शक् 14 फाल्गुन 1938
विक्रमी 22 फाल्गुन 2073

MARCH 2017
मार्च रविवार

SUNDAY 05

Mobile Security : which refers to the protection of mobile device against cyber security threats

- due to posted sensitive information stored on and transmitted by laptops, smartphones, tablets and other portable devices.

- Main goal is to prevent data from un authorized user

Engagements

Mobile device : - important part in net-work (smartphones, Tablets, memory

शक् 15 फाल्गुन 1938
विक्रमी 23 फाल्गुन 2073

- easy to use.

MARCH 2017
मार्च सोमवार

MONDAY 06

Threats :-

1) Lack of physical security Controls → (move)

2) use of untrusted mobile devices (inc org^n)

3) use of untrusted n/w - (personal hotspot)

4) use of application created by unknown parties. (unknown app/website)

Engagements

प्रत्येक व्यक्तित्व विश्व का एक रहस्य है — जे. सी. पोविस

5) Interaction with other systems (automatic data sync.)

MARCH 2017
मार्च मंगलवार

शक 16 फाल्गुन 1938
विक्रमी 24 फाल्गुन 2073

07 TUESDAY

6) use of Untrusted Content - (QR Code)

7) use of location services (GPS)

Mobile Security strategies

We have (3) elements in mobile devices security

I) Device security :- security and privacy of device being used.

Engagements

→ Jailbroken devices should not be used

→ Auto lock enabled.

MARCH 2017
मार्च बुधवार

शक 17 फाल्गुन 1938
विक्रमी 25 फाल्गुन 2073

08 WEDNESDAY

→ password/pin protection

→ autofill usernames/passwords.

→ s/w and OS upto date

→ disable location services.

→ avoid installing third party applications

→ security trainings should be given.

II) Traffic security :-

Engagements

Based on authentication and encryption

बुद्धि द्वारा सधा हुआ उत्साह ही लगन है — पास्कल

adv.

- All traffic in the n/w should be encrypted.

- All traffic should travel in secure channel (SSL / IPV6).

- VPN should be used Virtual private N/w.

- Strong authentication protocols. (HTTPS Kaberos, PGP).

5) Passive Security :-
Engagements
Establishing barriers to prevent unauthorised sources into the n/w.
→ firewalls.
→ intrusion detection systems and prevention

Hackers :-

1) White Hat → legal
2) Black Hat → illegal
3) Grey Hat → illegal + legal

Engagements

MARCH 2017
मार्च शनिवार

शक 20 फाल्गुन 1938
विक्रमी 28 फाल्गुन 2073

11 SATURDAY

Web application :- is a piece of s/w which can be accessed from a browser, and stored on web server.
(also called as web service) → can host multiple app.

↓ is an application that we use for browsing on internet
eg:- IE, firefox, google chrome
• browser is also known as web client or user agent. (→ url, telnet)

Engagements

IE, google chrome, firefox.

MARCH 2017
मार्च रविवार

(protocol)

शक 21 फाल्गुन 1938
विक्रमी 29 फाल्गुन 2073

12 SUNDAY

web client / user agent → url, Telnet
web application / web server

• protocol → same set of rules, grammer for the comm. of 2 applications.

• HTTP → mostly used (web server and web client communicates with HTTP protocol.
• FTP
• SMTP etc.

• Web resource is a document like → PDF, HTML, xml file, JSON ~~
Engagements
hosted by web server.

काम सरल है, विचार कठिन – गेट

Web Client can access the resources or these file ~~from~~ through web server.

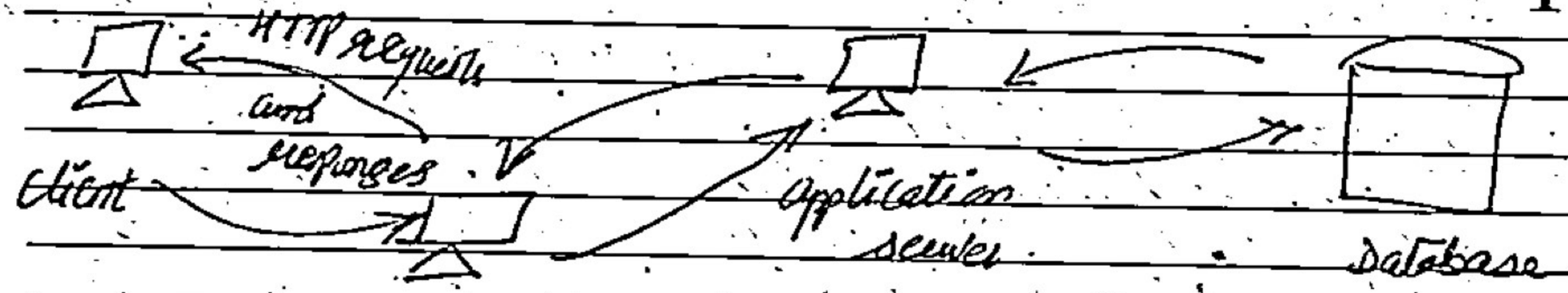
- Resources. (Static / Dynamic.

Standalone application :
- Need to install in your system.
- Does not require internet connection.
- eg:- msoffice, Powerpoint.

Web application examples are → facebook, Netflix, Gmail.

- Source code is present on web server, so to access it we need internet

How Web application works:-



- Web app. uses app. server and Database
- After giving response back to the web client, the connection is closed and the web server does not ~~require~~ remember about the past connections, who the client, where.

जिस आदत से आनन्द मिले, वह आदत मत डालो — इमर्सन

- Next time, client sends another request web server consider that as a new request, coming from new client.

15 WEDNESDAY — because of this nature HTTP is protocol known as stateless protocol.

Hacking web applications :-

Some common forms of attacks are :

1) cross site scripting (XSS)

2) cross site request forgery (CSRF) — is an attack that forces a user to perform an unintended action e.g. get them to change their password or transfer funds to the attackers account.

Engagements

16 THURSDAY

3) SQL injection → login page related problem.

4) broken authentication → This includes vulnerabilities that allow users to set weak passwords, have weak or easily guessable recovery password questions, allowing brute force login attempts. → Credential stocking.

5) broken access control :

Problem in Access ↓ Attacker can take the access of Admin

Engagements

अतिशय मोह ही मनुष्य को कमजोर बना देता है — चाणक्य

browser.
Cookies → Stores the data.
Inside browser. (sniffing what data for how long)

Web application security mechanism

- Authentication.
- Session management → Login id / Password (web server matches with data base)
- Access Control.

if Correct
↓
then generate session id (long string)
↓
(send through cookies) passes in url.

Browser Extensions It is a small s/w module for customizing web browser.

- browsers allows variety of extensions including user interface modifications
- Cookie management, ad blocking, Pop ups and customer scripting and styling of web pages.

- Extensions are typically used to add features and enhance the functionality of a website they can also be used to remove unwanted websites elements such as pop up ads and features such as auto play for online videos.