Application/SaaS Security Standards Checklist

Section	Main head	Objective	Risk Statement	Risk Rating	Techical Check/ Procedural Check	Available (Yes/No)	Policy
1	Data Validation	Protection against invalidated inputs	Validation against SQL injection, Cross Site Scripting, HTTP Splitting and Smuggling may occur which may further lead to unauthorized access.	High	Technical		
2	Data Validation	Client side validation checks	Client side validation technique heavily relies on client side scripting languages likes JavaScript or vbscript which can be easily manipulated. Applications completely relying on client side validations are highly vulnerable as an attacker can easily bypass the validation since he has control over the client side validation	High	Technical		
3	Data Validation	Authentication of file upload	Lack of scanning before allowing the uploading of the file may result into the entry of malware into a secure zone.	High	Technical		
4	Authentication	Password Management	* Weak passwords may result in to a successful brute force attack which may further lead to unauthorized access/change of data. * Changing of passwords at regular intervals * New password force change * Password change history * Password masking	High	Technical		
5	Authentication	User password change and login process	* The users password may be compromised if the password change process is not secure. * Login failure message	Medium	Procedural		

6	Authentication	User ID Management	* Last login details * Successful login message	High	Technical		
7	Authorization	Application access to the database with the drop and delete Permissions	The security of the database may get compromised if the access to applications is compromised and the connection to the database is not secured.	High	Technical		
8	Authorization	Database Access to underlying Operating System	Unrestricted access to underlying operating system may to lead to compromise or unauthorized access of the operating system.	High	Technical		
9	Provisioning & Reports	Different states of User ID	It will be impossible to perform effective user access management if the user states are not flagged.	Medium	Procedural		
10	Provisioning & Reports	Report	In the absence of the reports mentioned below **Auditing and Logging Report**, unauthorized activities related to creation/modification/disabling of user-ids and other such related activities will remain unnoticed.	High	Procedural		
11	Sensitive Data and Data Encryption	Use of vulnerable protocols	Passing sensitive data over the vulnerable protocols like HTTP, SOAP/HTTP, SOAP/JMS etc. may result into compromise of the data security.	Medium	Technical		

12	Sensitive Data and Data Encryption	Masking of input fields	Lack of appropriate masking of user input may result into compromise of data security through social engineering.	High	Technical		
13	Sensitive Data and Data Encryption	Password Encryption	In the absence of this, passwords can be sniffed using a sniffer and application misused.	Medium	Technical		
14	Sensitive Data and Data Encryption	Storing of Sensitive Data	Storing of sensitive data in clear text may result into compromise of the data security.	High	Technical		
15	Sensitive Data and Data Encryption	Communication Channel Security	If the communication channel does not implement strong encryption for transmission of all the sensitive information, confidentiality and integrity of the data in transit won’t be protected as the application will be vulnerable to eavesdropping.	Medium	Technical		
16	Session Management	Session time out	Unauthorized access to critical systems which could result in modification, deletion and theft of information or denial of service attacks may occur.	High	Technical		
17	Cryptography	Encryption Algorithm	Confidentiality & Integrity of information may get compromised	Medium	Procedural		

18	Cryptography	Key Management	Keys ensure non-repudiation of transaction. In case of loss, misuse of keys the organization may suffer loss of critical information and/or be held responsible for non-compliance. Identity of important persons/authorities may be spoofed.	High	Technical		
19	Auditing and Logging	Audit Log	Attempt of unauthorized access may go undetected if auditing is not enabled to capture security events	High	Procedural		
20	Auditing and Logging	Security of logs	Integrity and availability of the logs and the information therein can be altered	High	Procedural		
21	Auditing and Logging	Minimum information to capture audit logs	In sufficient information may render the logs to be less useful.	Medium	Procedural		
22	Node Hardening	Unnecessary Applications Services	Unnecessary network services if enabled on the server may be used by the attackers to compromise the security of the application	High	Technical		
23	Code Management	Storing confidential data in code	Confidential details like passwords etc. if hard coded may result in to the compromise of the application if the source code access is compromised.	High	Procedural		

24	Code Management	Source Code Protection	Lack of source code protection may result into development of exploits and rogue applications.	High	Technical		
25	Code Management	Third Party Library/Code	Use of commonly available library / code / sample code may introduce vulnerabilities into the application.	Medium	Technical		
26	Code Management	B.12.7. Application development based on secure coding guidelines	In the absence of secure coding guidelines, common coding vulnerabilities may creep into the software development processes, resulting into unse-cure applications.	High	Procedural		
27	Application Security Interface Controls	File Integrity Checks	Lack of data integrity checks renders the data being exchanged through the interfaces unreliable.	High	Technical		
28	Application Security Interface Controls	File Encryption	Lack of encryption control, renders the data being exchanged through the interfaces unsafe .	High	Technical		
29	Security Headers	Implementation of Security Headers	Absence of security headers makes an application vulnerable to various attacks like MITM, clickjacking, XSS, etc.	Medium	Procedural		

30	Web Based Technologies	Buffer Overflows	Web application components in some languages that do not properly validate input can be crashed and, in some cases, used to take control of a process. These components can include CGI, libraries, drivers, and web application server components.	Medium	~~Technical~~		
31	Web Based Technologies	Denial of Service	Attackers can consume web application resources to a point where other legitimate users can no longer access or use the application. Attackers can also lock users out of their accounts or even cause the entire application to fail.	High	Technical		
32	Web Based Technologies	Storing System Data in Documents	Storing of confidential information in the code / application documents may result into compromise of the data security.	Medium	Technical		
33	Webservices	Authentication and Authorization	Unauthorized Access to application	High	Technical		
34	Webservices	Session-Based Authentication	If the session tokens are exposed in the URLs, it might lead to session hijacking.	High	Technical		
35	Webservices	Anti-farming	If access to API by third-party aggregators is not throttled properly, this could impose excessive load on the API backend, reducing the service quality for consumers and even denial of service, denying service to legitimate users.	High	Technical		

36	Webservices	Protect HTTP methods	If HTTP method is not validated, it might result in an invalid action being performed.	High	Technical		
37	Webservices	SAML Assertion	Unauthorized access	High	Technical		
38	Webservices	Schema Validation	The Schema defination have various paramters to be passed with each parameter, the improper validation on the parameters may lead to improper input validation attacks or XML Injection attacks.	Medium	Technical		
39	Webservices	Input Validation (Content Validation)	Improper Content validation may lead to XML Bomb Attacks, XML Injections, Malformed XML can be passed.	High	Technical		
40	Webservices	Validate incoming content-types	If the content-type is not validated, it might result in acceptance of malicious data.	High	Technical		
41	Security standards for applications that store/process/transmit cardholder data	Authenticate access to databases containing confidential data	If the access to critical databases is not restricted through proper authentication measures, sensitiveity & integrity of the confidential data can be compromised.	High	Technical		

42	Security standards for applications that store/process/transmit cardholder data	Confidential data and SAD logging, in debugging environment	Confidential data and Sensitive Authentication data (SAD) can be compromised if adequate controls are not enabled in debugging mode.	High	Technical		
43	Security standards for applications that store/process/transmit cardholder data	Storage of Sensitive Authentication Data (SAD) not permitted	Storing sensitive authentication e.g. data contained in the payment card's storage chip or full magnetic stripe, including the printed 3-4 digit card validation code on the front or back of the payment card after authorization will automatically result into PCI DSS non-compliance.	High	Technical		
44	Security standards for applications that store/process/transmit cardholder data	Audit logs - date & time synchronization	Investigating on incidents will become cumbersome if time is not synchronized with the centralized server/device.	High	Technical		
45	Security standards for applications that store/process/transmit cardholder data	Audit log reports (In addition to B.9.1)	Attempt of unauthorized access may go undetected if auditing is not enabled to capture security events.	High	Procedural		
46	Security standards for applications that store/process/transmit cardholder data	Minimum information to capture audit logs (In addition to B.9.3)	In sufficient information may render the logs to be less useful.	Medium	Procedural		
47	Security standards for applications that store/process/transmit cardholder data	Audit Logs protection (In addition to B.9.4)	In the absence of this, logs may be tampered with or logs may be disabled.	High	Procedural		

48	Code Signing	Code signatures	Improperly signed code may lead to mobile application tampering/modification.	High	Technical		
49	Code Signing	Certificates/crypto keys	Improper custody of certificates /code signing keys may lead to application tampering/modification	High	Technical		
50	Code Signing	Manifest/configuration files parameter tampering	tampering/modification of manifest/configuration files may lead to application piracy, MITM attacks	High	Technical		
51	Code Signing	File / process permissions	improper process permissions from the application on the device may lead to privacy issues	Low	Technical		
52	Communication Channels Security	Secure application data/messages transmission over communication channels (https etc)	Insecure data transmission over communication protocols may lead to tampering/modification of application messages/data	Medium	Technical		
53	Communication Channels Security	Certificate Pinning	If a certificate authority is compromised, sending fraudulent certificates could have an impact on the confidentiality of the transmitted information, due to the fact that the application would trust these certificates because they are provided by a known certificate authority.	Medium	Technical		

54	Local Database Storage	Secure local database storage	1. Clear text data stored at local device memory/external memory card can cause sensitive information disclosure. 2. Clear text data stored at local device memory/external memory card, can be modified/tampered for malicious activities	High	Technical		
55	Local Database Storage	UI Declarations in local database	UI impersonation through modification/tampering of UI declarations available in device memory/external card may lead to fradulent transactions	Medium	Technical		
56	Session Management	Unique session ID transmission	Improper session creation, session ID transmissions or no session ID's may cause for privilege escalations , session hijacking or session fixation attacks.	Medium	Technical		
57	Session Management	Server side Session ID validations	Improper server side session validations may lead to session reply, privileges escalations attacks	High	Technical		
58	Session Management	Session Timeout	If the device is stolen/lost or accessed by an unauthorized person, he/she can get access to the application and user's data.	Medium	Technical		
59	API Design & Working	Encryption/Masking on Sensitive Data parameters	Sensitive data like ATM PIN, Credit card numbers, PII etc. can be used by an attacker for carrying out fraudulent transactions on behalf of legitimate user.	High	Technical		

60	API Design & Working	Follow Secure Coding Practices on below security controls and vulnerabilities - 1- Authentication & Authorization 2- Data Validation 3- Session Management	Not following secure coding guidelines may introduce security loop holes at coding level which in turn may lead to security breach.	Medium	Technical		
61	Container	Host Security	In case the Host gets exploited, the underlying process will get impacted.	High	Technical		
62	Container	Runtime Security	In event of missing runtime restrictions may lead auto	High	Technical		
63	Container	Image Authenticity	The images from unofficial resources pose risk of having malware in them	High	Technical		
64	Container	Resource Utilisation	Overusage may lead to DOS	High	Technical		
65	Container	Excess Privileges	Apps having System or Kernel level priviledges may lead to priviledge abuse	High	Technical		