IDENTITY FORGERY

DESCRIPTION

Use a fake certificate signed by rogues certificate authorities to forge the identity of a legitimate services or users

IMPACT

Make user believe the service or website is from legitimate provider or the opposite

a_A0

MAN-IN-THE-MIDDLE ATTACK

DESCRIPTION

Adversary replace or intercept the certificate and encryption parameter with its own and fake their identity by using a certificate signed by rogue authorities which the user wrongly assume it is coming from legitimate service, allowing the adversary to observe all information transfer between the user and the legitimate service

IMPACT

Steal data encrypted by parameter sent with the rogue certificate

a_A1

IDN HOMOGRAPHS ATTACKS

DESCRIPTION

Register a rogue website domain name similar to a legitimate one by replacing certain character to similar shaped character in other language to fool the user to access the rogue website instead

IMPACT

Gain illegal knowledge or access of user

a_H0

SMUDGE ATTACK

DESCRIPTION

Observe fingerprinting patterns on physical device to guess credential or password patterns

IMPACT

Gain illegal access by knowing the credentials of legitimate users

a_H1

SHOULDER SURFING

DESCRIPTION

Illegally gain secret or credential by peeking the input process of a legitimate user

IMPACT

Gain illegal knowledge

a_H2

RAGE ATTACK

DESCRIPTION

An insider abuse its legitimate access to the services for redemption of rage or fire

IMPACT

All service accessible by a rage insider / stakeholder

a_H3

SOCIAL ENGINEERING

DESCRIPTION

Use different means to lure legitimate users to give away their access or knowledge

IMPACT

Gain illegal knowledge or access

a_H4

SQL INJECTION

DESCRIPTION

Malicious SQL statement inserted into entry fields for illegal execution to attack data-driven services.

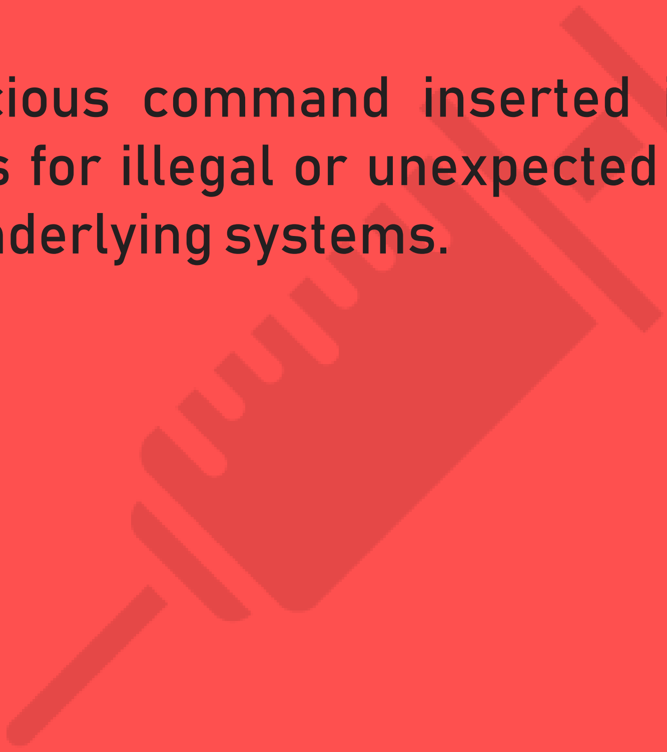
IMPACT

Pollute the database or leaking out data from the database

COMMAND INJECTION

DESCRIPTION

Malicious command inserted into entry fields for illegal or unexpected execution on underlying systems.



IMPACT

Pollute the local system / gain illegal access and knowledge

a_I1

SCRIPT INJECTION

DESCRIPTION

Malicious script injected to legitimate script or displayable content to attack servers or other users of the services or contents.

IMPACT

Pollute local system / Perform client side attack to other legitimate users

a_I2

SECOND ORDER INJECTION

DESCRIPTION

Malicious code or script that is sent and stored at a system. It only takes effect when the system retrieves, renders and executes the stored malicious script.

IMPACT

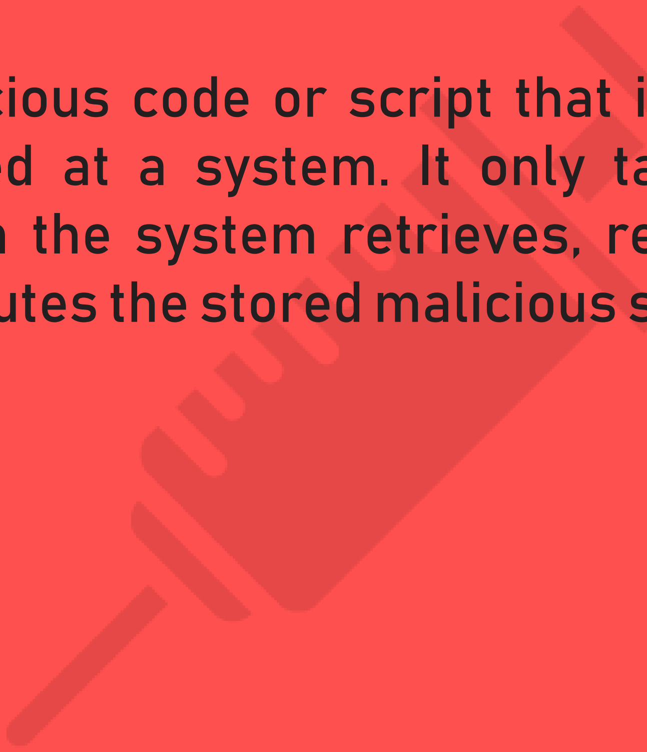
Pollute local system / Perform client side attack to other legitimate users

a_I3

HIGH ORDER INJECTION

DESCRIPTION

Malicious code or script that is sent and stored at a system. It only takes effect when the system retrieves, renders and executes the stored malicious script.



IMPACT

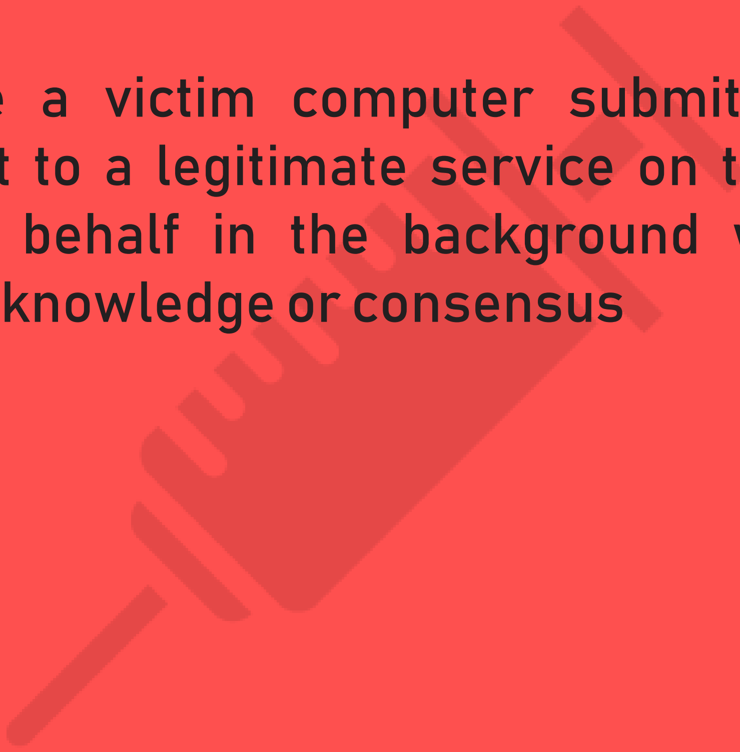
Pollute local system / Perform client side attack to other legitimate users

a_I4

CSRF

DESCRIPTION

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



IMPACT

Complete unknown web request with victim's identity or on behave of them

a_I5

CODE CORRUPTION

DESCRIPTION

Modify compiled program codes or variables to chance the execution behaviour or simply crashing the program

IMPACT

Change the service behaviour

a_M0

CONTROL FLOW HIJACKING

DESCRIPTION

Modify the execution flow of a compiled program by redirecting memory pointers to other memory locations

IMPACT

Make the program execute specific code in specific memory

a_M1

PRIVILEGE ESCALATION

DESCRIPTION

Modify certain privilege variables in order to gain a higher privilege illegally

IMPACT

Change certain variable in the memory to gain high privilege

a_M2

MEMORY THIEF

DESCRIPTION

Invalid memory access that attempts to make the program exfiltrate information stored in memory which is normally illegal to access

IMPACT

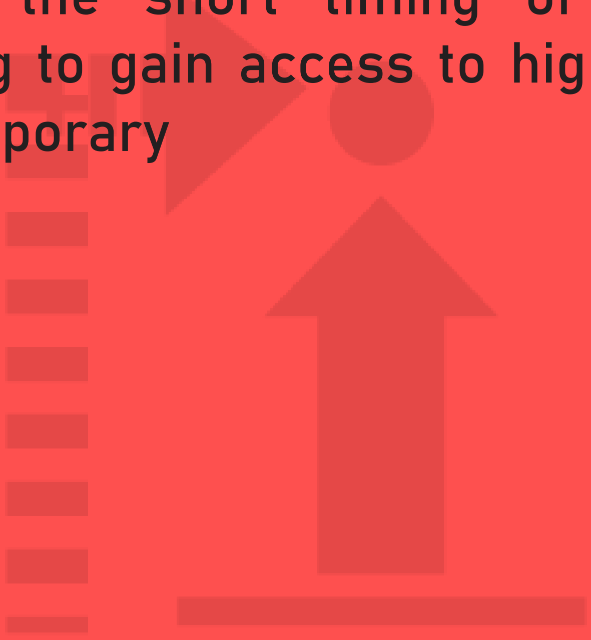
Gain illegal knowledge of data stored in the memory

a_M3

PROCESS RACE CONDITION

DESCRIPTION

Abusing the short timing of process switching to gain access to higher privilege temporary



IMPACT

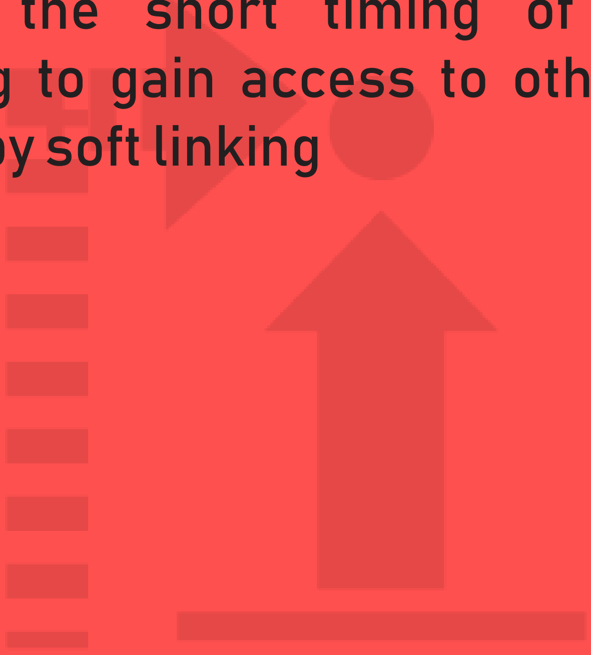
Execute some actions which require higher privilege

a_R0

SESSION RACE CONDITION

DESCRIPTION

Abusing the short timing of process switching to gain access to other active session by soft linking



IMPACT

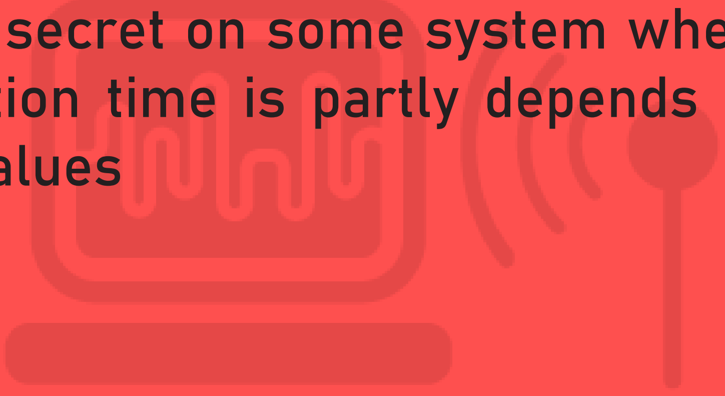
Gain illegal access to services and data in other active sessions

a_R1

TIMING SIDE CHANNEL

DESCRIPTION

Observe the processing time and make use of that as a hint to guess the correct data / secret on some system where the execution time is partly depends by the data values



IMPACT

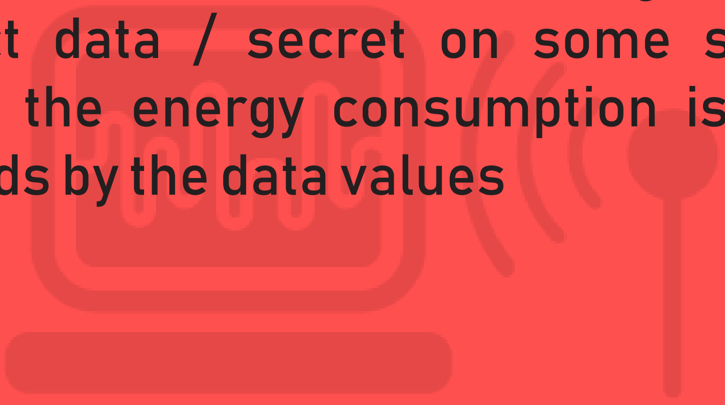
Gain illegal knowledge

a_C0

ENERGY SIDE CHANNEL

DESCRIPTION

Observe the energy consumption and make use of that as a hint to guess the correct data / secret on some system where the energy consumption is party depends by the data values



IMPACT

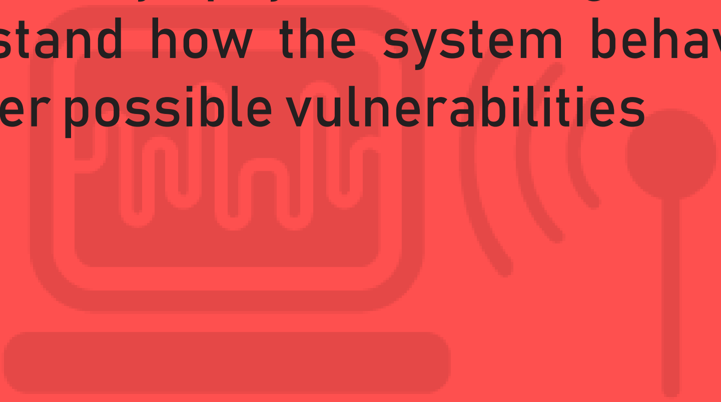
Gain illegal knowledge

a_C1

PHYSICAL FAULT-INJECTION

DESCRIPTION

Purposely stress the target system with some faulty physical configuration to understand how the system behave and discover possible vulnerabilities



IMPACT

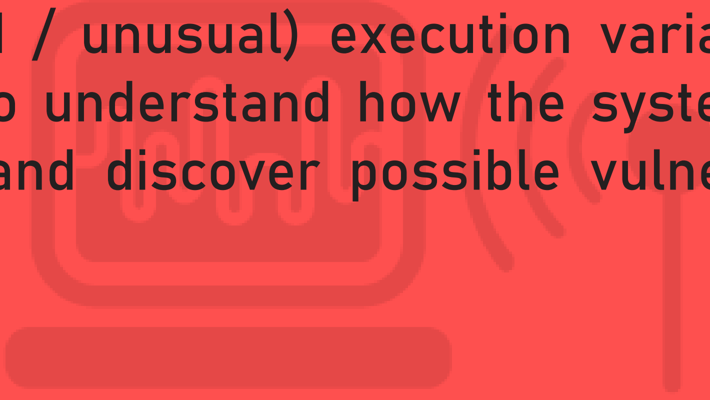
Gain knowledge of execution flow and potential vulnerabilities

a_C2

SOFTWARE FAULT-INJECTION

DESCRIPTION

Purposely stress the target system with some specially crafted or faulty (unexpected / unusual) execution variable or flow to understand how the system behave and discover possible vulnerabilities



IMPACT

Gain knowledge of execution flow and potential vulnerabilities

a_C3

ILLEGAL CODE EXECUTION

DESCRIPTION

Adversary try to hide malicious code in browser extension and execute them when unaware users assume it is legitimate and install it.

IMPACT

Execute some activities or data stealing logic without the user consensus and notice

a_S0

CONFUSED DEPUTY ATTACK

DESCRIPTION

A legitimate, more privileged services being tricked by misusing its authority on the system to complete request for another service which does not have the authority to finish that request

IMPACT

Gain access to service or storage which is illegal

a_S1

DISTRIBUTED DENIAL OF SERVICE

DESCRIPTION

Flood the system with communications to make it fail to response to legitimate users’ request, generally the requests are initiated from a large set of computers which are inflected by a botnet malware and being secretly controlled by the attacker

IMPACT

Make a service unavailable to legitimate users

a_S2

REGISTRY OVERWRITING

DESCRIPTION

Stay fileless in the computer memory once inflected and rely on processes memory to stay alive and possibly affect the memory and wipe out / overwriting data in the memory and computer registry to change the execution behaviour is the computer.

IMPACT

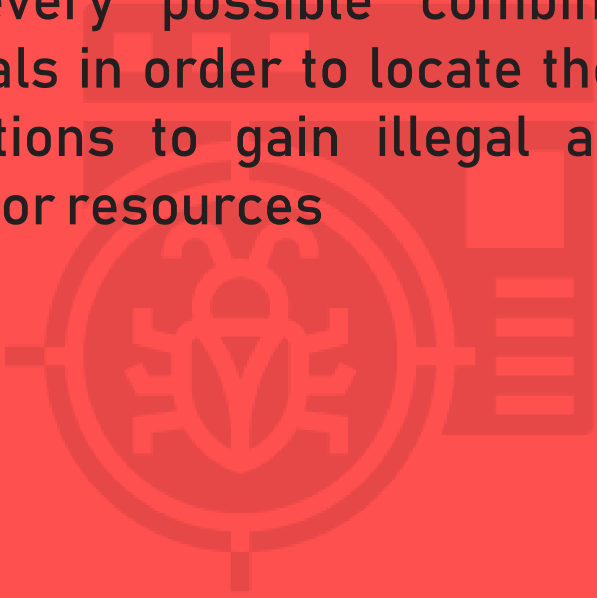
Control data flow and manipulate data in memory or registry

a_S3

BRUTE FORCE

DESCRIPTION

Trying every possible combination of credentials in order to locate the correct combinations to gain illegal access to services or resources



IMPACT

Gain illegal knowledge or access

a_S4

DNS FAST-FLUX

DESCRIPTION

Keep changing the domain name for the botnet control machine in order to harden and delay the tracing to the botnet control server and the malware attached

IMPACT

Hide the existence of botnet

a_S5

PARAMETER MANIPULATION

DESCRIPTION

Adversary replace user input parameter sent in plaintext to change the system behaviour or get knowledge of the user choice or secret information

IMPACT

Pollute the user input or get illegal knowledge of user input

a_W0

UNCONSENSUS DOWNLOAD

DESCRIPTION

Provide automatic legitimate download with user authorization without notifying possible additional privilege needed or consequence of such download

IMPACT

Gain additional privilege which the user did not know

a_W1

UNINTENTIONAL DOWNLOAD

DESCRIPTION

Provide any kind of automatic download without notifying the user

IMPACT

Illegally control or gain knowledge of user’s computer

a_W2

HEARTBLEED

DESCRIPTION

Abuse the inappropriate size checking of OpenSSL heartbeat feature by providing a much larger size and force the vulnerable service to return more data from memory which is normally prohibited to access

IMPACT

Gain illegal knowledge of data stored in the memory

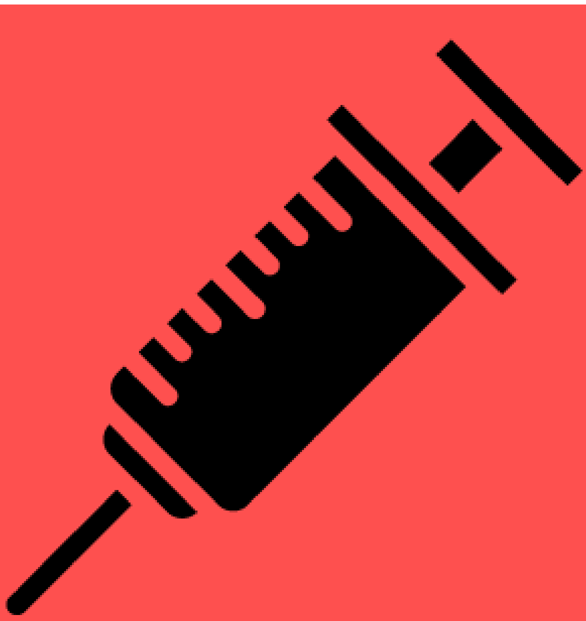
a_W3

MEMORY

Targets the memory and storage of modern computers or hides its existence in the memory in fileless status.

a_M

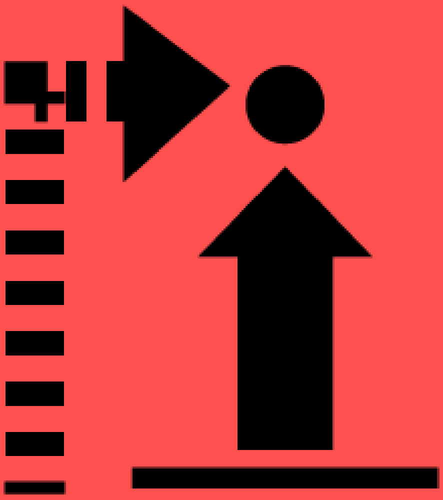
INJECTION



Alters original functionality or adds extra executions on the original services.

a_I

RACE CONDITION



Abuses race conditions to get undesired ouput.

Race conditions are conditions of systems where their substantive behaviours are dependent on the sequence or timing of multiple uncontrollable events.

SIDE CHANNEL

Studies the outside behaviour to get information of the execution paths, resources used or other hidden details for further attack.

a_C

AUTHENTICATION

Breaks normal authentication process to perform actions with fake or privileged identity.

a_A

WEB

Targets web services or redirects attacks towards other users by abusing web services.

a_W

SYSTEM

Spreads through computers without user notice in the form of malicious software or bundle of attack commands that target basic system functionality and settings.

a_S

HUMAN FACTOR

Trick users to providing information of some privileged access or resources. Also refers to insiders purposely doing damage to internal services.

a_H

DETECTION

Detect and notify the administrator about possible attacks happening. Allows live defence and tracing for forensic purposes.

d_D

MITIGATION

Decrease the possibility or effect of certain attacks.

d_M

PREVENTION

Stop some types of attack.

d_P

EDUCATION

Provide education to users to decrease the chance of being targeted.

d_E

ENVIRONMENT

Badly configured execution environment can leak out information and allow malicious users to attack the services above it.

v_E

CODE

Badly written code can allow malicious users to alter the functionality, getting extra information or crashing the services.

v_C

HUMAN

Bad practice by careless user or bad defence against corrupted internal user can allow malicious users to gain insider knowledge or privilege through social and psychological skills.

v_H

CODE ASSERTIONS

DESCRIPTION

Inject assertive statement to service code to verify the status of certain variables during execution to ensure it runs as expected

d_DO

AUTOMATED CODE REVIEW

DESCRIPTION

Perform code reveal by automatic analysing tools to discover possible vulnerability and bad implementation that could lead to security problem

d_D1

OWNERSHIP VERIFICATION

DESCRIPTION

Verify the ownership and related information of an artefacts just before use to avoid race condition and last minutes changes.

d_D2

ALIAS TRANSLATION

DESCRIPTION

Resolve alias of artefacts to review the absolute path for an artefact to ensure it is not pointing to unexpected artefact and verify again during real usage of the artefact

d_D3

MONITORING

DESCRIPTION

Background monitoring of the execution status and memory changes to detect abnormal behaviour

d_D4

THREAT MODELLING

DESCRIPTION

Analyse and model possible threats and risk level to help prescribe necessary security measures for the development process

d_D5

STACK CANARIES

DESCRIPTION

Add in some static specific values in specific address in the memory. Check if they have been modified by illegal memory overflow before executing or using something from memory

d_D6

CONTROL FLOW INTEGRITY

DESCRIPTION

Make a copy of the execution flow before execution and use it to verify if the control flow has been altered illegally by memory overflow during execution.

d_D7

TAINT ANALYSIS

DESCRIPTION

Scan the service and program to detects any injection vulnerability pattern in source code that accept malformed or untrusted user input

d_D8

INFORMATION FLOW ANALYSIS

DESCRIPTION

Scan the flow of data managed by the system or service to detect potential risk, including leaking or replacing of data.

d_D9

PROGRAM VERIFICATION

DESCRIPTION

Design formal specification for security requirements and use it to demonstrate that programs behave according by formal proof strategy.

d_D10

PENETRATION TESTING

DESCRIPTION

Hire expert to launch simulated cyber attack against your computer system or services to discover exploitable vulnerabilities

d_D11

ANALYSING EXECUTION ENVIRONMENT

DESCRIPTION

Analyse environment settings to detect abnormal behaviour that affect some executions which are relying the environment

d_D12

MALWARE SCANNING

DESCRIPTION

Match processes with known malicious behaviour to detect possible hidden malware in the system or memory

d_D13

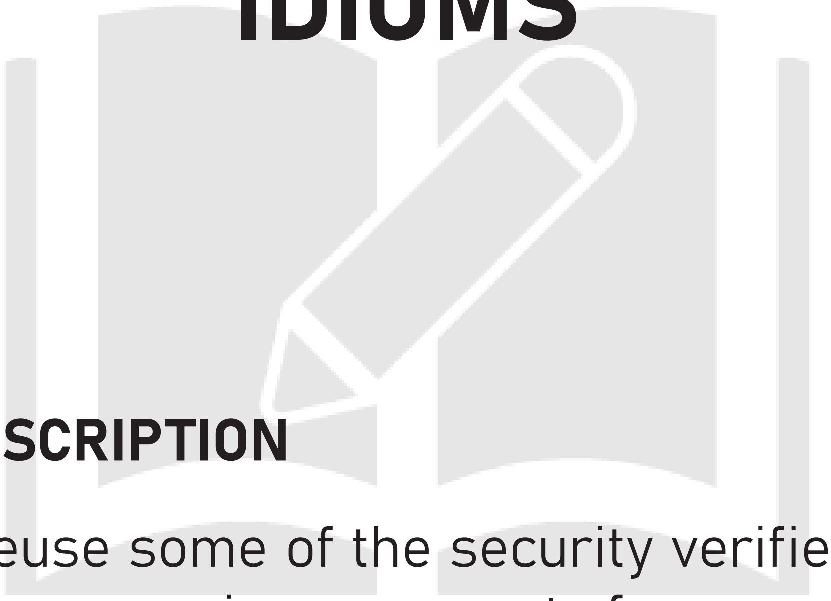
NETWORK MONITORING

DESCRIPTION

Background monitoring of border network traffic to discover abnormal request

d_D14

USE VERIFIED PROGRAMMING IDIOMS

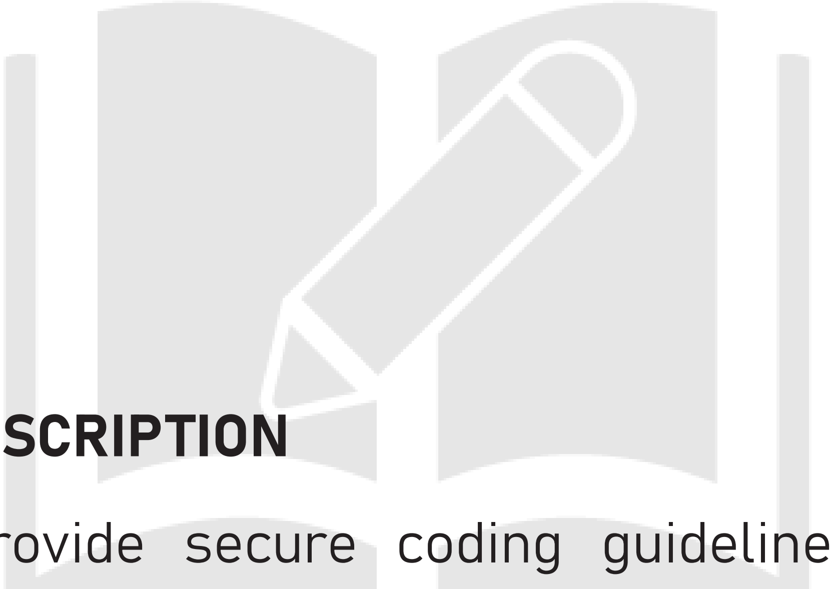


DESCRIPTION

Reuse some of the security verified programming segment for some repeating functionality to ensure correct security consideration has been implemented to the functionality

d_E0

CODE GUIDELINES



DESCRIPTION

Provide secure coding guidelines and requirements to developer and urge them to follow the practice during development

d_E1

ANTI-PHISHING TRAINING

DESCRIPTION

Provide security awareness training for user on phishing attempts and signature identification or possible verification method for incoming request

d_E2

PROVIDE SECURITY AWARENESS TRAINING

DESCRIPTION

Provide general security awareness training for user to educate them of possible threats, security pitfall and measures

d_E3

SAFE LANGUAGE

DESCRIPTION

Use some language with safer setting like memory protection or type safety

d_M0

DEFENSIVE PROGRAMMING

DESCRIPTION

Ensure continue functionality of a service under future unforeseen situation by maintaining code quality and add it all kind of secure measures even it may never be triggered in normal circumstances.

d_M1

AVOID / VERIFY THE USE OF DANGEROUS FUNCTIONS

DESCRIPTION

Avoid using dangerous function or ensure it is correctly configured and implemented if it is necessary to use them

d_M2

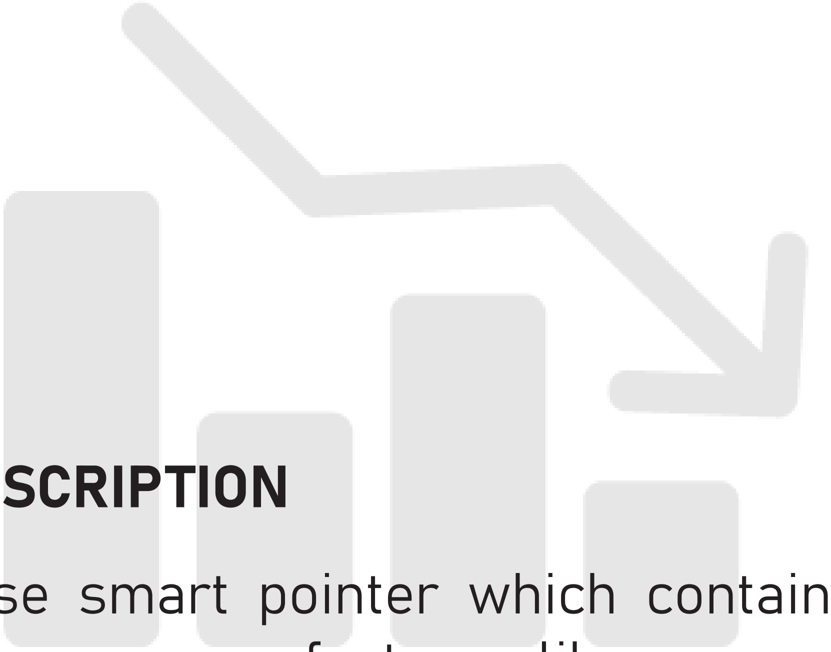
INITIALISATION OF ALL RESOURCE ACQUISITION

DESCRIPTION

Manually initialize all resource and variables to protect against attacks directed to uninitialized or default initialisation of variable and resources

d_M3

ADOPTION OF SMART POINTERS



DESCRIPTION

Use smart pointer which contains more secure features like memory safe and auto destruction to ensure less vulnerability on memory management

d_M4

USE APPROVED TOOLS

DESCRIPTION

Use approved tools which has been repletely analysed and verified for certain critical service

d_M5

SANDBOXING

DESCRIPTION

Logically separating memory, resources and processes of different services to avoid the spreading of malicious activity or privilege escalation

d_M6

PRINCIPLE OF LEAST PRIVILEGE

DESCRIPTION

Only provide the least privilege to service for completing their necessary execution to limit the possible damage when it is been hijacked.

d_M7

CONTRACTS

DESCRIPTION

Sign contract with contractor to stat their responsibility of adding security features to the service or code and their liability if attack does success in their designed services

d_M8

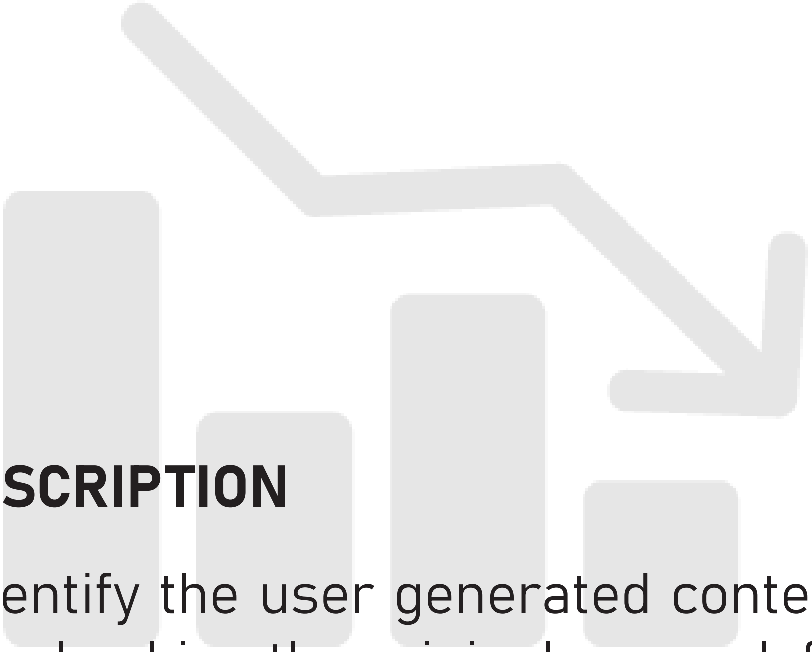
SAME ORIGIN POLICY

DESCRIPTION

Only allow a website to execute script that is targeted to components in the same domain to avoid data thief and out of scope illegal request

d_M9

CONTENT SECURITY POLICY



DESCRIPTION

Identify the user generated content by checking the original scope definition of a website and refuse executing script or code in the those section to mitigate the effect of injection and client side attack.

d_M10

VULNERABILITY RESPONSE AND DISCLOSE

DESCRIPTION

Provide update and quick response on vulnerability to urge users to patch the vulnerability asap to decrease the rate of being attacked

d_M11

SECURE DEVELOPMENT PLANNING AND ANALYSIS

DESCRIPTION

Complete risk analysis and plan necessary secure measures and implementation ahead of the real design and implementation stage to make sure secure development has been carefully considered and applied to the service

d_M12

RISK ASSESSMENT FOR THIRD-PARTY COMPONENT

DESCRIPTION

Analyse and include possible risks and vulnerabilities of using third-party component and add them to the necessary list of secure development and implementation

d_M13

ADDRESS SPACE LAYOUT RANDOMIZATION

DESCRIPTION

Randomize the address space to avoid easy guessing of the arrangements and location of critical data and execution commands

d_M14

LOAD BALANCERS

DESCRIPTION

Install a proxy in front of main service machine to equally distribute (or reject) request load to multiple machine to avoid flooding of request

d_M15

PERMISSION DIALOG BASED ACCESS CONTROL

DESCRIPTION

Popup and warn the user before executing some dangerous process and obtain the user consensus before executing them

d_M16

KEEP CREDENTIAL SAFE

DESCRIPTION

Educate the user to keep their own credential in safe, better not written physically

d_M17

PRACTICE SECURITY HYGIENE

DESCRIPTION

Maintain a certain level of code quality on development to decrease the number of vulnerability introduced from bad implementation or wrong use of dangerous functions and libraries

d_M18

CORRECT USE OF FUNCTIONS

DESCRIPTION

Follows the guideline of functions call to ensure it is used safely as expected without opening vulnerability

d_P0

CORRECT IMPLEMENTATION OF LIBRARY AND API

DESCRIPTION

Correct implementation and limit further processing of API and library to ensure keeping the original security standard and requirement

d_P1

IMMUTABLE STATE

DESCRIPTION

Lock some of the variable and throws error if they are being modified during executions or after initialisation

d_P2

INPUT SANITISATION

DESCRIPTION

Check, clean and filter special characters from user input to avoid polluted input got accidently executed or stored

d_P3

METADATA FILTERING

DESCRIPTION

Remove unknown or misuse meta data before processing, storing or executing services related to them

d_P4

ONE-TIME PASSWORDS

DESCRIPTION

Introduce the use of one-time password to deny replay attack from attacker which attempt to use previously known password

d_P5

NON-EXECUTABLE MEMORY

DESCRIPTION

Deny executing some commands if it is stored in some marked or protected memory section which avoid attacker overflowing malicious command into those memory address space

d_P6

TOKENISATION OF SENSITIVE DATA

DESCRIPTION

Generate undecipherable token for sensitive data and transfer them through insecure channel without using the original data to avoid leaking

d_P7

DEVELOP SECURE UPGRADE PROCESS

DESCRIPTION

Develop a way to allow server and remote client to share an upgrade or patch of a client side service by matching some cryptographic token to avoid polluted upgrade being installed to ruin the security of the service and the client machine

d_P8

INCORRECT CONSTRUCT OF SQL STATEMENT

DESCRIPTION

Incorrect construct of SQL statement allows rogue user input included for execution

ATTACK VECTOR

Parameter with SQL meta-character. Attack Codes: a_I0

CONSEQUENCE

Unexpected SQL statement being executed. Defence Codes: d_D0 d_D1 d_D8 d_D10 d_E0 d_E1 d_P3 d_P4

v_C0

INCORRECT SANITIZATION OF STORED DATA

DESCRIPTION

Reuse of stored rogue user input being executed as legitimate SQL statement unexpectedly

ATTACK VECTOR

Parameter with double layer SQL meta-character. Attack Codes: a_I0 a_S0

CONSEQUENCE

Unexpected SQL statement being executed. Defence Codes: d_D0 d_D1 d_D8 d_D10 d_E0 d_E1 d_P3 d_P4

v_C1

IMPROPER INPUT NEUTRALIZATION FOR OS COMMANDS

DESCRIPTION

Improper sanitize of user input result in unexpected command execution

ATTACK VECTOR

Input with OS special character. Attack Codes: a_I1

CONSEQUENCE

Unexpected OS command being executed. Defence Codes: d_D0 d_D1 d_D8 d_D10 d_E0 d_E1 d_P3 d_P4

v_C2

IMPROPER INPUT NEUTRALIZATION FOR WEB CONTENT GENERATION

DESCRIPTION

Improper sanitize of user input allow extra script embedded to web content feeding to other user and got unexpected script executed on other user's computer

ATTACK VECTOR

Input with script special character. Attack Codes: a_I2

CONSEQUENCE

Unexpected script redirect to user and executed locally on user's computer. Defence Codes: d_D0 d_D1 d_D8 d_D10 d_E0 d_E1 d_M9 d_M10 d_P3 d_P4

v_C3

IMPROPER INPUT VALIDATION

DESCRIPTION

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

ATTACK VECTOR

Parameter with special character decoded. Attack Codes: a_I0 a_I1 a_I2 a_I3 a_I4 a_S0 a_W0

CONSEQUENCE

Unexpected command or statement executed. Defence Codes: d_D0 d_D1 d_D8 d_D10 d_E0 d_E1 d_M1 d_M9 d_M10 d_M18 d_P3 d_P4

v_C4

HIGHER-ORDER INJECTION VULNERABILITIES

DESCRIPTION

Fail to check and sanitize special characters or commands that originate from users and has been passed through multiple internal services with no effect.

ATTACK VECTOR

Parameter with special character with no immediate effect. Attack Codes: a_I0 a_I1 a_I2 a_I3 a_I4 a_S0

CONSEQUENCE

Unexpected command or statement executed. Defence Codes: d_D0 d_D1 d_D8 d_D10 d_E0 d_E1 d_M1 d_M9 d_M10 d_M!d_8 d_P3 d_P4

v_C5

MISUSE OF DANGEROUS FUNCTIONS

DESCRIPTION

Ignoring implementation requirement for dangerous functions or implementing them incorrectly and open up some memory and execution vulnerabilities.

ATTACK VECTOR

Misused dangerous function. Attack Codes: a_M0 a_M1 a_M2 a_M3 a_S5 a_W0 a_W3

CONSEQUENCE

Open up memory or process vulnerability. Defence Codes: d_D0 d_D1 d_M1 d_D10 d_E0 d_E1 d_M0 d_M2 d_M5 d_M18 d_P0 d_P1

v_C6

MISSING DEFAULT INITIALISATION FOR INPUT

DESCRIPTION

Abuse some non-type system and sending in much larger data to initialize an un-initialized variable cause integer or variable overflow

ATTACK VECTOR

Overflow or underflow input. Attack Codes: a_H1 a_M2 a_M3

CONSEQUENCE

Integer or variable overflow. Defence Codes: d_D0 d_D1 d_D10 d_E1 d_M0 d_M3 d_M18

v_C7

SENDING UNPROTECTED PARAMETER

DESCRIPTION

Accept user parameter send through plaintext address bar and risk adversary seeing and tempering them

ATTACK VECTOR

Parameter send through open HTTP request. Attack Codes: a_A1

CONSEQUENCE

Leaking out information or unexpected user input or parameter integrity violation.

Defence Codes: d_D0 d_D1 d_M3 d_M5 d_M9 d_M18 d_P3 d_P7

v_C8

INSUFFICIENT VALIDATION OF DATA AND REQUEST AUTHENTICITY

DESCRIPTION

Does not correctly validate that the data or request send by a legitimate user is indeed initiate with the user's consensus

ATTACK VECTOR

Cross Site scripting / Phishing links. Attack Codes: a_I1 a_I2 a_W1 a_W2 a_W3

CONSEQUENCE

Illegal request on behave of the user has been executed without user notice. Defence Codes: d_D0 d_D1 d_D2 d_D8 d_D10 d_E0 d_E1 d_M9 d_P3 d_P4 d_P7

v_C9

INSUFFICIENT SESSION EXPIRATION

DESCRIPTION

Does not correctly identify old or exposed session credentials or identifiers of a request or does not provide reasonable session expiration period

ATTACK VECTOR

Cross Site scripting / Phishing links. Attack Codes: a_I5 a_W1 a_W2

CONSEQUENCE

Illegal request with user's session has been executed without user notice. Defence Codes: d_D0 d_D1 d_D10 d_E1 d_M0 d_M5 d_P0 d_P1 d_P2 d_P4 d_P7

v_C10

INSUFFICIENT ORIGIN VALIDATION

DESCRIPTION

Does not verify if the request does initiate from the same domain as the session which has the user’s consensus

ATTACK VECTOR

Cross Site scripting / Phishing links. Attack Codes: a_I5 a_W1 a_W2

CONSEQUENCE

illegal request from different domain has been executed without user notice. Defence Codes: d_D0 d_D1 d_D10 d_E1 d_M9 d_P7

v_C11

BLIND TRUST OF USER INPUT

DESCRIPTION

System relies on user input blindly trust those data and use it directly which cause unexpected execution or side effect

ATTACK VECTOR

rogue user input with attack attached.
Attack Codes: a_I0 a_I1 a_I2 a_I3 a_I4 a_M0 a_M1 a_M2 a_M3 a_S0 a_S3 a_W0 a_W1 a_W2 a_W3

CONSEQUENCE

rogue user input being used as legitimate input and causing different side effect.
Defence Codes: d_D0 d_D1 d_D5 d_D10 d_D11 d_E0 d_E1 d_M4 d_E3 d_M18 d_P3

v_C12

MEMORY OUT-OF-BOUND READ / WRITE

DESCRIPTION

Missing size and boundary checking cause more data then excepted flooded into the memory, resulting in illegal execution or memory data leakage

ATTACK VECTOR

Lengthy and special crafted input. Attack Codes: a_M0 a_M1 a_M2 a_M3 a_S3 a_W3

CONSEQUENCE

Illegal execution or leaking of data in memory. Defence Codes: d_D0 d_D1 d_D6 d_D7 d_D9 d_D10 d_D11 d_E0 d_E1 d_M4 d_M7 d_M14 d_P2 d_P3 d_P5

v_C13

LOAD BALANCING FAILURE

DESCRIPTION

Fail to do a good load balancing when a huge amount of request flies in, resulting in system service offline for a period of time

ATTACK VECTOR

Automated repeating logic. Attack Codes: a_C2 a_C3 a_S2 a_S4 a_S5

CONSEQUENCE

Fail to keep an service available. Defence Codes: d_D0 d_D1 d_M15D4 d_D5 d_D11 d_E1 d_M1 d_M5

v_E0

RACE CONDITION

DESCRIPTION

Unintentionally provide a big time or resources gap between the checking and using of the data or resources, leaving a window for attacker to illegally change the execution behaviour or resources.

ATTACK VECTOR

Multiple process executing on the same artefacts. Attack Codes: a_R0 a_R1

CONSEQUENCE

Privilege escalation or data out of sync. Defence Codes: d_D2 d_D3 d_D4 d_D5 d_D10 d_D11 d_D12 d_M1 d_M5

v_E1

SIDE CHANNEL

DESCRIPTION

Continue to feed input to the process and observe its physical and logical performance to guess the hidden logic or correct credentials

ATTACK VECTOR

Automated repeating logic. Attack Codes: a_C0 a_C1 a_C2 a_C3

CONSEQUENCE

Gain illegal access to obfuscated logic or credentials. Defence Codes: d_D4 d_D5 d_D11 d_D12 d_E1 d_M1 d_M5 d_M15

v_E2

NO NON-EXECUTABLE CONTROL IN CRITICAL MEMORY SECTION

DESCRIPTION

Fail to deny execution in some critical memory section, result in illegal execution with high privilege or leakage of critical system data

ATTACK VECTOR

Lengthy and special crafted input. Attack Codes: a_M0 a_M1 a_M2 a_M3 a_S3

CONSEQUENCE

Crash the system or gain illegal execution rights. Defence Codes: d_D6 d_D7 d_D9 d_M5 d_M14 d_P2 d_P5

v_E3

BLIND TRUST OF CERTIFICATE AUTHORITIES

DESCRIPTION

Blind trust of the signing authorities of the received certificate without further verification of the authorities or the certificate revoking list

ATTACK VECTOR

Self-signed certificate or certificate signed by rogue RA. Attack Codes: a_A0 a_A1 a_S0 a_S5

CONSEQUENCE

Possible leaking out communication information to adversary. Defence Codes: d_D2 d_D5 d_D10 d_D11 d_D13 d_D14 d_E1 d_M1 d_M5 d_M18 d_P0 d_P1 d_P8

v_E4

SKIP CERTIFICATE CHECKING

DESCRIPTION

Blind trust of any certificated received

ATTACK VECTOR

rogue certificate. Attack Codes: a_A0 a_A1 a_S1

CONSEQUENCE

Possible leaking out communication information to adversary. Defence Codes: d_D1 d_D10 d_D11 d_D13 d_D14 d_E1 d_M18 d_P8

v_E5

WEAK ISOLATION BETWEEN SERVICES OR PROCESSES

DESCRIPTION

Does not have enough authentication and checking between for cross border request initiated from logical separated service reside in the same physical machine

ATTACK VECTOR

Malicious code towards the physical device. Attack Codes: a_M2 a_M3 a_R0 a_R1 a_S1

CONSEQUENCE

Gain illegal access and data from logically isolated service co-located in the same physical servers. Defence Codes: d_D2 d_D3 d_M7D4 d_D5 d_D9 d_D11 d_D12 d_D13 d_D14 d_M5 d_M6 d_M9 d_M11 d_M12

v_E6

DEFAULT PASSWORDS AND CREDENTIALS

DESCRIPTION

Does not force legitimate users to change their default credentials or passwords, allowing the adversary has more time to guess, or easier to gain access to the service or systems with the default credential of a legitimate user

ATTACK VECTOR

Automated repeating logic. Attack Codes: a_H4 a_S4 a_W3

CONSEQUENCE

Illegal access with others credential. Defence Codes: d_D5 d_D10 d_D11 d_E2 d_M7 d_E3 d_M17

v_H0

HAND-WRITTEN CREDENTIALS

DESCRIPTION

Write down the credential and store in open area, allowing people to read and get knowledge with your credentials

ATTACK VECTOR

Careless user. Attack Codes: a_H1 a_H2 a_H4 a_S4

CONSEQUENCE

Illegal access with others credential. Defence Codes: d_D5 d_D11 d_E2 d_E3 d_M7 d_M8 d_M12 d_M13 d_M17 d_P7

v_H1

CARELESS INSIDER

DESCRIPTION

Careless legitimate user carelessly lost some physical or digital data or credentials or being lure to install malware into the internal network

ATTACK VECTOR

Careless user. Attack Codes: a_H0 a_H1 a_H2 a_H3 a_H4 a_S0 a_S5 a_W0 a_W1 a_W2

CONSEQUENCE

Leak out digital or physical information or introducing malware into the internal system accidently. Defence Codes: d_D4 d_D11 d_D13 d_D14 d_E2 d_E3 d_M6 d_M7 d_M8 d_M10 d_M11 d_M16 d_M17 d_P4 d_P7 d_P8

v_H2

EXPOSURE OF SENSITIVE INFORMATION TO UNAUTHORISED ACTOR

DESCRIPTION

Use different kind of means to lure user to give away their secret or credentials

ATTACK VECTOR

Careless user. Attack Codes: a_H0 a_H4 a_S4 a_S5 a_W1 a_W2

CONSEQUENCE

Illegal access with others credential. Defence Codes: d_D2 d_D3 d_D4 d_D5 d_D11 d_D13 d_D14 d_E2 d_E3 d_M6 d_M7 d_M16 d_M!d_7 d_P4 d_P7 d_P8

v_H3

CORRUPTED / RAGE INSIDER

DESCRIPTION

Legitimate user of the system perform malicious action to leak out data or damage the services and data with its legitimate user privilege because of rage or being lured to do so

ATTACK VECTOR

Insider. Attack Codes: a_H3 a_S2 a_S4

CONSEQUENCE

Unexpected data leakage or damage. Defence Codes: d_D4 d_D5 d_D11 d_M1 d_M6 d_M7

v_H4

DEVELOPER BIAS

DESCRIPTION

Wrongly assume the security necessity of certain features or does not follow or trusting the risk analysis, resulting in missing security protection in some of the features.

ATTACK VECTOR

Users / system administrator. Attack Codes: a_A0 a_A1 a_W3

CONSEQUENCE

illegal access with others credential. Defence Codes: d_D0 d_D1 d_D5 d_E1 d_E2 d_E3 d_M5 d_M8 d_M11 d_M12 d_M13 d_M18 d_P8

v_H5

SECURITY FATIGUE

DESCRIPTION

Fatigue of security measure make human try to skip security consideration or skip the patching and updates of old problems resulting in increasing number of vulnerabilities

ATTACK VECTOR

Users / system administrator. Attack Codes: a_A1 a_H2 a_H4 a_C0 a_C1 a_C2 a_C3 a_S4 a_W1 a_W2

CONSEQUENCE

Fail to keep up of normal security procedure. Defence Codes: d_D0 d_D1 d_D5 d_D11 d_E2 d_E3 d_M5 d_M8 d_M10 d_M11 d_M12 d_M16 d_M17 d_P7 d_P8

v_H6

USING HARD CODED CREDENTIALS OR CERTIFICATES

DESCRIPTION

Tired of repeating authentication and hard-coded some credentials into automated logic or code that may leak out to an attacker

ATTACK VECTOR

Users / system administrator. Attack Codes: a_A1 a_H2 a_H4 a_S1 a_S3 a_S4 a_S5

CONSEQUENCE

Illegal access with the hard coded credentials. Defence Codes: d_D0 d_D1 d_D4 d_D5 d_D10 d_D11 d_D13 d_D14 d_E1 d_E2 d_E3 d_M6 d_M7 d_M8

v_H7

INAPPROPRIATE MANAGEMENT DECISION

DESCRIPTION

Management decision from non-expert to skip some of the risk analysis and security implementation because of time and budget pressure

ATTACK VECTOR

Unaware stakeholder. Attack Codes: a_A0 a_S0 a_S5

CONSEQUENCE

Fail to keep up of some security procedure. Defence Codes: d_D5 d_D11 d_E2 d_E3 d_M7 d_M8 d_M12 d_M13

v_H8