
THE UNIVERSITY
of ADELAIDE
Web and Database Computing
adelaide.edu.au
Web Security: Introduction to Web Application Security

Security Fundamentals

Web Applications and Security

Web applications have become and increasingly dominant way of delivering applications and services to users.

- By design, web applications are widely accessible.
- This accessibility makes them an easier target for attack by malicious users.
- Poor security practices can result in compromise of your services, resulting which could lead to financial loss, users abandonning your service or legal action.
- An increasing number of high-profile breachs has made this widely recognised as a major area of security research and study
- The Open Web Application Security Project (OWASP) is the main organisation that monitors and set security standards:
  - https://www.owasp.org/
- Our current application has several vulnerabilities; we'll be looking at how to fix these over the coming lectures.

Terminology

Vulnerability

- A weakness or flaw in software, hardware or processes that could lead to a security breach.

Threat

- A circumstance which could lead to unauthorised access or damage to data.
- A **Threat agent** is the person/group running the attack

Risk

- The probability of a threat occurring and the degree of impact of such an event.
- Usually expressed as Low, Medium or High

Mitigation

- Action take to reduce the risk of a threat

Elements of a Secure System

Authentication: Ability to identify a user.

Authorization: Ability to limit what a user can and can not do.

Auditing: Tracking of actions by users, can identify who made a request?

Confidentiality: Ability to control what information can be accessed.

Integrity: Ability to control what information is changed.

Availability: Ability to provide the web application service.

If our system does not have all of these, then our system is vulnerable.

Basic steps for checking security

1. Identify vulnerabilities

Use the cheathseets available at https://cheatsheetseries.owasp.org/cheatsheets/Index.html to identify possible issues in your services or follow a testing guide such as https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Testing_Guide_v4.pdf

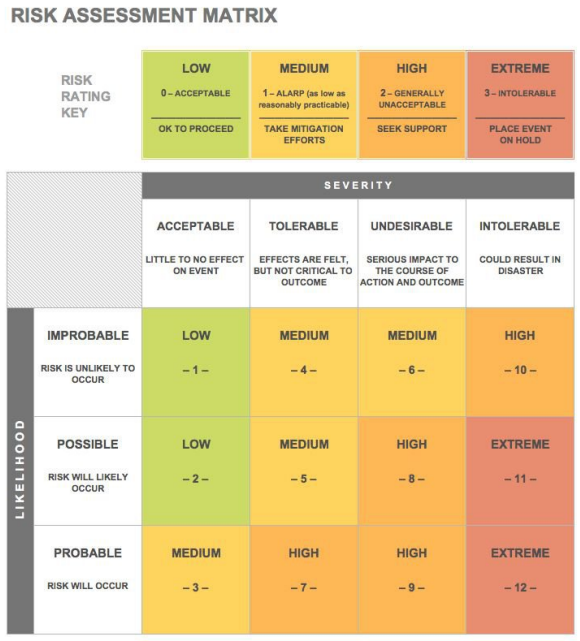
2. Identify Threats for any vulnerbilities

Dermine how any vulnerbilities may be exploited

3. Identify the Level of Risk

Use a risk matrix to dermine the level of risk associated with each threat

4. Take action



Can you identify any vulnerabilities in or threats to your web application?
How would you mitigate against these?

Summary

- Security is especially important in Web Applications
- To be secure, our system needs to ensure Authentication, Authorization, Auditing, Confidentiality, Integrity and Availability.
- We can assess our applicaiton's security using the following steps:
    1. Identify vulnerabilities
    2. Identify Threats for any vulnerbilities
    3. Identify the Level of Risk
    4. Take action

THE UNIVERSITY
of ADELAIDE