web application security

Security breach

- **Loss in revenue**
  - **Directly**
    - Failing transactions
  - **Indirectly**
    - Losing clients trust

Security breach

- data protection and privacy laws
- Security **Vulnerabilities** and **Misconfigurations** are discoverable and accessible

web application security **must be** a key component of your company strategy

How do I tackle web application security?

- **Awareness**
  - Knowing your **assets** (data, infrastructure, ...)
  - Knowing different types of **threats**
  - Knowing ecosystem **vulnerabilities**
  - **Monitoring**
- **Preparedness**
  - Being prepared is half the battle

What if a security incident happens despite our best efforts?

Expect the best, plan for the worst, and prepare to be surprised.

— Denis Waitley —

Disaster planning

Make sure your data and system backups are

- Uncorrupted
- Up-to-date and ready to load

Make sure

- Your teams are fully aware of how to recognize an incident
- How to execute the procedures you’ve put in place

OWASP

Open Web Application Security Project

OWASP

- **Mission** Dedicated to enabling organizations to **conceive**, **develop**, **acquire**, **operate**, and **maintain** applications that can be **trusted**.
- **OPEN** Everything at OWASP is radically transparent from our finances to our code.
- **INNOVATION** OWASP encourages and supports innovation and experiments for solutions to software security challenges.
- **GLOBAL** Anyone around the world is encouraged to participate in the OWASP community.
- **INTEGRITY** OWASP is an honest and truthful, vendor neutral, global community.

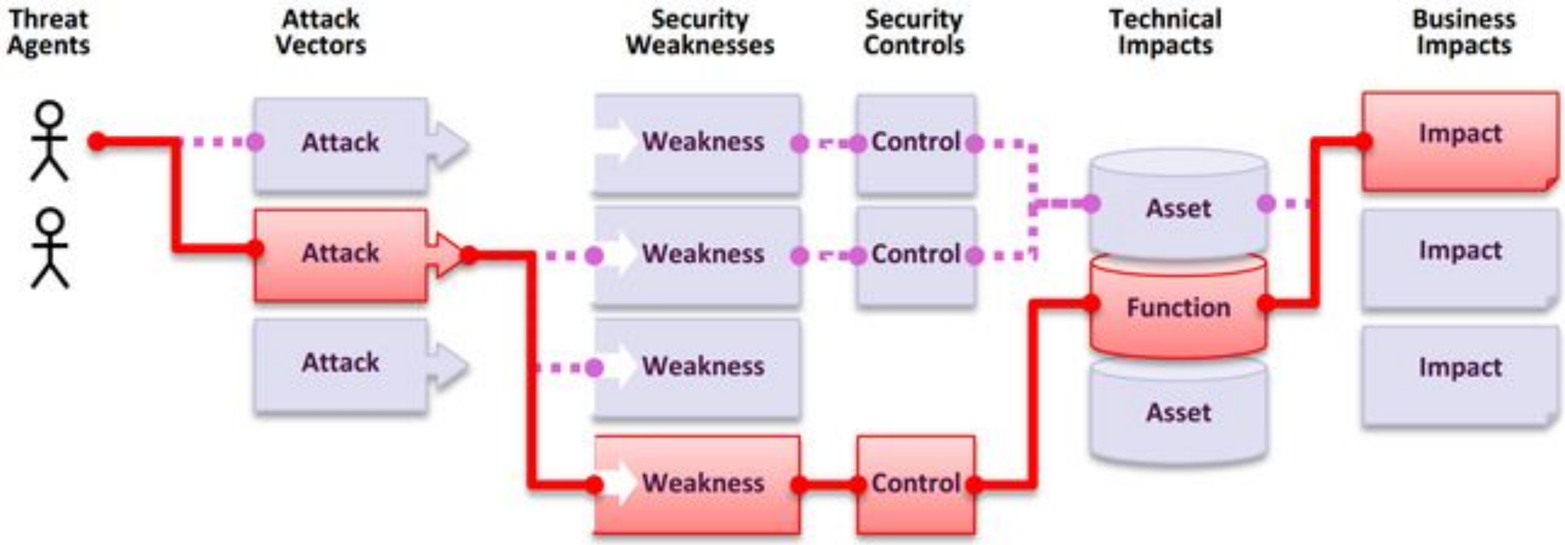
where to start?

what are the threats out there?

2017 OWASP Top 10 attack types

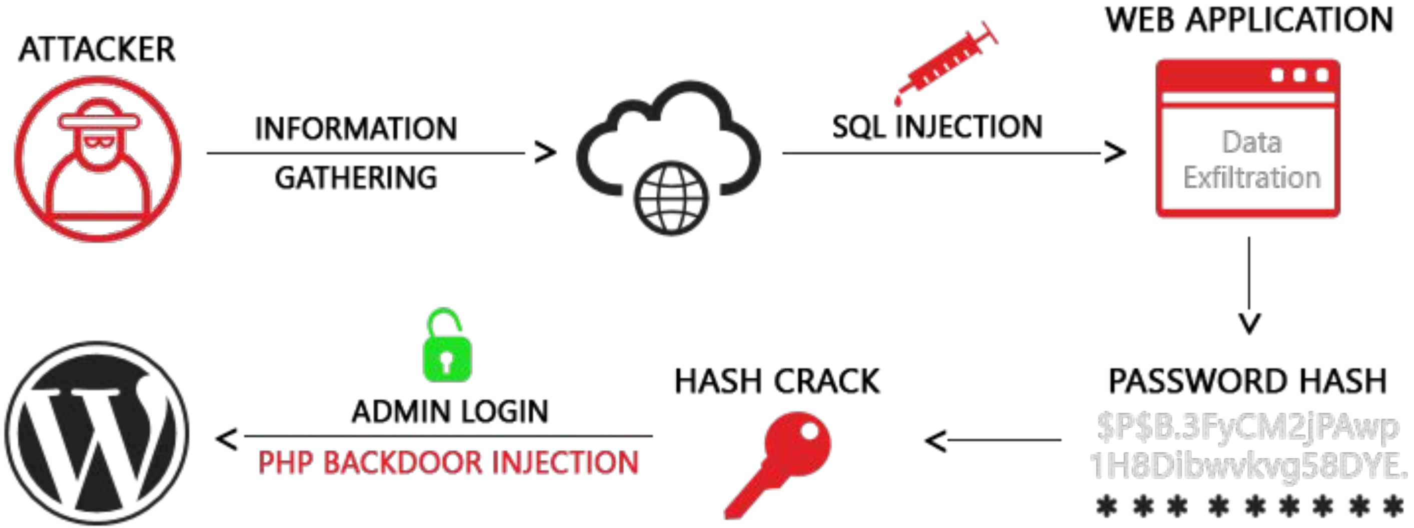
Aims to

Educate developers, designers, architects, managers, and organizations about the consequences of the most common and most important web application security weaknesses.



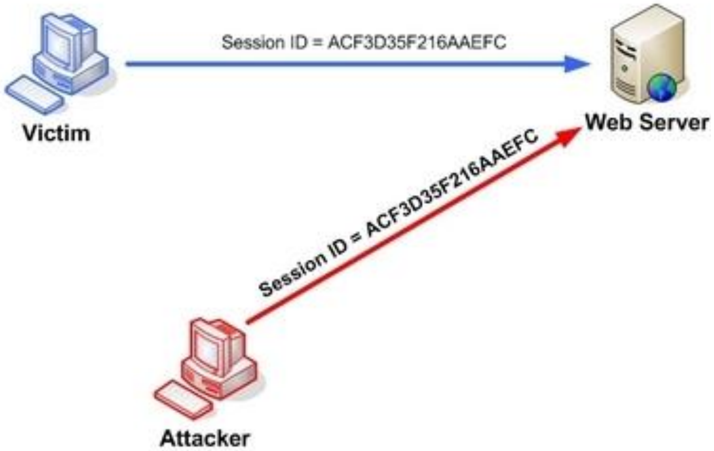
2017 OWASP - Top 10 attack types

- Injection
  - Send hostile data to an interpreter.
  - Scanners and fuzzers can help attackers find injection flaws.
  - Data loss, corruption, or disclosure to unauthorized parties, loss of accountability, or denial of access.



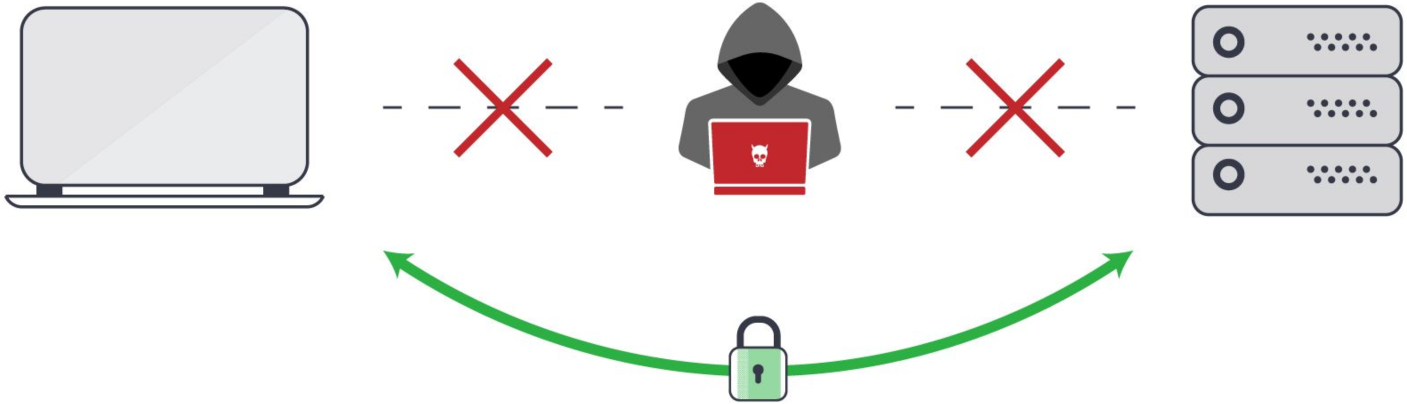
2017 OWASP - Top 10 attack types

- Broken Authentication
  - Unexpired session tokens
  - Attackers can detect broken authentication using manual means and exploit them using automated tools with password lists and dictionary attacks.
  - Depending on the domain of the application, this may allow money laundering, social security fraud, and identity theft, or disclose legally protected highly sensitive information.



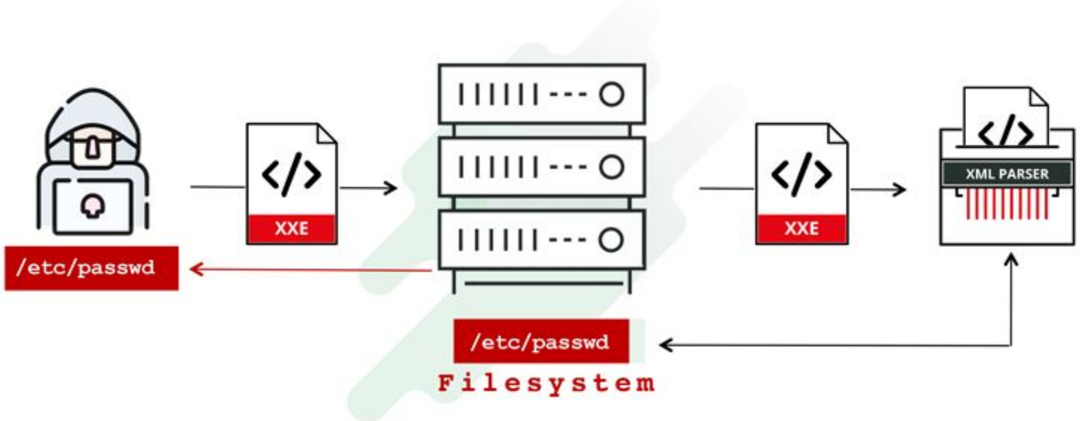
2017 OWASP - Top 10 attack types

- Sensitive Data Exposure
  - Attackers steal keys, execute man-in-the-middle attacks, or steal clear text data off the server, while in transit, or from the user's client, e.g. browser.
  - When crypto is employed, weak key generation and management, and weak algorithm, protocol and cipher usage is common, particularly for weak password hashing storage techniques.
  - Failure frequently compromises all data that should have been protected.



2017 OWASP - Top 10 attack types

- XML External Entities (XXE)
  - Attackers can exploit vulnerable XML processors if they can upload XML or include hostile content in an XML document
  - Many older XML processors allow specification of an external entity, a URI that is dereferenced and evaluated during XML processing.
  - These flaws can be used to extract data, execute a remote request from the server, scan internal systems, perform a denial-of-service attack, as well as execute other attacks.

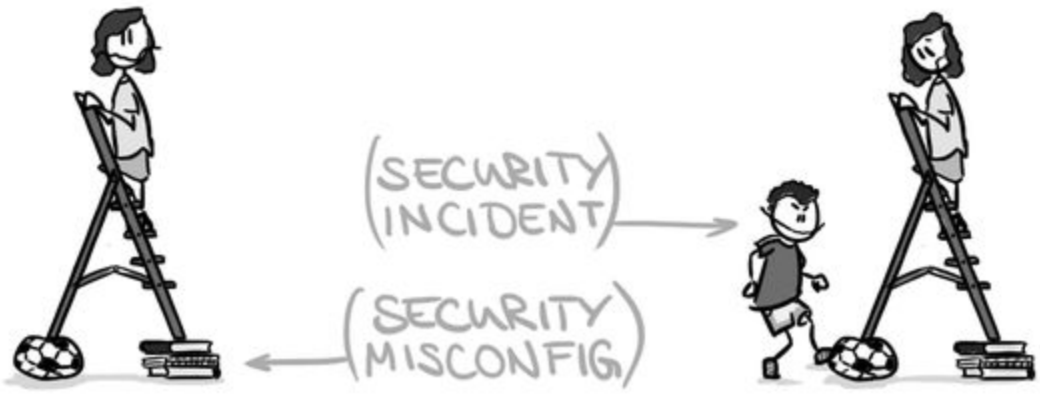


2017 OWASP - Top 10 attack types

- Broken Access Control
  - Access control is detectable using manual means, or possibly through automation for the absence of access controls in certain frameworks.
  - Manual testing is the best way to detect missing or ineffective access control, including HTTP method (GET vs PUT, etc), controller, direct object references, etc.
  - The technical impact is attackers acting as users or administrators, or users using privileged functions, or creating, accessing, updating or deleting every record.

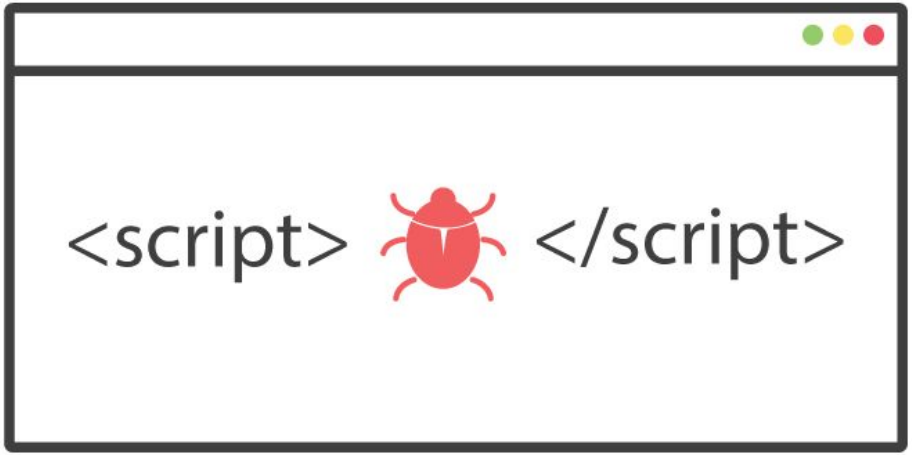
2017 OWASP - Top 10 attack types

- Security Misconfiguration
  - Access default accounts, unused pages, unprotected files and directories, etc
  - Automated scanners are useful for detecting misconfigurations, use of default accounts or configurations, unnecessary services, legacy options, etc.
  - Give attackers unauthorized access to some system data or functionality.



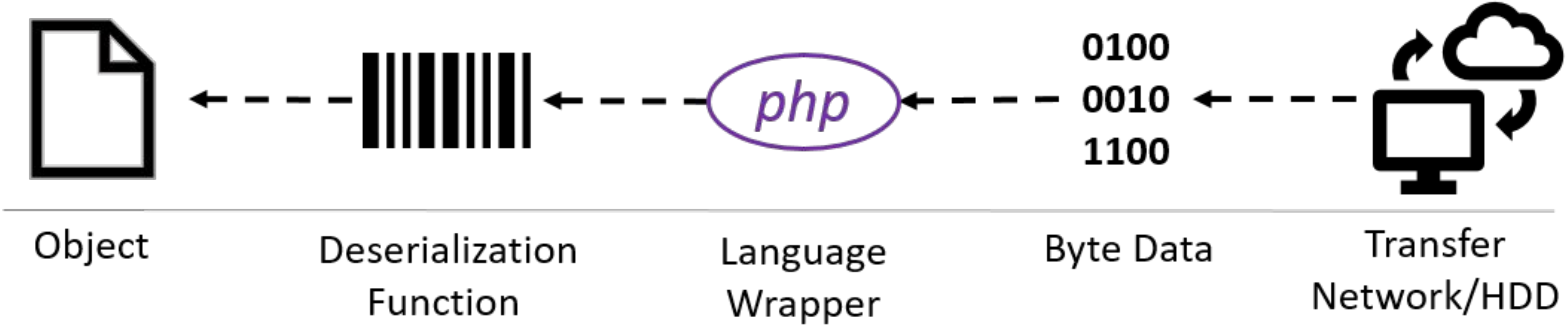
2017 OWASP - Top 10 attack types

- Cross-Site Scripting (XSS)
  - Automated tools can detect and exploit all three forms of XSS, and there are freely available exploitation frameworks.
  - The impact of XSS is moderate for reflected and DOM XSS, and severe for stored XSS, with remote code execution on the victim's browser, such as stealing credentials, sessions, or delivering malware to the victim.



2017 OWASP - Top 10 attack types

- Insecure Deserialization
  - Some tools can discover deserialization flaws, but human assistance is frequently needed to validate the problem.
  - It can lead to remote code execution attacks.
  - https://www.youtube.com/watch?v=pvS3j8VtanM



2017 OWASP - Top 10 attack types

- Using Components with Known Vulnerabilities
    - While it is easy to find already-written exploits for many known vulnerabilities, other vulnerabilities require concentrated effort to develop a custom exploit.
    - Some scanners such as retire.js help in detection, but determining exploitability requires additional effort.

2017 OWASP - Top 10 attack types

- Insufficient Logging & Monitoring
    - Exploitation of insufficient logging and monitoring is the bedrock of nearly every major incident. Attackers rely on the lack of monitoring and timely response to achieve their goals without being detected.
    - Most successful attacks start with vulnerability probing. Allowing such probes to continue can raise the likelihood of successful exploit to nearly 100%.