EXPOSURE

Opportunist cyber attack on infrastructure

FOR ASSET:

VULNERABILITY	EXPOSURE?
Running version of infrastructure dependency with known vulnerability	☐
Running version of application dependency with known vulnerability	☐
Leakage of unnecessary system information which can assist an attacker	☐
Developer mode tools or default admin credentials are enabled	☐
Unnecessary network services are exposed by underlying infrastructure	☐
Fails to filter network (layer 2/3) denial of service from the Internet	☐
Possible for another tenant to read deallocated cloud storage	☐

EXPOSURE

Determined cyber attack on infrastructure

FOR ASSET:

VULNERABILITY	EXPOSURE?
Running version of a dependency with 'zero day' vulnerability	☐
Possible to escalate privlege from another system	☐
Able to escalate privlege via cloud vendor side channel attack	☐
Possible to spawn a malicious process	☐
Possible for malicious process to read plaintext secret configuration at rest	☐
Possible for malicious process to read plaintext credentials at rest	☐
Possible for malicious process to read sensitive information from logs	☐
Possible to steal plaintext data from disc	☐
Possible to mount attack on other system components via network	☐

EXPOSURE

Access to data or services

FOR ASSET:

VULNERABILITY	EXPOSURE?
Lack of access control, i.e. any form of authentication	☐
Use of shared accounts and credentials	☐
Reliance on a single factor for authentication	☐
Failure to configure access, i.e. based on least privlege	☐
Lack of identity or entitlement checks in setting up a new account	☐
Weakness in offline process to reset credentials	☐
Lack of audit log showing user access to sensitive data	☐
Lack access control to audit log showing user access to sensitive data	☐
Lack of awareness material to communicate audit and abuse policy to user	☐

EXPOSURE

Support for GDPR subject access rights

FOR ASSET:

VULNERABILITY	EXPOSURE?
Lack of means to purge personal data for a data subject in response to request	☐
Lack of means to correct personal data for a data subject in response to request	☐
Lack of features to package personal data for access request or transfer to a competitor	☐
Lack of data retention policy for personal data	☐
Personal data is being stored without a justification for processing	☐

EXPOSURE

Server-side web implementation

FOR ASSET:

VULNERABILITY	EXPOSURE?
Fails to prevent stored or reflected Cross Site Scripting (XSS)	☐
File upload feature fails to block malware	☐
Fails to prevent SQL, XML (XXE) or LDAP injection	☐
Fails to prevent shell injection	☐
Fails to prevent open redirects	☐
Fails to prevent Cross-site request forgery (CSRF)	☐
It is possible for attacker to tamper with cookies	☐
Framework support for mass binding can be exploited	☐
Alternate character encodings can be used to circumvent protections	☐
User forms can be completed in a scripted manner	☐
Lack of rate limiting allows 'scraping' or 'spidering' of valuable data	☐
URL paths can be manipulated to access system files or load remote files	☐
URL paths can be manipulated to access unauthorised resources	☐
Developers have disabled framework security protections	☐
Application is sensitive to application layer denial of service	☐
Triggering an exception leaks unnecessary information that can assist attacker	☐

EXPOSURE

Access control implementation

FOR ASSET:

VULNERABILITY	EXPOSURE?
Authentication, authorisation or session management has been coded from scratch	☐
Authentication mechanism subject to brute force attack	☐
Input can be manipulated to enumerate all users	☐
Failure to allow use of password manager and strong credentials	☐
Failure to prevent users creating weak credentials	☐
An attacker can trivially guess session identifier	☐
Lack of access control on resources not intended to be discoverable to user	☐
Lack of protection against an attacker hijacking a session	☐
It is possible for attacker to tamper with session cookies	☐
Failure to check authorisation to more sensitive resources	☐
Failure to reauthenticate session when taking destructive actions, such as delete account	☐
Failure of session to timeout after a reasonable duration of time	☐
Failure to prevent caching of credentials on a shared computer	☐
Failure of user interface obscure entry of credentials	☐
Can authenticate with credentials harvested from other breaches	☐

EXPOSURE

End users

FOR ASSET:

VULNERABILITY	EXPOSURE?
Lack of control over malware or shared logins on endpoint devices	☐
Lack awareness of audit and access policy	☐

EXPOSURE

Developers or Devops Users

FOR ASSET:

VULNERABILITY	EXPOSURE?
Secrets are stored in plain text in source control	☐
Lack of full disc encryption on devices containing configuration secrets or data	☐
Lack of tooling to prevent pushing configuration secrets to source control	☐
Lack of access control based on least privlege in delivery infrastructure, scm or cloud console/API	☐
Failure to revoke access to delivery infrastructure rapidly when someone leaves	☐
Lack of policy and awareness for troubleshooting with copies of production data	☐
Sensitive information is present in log files	☐
Lack of peer review prior to deployment of code to production	☐
Lack of audit log showing user actions within delivery infrastructure	☐
Lack of integrity signatures on artefacts passing through delivery pipeline	☐
Lack of tests to verify functionality of security enforcing application code	☐
Lack of awareness of threat from phishing to developer devices	☐
Lack of protection from malware on developer devices	☐
Poor morale or short term staff in production support roles	☐

EXPOSURE

Mobile app implementation

FOR ASSET:

VULNERABILITY	EXPOSURE?
Guessable values such as IMEI number used in authentication	☐
Sensitive data stored in unencrypted storage	☐
Sensitive data is leaked into logs	☐
Sensitive data is stored in predictable locations in memory	☐

EXPOSURE

Browser based app implemention

FOR ASSET:

VULNERABILITY	EXPOSURE?
Fails to prevent DOM based Cross Site Scripting (XSS)	☐
Fails to prevent clickjacking	☐
Authenticated data is not removed from browser storage when session ends	☐
Lack of Client Security Policy (CSP) configration allows loading of untrusted resources	☐
Lack of Cross Origin Resource Sharing (CORS) configration allows loading of untrusted resources	☐
Dependency on browser-based access control implementation	☐
Dependency on browser based business logic	☐
Scripts to display advertising contain malicious code	☐
Code injection is possible via JSON responses recieved from server	☐
Transfers between DOM contexts are subject to code injection	☐

EXPOSURE

Network transport of data

FOR ASSET:

VULNERABILITY	EXPOSURE?
Cleartext transport of credentials or data over Wifi	☐
Cleartext transport of credentials or data across Internet	☐
Cleartext transport of credentials or data between system components	☐
Configuration of TLS is vulnerable to a 'downgrade' attack	☐
TLS Cyphers configured are not upto date or do not provide forward secrecy	☐
Lack of anti-caching headers to prevent caching of sensitive HTTP requests or responses	☐
Lack of measures to prevent domain spoofing, such as Strict Transport Security	☐