WHAT IS APPLICATION SECURITY?

Prepared by: Dr. Alia Alabdulkarim

What is Application security (AppSec)?

- **Application security** encompasses measures taken throughout the application's life-cycle to prevent exceptions in the security policy of an application or the underlying system through flaws in the design, development, deployment, upgrade, or maintenance of the application.

*wikipedia

So From Where Should We Start?

* https://images.app.goo.gl/L3g8FjVz2Q5L27pD9

What is Penetration Testing?

- **A penetration test,** occasionally **pentest**, is a method of evaluating the security of a computer system or network by **simulating an attack** from malicious outsiders (who do not have an authorized means of accessing the organization's systems) and malicious insiders (who have some level of authorized access).

يسوي نفسه هاكر ويختبر البرنامج
فيال

- The process involves an active analysis of the system for any potential vulnerabilities that could result from poor or improper system configuration, both known and unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker and can involve active exploitation of security vulnerabilities.

*wikipedia

أهمية

Why Penetration tests are valuable?

- Determining the feasibility of a particular set of attack vectors (1) لأنه عرضه لمجموعة اختراقات هل ستكون مجدية أو لا
- Identifying higher-risk vulnerabilities that result from a combination of lower-risk vulnerabilities exploited in a particular sequence (2) تضيفها الى High- أو lower ، وتربين مجموعة من low-risk vulnera تعز
- Identifying vulnerabilities that may be difficult or impossible to detect with automated network or application vulnerability scanning software (3)
- (4) Assessing the magnitude of potential business and operational impacts of successful attacks في حال صارت نصير نعرف كمية الأذى
- Testing the ability of network defenders to successfully detect and respond to the attacks
- Providing evidence to support increased investments in security personnel and technology

Testing Types

White Box Testing // يصير عارف كل شي صير داخلي (موظف)

- In penetration testing, white-box testing refers to a methodology where an ethical hacker has full knowledge of the system being attacked. The goal of a white-box penetration test is to simulate a malicious insider who has some knowledge and possibly basic credentials to the target system.

Black Box Testing ⇒ إذا كنت ما عرف شي شي من داخل

- In penetration testing, black-box testing refers to a methodology where an ethical hacker has no knowledge of the system being attacked. The goal of a black-box penetration test is to simulate an external hacking or cyber warfare attack.

Grey Box Testing → عنده معلومات محدودة مابعرف كل شي

- Between a black box test and a white box test is a gray box test, in which some limited information has been provided to the tester.

What is Ethical Hacking? ⇒ أوسع من البرتيشن تيستق

🔒 **Ethical hacking** is a term meant to imply a **broader category than just penetration testing**. An ethical hacker specializes in penetration testing and in other testing methodologies (e.g. Social Engineering) that ensures the security of an organization's information systems.

مثال عليها
لما الاتكر بينفرض قدرته على الكلام ويسحب معلومات

*wikipedia

فيه فيديو لازم أشوفه

Penetration Testing vs Ethical Hacking

Penetration Testing	Ethical Hacking
A narrow term focuses on performing cyber security assessment فقط يركز على بيكيتي	A comprehensive term in which penetration testing is only one feature يعتبر كل اختبار كنز
knowledge and skills only in a specific area	A comprehensive knowledge of various programming and hardware techniques توصل للهاردوير
Familiarity with penetration testing	requires an obligatory certification يأخذ شهادة
Access to specific systems	Access to wider range of system (infrastructure)
E.g. EC-Council Certified Penetration Tester (CPENT)	E.g. EC-council Certified Ethical Hacker (CEH)

This table is taked from [https://resources.infosecinstitute.com/category/certifications-training/pentesting-certifications/ethical-hacking-vs-pentesting/]

Who are my enemies?

- Hackers
  - White-hat
  - Black-hat
  - Grey-hat
- Insider Attacks
  - Disgruntled Employees
  - Corporate Spying
- Script Kiddies

Key Terms

- Vulnerability
- Threat
- Risk

What are some likely threats facing my AppSec Program?

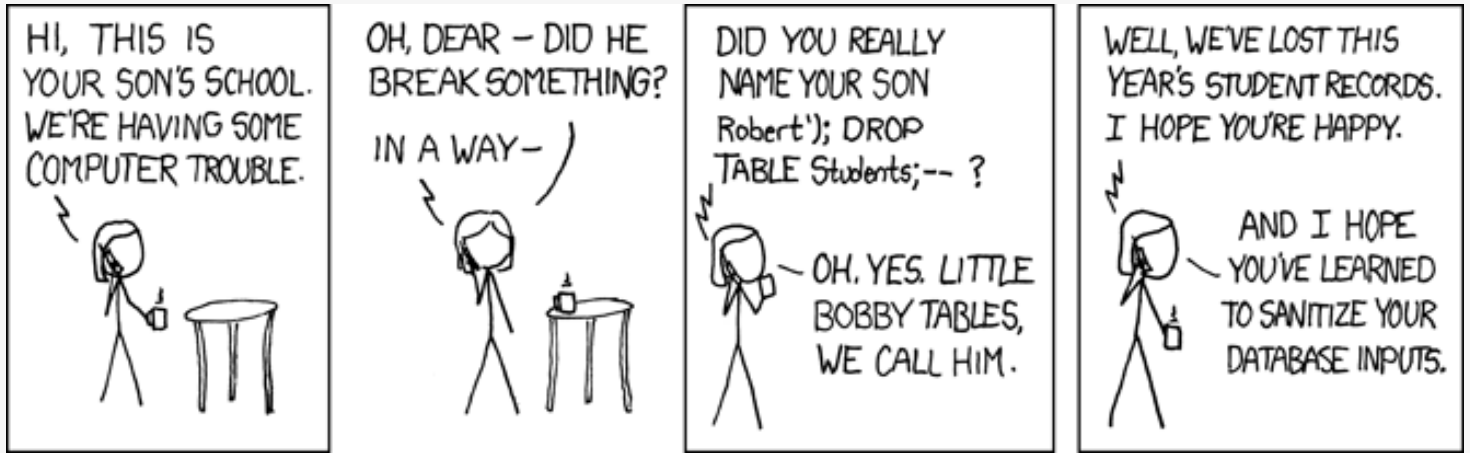
- Cross-Site Scripting (XSS)
- SQL Injection (SQLi)
- Weak Authentication
- Secure Session Vulnerabilities
- Secure Transmission Vulnerabilities
- Privilege Escalation
- Information Leakage and Improper Error Handling

Cross-Site Scripting (XSS)

- Cross-Site Scripting attacks are a type of injection problem, in which malicious scripts are injected into the otherwise benign and trusted web sites. => يكتب كود سكربت داخل الويب

SQL Injection

- A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application.
- A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system.



Weak Authentication Vulnerabilities

- Weak Passwords
- User Enumeration
- Lack of Account Lockout

Secure Session Vulnerabilities

Sessions represent a user's authentication and authorization for the duration of a user's interaction with your web application.

- Session Poisoning
  - A method to exploit insufficient input validation within a server application
- Session Fixation
  - An attack that enables an attacker to steal a valid user session
- Persistent Cookies
  - Remain on your hard drive until you erase them or they expire
  - Stored with your browser when you click the "remember me" button on the login form

Insecure Communication

- Login Forms without SSL Encryption
- Old or Outdated Algorithm use

استخدام القوائم مشفرة

Privilege Escalation

- Occurs when a user gets access to more resources or functionality than they are normally allowed, and such elevation/changes should have been prevented by the application

رفع الصلاحيات الحالية

Information Leakage and Improper Error Handling

- Applications can unintentionally leak information about their configuration, internal workings, or violate privacy through a variety of application problems

- Applications can also leak internal state via how long they take to process certain operations or via different responses to differing inputs, such as displaying the same error text with different error numbers

- Web applications will often leak information about their internal state through detailed or debug error messages

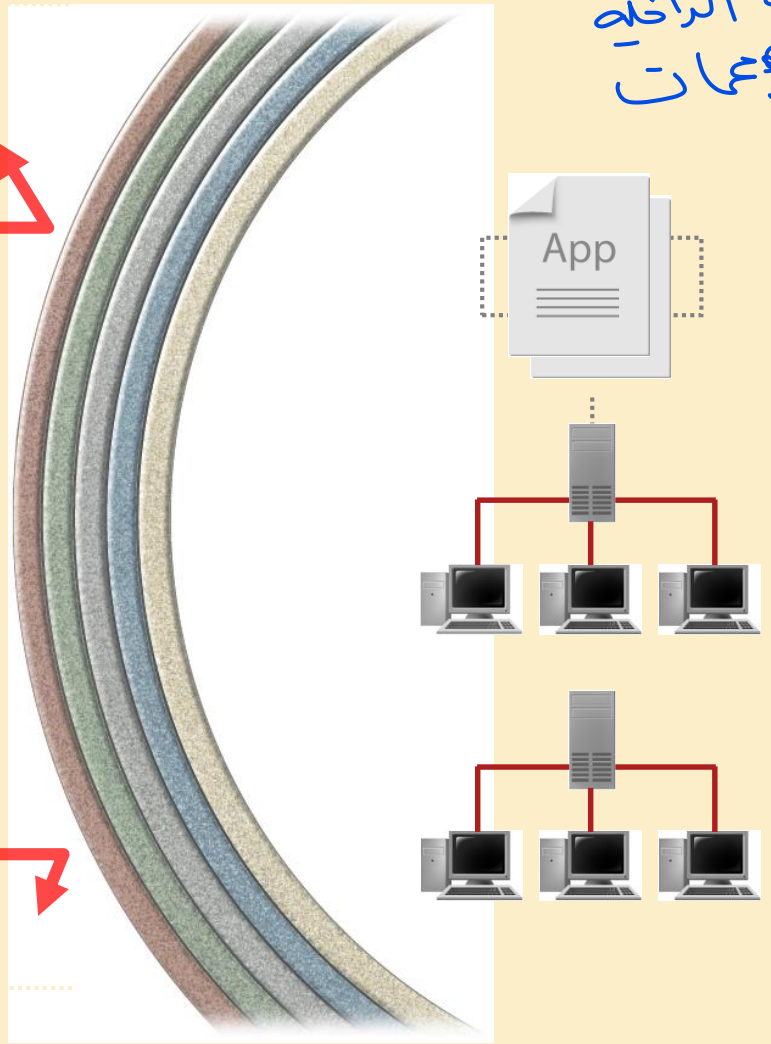
What happened to the Firewall???

لا يحمي
الشبكة الداخلية
من الهجمات

Hackers

Worms &
Viruses

Malicious Insiders



Fundamentally Flawed Perception

Fails to protect the most critical component - the Applications

Outsourcing

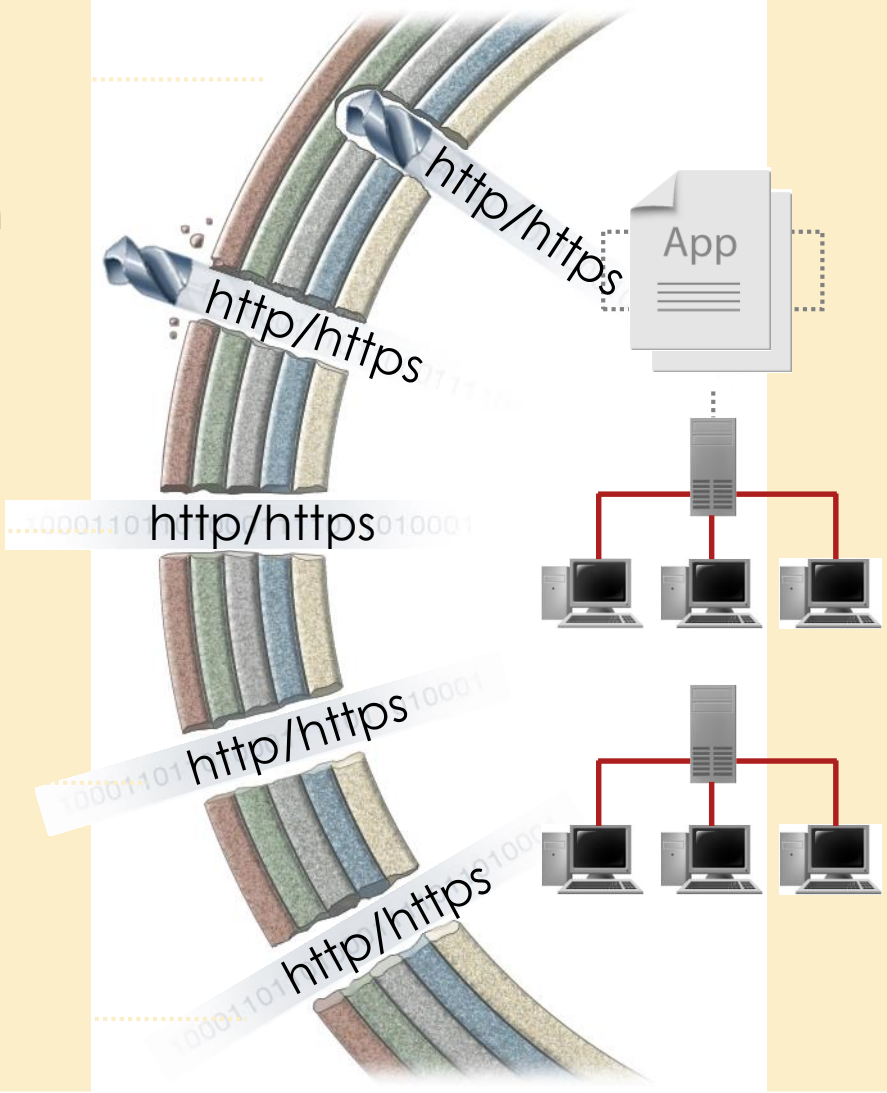
Legacy Application Integration

Web-facing Applications

Employee Self-Service

Today, even the code itself is sometimes "outside the firewall!"

Connectivity with Partners, Suppliers



What the user sees…

File Edit View History Bookmarks Tools Help

http://capitalone.com/

Capital One Credit Cards, Banking, Au...

Find a bank branch/ATM | Enter your five-digit ZIP Code | Access your account

ZIP or City, ST | Go | Advanced Search | Ask your question here. | Search

Credit Cards | Banking | Loans | For Business | Customer Service

Manage Your Accounts

Select an account: Credit Cards | Log In

Enroll here | Learn more | UK customers

Identity Protection Center

Privacy | Security | Fraud Prevention

Protect your identity with Creditinform®

Mail Offer

Respond to an offer you received in the mail.

InterestPlus Online Savings

Get paid. Twice.

Earn a superior 1.60% APY plus a 10% bonus on your interest earned*

Get Started

264.00 | 24.00 → PLUS 10% BONUS | 240.00 → Capital One 1.60 APY* | 73.50 national average 0.49 APY†

Annual earnings on $15,000 balance ‡

Savings Accounts — Earn With Great Rates

Credit Cards — Transfer Your Balances

Auto Finance — Refinance Your Loan

Top Requests

- Transfer balances and save
- Redeem & learn about rewards
- View popular credit cards
- Go paperless
- Protect your identity
- View guide to Credit CARD Act
- Contact Capital One

Capture Your Life on Your Card

Image Card lets you create a card that's uniquely you

Personalize your card with an image of your choice

Get Started

Need a new card? Click here.

Current Rates

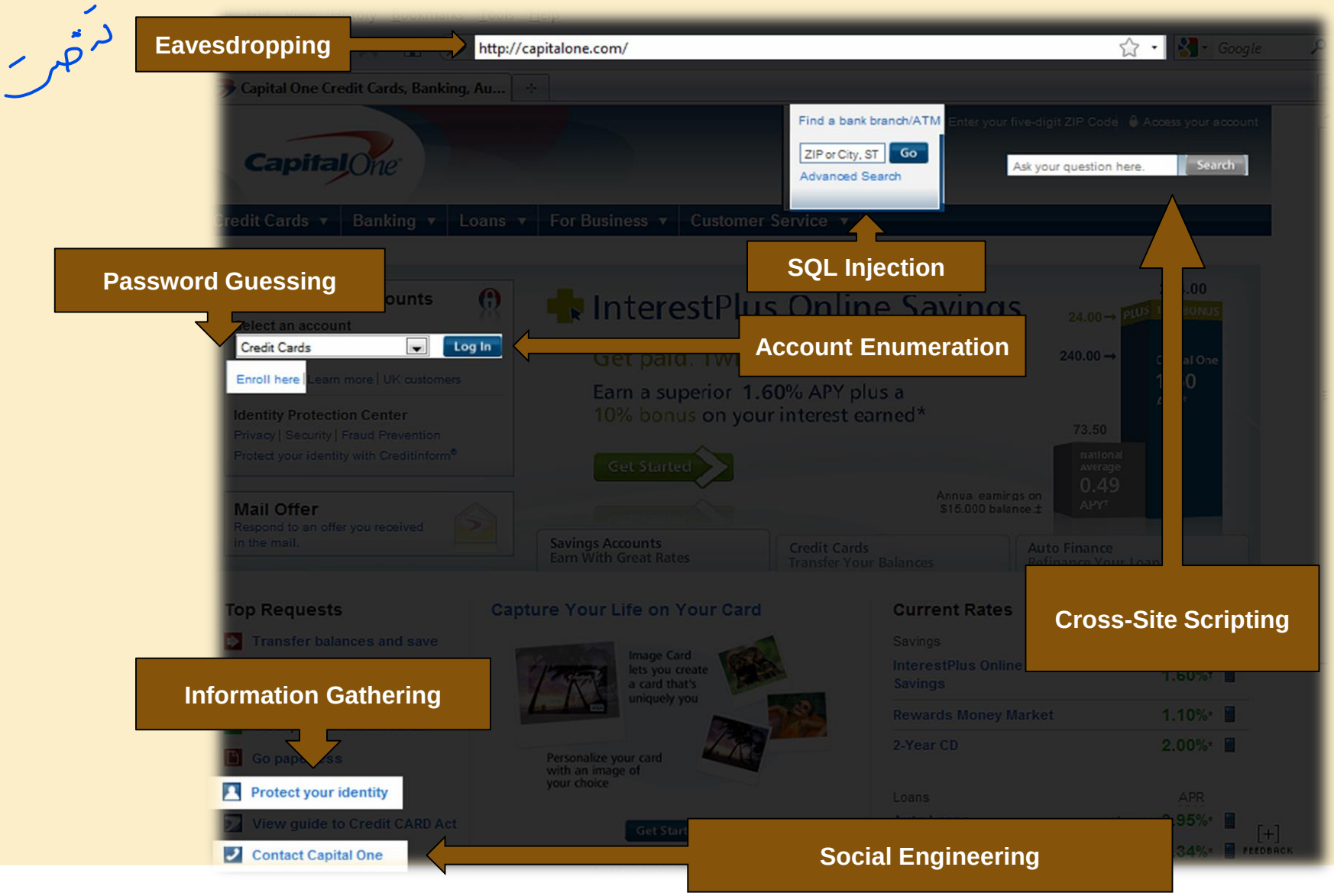
Savings	APY
InterestPlus Online Savings	1.60%†
Rewards Money Market	1.10%*
2-Year CD	2.00%*

Loans	APR
Auto Loans	as low as 3.95%*
Auto Refinancing	as low as 4.34%*

*Balance at least $2,500

[+] FEEDBACK

What a Hacker sees…



OWASP

🔒The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to develop, purchase, and maintain applications and APIs that can be trusted. →

يدعمون الناس أصحاب
الأبلكيشن

OWASP Top 10 ⇒ تطلع list for attacks

A1:2017-Injection	Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2:2017-Broken Authentication	Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
A3:2017-Sensitive Data Exposure	Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
A4:2017-XML External Entities (XXE)	Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

OWASP Top 10

A5:2017-Broken Access Control	Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
A6:2017-Security Misconfiguration	Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion.
A7:2017-Cross-Site Scripting (XSS)	XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

OWASP Top 10

A8:2017-Insecure Deserialization	Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.
A9:2017-Using Components with Known Vulnerabilities	Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
A10:2017-Insufficient Logging & Monitoring	Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

References

https://slideplayer.com/slide/4775417/

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project