Elevate lab Internship

Task -1
Understanding Cyber Security Basics & Attack Surface

CIA Triad (Core of Cyber Security)

Cyber security is mainly based on **CIA Triad**:

(1) Confidentiality

Confidentiality means **only authorized people should access data**.

Real-world examples:

- **Banking apps:** only the account holder should view balance and transactions.
- **Social media (Instagram/Facebook):** private chats should be readable only by the users.

If confidentiality fails:

- data leakage
- stolen passwords
- privacy breach

(2) Integrity

Integrity means **data should not be modified without permission**. Data must remain accurate.

Real-world examples:

- Banking: attacker should not change "₹10,000" into "₹1,00,000".
- Online exams: marks should not be altered by anyone.

If integrity fails:

- fake transactions
- modified records
- incorrect data in databases

(3) Availability

Availability means systems/services must be **accessible whenever needed**.

Real-world examples:

- ATM service should work 24/7.
- WhatsApp or Gmail must be available continuously.

If availability fails:

- DDoS attacks
- server crashes
- loss of productivity

---

2. Types of Attackers

Different attackers have different motives, skill levels, and targets:

Script Kiddies

- beginners using already-made hacking tools
- don't understand deep techniques
- mostly attack for fun or fame

Example: using free tools to deface a website

Insider

- attacker is inside the organization
- may be employee, contractor, or partner
- can misuse access privileges

Example: employee stealing customer data from company database

Hacktivists

- attackers driven by ideology or political reasons
- target governments/companies for protest

Example: defacing a site to send a message

Nation-State Actors

- highly skilled groups supported by a country/government
- target other nations for spying and cyber warfare
- very advanced attacks (APTs)

Example: attacks on power grids, defense systems, national databases

---

3. Common Attack Surfaces

Attack surface means **all possible entry points** where an attacker can exploit.

Major attack surfaces:

1) Web Applications

Examples: websites, login portals, admin dashboards
Possible attacks:

- SQL Injection
- XSS
- CSRF
- Broken Authentication

2) Mobile Applications

Examples: WhatsApp, PhonePe, Banking apps
Possible risks:

- insecure storage
- weak encryption
- reverse engineering APK

3) APIs

APIs are used between app and server.
Example: WhatsApp app communicates with server using APIs.
Possible attacks:

- broken access control
- token hijacking

- API abuse

4) Networks

Examples: WiFi routers, LAN, ISP
Possible attacks:

- Man-in-the-middle
- sniffing
- spoofing

5) Cloud Infrastructure

Examples: AWS, Azure, Google Cloud
Possible risks:

- misconfigured storage (S3 bucket public access)
- exposed keys
- weak IAM permissions

---

4. OWASP Top 10 (Web Application Vulnerabilities)

OWASP Top 10 explains major security issues in web apps.

Most important vulnerabilities:

1. **Broken Access Control** – user can access admin pages
2. **Cryptographic Failures** – weak/no encryption
3. **Injection** – SQL/command injection
4. **Insecure Design** – bad application design security
5. **Security Misconfiguration** – default passwords, open ports
6. **Vulnerable Components** – outdated libraries
7. **Identification & Authentication Failures** – weak password, no MFA
8. **Software/Data Integrity Failures** – tampered updates
9. **Logging & Monitoring Failures** – attacks not detected
10. **SSRF** – server forced to access internal URLs

These are dangerous because they allow attackers to steal data, take control, or shut down services.

---

5. Mapping Daily-Used Apps to Attack Surfaces

Application	Possible Attack Surface
Email (Gmail)	login page, password reset, phishing
WhatsApp	mobile app, API, cloud servers
Banking Apps	authentication system, server APIs, database
Instagram/Facebook	web app + API + user data storage

---

6. Data Flow (User → App → Server → Database)

A normal application flow looks like:

1. **User enters credentials** in app/website
2. **App sends request** to server using API
3. **Server processes request** and checks logic
4. **Server accesses database** to verify data
5. **Database returns response**
6. **Server sends result back** to application
7. **User receives output**

---

7. Where Attacks Can Happen in This Flow

Attack Points in Data Flow

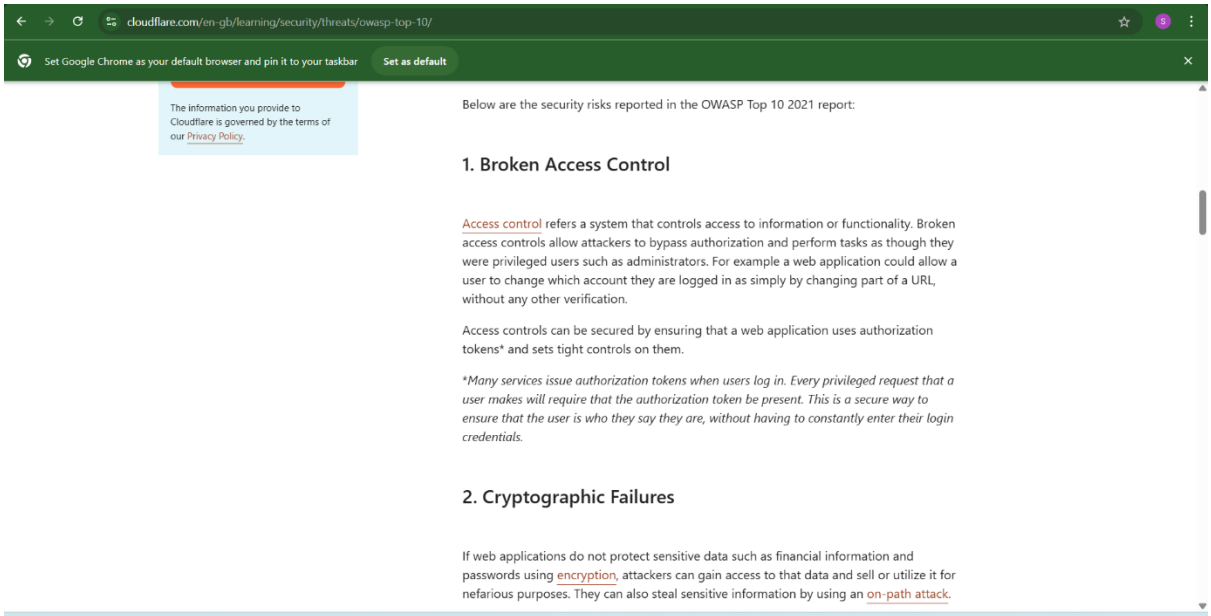
1. **User level**
    - phishing attacks
    - stolen passwords
    - malware/keylogger
2. **Application level**
    - insecure coding

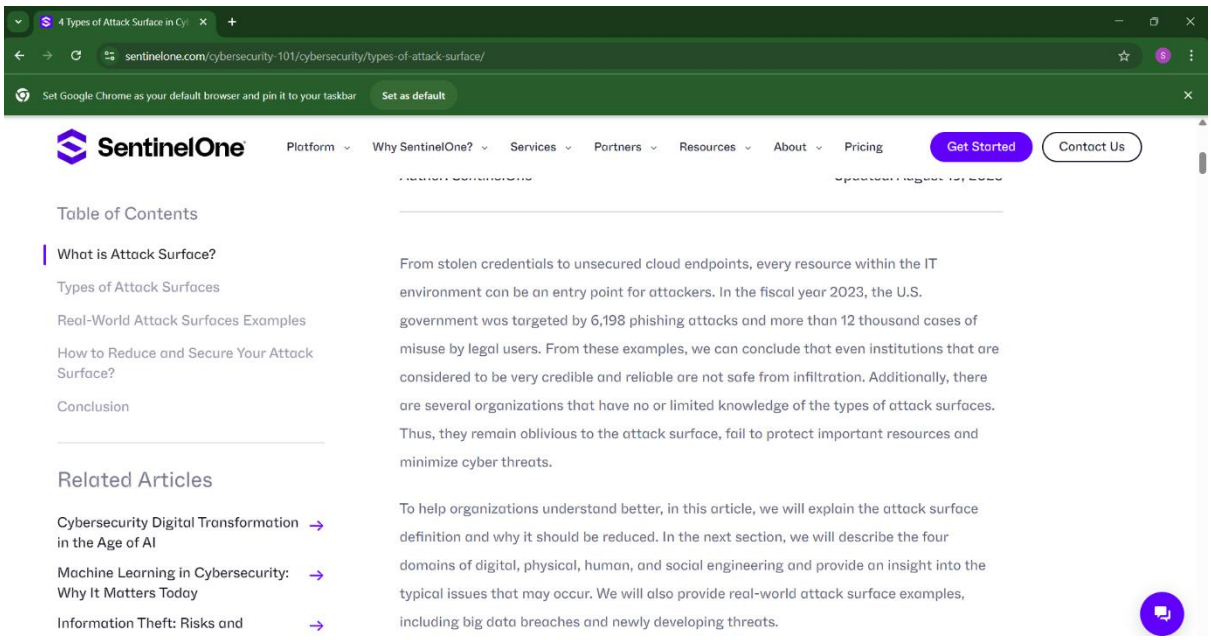
    - XSS attacks
    - weak session handling
3. **API communication**
    - token hijacking
    - man-in-the-middle attacks
    - request manipulation
4. **Server side**
    - injection attacks
    - misconfigured server
    - RCE attacks
5. **Database**
    - SQL injection
    - data theft
    - unauthorized modifications

---

8. Summary

Cybersecurity is basically about keeping our systems and data safe by focusing on the **CIA triad—confidentiality** (keeping data private), **integrity** (making sure data isn't changed or damaged), and **availability** (ensuring systems work when needed). Different attackers have different motives: some do it just for fun (**script kiddies**), some for revenge or money (**insiders**), some for beliefs (**hacktivists**), and some for national-level reasons (**nation-state actors**). Applications can be attacked through many entry points like **websites, mobile apps, APIs, networks, and cloud platforms**, and the **OWASP Top 10** highlights the most common and serious web app weaknesses. By understanding how we use apps daily and tracking how data moves from the user to the database, we can spot where attacks may happen and build stronger security.


cloudflare.com/en-gb/learning/security/threats/owasp-top-10/
Set Google Chrome as your default browser and pin it to your taskbar
Set as default
The information you provide to Cloudflare is governed by the terms of our Privacy Policy.
Below are the security risks reported in the OWASP Top 10 2021 report:
1. Broken Access Control
Access control refers a system that controls access to information or functionality. Broken access controls allow attackers to bypass authorization and perform tasks as though they were privileged users such as administrators. For example a web application could allow a user to change which account they are logged in as simply by changing part of a URL, without any other verification.
Access controls can be secured by ensuring that a web application uses authorization tokens* and sets tight controls on them.
*Many services issue authorization tokens when users log in. Every privileged request that a user makes will require that the authorization token be present. This is a secure way to ensure that the user is who they say they are, without having to constantly enter their login credentials.
2. Cryptographic Failures
If web applications do not protect sensitive data such as financial information and passwords using encryption, attackers can gain access to that data and sell or utilize it for nefarious purposes. They can also steal sensitive information by using an on-path attack.


4 Types of Attack Surface in Cy
sentinelone.com/cybersecurity-101/cybersecurity/types-of-attack-surface/
Set Google Chrome as your default browser and pin it to your taskbar
Set as default
SentinelOne
Platform
Why SentinelOne?
Services
Partners
Resources
About
Pricing
Get Started
Contact Us
Table of Contents
What is Attack Surface?
Types of Attack Surfaces
Real-World Attack Surfaces Examples
How to Reduce and Secure Your Attack Surface?
Conclusion
Related Articles
Cybersecurity Digital Transformation in the Age of AI
Machine Learning in Cybersecurity: Why It Matters Today
Information Theft: Risks and
From stolen credentials to unsecured cloud endpoints, every resource within the IT environment can be an entry point for attackers. In the fiscal year 2023, the U.S. government was targeted by 6,198 phishing attacks and more than 12 thousand cases of misuse by legal users. From these examples, we can conclude that even institutions that are considered to be very credible and reliable are not safe from infiltration. Additionally, there are several organizations that have no or limited knowledge of the types of attack surfaces. Thus, they remain oblivious to the attack surface, fail to protect important resources and minimize cyber threats.
To help organizations understand better, in this article, we will explain the attack surface definition and why it should be reduced. In the next section, we will describe the four domains of digital, physical, human, and social engineering and provide an insight into the typical issues that may occur. We will also provide real-world attack surface examples, including big data breaches and newly developing threats.

White Hat Hackers

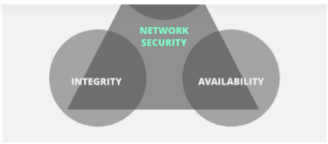
White hat hackers are the one who is authorized or certified hackers who work for the government and organizations by performing penetration testing and identifying loopholes in their cybersecurity. They also ensure the protection from the malicious cyber crimes. They work under the rules and regulations provided by the government, that's why they are called ***Ethical hackers*** **or** ***Cybersecurity experts***.

Black Hat Hackers

They are often called *Crackers*. **Black Hat Hackers can gain unauthorized access to your system** and destroy your vital data. The method of attack they use common hacking practices they have learned earlier. They are considered to be criminals and can be easily identified because of their malicious actions.

Gray Hat Hackers

Gray hat hackers fall somewhere in the category between white hat and black hat hackers. They are not legally authorized hackers. **They work with both good and bad intentions**, they can use their skills for personal gain. It all depends upon the hacker. If a gray hat hacker uses his skill for his personal gains, he/she is considered as black hat hackers.



Confidentiality

Confidentiality ensures that sensitive data is accessible only to authorized individuals or systems. Its purpose is to prevent unauthorized viewing, access, or misuse of private information.

Risks to Confidentiality

- Unauthorized Access: Attackers exploit vulnerabilities to access protected data.
- Weak Encryption: Outdated or weak encryption can be easily broken, exposing sensitive information.
- Insider Threats: Employees or trusted users may leak or accidentally expose confidential data.

How to Ensure Confidentiality

- **Encryption:** Use strong encryption methods like AES or RSA to protect data from unauthorized reading, even if intercepted. (Note: DES is outdated and insecure.)
- **VPN:** A Virtual Private Network creates an encrypted tunnel for internet communication, preventing