater, a decoder, an extender, a sequencer and a comparer.

It is an advanced automatic tool built for custom attacks on the applications. It improvises the speed and accuracy of manual testing.

This tool is commonly used for finding the vulnerabilities, extract sensitive data, and trying to exploit discovered vulnerabilities. It can perform various automatic modification of responses to improvise testing. E.g. unhide the hidden fields, enable the disabled fields.

Sometimes there is a necessity for custom modification of requests and responses, so Burp suite is capable of matching and replacing rules as and when required. User can create rules for headers, body, request parameters and the URL file path.

It supports invisible proxying for non-proxy-aware clients, enabling the testing of non-standard user agents such as thick client applications and some mobile applications. [28]

4.3 Recommended Tool for Penetration Testing of Database/Storage – SQLMap

It is an open source tool. It automates the process of detecting and exploiting the SQL injection flaws.

Following are the reasons why SQLMap is good for testing the db.

- It has support for almost all the database like MySQL, MSSQL, SQLite, Oracle, Firebird, Sybase, SAP MaxDB and PostgreSQL. SQL injection technique supported are Boolean-based blind, time-based blind, error-based, UNION query-based, stacked queries and out-of-band.
- SQLMap can enumerate through users, password hashes, roles, databases. It also recognizes password hash formats and crack them using a dictionary-based attack.
- It is very flexible in manipulating the data. It can delete the table entirely or specific entries or specific columns according to the choice of the user. It can also delete a range of characters from each columns entry.
- It has support to search for specific database names and tables from all databases. It is useful in conditions where identifying columns, which contains credentials like username and password. If the database is MySQL, PostgreSQL or Microsoft SQL Server user can download and upload any file from/to the database.
- It is useful in executing arbitrary commands and get the output from the database for databases like MySQL, PostgreSQL or MSSQL. It can establish a stateful TCP connection between the attacker and the database so that the channel act as an interactive command prompt or a graphical user interface session according to the choice of the user. [3]

5. CONCLUSION

There are several reasons for spending money, time, and effort on data protection. The primary one is to protect the sensitive data from falling into wrong hands and indirectly minimizing financial loss, followed by compliance with regulatory requirements, maintaining high levels of productivity, and meeting customer expectations. Data is an important asset of the organization that needs to safe from being into wrong hands. Just conducting a Pen Test is not enough. Choosing the best test tailor made for the organization is vital for its sustainability.

This paper proposes the best tool for web pen testing, based on the comparison given above, which is Acunetix with its features and specific tools for specific purposes.

Future work is to find more vulnerabilities that are critical and to build a common open source tool based on those vulnerabilities, which will be free to use.

6. REFERENCES

[1]. Pentesting on Web Applications using Ethical Hacking- Rina Elizabeth Lopez de Jimenez, Escuela de Computacion,Itca-Fepade,Santa Tecla, EI Salvador

[2]. Testing Techniques and Analysis of SQL Injection Attacks 2017 - 2nd International Conference on Knowledge Engineering and Applications.

[3]. Sqlmap: automatic SQL injection and database takeover tool (2018, May 19). [Online] Available: http://sqlmap.org/

[4]. What is SQL Injection & How to Prevent it | Netsparker - (2018, June 5). [Online] Available: https://www.netsparker.com/blog/web-security/sql-injection-vulnerability/

[5]. Types of SQL Injection? - (2018, June 5). [Online] Available: https://www.acunetix.com/websitesecurity/sql-injection2/

[6]. Stacked Queries - SQL Injection Attacks - (2018, June 5). [Online] Available: http://www.sqlinjection.net/stacked-queries/

[7]. XPATH Injection – OWASP (2018, May 19). [Online] Available: https://www.owasp.org/index.php/XPATH_Injection

[8]. Cross-site Scripting (XSS) – OWASP (2018, May 19). [Online] Available: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

[9]. Denial of Service - OWASP - (2018, June 5). [Online] Available: https://www.owasp.org/index.php/Denial_of_Service

[10]. Session hijacking attack - OWASP (2018, May 19). [Online] Available: https://www.owasp.org/index.php/Session_hijacking_attack

[11]. Session Prediction – OWASP - (2018, June 5). [Online] Available: https://www.owasp.org/index.php/Session_Prediction

[12]. Session hijacking attack – OWASP - (2018, June 5). [Online] Available: https://www.owasp.org/index.php/Session_hijacking_attack

[13]. Man-in-the-middle attack - OWASP- (2018, June 5). [Online] Available: https://www.owasp.org/index.php/Man-in-the-middle_attack

[14]. Man-in-the-browser attack – OWASP - (2018, June 5). [Online] Available: https://www.owasp.org/index.php/Man-in-the-browser_attack

[15]. Heartbleed Bug- OWASP (2018, May 19). [Online] Available: http://heartbleed.com/

[16]. Shellshock "Bash Bug" Vulnerability Explained | Netsparker (2018, May 19). [Online] Available: https://www.netsparker.com/blog/web-security/cve-2014-6271-shellshock-bash-vulnerability-scan/

[17]. Cross Site Tracing – OWASP - (2018, June 06). [Online] Available: https://www.owasp.org/index.php/Cross_Site_Tracing

[18]. What is Local File Inclusion (LFI)? – Acunetix - (2018, June 06). [Online] Available: https://www.acunetix.com/blog/articles/local-file-inclusion-lfi/

[19]. Category: Vulnerability Scanning Tools - OWASP (2018, May 19). [Online] Available: https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools

[20]. Acunetix- (2018, June 4). [Online] Available: https://www.acunetix.com/vulnerabilities/web/

[21]. Wapiti - Web Application Vulnerability Scanner v2.3.0 (2018, May 19). [Online] Available: https://www.darknet.org.uk/2015/05/wapiti-web-application-vulnerability-scanner-v2-3-0/

[22]. Crawl coverage and vulnerability detection - Arachni - Web Application Security Scanner Framework (2018, May 19). [Online] Available: http://www.arachni-scanner.com/features/framework/crawl-coverage-vulnerability-detection/

[23]. Issue Definitions (2018, May 19). [Online] Available: https://portswigger.net/kb/issues

[24]. Web Vulnerability & Security Checks | Netsparker (2018, May 19). [Online] Available: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/

[25]. Acunetix Vulnerability Scanner: Web Application Security (2018, May 19). [Online] Available: https://www.acunetix.com/vulnerability-scanner/

[26]. Highest Crawl & Analysis Rate for HTML5 JavaScript Security - (2018, June 4). [Online] Available: https://www.acunetix.com/vulnerability-scanner/javascript-html5-security/

[27]. How Acunetix Compares With Other Web Application Scanners - (2018, June 4). [Online] Available: https://www.acunetix.com/blog/news/acunetix-comparison-web-application-scanners/

[28]. Burp Suite Scanner | PortSwigger - (2018, May 19). [Online] Available: https://portswigger.net/burp