Web Systems Fundamentals and Databases - (Grundläggande webbsystem och databaser) 11 HP- DI4020

Project
Incident Response Portal

Background[1]

A security incident refers to any event or occurrence that compromises the confidentiality, integrity, or availability of an organization's information systems, data, or resources. Security incidents can take various forms and may result from intentional attacks, accidental actions, or natural disasters. Examples of security incidents include:

- Unauthorized access: Attempts to gain unauthorized access to sensitive systems, applications, or data, often through exploitation of vulnerabilities or weak authentication mechanisms.
- Data breaches: Unauthorized disclosure or exposure of sensitive or confidential information, such as personal data, financial records, or intellectual property, to unauthorized parties.
- Malware infections: Infections caused by malicious software (malware), including viruses, worms, Trojans, ransomware, and spyware, which can disrupt operations, steal data, or cause other harmful effects.
- Denial-of-service (DoS) attacks: Attempts to disrupt or degrade the availability of services, applications, or networks by overwhelming them with a flood of traffic or malicious requests.
- Insider threats: Breaches or incidents caused by authorized users or employees who misuse their privileges, intentionally or unintentionally, to compromise security or harm the organization.
- Social engineering attacks: Manipulative tactics used to deceive or manipulate individuals into divulging sensitive information, such as passwords, credentials, or financial details.
- Physical security breaches: Incidents involving unauthorized access to physical premises, theft of hardware or storage media, or destruction of equipment or facilities.
- Compliance violations: Instances where organizations fail to comply with legal, regulatory, or industry-specific requirements related to data protection, privacy, or security.

Security incidents pose significant risks to organizations, including financial losses, reputational damage, legal liabilities, and disruptions to operations. Effective incident detection, response, and mitigation strategies are essential for minimizing the impact of security incidents and safeguarding organizational assets and stakeholders.

[1] Inspired by https://www.w3schools.com/cybersecurity/index.php

Project Description

The goal of this project is to develop an Incident Response Portal, which is a web-based platform designed to streamline and manage the process of incident response within an organization. The portal serves as a centralized hub for reporting, tracking, and resolving security incidents, enabling timely response and mitigation efforts by security teams and incident responders.

Project Features (Requirements)

1. User Authentication and Authorization
    a. The portal supports user authentication, allowing registered users to log in and logout using their credentials.
    b. User roles and permissions are enforced to ensure that users have appropriate access levels based on their responsibilities.
    c. User roles are: “incident reporters”, “incident responders”, and “administrators”. Each have distinct sets of permissions and access rights.
2. User Management
    a. Administrators have access to a dedicated user management interface within the portal.
    b. Using the user management interface, administrators can register new users directly within the system.
    c. When registering new users, administrators input necessary user information, including username, email address, password, and user role.
    d. Administrators can assign specific roles (see 1.c) and permissions to newly registered users, customize user attributes, and manage user accounts effectively. More specifically:
        i. Incident reporters: report incidents and see **their** reported incidents and their statuses. Can add comments and evidence to their reported incidents.
        ii. Incident responders: report incidents and see **all** reported incidents and their statuses. Can add comments and evidence to **all** reported incidents. Can change the status of a reported incident.
        iii. Administrators: report incidents and see **all** reported incidents and their statuses. Can add comments and evidence to **all** reported incidents. Can change the status of a reported incident. Can manage users and see web site statistics.
3. Incident Reporting
    a. Users can report security incidents through the portal by filling out a structured incident report form.
    b. The form collects essential information such as incident type[2], severity[3], description, affected assets, and timestamps.
    c. Users must have the option to attach relevant files or evidence to their incident reports for further analysis.

[2] Denial of service, Insider threats, Man-in-the-middle, Password attack, Phishing attacks, Privilege escalation, Ransomware, Unauthorized access attacks, Theft.
https://www.w3schools.com/cybersecurity/cybersecurity_security_operations.php

[3] Low (minimal impact), Medium (compromise some confidentiality, integrity, or availability), High (partial loss of confidentiality, integrity, or availability), Critical (catastrophic consequences).

4. Incident Tracking and Management
    a. Reported incidents are logged into a centralized database and assigned unique identifiers for tracking purposes.
    b. Users can view the status of reported incidents, including pending, in progress, and resolved incidents.
    c. Incident responders can update incident status[4], add comments, and collaborate on incident resolution efforts within the portal.

5. Incident Analytics and Reporting
    a. The portal includes built-in analytics and reporting features to generate insights into incident trends, patterns, and metrics.
    b. Users can view reports (tabular format) and visualizations (graphs) to analyze incident data over time, identify recurring threats, and assess the effectiveness of incident response strategies.
6. Page Visit Tracking
    a. The portal will track and record page visits to analyze user behavior and improve user experience.
    b. Each time a user visits a page, the visit will be logged in the database along with the user's ID (if logged in), host IP, host web browser, and the timestamp of the visit.
    c. Administrators can view:
        i. Full visit log reports (tabular format),
        ii. Visit log reports (tabular format) per user,
        iii. Summary of page visits by page.
7. The following users, and respective credentials, must exist in the system:
    a. System Administrator:
        - User Name: administrator
        - Password: administrator
    b. Incident Reporter:
        - User Name: reporter
        - Password: reporter
    c. Incident Responder:
        - User Name: responder
        - Password: responder
8. Students are more than welcome to add more features to the system!

Project Team

- Each project group must have a project manager. The project web site will be deployed on the project manager account, i.e., http://project_manager_username.ddi.hh.se/project
- All group members are expected to participate in the design, implementation, and testing, i.e., having roles such as database designer, and frontend and backend developer.
- The group can collaborate using OneDrive manage code changes and track project progress. You can also use version control systems such as Git.
- The group is responsible for managing the work.

[4] Pending, in progress, or resolved.

Technologies

- Frontend: HTML5, CSS, JavaScript
- Frameworks/Libraries: Bootstrap, jQuery, Chartjs
- Backend: PHP
- Database: MySQL
- Development Environment: LAMP stack (Linux, Apache, MySQL, PHP) solution stack at ideweb2
- Deployment: http://project_manager_username.ddi.hh.se/project
- Real-time bidirectional communication (optional): AJAX, WebSockets, and Server-Sent Events (SSE).
- Templates: Students are encouraged to reuse and modify web page and website templates.
    - https://html5up.net
    - https://www.w3schools.com/css/css_templates.asp
    - https://www.w3schools.com/css/css_rwd_templates.asp
    - https://getbootstrap.com/docs/5.3/examples
    - https://www.w3schools.com/bootstrap/bootstrap_templates.asp
- **Extensive use of generative AI to generate code** is not allowed.
- Students can investigate existing systems to get inspiration about designing the Portal.

Project Evaluation

The Project is graded as Fail or Pass.

Projects will be evaluated based on adherence to project requirements. Criteria such as design, functionality, usability, code quality, documentation will also be considered, including:

- Meaningful comments in the client- and server-side code.
- Good naming convention for variables.
- Forms validation.
- Relative links, so the web site is easy to move.
- Short user manual.

After the project presentation, the two best “Incident Response Portals” will be selected based on criteria abovementioned. Students in the group that developed the selected portals will have their final grade upgraded accordingly.

Regular progress updates and demonstrations will be conducted during the supervision sessions.

The final “Incident Response Portal” system will be peer reviewed and tested to assess the quality of the system. For that, the system must include the users described in Requirement 7.

Important activities and dates

- Week 9 – Project Introduction on Feb 25th
    - Purpose: the course responsible will present and distribute the projects.
- Week 11 – Supervision I
    - Purpose: discuss preliminary system designs, i.e., ER-diagrams and UI sketches.
    - Deliverable: “Initial Project Report“
        - Deadline: The day before supervision at 13h via Blackboard.
        - Preliminary system design (diagrams and sketches), expected results, and time plan.
- Week 15 – Supervision II
    - Purpose: discuss preliminary results.
    - Database schema design and Prototype I
    - Deliverables: “Updated Project Report“
        - Deadline: The day before supervision at 13h via Blackboard.
        - Design is ready, preliminary results are deployed at ddi.hh.se, and updated time plan.
- Week 17 – Supervision III
    - Purpose: discuss preliminary results, i.e., Prototype II
    - Deliverables: “Updated Project Report“
        - Deadline: The day before supervision at 13h via Blackboard.
- Week 19 – Supervision IV
    - Purpose: discuss results, i.e., Prototype III, and which aspects to highlight in the final seminar.
    - Deliverables: “Draft for Final Project Report“
        - Deadline: The day before supervision at 13h via Blackboard.
- Week 21 – Seminar
    - Purpose: present the implemented Portal.
    - Deliverables:
        - The “Incident Response Portal” results are deployed at the School Server environment by May 16th at 13h
        - “Final Project Report” by May 16th at 13h via Blackboard.
    - Peer review and system testing
        - On May 16th, each group will receive another group’s report to read and check deployed results. The group must test the deployed system and elaborate questions and comments about the results and report.

Cheating and plagiarism

The university takes cheating very seriously and investigates all students reported. It is important that you follow the rules that exist and ask for help if you think the studies are too difficult or do not understand the instructions.

Take a look at the rules that apply to cheating and plagiarism on Halmstad University's website: https://hh.se/student-web/content-a-z/cheating-and-plagiarism.html

Use of AI tools[5]

"In general, it is not allowed to use generative AI in examinations at Halmstad University, unless it is explicitly stated in the course description or in the examination instructions that it is a permitted aid. The reason is that in many cases the tools do not allow you to develop the abilities you need after the education or that your submission at an examination does not allow a teacher to assess what you actually know.

If you use AI tools in an examination where it is not allowed, it is a violation of Halmstad University's disciplinary rules and is seen as cheating. For examinations where AI is a permitted tool, you must be aware of the rules around plagiarism.

It cannot be assumed that the text and data generated by this type of tool is accurate or relevant. The tools can also exclude important or even crucial information for no good reason. Texts created may contain completely false claims, designed to fulfill what has been requested in the instructions. As a student, you are always responsible for what you submit for examination, regardless of what tools you have used. It is therefore important that you carefully check the content and sources cited."

[5] https://www.hh.se/student-web/content-a-z/cheating-and-plagiarism.html