Exercise – 7

Abdurrehman Syed
2308546

Task – 1

With the rapid advancement of technology, pressure, and complexity of laws in medical and automotive industries, sometimes it is hard to notice new emerging safety issues. The companies might try to speed up products to market without proper safety tests. In areas such as autonomous driving and medical advanced devices, the pace of innovation is too fast to keep up with comprehensive safety reviews. Also, changes in regulation barely manage to keep pace with new technology, and sometimes leave gaps in oversight.

High-profile accidents and large-scale recalls often bring immediate changes to both regulations and industry. Events such as autonomous vehicle crashes and malfunction of medical devices may result in industry-wide and regulatory reassessments of the standards in place to capture the risks that were previously unconsidered. This would be an effort toward ensuring safety for the general public and retaining confidence in the use of these technologies, just like recent automotive safety reviews and setting new standards for vehicle control systems.

Sources for this task were the lecture and AI

Task – 2

Static analysis is an analysis performed on source code without executing it. It analytically evaluates the structure, syntax, and semantic of code for possible vulnerabilities, bugs, and security risks. These tools find buffer overflows, SQL injection, and cross-site scripting. This is very effective in the early stages of development since it could locate problems before they are introduced into the codebase.
On the other hand, dynamic analysis necessitates code execution in order to study its behavior in given situations. It may find run-time errors, performance bottlenecks, security vulnerabilities-all of those problems that are not apparent while performing a static analysis. Dynamic analysis tools emulate real-life scenarios, like user input or network traffic, or system interaction, so as to be able to catch the very possibility of finding potential problems.

Advantages of Static and Dynamic Analysis during Production:

Static Analysis:

- Catches potential issues early in the development cycle, hence reducing the cost that might be used to fix them later.

- It can be integrated into the CI/CD pipeline, hence allowing automatic scanning of changed code.

Dynamic Analysis:

- This tests in real-world scenarios that may not be apparent in static analysis.
- It locates any performance bottlenecks and optimizes the code to work more efficiently.
- It finds security vulnerabilities that may be used by an attacker.

Sources:

https://www.datadoghq.com/knowledge-center/static-analysis/#:~:text=Static%20analysis%20(also%20known%20as,reports%20any%20issue%20related%20to

https://totalview.io/blog/what-dynamic-analysis#:~:text=Dynamic%20analysis%20is%20the%20process,program%20%E2%80%94%20while%20software%20is%20running.

Task – 3

Potential End User/Buyer of the Product

Good Incentives:

- A security certificate would breed confidence in the product's security to trust and buy it.
- A certified product would supposedly be tested for its securities, which, in turn, reduces the risk of data breaches or other security incidents.
- For most industries, highly controlled ones in particular, security certification might be obligatory by regulation and standards.

Bad Incentives:

- The certification itself may create a false sense of security because users rely solely on the certification, without seeking other methods of security.
- Some certifications may be designed to make users dependent on certain vendors or technologies, which could reduce their flexibility.
- Certifications are an additional cost added to the general cost of a product and may render it unaffordable for some users.

Vendor Funded

Good Incentives:

- It is among the major sources of income for these certifying authorities.
- The certification of products is one of the tools through which authorities may use to impact markets and set trends as far as security is concerned.

Bad Incentives:

- One major problem could be the conflicts of interest that may arise if the certifying authority is funded by vendors, which might result in biased / lenient processes of certification.
- When a certifying authority gets labeled as lenient or influenced by the vendors, it will affect its credibility.

Non-Profit

Good Incentives:

- Many non-profit certifying authorities are motivated by a need to fix cybersecurity and help secure the public.
- A non-profit authority could foster community among security professionals and encourage knowledge sharing.
-

Poor Incentives:

- Non-profit authorities may have limited resources, which, in some cases, can lead to lower-quality or less frequent certifications.
- The dependence on charity makes it difficult to offer long-term operational stability and investment in new initiatives.

Manufacturer/Designer of the Product

Good Incentives:

- Security certification can help in distinguishing a product from rival competitors and thereby enhances its market standing.
- Certification helps customers build confidence and loyalty as already mentioned.

Poor Incentives:

- Certification is a rather laborious process that involves huge resource costs.
- Certifications have the tendency to be very complex to comply with; at times, they even call for changes in product design or the process of development.

Task – 4

NIS2

Main Goal:

Enhancing overall cybersecurity across the European Union by strengthening existing regulations and expanding the scope.

Products Concerned:

Includes essential digital infrastructure, such as energy, transportation, and waste management, and other core entities that are critical to society and the economy, for example, manufacturers and online marketplaces.

Organizations Concerned:

All public and private organizations offering essential or key services within the EU.

Cybersecurity Measures:

Requires appropriate risk management and supply chain security, incident reporting, and cooperation with national authorities. Organizations should take the necessary technical and organizational measures that are relevant for risk management.

Compliance Date:

October 17, 2024

Penalties:

Fines and various corrective measures imposed by national authorities in cases of non-compliance.

My Thoughts:

Benefits:
1) Improves general EU Cybersecurity Posture by raising the bar for critical infrastructure and services.
2) Creates harmonized incident reporting and response requirements, hence making cross-border cooperation smooth.
3) It encourages organizations to invest in stronger security measures.

Negatives:

1. It Increases compliance burden for organizations, potentially impacting smaller entities.
2. Variations in national implementation may lead to some complexity.

Task – 5

Cybersecurity Tool: OWASP ZAP

Name: OWASP Zed Attack Proxy (OWASP ZAP)

Link: https://www.zaproxy.org/

Free or Paid: Free

Created: 2007 by OWASP (Open Web Application Security Project)

Open Source: Yes

Purpose: OWASP ZAP is a web application security scanner that helps identify and exploit vulnerabilities in web applications.

Capabilities:

- Active and passive scanning: This tool performs vulnerability identification both passively through observation and actively through testing.
- Proxy mode: It intercepts and analyzes the HTTP/HTTPS traffic.
- Spidering: Spidering: It is able to automatically discover components of the web application.
- Vulnerability scanning: Vulnerability scanning: Automatic detection for common vulnerabilities such as SQL injection, cross-site scripting, and cross-site request forgery.
- Session management: It monitors and analyzes user sessions.
- Customizable rules: Users can create rules for special testing scenarios.
- API integration: It can integrate third-party tools and platforms through its API.

Who would benefit from this tool:

- Web application developers and testers
- Security professionals
- Penetration testers
- IT admins

Potential use case: I can leverage OWASP ZAP as a web developer to start testing any web applications against common vulnerabilities before their deployment. I can disclose and then fix the security flaws which may be identified before they get exploited by any malicious actor. Furthermore, I could make use of this opportunity to learn about common web application vulnerabilities and enhance my knowledge in the domain of secure coding practices.