शक् 11 वैशाख 1939
विक्रमी 19 वैशाख 2074

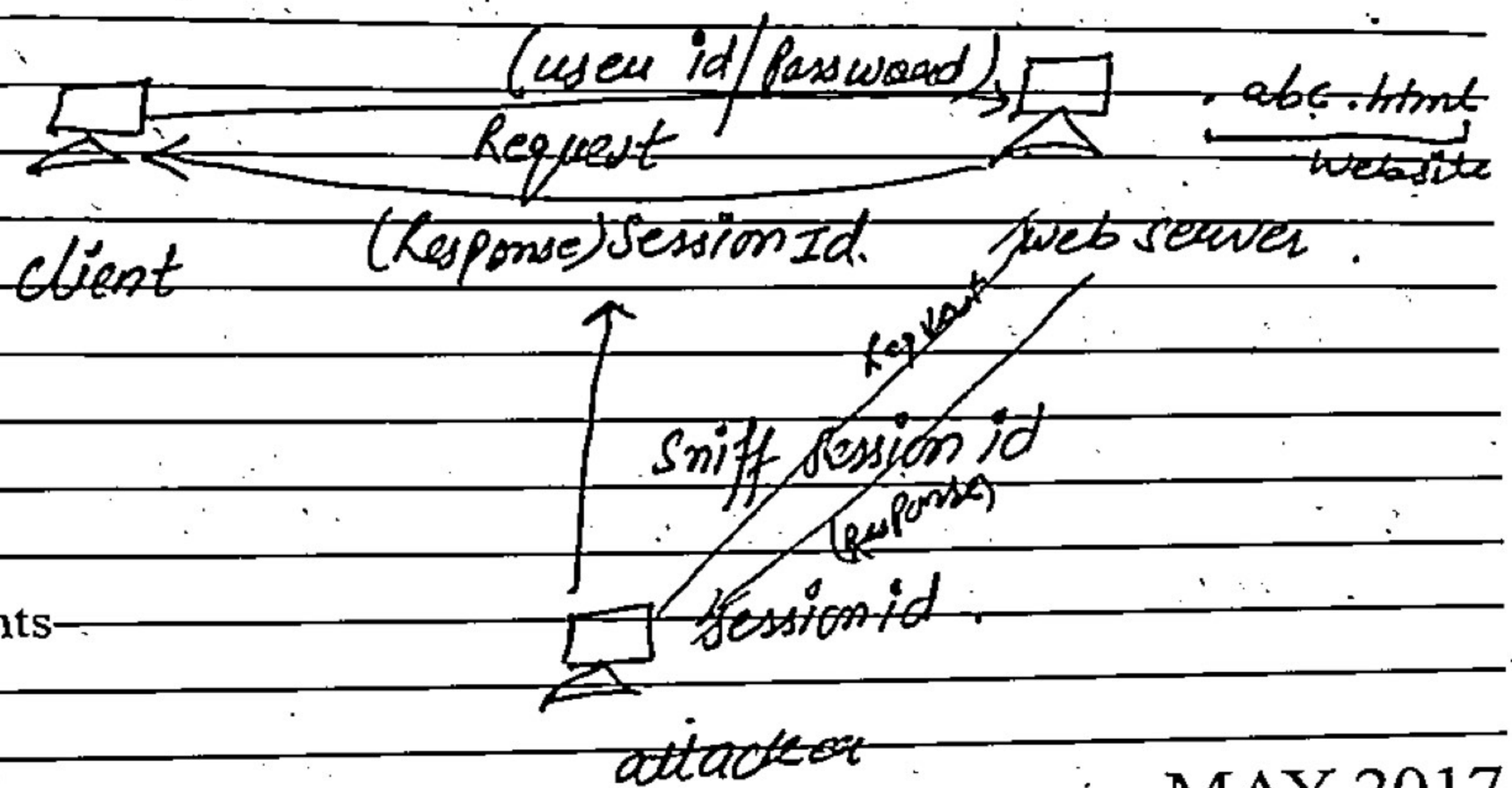
Session → interaction b/w two communication end points.

MAY 2017
मई सोमवार
MONDAY 01

Session Hijacking :-

- Session id's are stored in cookies, URL and hidden field of web pages.

Session :-



Engagements

शक् 12 वैशाख 1939
विक्रमी 20 वैशाख 2074

MAY 2017
मई मंगलवार
TUESDAY 02

- Session hijacking is also known as Tcp session hijacking.

- It is a method of taking over a web user session by secretly obtaining the session id and act as authorized user. After obtaining session id an attacker can do anything that authorized user is allowed to do on the network.

- The attacker can get access to server without having to authenticate to it.

Engagements

अत्याचार और भय परस्पर हाथ मिलाते हैं – बाल्जक

03 WEDNESDAY • session id is generally of 16 digits and in hexadecimal

• A session id is an identification string (usually a long, random, alpha/numeric string) that is transmitted b/w the client and server.

• Session id's are commonly stored in cookie URL's and hidden fields of web pages.

Engagements

Session sniffing :- This is one of the most basic techniques used

04 THURSDAY with application layer session hijacking. The attacker uses a sniffer, such a wireshark on a proxy such as OWASP zed to capture n/w traffic containing the session id b/w a website and a client.

• once the attacker captures this value he can use this valid token to gain unauthorized access.

Engagements

Reasons of session hijacking:- FRIDAY 05

1) Insecure way of handling session id. session id is transmitted over the n/w without any encryption mechanism. once attacker gains access to session id, it can be directly used.

2) The current session id generation algorithm are weak, so it becomes easy for attackers to predict the next session id.

3) once the attacker hijacks the session they no longer have to worry about authenticating to the server as long as communication session remains active, there is no auto time out.

4) The account does not get locked out due to invalid session id. (brute force) → attacker get chance to retry on random the session id.

Engagements

MAY 2017
मई रविवार

शक 17 वैशाख 1939
विक्रमी 25 वैशाख 2074

07 ~~SUN~~DAY Types or Methods of Session hijacking

1) Brute forces In brute-force attack, the attacker simply guesses the session id and uses it to perform the attack.

- Brute force attacks usually works only when the websites has weak security and uses short, easy to guess session key.

Engagements

2) Cross-site scripting :- A cross site scripting attack initially takes an advantages of weak security spots and vulnerabilities in a web server. Then, the attacker inserts scripts into a web pages that cause your web browser to reveal your session key to the attackers so they can take over the session.

MAY 2017
मई सोमवार

शक 18 वैशाख 1939
विक्रमी 26 वैशाख 2074

08 MONDAY

3) Malware :- One of the most common methods cyber criminals use is phishing attacks.

Engagements In this attack, hackers send you professional looking emails that contain malicious links, which

अत्याचार और भय परस्पर हाथ मिलाते हैं – बाल्जक

installs malware and viruses on your device allowing them to hijack a session.

• The malware then may conduct "session sniffing" to find of the session and send it to the criminals, who can then get your session id to take over your session.

4) Sesion fixation:- In a session fixation attack the criminal creates a session id and tricks the user into starting a session with it.

• one common way to do this is to send a malicious link through emails that lead to a login form for the attacker's website.

Then, when the user logs in with the phony (fake) sesion id, the attacker continues the hijack.

MAY 2017
मई वीरवार

शक 21 वैशाख 1939
विक्रमी 29 वैशाख 2074

11 THURSDAY # How to prevent session hijacking

1. Use strong passwords and multifactor Authentication.

2. only share session ID's with trusted sources.

3. Use a VPN. VPN helps to prevent attacks from intercepting traffic, making it more difficult for them to steal session ID's

Engagements

4. Keep s/w up to date.

5. use HTTPS only, as the use of https ensures that there is SSL/TLS encryption throughout the session traffic

MAY 2017
मई शुक्रवार

शक 22 वैशाख 1939
विक्रमी 30 वैशाख 2074

12 FRIDAY

5). HTTPS: The use of HTTPS ensures that there is SSL/TLS encryption throughout the session traffic. Attackers will be unable to intercept the plaintext session id.

first PC venus to PC owner

Engagements

मां का हृदय बच्चे की पाठशाला है – एच. डब्ल्यू. बीचर

Malware :- stands for malicious software

• Malware are the computer programs designed to infiltrate and damage computers without the users consent.

• Damage like → It can steal the information, Encrypt or delete or modifying the sensitive data without any permission.

Engagements

Types :- (3) Viruses can modify the program functionality
e.g :- files deletion or launching a media player application.

1) Viruses :-

V → Vital
I → Information.
R → Resources.
U → under
S → Seize

• depends on human action.

(2) Virus is a program or code that attaches itself to the application and runs whenever the application runs.

• Creeper → was the first virus in the N/w. Antivirus Reaper in Arpanet (ADV. Research project Agency Network).

2) Worms :- are like a virus, but implementation is different.

Engagements

• It does not modify program

• Independent

• it Replicates itself again and again

MAY 2017
मई सोमवार

शक 25 वैशाख 1939
विक्रमी 2 ज्येष्ठ 2074

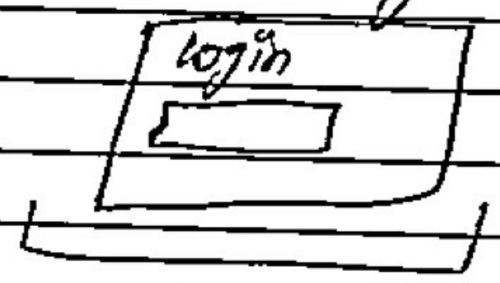
• it spreads allover the system (N/w).
as it uses the address book of the syl. and spread in all the system through the emails.

13 MONDAY → it Consumes lots of Computer Resources which makes the system work slow.

3) Trojan Horse :- It is a hidden piece of code which is intended to leak your Confidential information.

• it does not modify and don't replicate.

• Comes through fake email in a attachments



• space ↑
• clean memory
• memory ↑
• Virus Remove
• Protects from fake

Engagements

Trojan horse attached with browser so it is recording the keys you are typing. and send this credential info to the hackers.

MAY 2017
मई मंगलवार

शक 26 वैशाख 1939
विक्रमी 3 ज्येष्ठ 2074

16 TUESDAY

4) Ransomware :- Ransomware is a virus s/w that infects a users system and encrypts its data and demand a "Ransome" payment usually in a Crypto Currency or in bitcoin.

• once the amount is paid the vitim can decrypt / unlock its device/system.

any s/w can be denied.

5) Spyware :- as spyware if downloading without user's authentication.

Engagements

Its purpose is to steal private information from a computer system for a third party. Spyware collects

Video pictures
downloads
audio files
webcam

मालिक और उसकी सम्पत्ति दोनों को शीघ्र ही विलग होना पड़ता है — अंग्रेजी कहावत

information and sends it to the Hacker

6) Adware :- are programs that pop-ups various advertisements and offers, often based on the websites you visit. These ads are independent from popup windows that appear when visiting specific sites.

7) Bomb :- It enters in our system, remains inactive for a long time and it waits for specific date and time. When that time and date is active it suddenly do the disaster

eg:- Friday 13, etc.

1) Buffer overflow :- "Buffer" are memory storage regions that temporarily hold data while it is being transferred from one location to another.

Buffer overflow" occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations.

2) Buffer overflow is an example of bad programming.

20 bytes

2 marks → 5 Ques.
5 marks → 4 Ques
10 marks → 3 Ques.
60 marks

MAY 2017
मई शुक्रवार

शक 29 वैशाख 1939
विक्रमी 6 ज्येष्ठ 2074

19 FRIDAY

Buffer is Sequential Memory Buffer

1	2	3	4	5	6

→ We may overwrite another value

Program 1 (5 elements) 6 यहाँ store at adjacent memory loc.

Engagements

Experiment 6 : (foot printing) Website mirroring

MAY 2017
मई शनिवार

शक 30 वैशाख 1939
विक्रमी 7 ज्येष्ठ 2074

20 SATURDAY

website footprinting is a technique in which we gather information of any organization's official website. For gaining information such as versions of these software's, operating systems, sub-directories, database scripting information and other details.

Google → HTtrack.
↓
website copier.
↓
Download.
↓
Next
↓
Accept
↓
Next → (8)

Menu
↓
Notepad file close.
↓
next
↓
Set name
↓
next.

website URL fill
↓
finish
↓
copying data
↓
Close

Engagements

युद्ध ऐसा धन्धा है, जिसमें मनुष्य सम्मानपूर्वक नहीं रह सकता — मैकियावली

(3) • Buffer overflow, or buffer overrun occurs when more data is put into a fixed length buffer than the buffer can handle.

• The extra information, which has to go somewhere can overflow into adjacent memory space corrupting or overwriting the data held in that space.

• This overflow usually results in a system crash, but it also creates the opportunity for an attacker to run arbitrary code. Engagements- or manipulate the coding errors to prompt malicious actions. (Bound checking)

Encoding and escaping data :-

• Encoding is transforming data from one format into another format.

(1) • Encoding and escaping are defensive techniques meant to stop injection attacks.

(2) • Encoding involves translating special characters into some different but equivalent form that is no longer dangerous in the target interpreter.

Engagements-

(5) • For example translating the '<' character into the < string

MAY 2017
मई मंगलवार

शक 2 ज्येष्ठ 1939
विक्रमी 10 ज्येष्ठ 2074

23 TUESDAY When writing to an HTML page.

- Escaping involves adding a special character before the character string to avoid it being misinterpreted.
- For example adding a character before a " (double quote) character so that it is interpreted as text and not as closing a string.

(1). Escaping is a subset of encoding where not all characters need to be encoded, only some characters are encoded by using an escape character (\)

Engagements

MAY 2017
मई बुधवार

शक 3 ज्येष्ठ 1939
विक्रमी 11 ज्येष्ठ 2074

24 WEDNESDAY

e.g.- \n → new line, \t → Horizontal tab, \b → Backspace, \v → vertical tab, \' → single quotation mark, \" → Double quotation mark, \? → Question mark.

- escaping is to avoid cross-site scripting attacks

SQL Injection:- is a technique used to exploit user data through web page inputs by injecting SQL commands as statements.

Engagements

These statements can be used to manipulate the application's web server by malicious users.

प्रेम की सम्पूर्ण पेय मात्राओं में यौवन सर्वाधिक शक्तिशाली है — ऐलन

शक् 4 ज्येष्ठ 1939
विक्रमी 12 ज्येष्ठ 2074

MAY 2017
मई वीरवार

THURSDAY 25

- SQL injection is a code injection technique that might destroy your database.
- SQL injection is one of the most common web hacking techniques.

SQL injection detection Tools :-

- Netsparker
- SQLmap
- JSQL Injection
- Burp
- Acunetix web vulnerability scanner

Engagements

Java based tool
that helps IT team find database info. from distant server.
It supports linux, mac, os.

शक् 5 ज्येष्ठ 1939
विक्रमी 13 ज्येष्ठ 2074

MAY 2017
मई शुक्रवार

FRIDAY 26

Geolocation is the ability to locate a device's whereabouts using GPS, cell phones towers, wifi access points or a ~~computer~~ combination of these.

- It refers to the geographical location (latitudinal and longitudinal) of an internet connected device.

lat → symbol phi

Engagements

long → λ.

units that represent the coordinates of geographic co-ordinate sys.

N-S 0-90°

Max 180° E-W

प्रत्येक व्यक्तित्व विश्व का एक रहस्य है। जे. सी. वेस

Search of name place, city, state or address.

27 SATURDAY

VoIP :- Voice over internet protocol (VoIP), is a technology that allows you to make voice calls using a broadband internet connection instead of a regular phone line.

- Some VoIP services may only allow you to call other people using the same service, but others may allow you to call anyone who has a telephone number - including local, long distance mobile, and international numbers.

Engagements

How it works :-

28 SUNDAY

VoIP services convert your voice into a digital signal that travel over the internet. If you are calling a regular phone number, the signal is converted to a regular telephone signal before it reaches the destination.

- VoIP can allow you to make a call directly from a computer, a special VoIP phone, or a traditional phone connected to a special adapter.

- In addition, wireless "hotspot" in location such as airports, parks, and cafes allow you to connect to the internet and may enable you to use VoIP service wirelessly.

Engagements

दूसरों का सम्मान करो, लोग तुम्हारा भी सम्मान करेंगे – रविन्द्रनाथ ठाकुर

Input validation:-

- Any input that you receive, from anywhere must be validated to ensure that it is what you are expecting

For instance:

- It is the right type of data? - Date/string/integer/float/etc.
- It is within the appropriate range for size? Is it too long? Too short?
- Does that day actually exist? (June 31st is not a real day)
- Is the data is appropriate if you are expecting a username, why does it contain characters other than a-z, A-Z, 0-9? If the field is for the date of a future event why is the date entered in the past?
- Is the data is in the correct format? if it's a call to an API, is the call following the protocol of requested input?

Is the xml in the correct format?
Is it MM/DD/YY, DD/MM/YY or YYYY/DD/MM?

X path injection :- It is similar to SQL conceptually. It is also a query language and is used to locate specific elements in a XML document.

- X-path injection is a type of attack where a malicious input can lead to un-authorised access or exposure of sensitive information such as structure and content of xml document. It occurs when user's input is used in the construction of the query string.

XML → extensible markup language
- It was designed to store and transport data.

- xml does not do anything. xml is just information wrapped in tags.
- xml language has no predefined tags. tags in the examples are (like <to> and <from>) are not defined in any xml standard.
- These tags are "invented" by the author of the xml document.
- HTML works with predefined tags like <P>, <h1> <table> etc.

Engagements

Canonicalization Attack :-

Canonicalization is the process of mapping inputs to their canonical equivalent. It is often used for cryptographic algorithms and data that are intended to be secured from tampering, usually by hashing.

- Its aim to find or compute the mapping between two different inputs which produce the same output when processed by a given system.
- This technique is used to steal a victim's data from the server.
- The attacker just creates a domain, usually at different TLDs, for example :- .com, .co.uk or .info etc
- Then registers a website with that domain name, and finally publishes links to the site. from various social media or different blogs around the internet so that it will appear on search engines results pages for certain keywords searched by users.
- The attacker then waits for users who arrive at their fake site and enter their username/password in order to complete an action (eg. perform a payment).