Mohd. Aftab Alam
02013302717

INTRODUCTION

Aim :

Introduction to Web Security.

Theory :

Web Security is also known as "Cybersecurity". It basically means protecting a website or web application by detecting, preventing and responding to cyber threats. Websites and web applications are just as prone to security breaches as physical homes, stores, and government locations. Unfortunately, cybercrime happens every day, and great web security measures are needed to protect websites and web applications from becoming compromised.

That's exactly what web security does – it is a system of protection measures and protocols that can protect your website or web application from being hacked or entered by unauthorized personnel. This integral division of Information Security is vital to the protection of websites, web applications, and web services. Anything that is applied over the Internet should have some form of web security to protect it.

Web application security is a central component of any web-based business. The global nature of the Internet exposes web properties to attack from different locations and various levels of scale and complexity. Web application security deals specifically with the security surrounding websites, web applications and web services such as APIs.

The majority of web application attacks occur through cross-site scripting (XSS) and SQL injection attacks which typically are made possible by flawed coding and failure to sanitize application inputs and outputs. These attacks are ranked in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors.

Common Web Security Vulnerabilities

Your website or web application's security depends on the level of protection tools that have been equipped and tested on it. There are a few major threats to security which are the most common ways in which a website or web application becomes hacked. Some of the top vulnerabilities for all web-based services include :

1. Cross Site Scripting (XSS)

XSS is a vulnerability that allows an attacker to inject client-side scripts into a webpage in order to access important information directly, impersonate the user, or trick the user into revealing important information.

2. SQL Injection (SQi)

SQi is a method by which an attacker exploits vulnerabilities in the way a database executes search queries. Attackers use SQi to gain access to unauthorized information, modify or create new user permissions, or otherwise manipulate or destroy sensitive data.

3. Denial of Service (DoS) & Distributed Denial of Service (DDoS) Attacks

Through a variety of vectors, attackers are able to overload a targeted server or its surrounding infrastructure with different types of attack traffic. When a server is no longer able to effectively process incoming requests, it begins to behave sluggishly and eventually deny service to incoming requests from legitimate users.

4. Memory Corruption

Memory Corruption occurs when a location in memory is unintentionally modified, resulting in the potential for unexpected behaviour in the software. Bad actors will attempt to sniff out and exploit memory corruption through exploits such as code injections or buffer overflow attacks.

5. Buffer Overflow

Buffer Overflow is an anomaly that occurs when software writing data to a defined space in memory known as a buffer. Overflowing the buffer’s capacity results in adjacent memory locations being overwritten with data. This behaviour can be exploited to inject malicious code into memory, potentially creating a vulnerability in the targeted machine.

6. Cross Site Request Forgery (CSRF)

Cross Site Request Forgery involves tricking a victim into making a request that utilizes their authentication or authorization. By leveraging the account privileges of a user, an attacker is able to send a request masquerading as the user. Once a user’s account has been compromised, the attacker can exfiltrate, destroy or modify important information. Highly privileged accounts such as administrators or executives are commonly targeted.

7. Data Breach

Different than specific attack vectors, a data breach is a general term referring to the release of sensitive or confidential information, and can occur through malicious actions or by mistake. The scope of what is considered a data breach is fairly wide, and may consist of a few highly valuable records all the way up to millions of exposed user accounts.

Strategies to Mitigate Vulnerabilities

Important steps in protecting web apps from exploitation include using up-to-date encryption, requiring proper authentication, continuously patching discovered vulnerabilities, and having good software development hygiene. The reality is that clever attackers may be able to find vulnerabilities even in a fairly robust security environment, and a holistic security strategy is recommended.

1. Resource Assignment

By assigning all necessary resources to causes that are dedicated to alerting the developer about new web security issues and threats, the developer can receive a constant and updated alert system that will help them detect and eradicate any threats before security is officially breached.

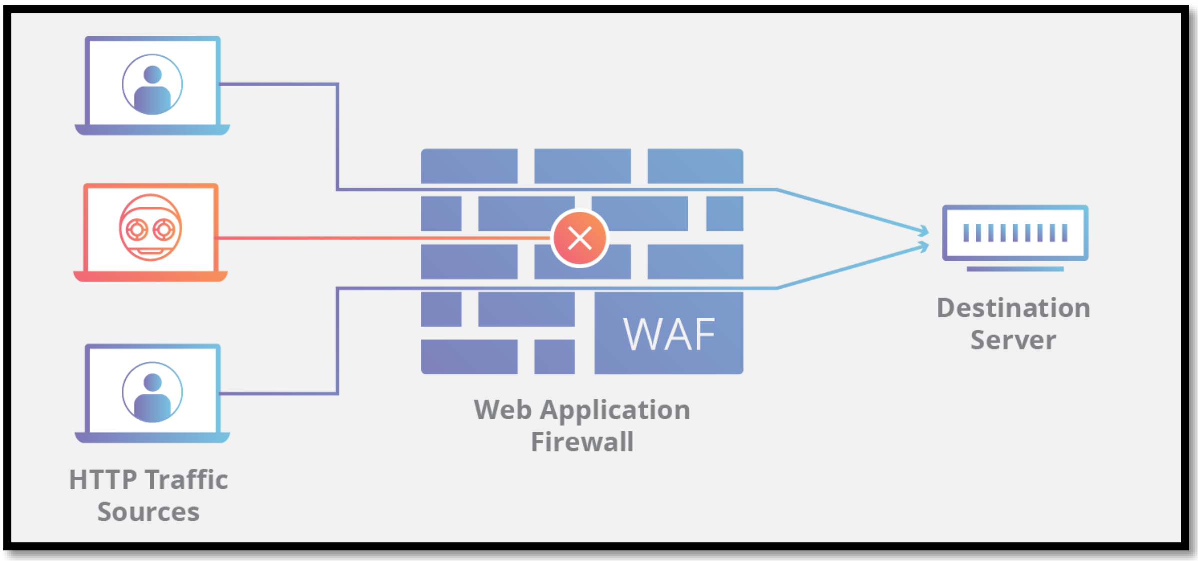
2. Web Scanning

There are several web scanning solutions already in existence that are available for purchase or download. These solutions, however, are only good for known vulnerability threats – seeking unknown threats can be much more complicated. This method can protect against many breaches, however, and is proven to keep websites safe in the long run.

Mohd. Aftab Alam
02013302717

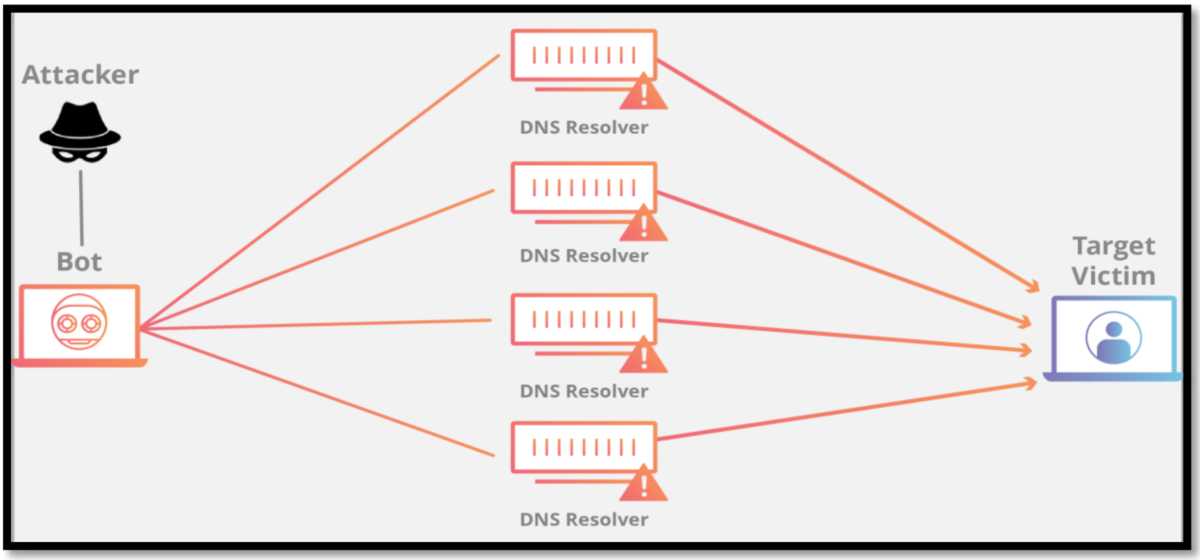
3. WAF – Protected Against Application Layer Attacks

A web application firewall helps protect a web application against malicious HTTP traffic. By placing a filtration barrier between the targeted server and the attacker, the WAF is able to protect against attacks like cross site request forgery (CSRF), cross site scripting (XSS) and SQL injection (SQi).



4. DDoS Mitigation

A Commonly used method for disrupting a web application is the use of distributed denial-of-service or DDoS attacks. It mitigates DDoS attacks through a variety of strategies including dropping volumetric attack traffic at the edge, and using Anycast network to properly route legitimate requests without a loss of service.



5. DNS Security – DNSSEC Protection

The domain name system is the phonebook of the Internet and represents the way in which an Internet tool such as a web browser looks up the correct server. Bad actors will attempt to hijack this DNS request process through DNS cache poisoning, man-in-the-middle attacks and other methods of interfering with the DNS lookup lifecycle. If DNS is the phonebook of the Internet, then DNSSEC is unspoofable caller ID.