APPROACHES, TOOLS AND TECHNIQUES FOR SECURITY TESTING

(/con

INTRODUCTION TO SECURITY TESTING

Security testing is a process that is performed with the intention of revealing flaws in security mechanisms and finding the vulnerabilities or weaknesses of software applications. Recent security breaches of systems at retailers like Target (http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data) and Home Depot (http://www.cbsnews.com/news/56-million-accounts-at-risk-in-home-depot-hack/), as well as Apple Pay competitor Current C (http://www.dispatch.com/content/stories/business/2014/11/03/contactless-payment-system-hacked.html), underscore the importance of ensuring that your security testing efforts are up to date.

The prime objective of security testing is to find out how vulnerable a system may be and to determine whether its data and resources are protected from potential intruders. Online transactions have increased rapidly of late making security testing as one of the most critical areas of testing for such web applications. Security testing is more effective in identifying potential vulnerabilities when performed regularly.

Normally, security testing has the following attributes:

- Authentication
- Authorization
- Confidentiality
- Availability
- Integrity
- Non-repudiation
- Resilience

WHY SECURITY TESTING

System testing, in the current scenario, is a must to identify and address web application security vulnerabilities to avoid any of the following:

- Loss of customer trust.
- Disturbance to your online means of revenue generation/collection.

- Website downtime, time loss and expenditures in recovering from damage (reinstalling services, restoring backups, etc.)
- Cost associated with securing web applications against future attacks.
- Related legal implications and fees for having lax security measures in place.

CLASSES OF THREATS

Here are the different types of threats which can be used to take advantage of security vulnerability.

Privilege Elevation

Privilege elevation is a class of attack where a hacker has an account on a system and uses it to increase his system privileges to a higher level than he/she was not meant to have. If successful, this type of attack can result in a hacker gaining privileges as high as root on a UNIX system. Once a hacker gains super-user privileges, he is able to run code with this level of privilege and the entire system is effectively compromised.

SQL Injection

SQL injection is the most common application layer attack technique used by hackers, in which malicious SQL statements are inserted into an entry field for execution. SQL injection attacks are very critical as an attacker can get critical information from the server database. It is a type of attack which takes the advantage of loopholes present in the implementation of web applications that allows a hacker to hack the system. To check the SQL injection we have to take care of input fields like text boxes, comments, etc. To prevent injections, special characters should be either properly handled or skipped from the input.

Unauthorized Data Access

One of the more popular types of attacks is gaining unauthorized access to data within an application. Data can be accessed on servers or on a network.

Unauthorized access includes:

- Unauthorized access to data via data-fetching operations
- Unauthorized access to reusable client authentication information by monitoring the access of others
- Unauthorized access to data by monitoring the access of others

URL Manipulation

URL manipulation is the process of manipulating the website URL query strings & capture of the important information by hackers. This happens when the application uses the HTTP GET method to pass information between the client and the server. The information is passed in parameters in the query string. The tester can modify a parameter value in the query string to check if the server accepts it.

Denial of Service

A denial-of-service (DoS) attack is an explicit attempt to make a machine or network resource unavailable to its legitimate users. Applications can also be attacked in ways that render the application, and sometimes the entire machine, unusable.

Data Manipulation

In data manipulation, a hacker changes data used by a website in order to gain some advantage or to embarrass the website's owners. Hackers will often gain access to HTML pages and change them to be satirical or offensive.

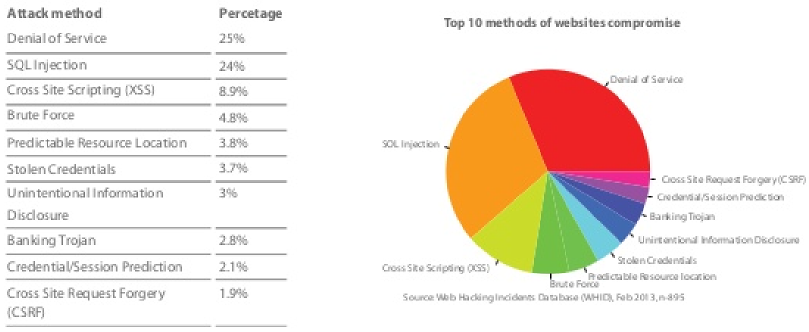
Identity Spoofing

Identity spoofing is a technique where a hacker uses the credentials of a legitimate user or device to launch attacks against network hosts, steal data or bypass access controls. Preventing this attack requires IT-infrastructure and network-level mitigations.

Cross-Site Scripting (XSS)

Cross-site scripting is a computer security vulnerability (http://en.wikipedia.org/wiki/Vulnerability_%28computer_science%29)found in web applications. XSS enables attackers to inject client-side script (http://en.wikipedia.org/wiki/Client-side_script) into Web pages (http://en.wikipedia.org/wiki/Web_page) viewed by other users and trick a user into clicking on that URL. Once executed by the other user's browser, this code could then perform actions such as completely changing the behavior of the website, stealing personal data, or performing actions on behalf of the user.

All of the attacks listed above are most critical threat classes but these are not all.



Attack method	Percetage
Denial of Service	25%
SQL Injection	24%
Cross Site Scripting (XSS)	8.9%
Brute Force	4.8%
Predictable Resource Location	3.8%
Stolen Credentials	3.7%
Unintentional Information Disclosure	3%
Banking Trojan	2.8%
Credential/Session Prediction	2.1%
Cross Site Request Forgery (CSRF)	1.9%

Top 10 methods of websites compromise

Source: Web Hacking Incidents Database (WHID), Feb 2013, n-895

(http://www.3pillarglobal.com/wp-content/uploads/2014/10/security-testing.png)

SECURITY TESTING TECHNIQUES

To prevent all of the above security testing threats/flaws and perform security testing on a web application, it is required to have good knowledge of the HTTP protocol and an understanding of client (browser) – server communication through HTTP. Also, basic knowledge of SQL injection and XSS is required. The following techniques will help in performing quality security testing:

Cross Site Scripting (XSS):

The tester should additionally check the web application for XSS (Cross site scripting). Any HTML e.g. <HTML> or any script e.g. <SCRIPT> should not be accepted by the application. If it is, the application can be prone to an attack by Cross Site Scripting.

Attackers can use this method to execute malicious scripts or URLs on a victim's browser. Using cross-site scripting attackers can use scripts like JavaScript to steal user cookies and information stored in the cookies.

Cross Site Scripting Testing can be done for:

1. Apostrophe
2. Greater-Than Sign
3. Less-Than Sign

Ethical Hacking

Ethical hacking means hacking performed by a company or individual to help identify potential threats on a computer or network. An ethical hacker attempts to bypass the system security and search for any vulnerability that could be exploited by malicious hackers aka Black hats. White hats may suggest changes to systems that make them less likely to be penetrated by black hats.

Password Cracking

Password cracking is the most critical part while doing system testing. In order to access the private areas of an application, hackers can use a password cracking tool or can guess a common username/password. Common usernames and passwords are easily available online along with open source password cracking applications. Until a web application enforces a complex password (e.g. a long password with a combination of numbers, letters, and special characters), it is easy to crack the username and password. Another way of cracking the password is if username/password is to target cookies if cookies are stored without encryption.

Penetration Testing

A penetration test is an attack on a computer system with the intention of finding security loopholes, potentially gaining access to it, its functionality and data.

Risk Assessment

This is a process of assessing and deciding on the risk involved with the type of loss and the possibility of vulnerability occurrence. This is determined within the organization by various interviews, discussions and analysis.

Security Auditing

A security audit is a systematic evaluation of the security of a company's information system by measuring how well it conforms to a set of established criteria.

Security Scanning

This is a program which communicates with a web application through the web front-end in order to identify potential security vulnerabilities in the web application, OS and Networks.

SQL Injection:

The next thing that should be checked is SQL injection. Entering a single quote (') in any textbox should be rejected by the application. Instead, if the tester encounters a database error, it means that the user input is inserted in some query which is then executed by the application. In such a case, the application is vulnerable to SQL injection.

SQL injection attacks are very critical as attackers can get vital information from the server database. To check SQL injection entry points into your web application, find out code from your code base where direct MySQL queries are executed on the database by accepting some user inputs.

SQL Injection Testing can be done for:

- Apostrophes
- Brackets
- Commas
- Quotation marks

Vulnerability Scanning

The automated computer program to proactively identify security vulnerabilities of computing systems in a network to determine where a system can be exploited and/or threatened.

Posture Assessment

This describes the overall security posture of an organization; it is a combination of Ethical hacking, Security scanning and Risk Assessment.

URL manipulation through HTTP GET methods:

HTTP GET method is used between application client and server to pass on the information. The tester needs to verify if the application is passing vital information in the query string. The information via HTTP is passed in parameters in the query string. To test this, a parameter value can be modified in the query string to check if the server accepts it.

Generally user information is passed through HTTP GET request to the server for either authentication or fetching data. Hackers can manipulate the input of this GET request to the server so that the required information can be gathered or to corrupt the data. Any abrupt behavior of application or web server, in such condition, is the key for a hacker to slip into the application.

Ad hoc Data Testing can also be done as a part of security testing:

- Testing random data which is included in requests.
- Testing random data which is included as parameters.
- Testing encoded random data included as parameters.

Buffer Overflow Testing

- Boundary value testing on Lengths of strings e.g. 128 bytes, 256 bytes, 1024 bytes
- Long strings of a single character
- Varied string patterns

SECURITY TESTING APPROACH:

We can take the following approach while preparing and planning for Security testing:

- Security Architecture Study: The first step is to understand the business requirements, security goals, and objectives in terms of the security compliance of the organization. The test planning should consider all security factors, like the organization might have planned to achieve PCI compliance (https://www.pcisecuritystandards.org/).
- Security Architecture Analysis: Understand and analyze the requirements of the application under test.
- Classify Security Testing: Collect all system setup information used for development of Software and Networks like Operating Systems, technology, hardware. Make out the list of Vulnerabilities and Security Risks.
- Threat Modelling: Based on above step, prepare Threat profile.
- Test Planning: Based on identified Threat, Vulnerabilities and Security Risks prepare test plan to address these issues.
- Traceability Matrix Preparation: For each identified Threat, Vulnerabilities and Security Risks prepare Traceability Matrix.
- Security Testing Tool identification: All security testing cannot be executed manually, so identify the tool to execute all security test cases faster & more reliably.
- Test Case Preparation: Prepare the Security tests case document.
- Test Case Execution: Perform the Security Test cases execution and retest the defect fixes. Execute the Regression Test cases.
- Reports: Prepare detailed report of Security Testing which contains Vulnerabilities and Threats contained, detailing risks, and still open issues etc.

SECURITY TEST TOOLS

These are just a few of the security testing tools available for web applications.

Tools	Description	Requirement

BeEF	BeEF (Browser Exploitation Framework) is a tool which focuses on the web browser – this means it takes advantage of the fact that an open web-browser is the crack into a target system and designs its attacks to go on from this point onwards.	Linux, Apple Mac OS X and Microsoft Windows
BFBTester – Brute Force Binary Tester	BFBTester is a tool for security checks of binary programs. BFBTester will perform checks of single and multiple argument command line overflows and environment variable overflows. This tool alerts the security professional for any programs using unsafe tempfile names by watching for tempfile creation activity.	POSIX, BSD, FreeBSD, OpenBSD, Linux
Brakeman	Brakeman is an open source vulnerability scanner which is designed for Ruby on Rails applications. It statically analyzes Rails application code to find security issues at any stage of development.	Rails 3
CROSS	The CROSS (Codenomicon Robust Open Source Software) program is designed to help open source projects, that are part of the infrastructure of the internet, fix critical flaws in their code. Codenomicon's product line is a suite of network protocol testing tools called DEFENSICS which helps the projects find and fix a large number of critical flaws very rapidly.	130 protocol interfaces and formats
Ettercap	Ettercap is a free and open source network security tool for man-in-the-middle attacks (MITM) on LAN. The security tool can be used to analyze computer network protocols within a security auditing context.	
Flawfinder	Program that scans C/C++ source code and reports potential security flaws. By default, it sorts its reports by risk level.	Python 1.5 or greater
Gendarme	Gendarme is an extensible rule-based tool to find problems in .NET applications and libraries. Gendarme inspects programs and libraries that contain code in ECMA CIL format (Mono and .NET) and looks for common problems with the code, problems that compilers do not typically check or have not historically checked.	.NET (Mono or MS runtime)
Knock Subdomain Scan	Knock is an effective scanning tool to scan Transfer Zone discovery, subdomains, Wildcard testing with internal or external wordlist. This tool can be very helpful in black box penetration test to find vulnerable subdomains.	Linux, Windows and MAC OS X with Python version 2.x
Metasploit	The Metasploit Framework is an advanced open-source platform for developing, testing, and using exploit code. This project initially started off as a portable network game and has evolved into a powerful tool for penetration testing, exploit development, and vulnerability research.	Win32 / UNIX
Nessus	The Nessus vulnerability scanner is the world-leader in active scanners, featuring high speed discovery, configuration auditing, asset profiling, sensitive data discovery and vulnerability analysis of your security posture. Nessus scanners can be distributed throughout an entire enterprise, inside DMZs, and across physically separate networks.	Linux, Solaris, Mac, Windows
Nikto	Nikto is an open source web server scanner that caters to web servers specially to detect outdated software configurations, invalid data and/or CGIs etc. It performs comprehensive tests multiple times against web servers.	Windows/UNIX
Nmap	Nmap (Network Mapper) is an open source scanner for network discovery and security auditing. Nmap uses raw IP packets to determine available hosts on the network, what services (app name, version) those hosts are offering, what operating systems and OS versions they are running on, what type of packet filters/firewalls are in use, and other such characteristics.	Linux, Windows, and Mac OS X.
nsiqcppstyle	nsiqcppstyle is aiming to provide an extensible, easy to use, highly maintainable coding style checker for C/C++ source code. The rules and analysis engine are separated and users can develop their own C/C++ coding style rules. Furthermore, there is a customizable rule server as well.	Platform Independent
Oedipus	Oedipus is an open source web application security analysis and testing suite written in Ruby. It is capable of parsing different types of log files off-line and identifying security vulnerabilities. Using the analyzed information, Oedipus can dynamically test web sites for application and web server vulnerabilities.	OS Independent
Zed Attack Proxy	The Zed Attack Proxy (ZAP) is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications. It is designed to be used by people with a wide range of security experience and as such is ideal for developers and functional testers who are new to penetration testing.	Windows, Linux, Mac OS
Paros	Paros is a Java based HTTP/HTTPS proxy for assessing web application vulnerability. All HTTP and HTTPS data between server and client, including cookies and form fields, can be intercepted and modified using this scanners.	Cross-platform, Java JRE/JDK 1.4.2 or above
Social Engineer Toolkit	The Social-Engineer Toolkit (SET) is an open source tool and the concept that it is based on is that attacks are targeted at the human element than on the system element. It enables you to send emails, java applets etc. containing the attack code.	Linux, Apple Mac OS X and Microsoft Windows
Skipfish	Skipfish is an active web application vulnerability security scanning tool. Security professionals use this tool to scan their own sites for vulnerabilities. Reports generated by the tool are meant to serve as a foundation for professional web application security assessments.	Linux, FreeBSD, MacOS X, and Windows
Vega	Vega is a GUI-based, multi-platform and open source web security tool which is used to find instances of SQL injection, cross-site scripting (XSS), and other vulnerabilities in web applications. Vega also includes an intercepting proxy for interactive web application debugging. Vega attack modules are written in JavaScript, users can easily modify them or write their own.	Java, Linux, Windows.