1

# IDENTITY FORGERY

## DESCRIPTION

The fradulent creation of one's personal identification without authorisation, which can be used for malicious purposes

## IMPACT

Makes users, applications or services trust the forged identity as if it was legitimate

## RELATED VULNERABILITIES

2

3

3

2

# MAN-IN-THE-MIDDLE ATTACK

## DESCRIPTION

Eavesdropping and intercepting communication between two or more users or systems without them knowing they are communicating with an attacker

## IMPACT

Observe or alter data transferred between the communicating users or systems

## RELATED VULNERABILITIES

1

3/4

6

3

1

# RAGE ATTACK

## DESCRIPTION

A rogue insider abuses their priviledge of access to sensitive systems and/or information for malicious purposes

## IMPACT

All sensitive systems and/or information is accessible to a rogue insider

## RELATED VULNERABILITIES

1/2

2

# SOCIAL ENGINEERING

## DESCRIPTION

Use different techniques to trick vulnerable users into giving away their identity, access rights or other sensitive information

## IMPACT

Gain access to sensitive systems or information wihout rights or consent to do so

## RELATED VULNERABILITIES

1

1

5

1

# SQL INJECTION

## DESCRIPTION

Malicious SQL (Structured Query Language) statement inserted into input fields to change the behaviour of systems or execute malicious code

## IMPACT

Tamper with or leak the information from the database

## RELATED VULNERABILITIES

1/2/3

2

# COMMAND / DATA INJECTION

## DESCRIPTION

Malicious command inserted into input fields for malicious execution of code on computer systems

## IMPACT

Tampering with web server or stored data in a malicious manner

## RELATED VULNERABILITIES

2/3/7

3

# CROSS SITE REQUEST FORGERY

## DESCRIPTION

Make a victim's computer submit a request to a legitimate service on the victim's behalf in the background without their knowledge or consent

## IMPACT

User unwillingly or unknowingly downloads malicious programs on their system

## RELATED VULNERABILITIES

7/8

1

# CODE CORRUPTION

## DESCRIPTION

Modify a program's source code to change its behaviour or cause it to crash when executed

## IMPACT

Change the behaviour of a program

## RELATED VULNERABILITIES




4

2

2

# CONTROL FLOW HIJACKING

## DESCRIPTION

Modify how a program is executed by redirecting a reference to data the program uses to a different location

## IMPACT

Altered program execution or data leakage

## RELATED VULNERABILITIES




4

2

3

# PRIVILEGE ESCALATION

## DESCRIPTION

Modify privilege variables or trick higher-privilege services into providing information that is only available to those authorised (who have higher privilege)

## IMPACT

Bypassing access control and privilege system

## RELATED VULNERABILITIES



3

4/5

2

4

# MEMORY THIEF

## DESCRIPTION

Exploit an invalid memory access, attempting to cause a program to leak sensitive information

## IMPACT

Gain illegal knowledge of data stored in memory

## RELATED VULNERABILITIES



3

4/5

2

1

# RACE CONDITION

## DESCRIPTION

Abusing the game between Time-of-Check to Time-of-Use, for example to overwrite entries in a database

## IMPACT

Bypass checking to gain access to services and data

## RELATED VULNERABILITIES

# SIDE CHANNEL

1

## DESCRIPTION

Exploit information produced (digital or physical) by the system during its normal operation for malicious purposes

## IMPACT

## RELATED VULNERABILITIES





4 2

# FAULT INJECTION

2

## DESCRIPTION

Maliciously alter configurations or variables to understand how a system behaves

## IMPACT

Gain knowledge of system operation and uncover potential vulnerabilities

## RELATED VULNERABILITIES



4

2


1

1

# ILLEGAL CODE EXECUTION

## DESCRIPTION

Hide malicious code in a seemingly legitimate program or service, which is then later executed stealthily by unaware users

## IMPACT

Execute code without user consent or notification

## RELATED VULNERABILITIES

2

1

2/3

3

2

# DISTRIBUTED DENIAL OF SERVICE

## DESCRIPTION

Flood a system with a large number of messages from lots of infected devices, leaving it failing to respond and ultimately crashing.

## IMPACT

Make a service unavailable to legitimate users

## RELATED VULNERABILITIES

2

1

3

# REGISTRY OVERWRITING

## DESCRIPTION

Hide the existence of malicious code by over-writing data in a computer system's registry or persistent memory

## IMPACT

Execute malicious code when a targeted service on the system starts

## RELATED VULNERABILITIES

1

2

4

# BRUTE FORCE

## DESCRIPTION

Trying every possible combination (e.g. passwords) to gain access to a system or sensitive information

## IMPACT

Gain access to a system or sensitive information illegally

## RELATED VULNERABILITIES

1

2/4

1

1

# PARAMETER MANIPULATION

## DESCRIPTION

Replace user input parameters to understand and/or change how a system behaves

## IMPACT

Tamper with a system's useful information or use behaviours for malicious purposes

## RELATED VULNERABILITIES

1

3/4

# ILLEGAL DOWNLOAD

2

## DESCRIPTION

Automatically download material on a victim's system without them noticing or receiving consent

## IMPACT

Downloaded malware would infect the victim's system

## RELATED VULNERABILITIES

1/4 7/8

# INCORRECT CONSTRUCTION OF SQL STATEMENT

1

## DESCRIPTION

Incorrect construction of Structured Query Language (SQL) statement allows for potentially malicious user input to be executed

## RELATED ATTACKS

1

## RELATED DEFENCES

1/7

1



2

# INCORRECT SANITIZATION OF STORED DATA

2

## DESCRIPTION

Fail to check and sanitize special characters or commands that originate from user input which have ended up in storage and can lead to malicious code execution

## RELATED ATTACKS

1/2

1

## RELATED DEFENCES

1/7

1

7/8

2

# IMPROPER INPUT VALIDATION

3

## DESCRIPTION

Special character without immediate effect stored normally and result in rogue execution when those data is reused

## RELATED ATTACKS

1/2

1

1

## RELATED DEFENCES

1/7

1

7/8

2

# MISUSE OF DANGEROUS FUNCTIONS

4

## DESCRIPTION

Ignoring implementation requirements for dangerous functions which may lead to memory and execution vulnerabilities.

## RELATED ATTACKS

1/2/3/4

1

## RELATED DEFENCES

1/7

1

1/3

1

# MISSING DEFAULT INITIALISATION FOR INPUT

5

## DESCRIPTION

Abuse of non-typed systems and sending in much larger data to an uninitialised variable causing integer or variable overflows

## RELATED ATTACKS

2 3/4

## RELATED DEFENCES

1/7 1/2

# SENDING UNPROTECTED PARAMETERS

6

## DESCRIPTION

Acceptance of plaintext (unprotected) parameters, exposing potentially sensitive data to attackers

## RELATED ATTACKS

2

## RELATED DEFENCES

1



2/3/7

2/5

# 7 INADEQUATE DATA AUTHENTICITY AND ORIGIN VERIFICATION

## DESCRIPTION

No verification of whether data was sent by a legitimate sender in some legitimate domain

## RELATED ATTACKS

2/3

2

## RELATED DEFENCES

1/2/7

1

7

2/5

# INADEQUATE SESSION EXPIRATION

8

## DESCRIPTION

Old or expired session information (e.g. request credentials) is not identified and verified, leaving requests for information vulnerable to attackers who may capture the session information

## RELATED ATTACKS

3

2

## RELATED DEFENCES

1/7



1/3

1/4/5

1

# RACE CONDITION

## DESCRIPTION

No verification of time checks and resource usage in programs, allowing attackers to modify the program's behaviour or its resources

## RELATED ATTACKS

1

## RELATED DEFENCES

2/3/7/8

3

# SIDE CHANNEL

2

## DESCRIPTION

Monitoring normal system behaviour through physical or digital means, such as analysing network traffic, could leak sensitive information

## RELATED ATTACKS

1/2

## RELATED DEFENCES

8

11/3

# WEAK SERVICES OR PROCESSES ISOLATION

3

## DESCRIPTION

Lack of authentication and verification off the origin and destination of requests can result in code being executed on the same system

## RELATED ATTACKS

3/4 1

## RELATED DEFENCES

2/3/4/8/9

3/4/5/7/9

1

# BAD CREDENTIALS HANDLING

## DESCRIPTION

Using default or easy-to-guess passwords, or writing them down on paper, can leave password-protected accounts vulnerable to attackers

## RELATED ATTACKS

2

2





3/4



## RELATED DEFENCES

1/4/7/8/9

2

13/4/5/6

5

# INAPPROPRIATE MANAGEMENT DECISION

2

## DESCRIPTION

Non-expert management may decide to skip parts of risk analysis and security implementations due to time or budget pressures

## RELATED ATTACKS

1

1

## RELATED DEFENCES

8

2

5/6

# LOAD BALANCING FAILURE

1

## DESCRIPTION

Failure to handle large volumes of traffic and/or balance large volumes of traffic properly can result in failures to service legitimate users

## RELATED ATTACKS

2

2/4

## RELATED DEFENCES

1/8

11/3

# NO EXECUTION CONTROL IN MEMORY

2

## DESCRIPTION

Failures to deny code execution which involves critical memory can result in malicious code execution or leakage of sensitive information

## RELATED ATTACKS

1/2/3/4

3

## RELATED DEFENCES

5/6

3/10

3/4

3

# BAD CERTIFICATE MANAGEMENT

## DESCRIPTION

Blindly trusting the authenticity of certificates and the authority who signed them could allow them to spy on communications

## RELATED ATTACKS

1/2

1

## RELATED DEFENCES

2/4/7/8/9



3

1

1

# CARELESS INSIDER

## DESCRIPTION

Legitimate users can fail to properly handle (e.g. lose) credentials, equipment or data due to a lack of care or attention to detail

## RELATED ATTACKS

1/2 1 1/2

## RELATED DEFENCES

4/8/9 2 12/13/4/5/6/8/9 5/6

# INSIDER ACTIONS

2

## DESCRIPTION

Legitimate users may be provoked to act maliciously, such as using their privilege to leak sensitive information to competitors or tamper with internal services

## RELATED ATTACKS

1

2/4

## RELATED DEFENCES

2/3/8

4/5

# DEVELOPER BIAS

3

## DESCRIPTION

Developers may wrongly judge the necessity of certain security features and miss out on verify security protection or risks involved

## RELATED ATTACKS

1/2

## RELATED DEFENCES

1

2

3/6/9

6

# SECURITY FATIGUE

4

## DESCRIPTION

Reluctance to deal with cybersecurity can lead to skipping key security decisions or updates, increasing the likelihood of attacks to happen

## RELATED ATTACKS

2 1/2 4 2

## RELATED DEFENCES

1/8 2 12/13/3/6/8/9 5/6

1

# CODE ASSERTIONS AND REVIEWS

## DESCRIPTION

Add a statement to service code to confidently verify the status of variables during execution to ensure it runs as expected

## RELATED VULNERABILITIES

1

3/4



1/2/3/4/5/6/7/8

1

2

# OWNERSHIP VERIFICATION

## DESCRIPTION

Verify the ownership of programs and services before they are executed to ensure they are legitimate

## RELATED VULNERABILITIES



2

1/3

7

3

# ALIAS TRANSLATION

3

## DESCRIPTION

Resolve program aliases (e.g. shortcuts) and check the file path they run from to make sure they are not pointing to un-expected locations or executing another program

## RELATED VULNERABILITIES





2 1/3

4

# MONITORING

## DESCRIPTION

Background monitoring of program execution, memory usage and network traffic to detect abnormal behaviour

## RELATED VULNERABILITIES

1

1

3



3

# STACK CANARIES

5

## DESCRIPTION

Add static values in specific memory spaces and check if they have been modified by illegal memory access before using something from memory

## RELATED VULNERABILITIES

2

6

# EXECUTION INTEGRITY

## DESCRIPTION

Make a copy of the execution flow before a program is executed and use it to verify it has been illegally altered

## RELATED VULNERABILITIES

2

7

# TAINT ANALYSIS

## DESCRIPTION

Scan the programs and services to detect any vulnerability patterns in their source code that accept illegal user input

## RELATED VULNERABILITIES



1 1 1/2/3/4/5/7/8 3

8

# PENETRATION TESTING

## DESCRIPTION

Simulate cyber attacks against computer systems or services to uncover vulnerabilities and identify appropriate security measures to use

## RELATED VULNERABILITIES


1/2


1/2/4


1/2/3




1/3

9

# MALWARE SCANNING

## DESCRIPTION

Match process or program behaviours with known malicious behaviour to detect malware hidden in the system or memory

## RELATED VULNERABILITIES

1

1

3



3

# CODE GUIDELINES

1

## DESCRIPTION

Provide secure coding guidelines and requirements for software development

## RELATED VULNERABILITIES

1/2/3/4/7

2

# SECURITY AWARENESS TRAINING

## DESCRIPTION

Provide general security awareness training for users to educate them on possible threats, security pitfalls and prevention measures

## RELATED VULNERABILITIES

1/2

1/3/4

1

# SAFE LANGUAGE AND DEFENSIVE PROGRAMMING

## DESCRIPTION

Use programming languages with safer settings and prevent incorrect use of dangerous functions or unsafe memory operations

## RELATED VULNERABILITIES

4/5/8

2

# INITIALISATION OF RESOURCE ACQUISITION

## DESCRIPTION

Initialise resources and variables to protect against attacks directed to uninitialised or default initialisation of variable and resources

## RELATED VULNERABILITIES

5/6

3

# USE APPROVED TOOLS

## DESCRIPTION

Use approved tools which have been analysed and verified

## RELATED VULNERABILITIES



3/4

1/2/3

4/6/8

1/2/3

4

# SANDBOXING

## DESCRIPTION

Logically separating the memory, resources and processes of different services to analyse malware and prevent it spreading

## RELATED VULNERABILITIES

1

1/2

3

5

# PRINCIPLE OF LEAST PRIVILEGE

## DESCRIPTION

Only provide the least privilege to a service for execution to limit the possible damage it may cause if hijacked

## RELATED VULNERABILITIES

1/2

1/2

3

6

# CONTRACTS

## DESCRIPTION

Sign contracts with contractor to enforce their responsibility for putting in place security features in services or code and to state their liability in case of incidents

## RELATED VULNERABILITIES

1/2

1/3/4

7

# SAME-ORIGIN POLICY

## DESCRIPTION

Only allow a web service to execute scripts from the same domain

## RELATED VULNERABILITIES





3 2/3/6/7

8

# CONTENT SECURITY POLICY

## DESCRIPTION

Refuse executing a script or code from user-generated section in a web service

## RELATED VULNERABILITIES

1/4

2/3

9

# SECURE SOFTWARE DEVELOPMENT LIFE CYCLE

## DESCRIPTION

Address and include security measures during each stage of the software development life cycle

## RELATED VULNERABILITIES





1/3/4 3

10

# ADDRESS SPACE LAYOUT RANDOMIZATION

## DESCRIPTION

Randomise the address space to avoid easy guessing of where critical or sensitive data is located and arranged

## RELATED VULNERABILITIES

2

# LOAD BALANCERS

11

## DESCRIPTION

Install a proxy in front of main service machine to equally distribute (or reject) incoming messages to multiple machines to prevent a service becoming unavailable

## RELATED VULNERABILITIES



2

1

12

# PERMISSION DIALOG BASED ACCESS CONTROL

## DESCRIPTION

Popup and warn the user, and obtain their consent, before executing dangerous processes

## RELATED VULNERABILITIES

1/4

# SECURITY HYGIENE

13

## DESCRIPTION

Maintain code quality and best security practices during program development and execution to minimise risks

## RELATED VULNERABILITIES

1

1/4

1

# CORRECT USE OF FUNCTIONS

## DESCRIPTION

Follow guidelines of library or API functions to ensure security standards and requirements are met

## RELATED VULNERABILITIES

4/8

3

2

# INPUT SANITISATION AND FILTERING

## DESCRIPTION

Check, clean and filter special characters from user input to prevent malicious input from being processed, executed and/or stored

## RELATED VULNERABILITIES

1/2/3/6/7

3

# ONE-TIME PASSWORDS

## DESCRIPTION

Introduce the use of one-time passwords to prevent attackers from capturing and reusing old passwords

## RELATED VULNERABILITIES

2

4

# NON-EXECUTABLE MEMORY AND IMMUTABLE STATE

## DESCRIPTION

Deny executing commands or changing the state of memory if it is stored in either a protected memory section or a variable which cannot be changed

## RELATED VULNERABILITIES





8

2

5

# TOKENISATION OF SENSITIVE DATA

## DESCRIPTION

Generate secure tokens which references sensitive data when it is transferred over insecure channels and does not link to the meaning of the data

## RELATED VULNERABILITIES


1


1/4




6/7/8

6

# SECURE UPGRADE PROCESS

## DESCRIPTION

Implement a process to preserve the integrity of upgrade packages when deployed into existing services

## RELATED VULNERABILITIES

1/3/4