Sinhgad Institutes

DEPARTMENT OF COMPUTER ENGINEERING
SKN SINHGAD INSTITUTE OF TECHNOLOGY AND SCIENCE,

LONAVALA-410401

Savitribai Phule Pune University, Pune

2021-22

Case Study No.5

Cloud Security Tool : Acunetix

Name : - Rathod Akshay Raju

Class :- TE

Division :- B

Roll No. :- 20CETB28

PRN No. :- 72175915h

Acunetix

Introduction to Acunetix :- Why You Need To Secure Your Web Applications

Website security is today's most overlooked aspect of securing an enterprise and should be a priority in any organization. Increasingly, hackers are concentrating their efforts on web-based applications – shopping carts, forms, login pages, dynamic content, etc. Accessible 24/7 from anywhere in the world, insecure web applications provide easy access to backend corporate databases and also allow hackers to perform illegal activities using the attacked sites. A victim's website can be used to launch criminal activities such as hosting phishing sites or to transfer illicit content, while abusing the website's bandwidth and making its owner liable for these unlawful acts.

Hackers already have a wide repertoire of attacks that they regularly launch against organizations including SQL Injection, Cross Site Scripting, Directory Traversal Attacks, Parameter Manipulation (e.g., URL, Cookie, HTTP headers, web forms), Authentication Attacks, Directory Enumeration and other exploits.

The hacking community is also very close-knit; newly discovered web application intrusions, known as Zero Day exploits, are posted on a number of forums and websites known only to members of that exclusive underground group. Postings are updated daily and are used to propagate and facilitate further hacking.

Web applications – shopping carts, forms, login pages, dynamic content, and other bespoke applications – are designed to allow your website visitors to retrieve and submit dynamic content including varying levels of personal and sensitive data.

If these web applications are not secure, then your entire database of sensitive information is at serious risk. A Gartner Group study reveals that 75% of cyberattacks are done at the web application level .

Why are web applications vulnerable?

- Websites and web applications are easily available via the internet 24 hours a day, 7 days a week to customers, employees, suppliers and therefore also hackers.
- Firewalls and SSL provide no protection against web application hacking, simply because access to the website has to be made public.
- Web applications often have direct access to backend data such as customer databases.
- Most web applications are custom-made and, therefore, involve a lesser degree of testing than off-the-shelf software. Consequently, custom applications are more susceptible to attack.
- Various high-profile hacking attacks have proven that web application security remains the most critical. If your web applications are compromised, hackers will have complete access to your backend data even though your firewall is configured correctly and your operating system and applications are patched repeatedly.
- Network security defense provides no protection against web application attacks since these are launched on port 80 which has to remain open to allow regular operation of the business. It is therefore imperative that you regularly and consistently audit your web applications for exploitable vulnerabilities.

✞ The need for automated web application security scanning

Manual vulnerability auditing of all your web applications is complex and timeconsuming, since it generally involves processing a large volume of data. It also demands a high level of expertise and the ability to keep track of considerable volumes of code used in a web application. In addition, hackers are constantly finding new ways to exploit your web application, which means that you would have to constantly monitor the security communities, and find new vulnerabilities in your web application code before hackers discover them.

Automated vulnerability scanning allows you to focus on the already challenging task of building a web application. An automated web application scanner is always on the lookout for new attack paths that hackers can use to access your web application or the data behind it.

Within minutes, an automated web application scanner can scan your web application, identify all the files accessible from the internet and simulate hacker activity in order to identify vulnerable components.

In addition, an automated vulnerability scanner can also be used to assess the code which makes up a web application, allowing it to identify potential vulnerabilities which might not be obvious from the internet, but still exist in the web application, and can thus still be exploited.

Acunetix Vulnerability Management

Acunetix is an automated web application security testing tool that audits your web applications by checking for vulnerabilities like SQL Injection, Cross site scripting and other exploitable vulnerabilities. In general, Acunetix scans any website or web application that is accessible via a web browser and uses the HTTP/HTTPS protocol.

Acunetix offers a strong and unique solution for analyzing off-the-shelf and custom web applications including those utilizing JavaScript, AJAX and Web 2.0 web applications. Acunetix has an advanced crawler that can find almost any file. This is important since what is not found cannot be checked.

How Acunetix Works

Acunetix works in the following manner:

1. Acunetix DeepScan analyses the entire website by following all the links on the site, including links which are dynamically constructed using JavaScript, and links found in robots.txt and sitemap.xml (if available). The result is a map of the site, which Acunetix will use to launch targeted checks against each part of the site.

Acunetix AcuSensor Technology

Acunetix' unique AcuSensor Technology allows you to identify more vulnerabilities than other Web Application Scanners, whilst generating less false positives. Acunetix AcuSensor indicates exactly where in your code the vulnerability is and reports additional debug information.

The increased accuracy, available for PHP, .NET and JAVA web applications, is achieved by combining black box scanning techniques with feedback from sensors placed inside the source code. Black box scanning does not know how the application reacts and source code analyzers do not understand how the application will behave while it is being attacked. AcuSensor technology combines both techniques to achieve significantly better results than using source code analyzers and black box scanning independently.

AcuSensor can be installed in .NET, PHP and JAVA code transparently.

AcuSensor can be installed into pre-compiled .NET and JAVA assemblies, even if they are signed (strong-named), therefore, neither .NET or JAVA source code, nor a compiler (or any other dependencies) are required. In case of PHP web applications, the source is readily available. To date, Acunetix is the only web vulnerability security solution to implement this technology.

Advantages of using AcuSensor Technology

- Allows you to locate and fix the vulnerability faster because of the ability to provide more information about the vulnerability, such as source code line number, stack trace, affected SQL query, etc.
- Significantly reduces false positives when scanning a website because it understands the behavior of the web application better.
- Alerts you to web application configuration problems which can result in a security misconfiguration, or expose sensitive information. E.g. If 'custom errors' are enabled in .NET, this could expose sensitive application details to a malicious user.
- Advises you how to better secure your web server settings, e.g. if write access is enabled on the web server.
- Detects more SQL injection vulnerabilities. Previously SQL injection vulnerabilities could only be found if database errors were reported, whereas now the source code can be analyzed for improved detection.
- Ability to detect SQL injection vulnerabilities in all SQL statements, including in SQL INSERT statements. Using a black box scanner such SQL injection vulnerabilities cannot be found. This significantly increases the ability for Acunetix to find vulnerabilities.
- Scans run using AcuSensor run a back-end crawl, presenting all files accessible through the web server to the scanner; even if these files are not linked through the front-end application. This ensures 100% coverage of the application, and alerts users of any backdoor files that might have been maliciously uploaded by an attacker.
- AcuSensor Technology is able to intercept all web application inputs and build a comprehensive list with all possible inputs in the website and test them.
- Ability to test for arbitrary file creation and deletion vulnerabilities. E.g. Through a vulnerable script a malicious user can create a file in the web application directory and execute it to have privileged access, or delete sensitive web application files.

Network Vulnerability Scanning

In Acunetix Premium as part of a website audit, the online version of Acunetix will execute a network security audit of the server hosting the website. This network security scan will identify any services running on the scanned server by running a port scan on the system. Acunetix will report the operating system and the software hosting the services detected. This process will also identify Trojans which might be lurking on the server.

The network vulnerability scan assesses the security of popular protocols such as FTP, DNS, SMTP, IMAP, POP3, SSH, SNMP and Telnet. Apart from testing for weak or default passwords, Acunetix will also check for misconfiguration in the services detected which could lead to a security breach. Acunetix will also check that any other servers running on the machine are not using any deprecated protocols. All these lead to an insecure system, which would allow an intruder to damage your web site and your reputation.