Risk Assessment Report

DRP – Team 7

Table of Contents

1. Executive Summary

1.1. Purpose

The purpose of this risk assessment report is to systematically identify, assess, and mitigate potential risks associated with the DRP website. By conducting the risk assessment, we aim to provide a comprehensive understanding of the threats and vulnerabilities that may arise throughout the project lifecycle. This will enable the stakeholders to make informed decisions to enhance the website's resilience.

1.2. Summary of Key Findings

The website faced a myriad of potential risks, prompting a comprehensive professional assessment. The identified risks, prioritized based on likelihood and impact, include security misconfigurations, insecure third-party integrations, sensitive information exposure, data breaches, injection attacks, denial of service attacks, inadequate session management, and compliance risks. The organization's risk exposure is currently calculated at 46 out of 80, with a risk tolerance threshold set at 30. To mitigate and manage these risks effectively, an implementation plan spanning at least one month is recommended, with continuous monitoring and cross-team collaboration. By adhering to the outlined risk management strategies below, will substantially reduce the risk of exposure, ensuring the security and integrity of its systems and operations. Continuous vigilance and collaboration will be essential in maintaining a resilient and secure organizational environment.

1.3. Recommendations

To effectively mitigate potential vulnerabilities, it is imperative to establish a robust plan that encompasses proactive security measures. This plan should commence with a thorough and regular assessment of the website's security posture, identifying potential risks such as inadequate software security, operational availability concerns, and non-compliance with industry standards. Using tools like Static Application Security Testing (SAST), helps spot all prominent issues, such as XSS, SQL injection, CSRF, and insecure cookies. Once these vulnerabilities are identified, a targeted and swift response is essential. This may involve implementing necessary software updates, enhancing security protocols, and conducting thorough employee training programs. Regular monitoring and periodic reassessments are crucial components of the plan to ensure the ongoing effectiveness of security measures. By adopting a proactive and multifaceted approach, organizations can significantly enhance their resilience against potential threats and bolster the overall security posture of their website.

2. Introduction

2.1. Background

We are developing an innovative demand response and smart grid system as part of a larger ARC project focused on modeling renewables and empowering energy providers and consumers. Our solution leverages cutting-edge communication protocols such as OpenADR and advanced hardware like Typhoon HIL to create a seamless data exchange between providers and customers. This user-friendly web portal offers real-time data visualization, incentives load shedding during peak demand, and fosters transparency for both parties. By integrating advanced ARIMA models and analytics, our system ensures fair rewards for energy-saving behaviors while offering valuable insights for providers. Together, we are shaping the future of energy management and building a smarter, more sustainable grid. We are developing a responsive and accessible web portal that allows power customers and utilities to interact with demand response data in real time to ensure fair rewards for energy-saving behaviors while offering valuable insight for providers.

2.2. Objectives

The primary objectives of this risk assessment are to ensure the security of the website by proactively addressing potential challenges. Success of the project heavily relies on the website security. To achieve this, our team utilized the CIA security triad areas including confidentiality, integrity, and availably. We also prioritize compliance alignment with relevant laws and industry standards for security of users and their data. By systematically identifying, evaluating, and mitigating risks, we aim to deliver a robust and reliable website that operates within legal boundaries, adheres to industry standards, and provides a secure web portal for our demand response customers.

2.3. Scope

This scope covers key aspects of the website project, including website code security analysis, a thorough examination of database data security to prevent unauthorized access and data breaches, and compliance assessments focused on the electric company's adherence to regulatory requirements and industry standards. The aim is to provide targeted risk mitigation strategies tailored to these specific areas, ensuring the project's success and alignment with legal and industry benchmarks.

3. Methodology

3.1. Risk Identification

The foundation of our risk assessment includes following recommendations regarding the OWASP Top Ten web application security risks. The OWASP TOP 10 represents a regularly updated list of the most critical security risks for web applications, providing a standardized approach to identifying and mitigating common vulnerabilities.

These include issues such as injection attacks, broken authentication, sensitive data exposure, XML external entity (XXE) attacks, and more. By aligning our risk identification process with the OWASP TOP 10, we ensure a comprehensive evaluation of potential threats to the website's security, helping to prioritize and address high-impact risks effectively.

3.2. Risk Assessment

We employed the STRIDE framework, which focuses on Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege, to pinpoint potential security threats. Once identified, we conducted a thorough risk assessment using Qualitative framework (impact vs likelihood). With a clear understanding of the risks, we prioritized vulnerabilities and devised strategic countermeasures. This proactive approach not only allowed us to fortify the system against potential threats but also contributed to an elevated level of security throughout the entire development life cycle.

3.3. Risk Evaluation

Our evaluation heavily considers the financial, reputational, and operational risks that can be identified through vulnerabilities in the demand response portal. These include the ability for an adversary to exploit the website to retrieve data about other meters or organizations. Due to the public nature of our web portal and traditional methods of authentication, we rate the risk exposure and residual risk as a high priority. As power utilities, clients implementing our product are also under strict compliance obligations which can lower the risk tolerance compared to other industries.

3.4. Risk Mitigation

After identifying risks using STRIDE and prioritizing vulnerability management with Qualitative framework, the mitigation stage is initiated. This crucial phase involves implementing robust security measures, such as patching, code refactoring, and network segmentation, to address the identified vulnerabilities, ensuring a proactive and effective response to potential threats. By promptly mitigating these vulnerabilities, the organization enhances its overall resilience and fortifies its defenses against cybersecurity risks, thereby reducing the attack surface and strengthening the security posture of its systems.

4. Risk Identification

4.1. Definition of Risks

During the risk identification assessment, several risks were discovered:

1. **Security Misconfigurations**: This includes unnecessary services or features being enabled, or insecure defaults.
    - Insecure database account credentials.

- Utilizing root account instead of service accounts for application runtime.
- Not redirecting HTTP requests to HTTPS.

2. **Denial of Service (DoS) Attacks**: Lack of rate limiting, resource exhaustion vulnerabilities.
   - Allowing users to brute force login attempts
   - Lack of mechanisms to limit number of visualizations created in short time frames.

3. **Sensitive Information Exposure:** Exposure of sensitive information in error messages. Information leakage through logs.
   - Leaking environment variables in version control.
   - Displaying meter data to unauthorized individuals or organizations.

4. **Insecure Third-Party Integrations:** Vulnerabilities in third-party libraries, plugins, hardware, as well as lack of regular updates and patch management.
   - Failure to upgrade underlying OS and Docker infrastructure.
   - Failure to ensure routine patching of docker images.

5. **Data Breach:** Unauthorized access to sensitive information stored in the database.
   - Dumping user login usernames and passwords.
   - Unauthorized access to organization meter mapping.

6. **Injection Attacks**: Exploitation software vulnerabilities to inject malicious code into the website or database.
   - Inadequate input validation may allow for XXS attacks.
   - Inadequate prepared statements may allow for SQL injection attacks.
   - Improper website security may result in exposure to the other risk allowing for remote code execution, data breach, compliance and other.

7. **Inadequate Session Management**: Weaknesses in how user sessions are handled, leading to unauthorized access. session hijacking or session fixation risks.
   - Session hijacking could allow a malicious actor to get access to admin session or session with elevated privileges.

8. **Compliance Risks:** Failure to comply with industry regulations or data protection laws. Potential legal consequences and damage to the organization's reputation.
   - Failure to comply with energy-sector compliance programs (North American Reliability Council).
   - Compliance with internal organization policies.

4.2. Sources of Risk

Sources of these risks primarily involve internal factors, such security misconfigurations, or the failure for system administrators to patch and maintain infrastructure. External factors encompass threats stemming from malicious actors, evolving cyber-attack techniques, and vulnerabilities in third-party systems.

4.3. Risk Categories

To effectively manage and prioritize the identified risks, they have been categorized into relevant groups:

1. **Technical Risks**
   - Security Misconfigurations (Credential Management, secure architecture).
   - Tampering with Data (SQL Injection, Cross-Site Scripting, MITM).
   - Repudiation (Lack of digital signatures, inadequate session management)
   - Information Disclosure (SQL Injection, Cross-Site Scripting)
   - Denial of Service (DoS) attacks (Rate Limiting).
   - Elevation of Privilege (Cookie/Session Poisoning, Privilege Escalation)

2. **Financial Risks:**
   - Business sensitive data exposure.
   - Loss of revenue due to system downtime.

3. **Operational Risks:**
   - Loss of data to downstream historians or IT systems.
   - Inability for organizations to view saving rates.

4. **Regulatory and Compliance Risks:**
   - NERC/CIP BCSI compliance standards.

5. **Reputational Risks:**
   - Loss of reputation due to website downtime.
   - Incorrect predictions reducing public trust.

By classifying risks into distinct categories, organizations can tailor their risk management strategies, allocate resources effectively, and prioritize actions based on the nature and potential impact of each risk.

5. Risk Assessment

5.1. Risk Diagram

To enhance the transparency and comprehensibility of our risk assessment process, we have incorporated a visual representation through a comprehensive diagram. This diagram serves as a structured framework, illustrating the qualitative factors and their interrelationships, thereby facilitating a clearer understanding of the risk landscape. Impact refers to the magnitude of the potential consequences that may arise from a risk event, assessing the severity of its effects on organizational objectives. Likelihood assesses the probability or frequency with which a specific risk event may occur.

Likelihood Rating	**Almost Certain - 5**	Moderate	High	Extreme	Extreme	Extreme
	Likely - 4	Moderate	Moderate	High	Extreme	Extreme
	Possible - 3	Low	Moderate	Moderate	High	Extreme
	Unlikely - 2	Low	Low	Moderate	High	High
	Rare - 1	Low	Low	Low	Moderate	Moderate
		1 Insignificant	**2 Minor**	**3 Moderate**	**4 Major**	**5 Critical**
	Consequences – Maximum Reasonable Impact					

5.2. Probability Assessment

Due to utilizing the qualitative risk assessment approach we have concluded the following likelihood for the specified risk areas.

Likelihood	
Security Misconfigurations	**4**
Denial of Service (DoS) Attacks	**3**
Sensitive Information Exposure	**4**
Insecure Third-Party Integrations	**5**
Data Breach	**3**
Injection Attacks	**3**
Inadequate Session Management	**2**
Compliance Risks	**3**

5.3. Impact Assessment

Due to utilizing the qualitative risk assessment approach we have concluded the following impact for the specified risk areas.

Impact	
Security Misconfigurations	**5**
Denial of Service (DoS) Attacks	**3**
Sensitive Information Exposure	**3**
Insecure Third-Party Integrations	**3**
Data Breach	**4**
Injection Attacks	**4**
Inadequate Session Management	**3**
Compliance Risks	**2**

5.4. Risk Prioritization

Based on the above probability and impact assessments, we have listed below the highest priority risks.

Prioritization (Likelihood * Impact) / 2	
Security Misconfigurations	**10**
Insecure Third-Party Integrations	**7.5**
Sensitive Information Exposure	**6**
Data Breach	**6**
Injection Attacks	**6**
Denial of Service (DoS) Attacks	**4.5**
Inadequate Session Management	**3**
Compliance Risks	**3**

6. Risk Evaluation

6.1. Risk Exposure

Using the formula $\sum(Likelihood * Impact)$ / (2 * # Risks), we calculate a risk score of 46 out of 80. This score is derived from assessing the likelihood and impact of various risks your organization faces.

6.2. Risk Tolerance

The maximum acceptable risk tolerance for your organization is set at 30 out of 80. This is the level of risk that your organization considers acceptable or manageable. If the calculated risk exposure (46 out of 80) exceeds this threshold, it indicates that your organization is currently exposed to more risk than it deems acceptable.

6.3. Residual Risk

After mitigation strategies are implemented, we expect a baseline level of risk to be 15 out of 80.

7. Risk Mitigation

7.1. Mitigation Strategies

Identified Risk	Mitigation Strategy
Security Misconfigurations	Follow secure installation steps provided by the product. Ensure that system administrators change default credentials and maintain service accounts.
Denial of Service (DoS) Attacks	Consider placing public web stack behind a security proxy such as Cloudflare. Add mechanisms to limit the number of API calls. Require captcha for multiple invalid sign-on attempts.
Sensitive Information Exposure	Ensure that developers are maintaining industry best practices with development environments and audit within-application user permissions.
Insecure Third-Party Integrations	Audit software bill of materials (SBOM) for all vendor products to ensure known vulnerabilities have been patched.
Data Breach	Restrict access to application databases to service accounts.
Injection Attacks	Audit all input methods within the website using common security tools.

	Require prepared statements for all SQL queries.
Inadequate Session Management	Rely on multiple factors (Timestamp, IP address, browser fingerprint) to validate sessions. Require users to re-authenticate if suspicious activity is discovered.
Compliance Risks	Ensure a thorough compliance review of application features and implementation before use in an organization.

7.2. Responsibility

Identified Risk	Responsible Person(s)
Security Misconfigurations	System Administrator
Denial of Service (DoS) Attacks	System Architect
Sensitive Information Exposure	Software Engineering Team
Insecure Third-Party Integrations	Cybersecurity Engagement
Data Breach	System Administrator & Database Administrator
Injection Attacks	Software Engineering Team
Inadequate Session Management	Software Engineering Team
Compliance Risks	Compliance & Cybersecurity Risk Teams

7.3. Implementation Plan

Organizations should designate at least 1 month to implement risk mitigation strategies. Security misconfigurations, denial of service attacks, and compliance risks should occur throughout application installation and setup. Software engineers will need time to implement, test, and verify security controls to prohibit injection attacks, sensitive information exposure, and inadequate session management. Compliance & Cybersecurity Risk teams should continuously monitor applications to identify and mitigate future risks.

7.4. Monitoring and Control

After a thorough review of risks, mitigations, and responsible parties, it is important to continuously monitor progress towards mitigations. Organizations should designate a project controls specialist role to create tasks for each of the mitigations, assigning subject matter experts and due dates. This chart should be shared with all respective teams and interested parties, and audited to ensure that the project remains on time.

8. Conclusion

8.1. Summary of Key Risks

In summary, the risk assessment has identified and evaluated several key risks that demand immediate attention. The prioritized risks include Security Misconfigurations, Insecure Third-Party Integrations, Sensitive Information Exposure, Data Breach, Injection Attacks, Denial of Service (DoS) Attacks, Inadequate Session Management, and Compliance Risks. These risks were assessed based on their likelihood and impact, resulting in a comprehensive understanding of the potential threats facing the organization.

8.2. Risk Management Plan

The risk management plan is a proactive approach to addressing the identified risks. It outlines a set of targeted strategies to mitigate and manage the identified risks effectively. Each risk has a dedicated mitigation strategy, responsible personnel, and an implementation plan. The plan emphasizes a collaborative effort across various teams, ensuring a holistic approach to risk mitigation. The strategies proposed involve targeted mitigation efforts for each risk category:

- **Security Misconfigurations:** System administrators will follow secure installation steps, change default credentials, and maintain service accounts.
- **Insecure Third-Party Integrations:** A cybersecurity engagement team will audit the software bill of materials for all vendor products to ensure known vulnerabilities are patched.
- **Sensitive Information Exposure:** The software engineering team will ensure industry best practices with development environments and conduct audits of within-application user permissions.
- **Data Breach:** Access to application databases will be restricted to service accounts by the system administrator and database administrator.
- **Injection Attacks:** Software engineering teams will audit input methods, use common security tools, and require prepared statements for all SQL queries.

- **Denial of Service (DoS) Attacks:** The system architect will consider placing the public web stack behind a security proxy and implement mechanisms to limit API calls and require captchas for multiple invalid sign-on attempts.

- **Inadequate Session Management:** Software engineering teams will use multiple factors for session validation and require users to re-authenticate in case of suspicious activity.

- **Compliance Risks:** Compliance and cybersecurity risk teams will conduct thorough compliance reviews before implementing application features.

8.3. Recommendations

At last, to reiterate the plan and ensure project success the following recommendations are emphasized:

1. **Timely Implementation:** Organizations should allocate at least one month to implement the risk mitigation strategies, with specific attention to security misconfigurations, denial of service attacks, and compliance risks during the initial application installation and setup phases.

2. **Continuous Monitoring:** The risk management plan requires continuous monitoring of progress towards mitigations. A designated project controls specialist should create tasks for each mitigation, assign subject matter experts, and set due dates. Regular audits will ensure the project remains on schedule.

3. **Cross-Team Collaboration:** Collaboration among system administrators, cybersecurity engagement teams, software engineering teams, and compliance and cybersecurity risk teams is crucial. Continuous communication and information sharing will enhance the effectiveness of risk mitigation efforts.

By adhering to the outlined risk management plan and recommendations, the organization can significantly reduce its overall risk exposure, ensuring the security and integrity of its systems and operations.