Pentesting Lab

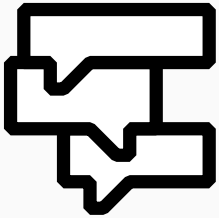
Pentesting 101

Possegger, Prodinger, Schauklies, Schwarzl

04.03.2024

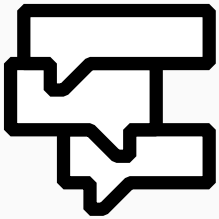
Summer 2023/24, www.iaik.tugraz.at/ptl

Importance of Penetration Testing



- Identifies vulnerabilities before attackers do
- Enhances security posture and resilience
- Compliance with regulatory requirements
- Helps protecting customer data and provide trust
- Mitigates financial and reputational risk

Basic Terminology



- Vulnerability: Weakness in a system
- Exploit: Method to take advantage of a vulnerability
- Payload: Code that performs malicious action
- Scope: Specifies which systems will be evaluated
- Threat: Anything that can negatively impact your business
- Risk: Potential for loss or damage when threat exploits vulnerability
- Likelihood: Probability of a threat exploiting a vulnerability
- Impact: Magnitude of damage that can result from a threat
- Severity: Combined assessment of likelihood and impact

Recap: CIA Principle

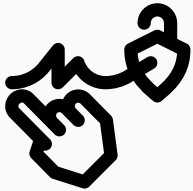
- Confidentiality: Protecting information from unauthorized access and disclosure
- Integrity: Ensuring the accuracy and completeness of data
- Availability: Ensuring information and resources are accessible when needed

- Identifies potential threats and vulnerabilities
- Multiple approaches to enumerate threats:
  - STRIDE
  - DREAD
  - MITRE ATT&CK Framework
  - ...

- Impersonating something or someone else
- Targets: User identities, IP addresses, DNS servers
- Mitigation: Authentication mechanisms, encryption, and secure communication protocols

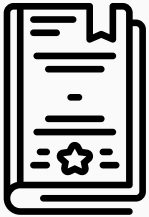
STRIDE: Tampering

- Unauthorized modificiation of data
- Targets: Data in transit or at rest
- Mitigation: Integrity checks, digital signatures, secure transmission protocols

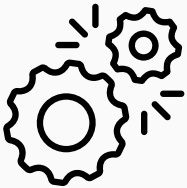


- Denying the performance of an action
- Example: Bank transaction and client denies to have performed it
- Mitigation: Secure audit trails, logging, and monitoring

STRIDE: Information Disclosure



- Information Disclosure: Unauthorized access to data
- Targets: Personal data, trade secrets, confidential information
- Mitigation: Data encryption, access controls, and data classification policies



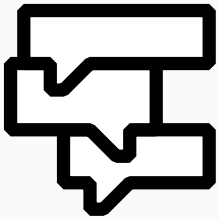
- Denial of Service (DoS): Disrupting service availability
- Targets: Networks, servers, specific applications
- Mitigation: Redundancy, traffic filtering, and rate limiting

- Gaining higher access levels without authorization
- Risk: Unauthorized access to restricted data or operations
- Mitigation: Principle of least privilege, regular software updates, and access reviews

Estimating Likelihood

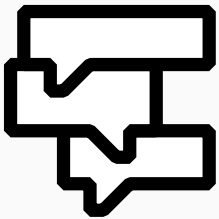
- Assess the probability of a threat exploiting a vulnerability
- Consider threat actor capabilities and presence of existing controls
- Use historical data, industry benchmarks, and threat intelligence
- Rate likelihood as high, medium, or low

Likelihood Ratings



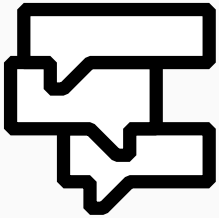
- High:
  - No special exploitation skills required
  - Vulnerability is easily accessible.
- Medium:
  - Some experience required
  - Vulnerability may be restricted by environment.
- Low:
  - Special skill required
  - Vulnerabilities requires special access to system.

- Measure the potential consequences
- Evaluate the impact on confidentiality, integrity, and availability
- Consider financial loss and reputational damage
- Rate impact as high, medium, or low



- High:
  - System fully compromised
  - Business operations are strongly influenced
  - Large mitigation efforts
- Medium
  - Short-term system compromise
  - Moderate business operations impact
  - Difficult attack chain
- Low:
  - Exploitation does not provide system access
  - No impact on business operations

Assessing Severity



- Combines likelihood and impact
- Utilizes frameworks like CVSS, NIST SP 800-30 for standardization
- Helps to prioritize the remediation efforts
- Severity levels help allocate resources effectively to address most critical vulnerabilities first

Risk Assessment Matrix

STRIDE exercise: You have to assess an online webshop that specializes in selling shoes. This webshop features a product catalog, a shopping cart, user accounts including purchase history and tracking, payment processing, and administrative functions for inventory and order management. Apply the STRIDE framework to identify potential security threats to the webshop.

- Ethics are important
- Tests responsibly and respectfully
- Balances test w.r.t privacy and legality

Legal Considerations

- Understand and comply with relevant laws and regulations
- Scope of authorization is crucial to avoid legal issues
- Documentation and agreements should be clear and detailed

Reporting and Disclosure

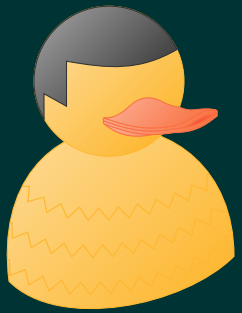
- Transparent reporting of findings to the client
- Provide detailed mitigation recommendations
- Responsible Disclosure of vulnerabilities respecting deadlines with customers

- Executive summary
- Table of findings
- Scope of pentest
- Methodology
- Overall risk estimation (Risk matrix)

- Severity (Impact, Likelihood)
- Finding category: e.g. Configuration Mgmt
- Simple Description of finding
- Proof-of-concept (Step-by-step)
- Mitigation recommendations
- References

- Cure53 https://cure53.de/
- Syslifters https://github.com/Syslifters/sysreptor
- DefectDojo https://www.defectdojo.org/

Create your own finding template and use it to describe one vulnerability.



Pentesting Stories

Any Questions?