Web Security

Security Principle: CIA Triad

One of the most important security principles is the CIA triad, which stands for Confidentiality, Availability, and Integrity.

Web Development & Security

As a web developer, you should assume that by default, things are NOT safe. Vulnerabilities exist in all corners. In order for web applications to function, there are many parts that work with each other:

- The user's browser
- The HTML/CSS/JavaScript code including any third-party API's
- The HTTP(S) protocol
- And more!

This means there are many points of attack.

Web Attacks & Damages

Cyberattacks against websites are extremely common. An attack could result in:

- Website Defacement
- Loss of Website Availability
- Total Denial-of-Service (DoS)
- Leaking of Sensitive Customer Data
- An Attacker Gaining Control Over the Website
- An aAttacker Using the Website as a Vector for Other Attacks
- Loss of User Trust in the Website
- Reputational Damage
- And more

OWASP Top Ten

The OWASP Top Ten are the most critical security risks to web applications.
The list contains:

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging and Monitoring

Injection

Injection is part of the OWASP Top Ten.
Injection an attack where a malicious actor injects code into an interpreter, usually through an input field.
It's dangerous because it can allow attackers to gain access to or damage systems or sensitive data by tricking the interpreter into executing a command.
The code is an example of an innocent search for `soap` combined with a dangerous SQL command.

```
SELECT product_name, product_cost FROM
product_table WHERE product_name = 'soap'
UNION SELECT username,password,NULL FROM
user_table;-- -';
```

Broken Authentication

Broken Authentication is part of the OWASP Top 10.
Broken Authentication is improperly implemented authentication and session management.
It's dangerous because it can allow attackers to compromise data or assume others' identities.

Sensitive Data Exposure

Sensitive Data Exposure is part of the OWASP Top Ten.
Sensitive Data Exposure is improperly protecting, hiding, or encrypting sensitive data.
It's dangerous because it can allow attackers to steal, modify, or delete data.

XML External Entities (XXE)

XML External Entities (XXE) is part of the OWASP Top Ten. XXE is allowing outside users to upload potentially malicious XML documents without properly configuring or securing XML processor.
It's dangerous because it can allow attackers access files, execute remote code, or execute Denial of Service attacks.

Broken Access Control

Broken Access Control is part of the OWASP Top Ten. Broken Access Control is improperly implemented authorization.
It's dangerous because it can allow attackers to access functions or data, like sensitive user data, they should not be able to access.

Security Misconfiguration

Security Misconfiguration is one of the OWASP Top Ten. Security Misconfiguration refers to situations like:

- Insecure security configurations, often as a result of keeping default or badly configured security configurations
- Not making data private
- Misconfiguring HTTP Security headers
- Error messages containing sensitive information

It's dangerous because it can allow attackers to easily access systems or sensitive data.

Cross-Site-Scripting (XSS)

Cross-Site Scripting (XSS) is a part of the OWASP Top Ten. XSS is when an application allows untrusted data, potentially user-supplied data, into a web page without proper validation or sanitization.
It's dangerous because it can allow attackers to execute malicious scripts in a victim's browser leading to hijacked sessions, or malicious page alterations or redirections.
The code is an example of some code that may be used as part of a XSS attack. It could be inserted into a URL.

```
<script>alert(1);</script>
```

Insecure Deserialization

Insecure Deserialization is part of the OWASP Top Ten.
Insecure Deserialization is when data from an untrusted source is deserialized into an object, potentially containing malicious code or data, within a program.
It’s dangerous because it can allow attackers to remotely execute code.

Using Components with Known Vulnerabilities

Using Components with Known Vulnerabilities is part of the OWASP Top Ten.
Using Components with Known Vulnerabilities is using vulnerable components while allowing those components to have the same privileges as the application.
This is dangerous because it can allow attackers who have breached those components to directly attack the application.

Insufficient Logging and Monitoring

Insufficient Logging & Monitoring is part of the OWASP Top Ten.
Insufficient Logging & Monitoring is insufficient recording, reporting, and oversight of systems as well as ineffective incident response.
It’s dangerous because it allows attackers extra time to attack systems and cause harm.