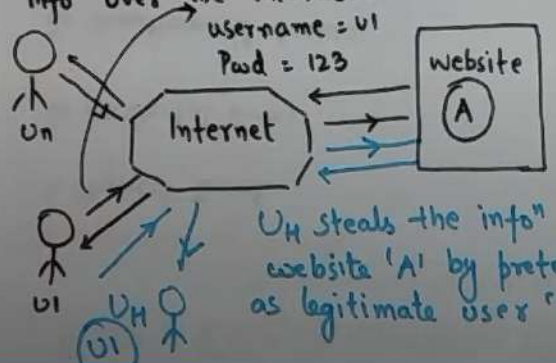
Easy Engineering Classes – Free YouTube Lectures

For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India

Security Threats: Today Information System is an integrated set of components for collecting, storing processing and communicating. Most of the Business organization rely on info" system to manage the work. But among legitimate user there are many malicious users trying to access the info" over the internet.



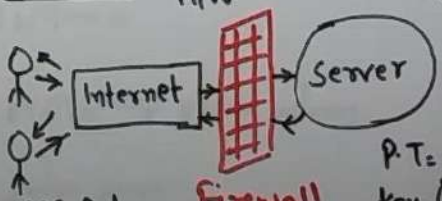
U_H steals the info" from website 'A' by pretending as legitimate user 'U1'.

Security Measure:

- i) Physical Authentication < Key, Smart Card
- ii) Biometric Authentication < fingerprint, Iris, face
- iii) Passwords → Easy to Implement.
- iv) Firewalls
- v) Data Encryption

→ IMP.

Firewall: < S/W, H/W



Data Encryption.

→ Encrypt your content into C.T.

Caesar cipher.

P.T: ABC → CDE

Key: 2

C.T: P.T+2

Classification of Threats:

i) Physical Threat → damage to H/W.
↳ Tsunami, Earthquake.

ii) Accidental Error → Corruption of data caused by Programming Error.

iii) Unauthorized Access → Info" is accessed by malicious user.

iv) Malicious Misuse → Tampering with the System. < Trojan Horses
Viruses.

Types of Threats:

i) Worm: type of virus that replicates itself but donot alter the files.

ii) Logic Bomb: Prog. code that will execute on completion/ occuring of a logic.

iii) Trapdoor: Method of gaining access to a system.

iv) Trojan Horse:

v) RATs (Remote Admin Trojans):

vi) Malware:

vii) RootKits:

viii) Virus:

(Web Engineering)

L52: Network and Denial of Service(DOS) Attack | Difference between DDOS and DOS | Web Technology

Easy Engineering Classes – Free YouTube Lectures

For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India

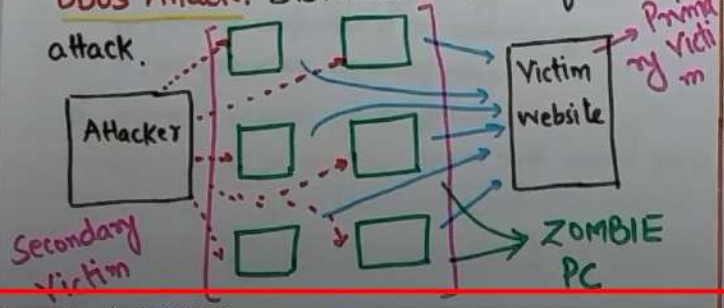
N/W and Denial of Service Attack:

DOS Attack: A denial of service (DOS) attack is a malicious attempt to make a server or a N/W resource unavailable to users.

- → TCP-SYN Flooding
- → PING OF DEATH

i) Using Internet Insecure channel
ii) Huge Traffic
iii) Security defense of a victim.
iv) Hiding attacker's ID.

DDOS Attack: Distributed Denial of Service attack.



Difference b/w DOS and DDOS Attack

DOS	DDOS
DOS attack means that one Computer and one Internet Connection is being used to flood a website/server with packets (TCP/UDP). → Intends to Overload the targeted website bandwidth and other resources.	DDOS attack means using Several Computers and Connections. The Computers behind such an attack are often distributed around the world and will be a part of BOTNET.

8:09 / 9:24

(3)

WEB SECURITY MODEL: There are many levels of Security threats to a Business.

i) Unauthorized Internal user (U1, U2) — Payment ✓/✗

ii) Former employee of an organization U1

iii) Weak Access point

iv) Wrong Management

U1 ... Um → X

Main Concepts of Security: (CIA)

i) Confidentiality (Encryption) — m1 → X → Y

ii) Integrity → Correct Message

X (m1) → Y [HASH]

m1 → O → m2 (h2)

iii) Availability

↳ Server/ Resource (DOS)

Security Features: Pwd, Biometric

i) Authentication: Verifies who you say are.

diff:

ii) Authorization: Allows only you to change your resources. → ACL

iii) Encryption: Info^n hiding.

↳ cipher text.

iv) Auditing: keeping records of op^r. (log)

Case Study: e-Commerce

The Players:

Attacker/ Hacker

S/w vendor

Provides s/w to Buyer

Internet

B2C website

Shopper/ Consumer

L53: Web Security Model | Case Study of e-Commerce Website | Web Engineering(Technology) Lectures

Press Esc to exit full screen

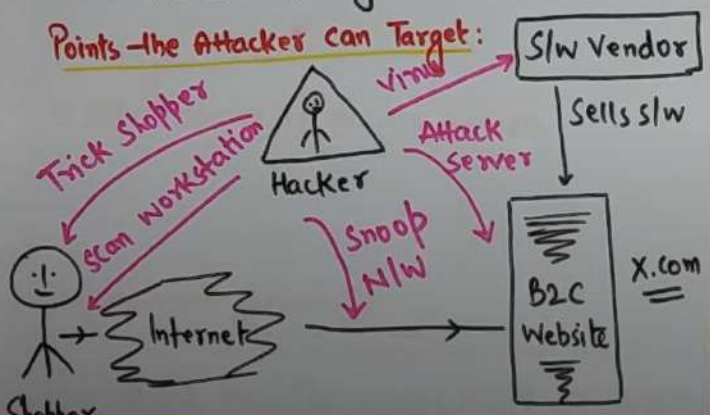
Easy Engineering Classes – Free YouTube Lectures

For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India

Criminal Incentive:

- i) Cheap Tools
- ii) Unimaginable Payoff.
- iii) Easy to locate the victim.
- iv) Anonymous
- v) Free and easy availability of info^n.

Points the Attacker can Target:



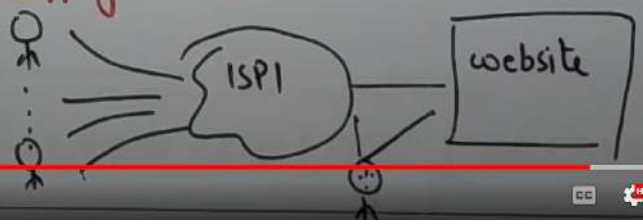
Attacks:

i) Tricking Shopper: Also called Social Engineering techniques.

- i) Gathering Info^n
- ii) Phishing → Buy P1 from X.com at 50% discount → X1.com, X.net

ii) Snooping Shopper's Computer:

iii) Sniffing the N/w:



23:31 / 25:29

L55: Web Attacks and their Prevention – SQL Injection, Cross Site Scripting(XSS), DDOS Attack

(Web Engineering)

Web Attacks and their prevention There are various web attacks like XSS, CSRF, iframe etc. To prevent them there are techniques such as firewall, data encryption etc.

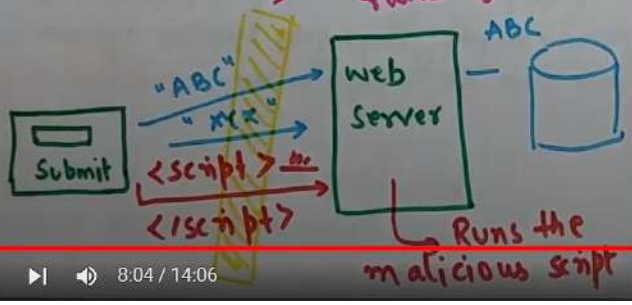
Easy Engineering Classes – Free YouTube Coaching

For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India

① Cross-Site Scripting (XSS) Attack: It allows the attacker to inject client-side script into web pages.

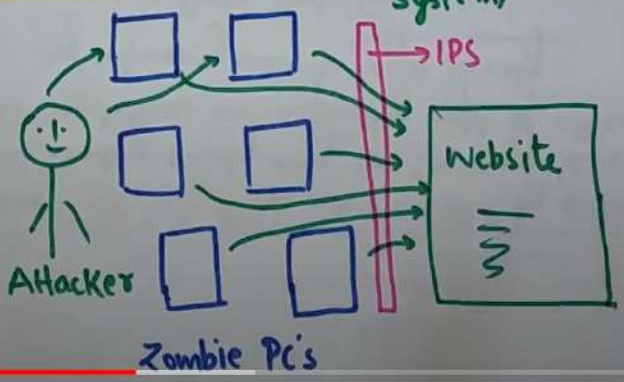
↳ May be used to by-pass access control.

Prevention:- Install Web Application Firewall (WAF)



② DDOS Attack: Known as Distributed-Denial of Service attack. In this, the malicious user tries to make a machine/NW resource unavailable to the users.

Prevention:- Firewalls → IDPS/IPS (Intrusion Prevention System)



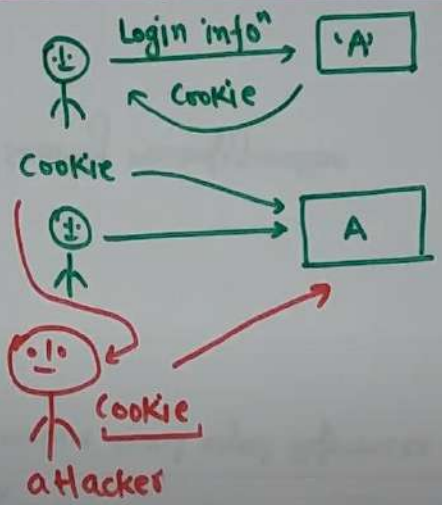
8:04 / 14:06

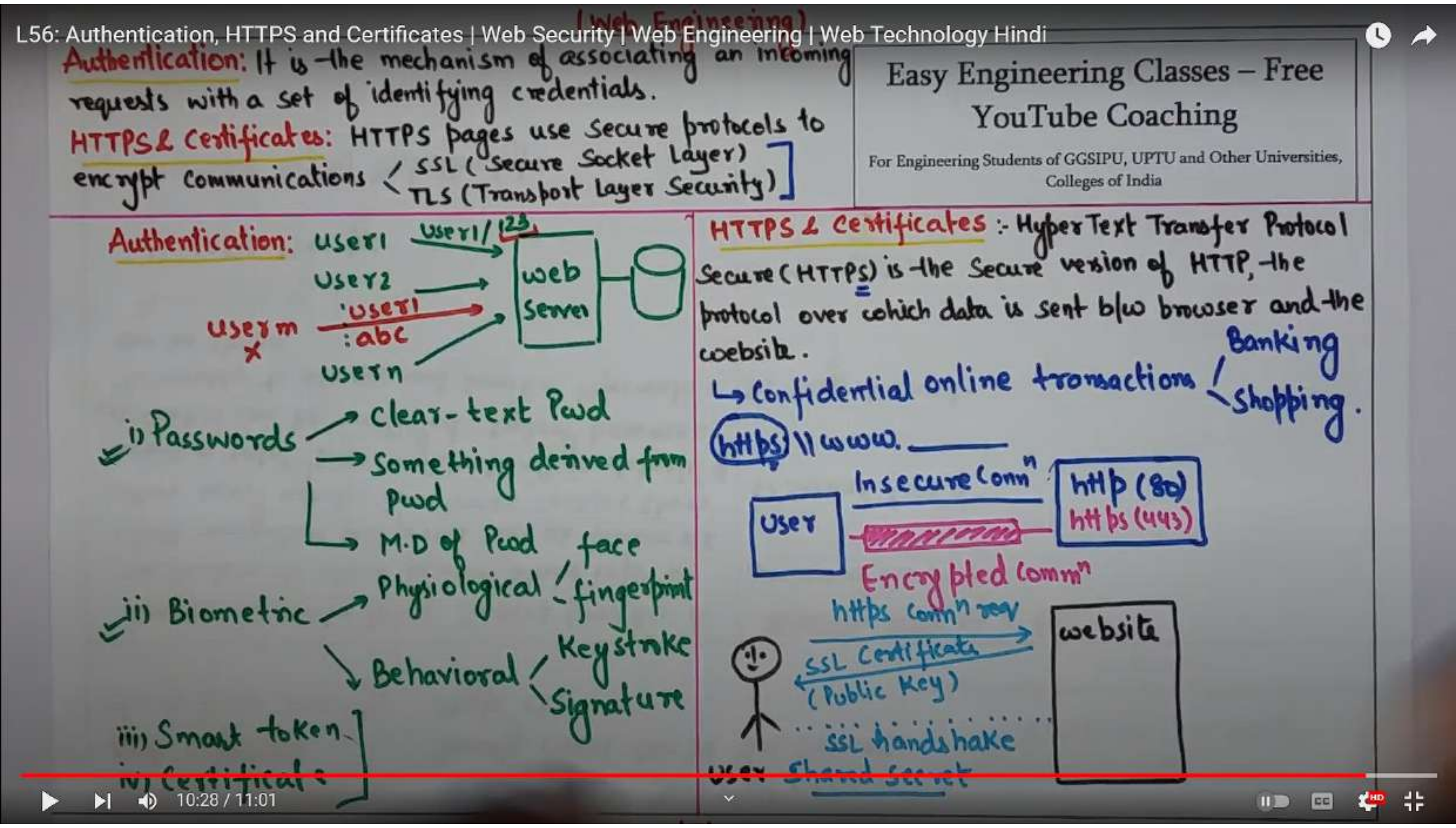
Control of databases and all the info^n.

Prevention: → Regular auditing
↳ Firewalls, IDPS/IPS.

④ Cookie Poisoning / Hijacking: Many web appl^n uses Cookies to save user info^n such as login, pwd and emails. Cookie poisoning allows the attacker to modify valid cookie & gain false authentication/authorisation information about another user and go on to steal your info^n.

Prevention: Avoid signup on website that you don't trust
↳ clear cookies before closing browser.




L56: Authentication, HTTPS and Certificates | Web Security | Web Engineering | Web Technology Hindi
Authentication: It is the mechanism of associating an incoming requests with a set of identifying credentials.
HTTPS & Certificates: HTTPS pages use secure protocols to encrypt communications < SSL (Secure Socket Layer) TLS (Transport Layer Security)
Easy Engineering Classes – Free YouTube Coaching
For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India
Authentication:
user1
user2
usern
userm
user1/123
'user1 :abc
web Server
i) Passwords
Clear-text Pwd
Something derived from Pwd
M.D of Pwd
ii) Biometric
Physiological
face
fingerprint
Behavioral
Keystroke
Signature
iii) Smart token
iv) Certificate
HTTPS & Certificates :- Hyper Text Transfer Protocol Secure (HTTPS) is the Secure version of HTTP, the protocol over which data is sent b/w browser and the website.
↳ Confidential online transactions
Banking
Shopping.
https://www.
Insecure Connⁿ
Encrypted commⁿ
User
http (80)
https (443)
https connⁿ req
SSL Certificate (Public Key)
SSL handshake
website
user
Shared secret
10:28 / 11:01

(Web Engineering)

Client-Side Security: It is related to JavaScript & Browser Security. client can be You, Browser, Skype etc.

Cookie-Security Policy: Cookies provides a mechanism to store session state info" on client navigation platforms such as browsers & other user-agents. Sometimes Cookies store Sensitive info" like registration/login details. If a Cookie can be modified, System becomes Vulnerable to attacks and Sensitive information can be stolen.

Parameters of Cookies:

1.) Cookie Max Age- → in minutes
↳ after which cookie will get automatically expired.

2.) Cookie Replay Protection type.
↳ used to prevent cookie replay attacks.

C1 C

Securing Cookie of a Site

3.) Custom Headers- Set custom headers so that a attacker can't launch cookie replay attack.

4.) Secure Cookie- "Yes"
↳ allows cookies to be returned to the web server if client uses HTTPS only.

5.) Days Allowed-
1 [C1 : Cn] no. of days for which unrecognized will not be rejected.

6.) MAC Code-
Cookie name + max age + Custom header → MD5/SHA
Cookie + Hash ↔ Hash!

L58: Plugin, Extension, Web Apps, Web User Tracking, Web Application Firewall(WAF), Fuzzer

Plugins Extensions and Web Apps: Web-Apps are basically web-sites that run's within the browser using Javascript and Html. An ex:- Google Maps, Gmail. An Extension affect something global on Your web Browser. eg:- Pop-up Blocker.

Easy Engineering Classes – Free YouTube Coaching

For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India

Web User Tracking:

- Campaign Reporting (Key words)
- Real-time Reporting (Live, opentracker)
- Why do the visitors Leave?
- Log Analysis
  - server.
  - user.

Plugins:- It is a third-party library that is plugged in to the browser and allows for being embedded on webpage. It affects only webpage that is using plugin, eg:- Adobe flash, Sun java.

Server Side Security Tools:

- (i) **Web Application Firewalls (WAFs):-** It is a firewall that monitors, filters or blocks data packets as they travel to and from a web Appl^n.
  - N/w-based WAFs — XSS, SQL-inj ection,
  - Host-based WAFs — Buffer overflow,
  - Cloud-Hosted WAFs — session hijacking.

ii) **Fuzzers:-** It is a program which injects automatically semi-random data into prog/ stack and detect bugs
- Generator (Data Generation)
- Debugging tools (Vulnerability identification)
- Appl^n fuzzing
- Protocol " "
- File format "

10:34 / 11:13

(Web Engineering)

WEB 2.0 :- It is the improved version of the web 1.0, characterized specifically by the change from static to dynamic or user-generated content & also growth of Social media.

Examples: → i) Interactive Social Media (FB, Twitter)
ii) BLOGS (Blogspot, Wordpress)
iii) WIKIS

Advantages:
- i) Availability
- ii) Variety of media
- iii) Easy to use
- iv) Dynamic
- v) Real-time discussion. (Comment, Forums)

Web 2.0 tools and features: — i) Free class"n of info".
ii) Rich User Exp.
iii) User can be a Contributor
iv) Dispersion.

Internet tools that allows the user to go beyond just receiving info" from website. Create Content / share [Drive, Twitter, Youtube]

Web 2.0 Technology Concepts:
i) Rich Internet Appl" (RIA): Graphics, Interactivity.
ii) Web-Oriented Architecture (WOA): (feeds, Rss feeds) (web services.)
iii) Social Web: user generated Content.

Issues/Limitations:
- Keyword-based
- Time Consuming
- Inconsistent terminologies
- Missing of Intelligence.
- failure to remove outdated info"

L60: Web 3.0 Introduction | Semantic Web Technologies/Concepts | Challenges/Issues | Web 2.0 Vs 3.0

Easy Engineering Classes – Free YouTube Lectures

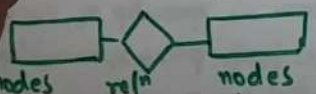
EEC Classes For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India EEC Classes

Web 3.0: It is Semantic Web. It is extension of Current web (2.0) in which info" is given well defined meaning, better enabling Computers and people to work in Cooperation.

Semantic Web Technologies/concepts:

i) XML: used for self-description of data. Also used for data-exchange.

ii) RDF: Provides foundation for publishing and king data. Used to express data/objects and ir relationships (data models).



i) Subject: Resource
ii) Predicate: Property
iii) Object: Value

iii) SPAROL: Query language and data access protocol for semantic web data sources.

iv) Ontology (OWL): Sharable Conceptualization of Specific domain of interest in machine-understandable format.

Challenges/Issues:

i) Vastness → Huge no. of class names, duplicacy.

ii) Vagueness → user Queries (Fuzzy Logic)

iii) Uncertainity → Patient (High temp.) ≤ Fever, Dengue, Malaria.

iv) Inconsistency — Delhi 01 <college>, Mumbai 02 <Institute>

v) Deceit → Producer is misleading. (IMP)

Comparison of web 2.0 and web 3.0

web 2.0	web 3.0
i) Today's web	Intelligent (Future) web
ii) Keyword based	Semantics (meaning)
iii) Human-Readable	Both Human and machine do things
iv) Place to find things	
v) No Intelligence	
vi) Inefficient.	

10:25 / 10:48

Easy Engineering Classes – Free YouTube Lectures

EEC Classes For Engineering Students of GGSIPU, UPTU and Other Universities, Colleges of India EEC Classes

Latest Trends in Web Technologies:

i) HTML5 <footer>, <header>, <main>

ii) Responsive Web Design → desktop < Mobile / Tablet

iii) Virtual Reality

iv) Security — MD5, https, certificates.
↳ Encryption

v) Motion User Interface → Animation, css Transitions.

vi) Speed and Performance → .js files compressed.

vii) Internet of Things (IOT)

viii) Artificial Intelligence (AI) } → Semantics.

Web Security Concerns:-

↳ i) SQL Injections

ii) Cross Site Scripting (xss)

iii) Broken Authentication and Session Management

iv) Security misconfiguration

v) CSRF

Applications of Web Engg. technologies in distributed systems.

i) Web Services

ii) XML → Extensible markup language.

iii) RDF → Resource Description framework.

iv) WSDL → Web Services Description Lang.

v) SOAP → Simple Object Access Protocol

vi) UDDI → Universal description discovery & Integration.

vii) SOA → Service-Oriented Architecture