IT WS04 REVIEWER

Chapter 1

Vulnerability – a weakness which allows for an attack.

Attack – an action exploiting a vulnerability or making a threat.

Threat – any potential event that could harm an asset, malicious or otherwise. In other words, any bad things that can happen to your assets, is a threat.

Web Vulnerability

- A or web application weakness or misconfiguration in a website code that enables an attacker to gain some level of control of the site, and possibly the hosting server.
- Most vulnerabilities are exploited through automated means, such as vulnerability scanners and botnets.

ANOTOMY OF ATTACK

Survey and Access - Surveying and assessing of the future target are performed in parallel. The first step normally taken by an intruder is to survey the possible target to define and assess its characteristics.

Exploit and penetrate - Having assessed the potential target, the next move is to exploit and penetrate. If the network and host are completely protected, then the next platform for attack will be your application.

Escalate Privileges - After attackers managed to enter an application or network by injecting code into the application or creating an authenticating session with the operating system, They will immediately try to escalate privileges. In particular, they are looking for administrative rights that are offered by accounts that are members of the Administrators group. They 're just searching for the high degree of rights the local network account provides.

- **Maintain Access** - When an intruder has obtained access to a network, he takes steps to encourage future access and cover his or her tracks
- **Deny Service** - Attackers who are unable to get access also launch a denial-of-service attack to discourage anyone from using the device. For other attackers, their target from the beginning is the denial of service to the application

KINDS OF ATTACKS ARE WEB APPLICATIONS VULNERABLE TO

When Users Provide Information

- **Human Attacks**
  - Abuse of Storage
  - Sock Puppets
  - Defamation
  - Griefers, Troll and Prankster

- **Automated Attacks**
  - Worms and Viruses
  - Spam
  - Automated User Input

When Information is Provided to Users

- **Harvesting email addresses**
- **Flooding an email address**
- **Screen scraping**
- **Improper archiving**

In Other Cases

- **Denial of Service**
- **DNS attacks**

FIVE GOOD HABITS OF A SECURITY-CONSCIOUS DEVELOPER

- **Nothing is 100% secure.**
- **Never trust user input.**
- **Defense in depth is the only defense.**
- **Simpler is easier to secure.**
- **Peer review is critical to security.**

Chapter 2

SQL injection - a code injection technique used to target data-driven applications, where malicious SQL statements are inserted into a data entry field for execution

How to Prevent SQL Injection

- Parameterized Statements
- Object Relational Mapping
- Escaping Inputs
- Sanitizing Inputs

Phising - Phishing is a form of identity theft in which a scammer uses an authentic-looking email from a legitimate business to trick recipients into giving out sensitive personal information, such as a credit card, bank account, Social Security numbers or other sensitive personal information.

Spear Phishing - Spear phishing is one of the common types of phishing attacks that are done by sending an email to a particular targeted individual. An attacker generally steals the user's information from social media sites like Linked-in, Facebook, etc.

Whale Phishing - It is a form of phishing attack that is used to achieve big targets. Whale phishing is a technique to trick organizations and companies for stealing their confidential data. This type of scam generally happens to board members of the company. Attackers can simply target them, as it only requires the company's email id to deceive them

Deceptive Phishing - Nowadays, it is one of the most common types of phishing attacks. Deceptive phishing emails involves threatening messages to scare users by creating urgency. Attackers such as PayTM scammers send emails to customers and ask them to click on a link to rectify a mistake in their account.

Pharming - It is a type of Phishing attack that hackers use to steal sensitive or personal information from the users on the internet. In this attack, the hacker uses malicious code injected into the user's computer system or the server that misdirects users to fraudulent websites without their consent.

Dropbox Phishing - Some phishers do not use 'baiting' to deceive their targets. Instead, they send attack emails to individuals or companies. They generally use common popular sites like Dropbox to target the users.

How to Prevent Phishing

- **Lock down your browser with pop-up and phishing blockers**
- **Use multi-factor authentication where possible.**
- **Configure your email providers spam filter for maximum effectiveness.**

Cross-site scripting (XSS) - a type of vulnerability which is usually found in web applications. XSS helps attackers to inject scripts client-side to web pages accessed by other users

How to Prevent Cross-Site Scripting

- **Keep Software Updated**
- **Sanitize Input Fields**
- **Use Client and Server-Side Form Validation**
- **Use a Web Application Firewall**