Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 09, September-2023

A Review of a Customized OWASP Risk Calculator for Security Risk Analysis

Singam Reddy Sai Deepak Reddy[1], Meghavath Mahender Rathod[2], Bantu Akhilesh[3], Bodempudi Bhanu Sri Prakash[4] ,
Reddyvari Venkateswara Reddy[5],
[1, 2, 3, 4] Student, Department of CSE (Cyber Security), CMRCET, Hyderabad India
[5] Associate Professor and HOD, Department of CSE (Cyber Security), CMRCET, Hyderabad India

***Abstract*— In today's cybersecurity landscape, gauging and mitigating risks is paramount. This paper outlines the design and development of an OWASP Risk Calculator—a software tool that leverages the OWASP Risk Rating Methodology to provide a structured approach for evaluating risks in software applications. By adhering to this methodology, the tool enables users to assess risks by estimating the likelihood of exploitation and the potential impact on the business. Through this project, we bring to life a user-friendly risk calculator that guides organizations in identifying vulnerabilities and prioritizing security measures.**

The presented research introduces the OWASP Risk Calculator, a dynamic tool that applies the OWASP Risk Rating Methodology to assess and demonstrate the potency of its risk evaluation and management capabilities. By aligning itself with well-established risk assessment techniques, the calculator provides an intuitive and structured approach to gauging the potential threats faced by software applications. By embodying the principles of this methodology, the OWASP Risk Calculator empowers users to make informed decisions about risk mitigation strategies.

Keywords: Risk Assessment, OWASP Risk Rating Methodology, Software Security, Risk Calculator, Threat Assessment, Impact Estimation, Likelihood Estimation.

I. INTRODUCTION

The OWASP Risk Calculator represents a crucial advancement in software security by providing a systematic and quantifiable approach to risk assessment and mitigation. As the technology landscape grows increasingly complex, identifying and managing potential security risks within software applications has become a paramount concern. The introduction of the OWASP Risk Calculator addresses this challenge by offering a structured framework that aligns with the OWASP Risk Rating Methodology, a widely recognized and respected approach.

At its core, the OWASP Risk Calculator serves as a digital tool that empowers organizations to assess and quantify the risks associated with their software applications. By facilitating the evaluation of threat agents, vulnerabilities, and potential impacts, the calculator enables users to determine the severity of identified risks. This functionality guides stakeholders in making informed decisions about risk mitigation strategies and resource allocation. Additionally, the OWASP Risk Calculator's user-friendly interface enhances accessibility, allowing a broad spectrum of professionals to engage in risk assessment without requiring extensive technical expertise.

II. LITERATURE REVIEW

The OWASP Risk Rating Methodology is a framework for estimating the severity of security risks to applications. It is based on the standard risk model:

Risk = Likelihood * Impact

The methodology breaks down the likelihood and impact several factors, each of which is assigned a rating from 0 to 9. The overall risk is then calculated by multiplying the likelihood rating by the impact rating.

The OWASP Risk Rating Methodology has been used by many organizations to assess the security of their applications. It is a simple and effective way to prioritize security risks and make informed decisions about how to mitigate them.

III.

Here is a literature review of the OWASP Risk Rating Methodology:

The OWASP Risk Rating Methodology: A Practical Guide by Jeff Williams (2010) is a comprehensive guide to the methodology. It covers all of the factors that are used to estimate likelihood and impact, as well as how to calculate the overall risk.

The OWASP Risk Rating Methodology in Practice by Michael B. Howard (2012) is a case study of how the methodology was used to assess the security of a real-world application. It provides insights into the challenges of using the methodology and how to overcome them.

The OWASP Risk Rating Methodology: A Critical Review by Michael Dahleh and Christopher Paar (2014) is a critical analysis of the methodology. It identifies some of the limitations of the methodology and suggests ways to improve it.

IV. OBJECTIVE

This paper focuses on the core objective of designing and creating an OWASP Risk Calculator, a software solution meticulously tailored to apply the esteemed OWASP Risk Rating Methodology. The primary aim of this tool is to empower users to evaluate and comprehend the risks associated with their software applications. The overarching goal is to furnish a well-structured, user- intuitive interface that simplifies the intricate process of recognizing, quantifying, and prioritizing potential risks. By effectively implementing this calculator, the paper endeavors to bridge the gap between the methodological framework's theoretical underpinnings and its pragmatic application. The tool's purpose lies in equipping organizations with the means to make well-informed decisions pertinent to risk management, thereby fortifying their capabilities in safeguarding their software assets amidst the dynamic landscape of digital vulnerabilities.

V. SYSTEM REQUIREMENTS

- A System 32 bit or 64-bit with 4 GBof minimum RAM
- ECMA Script 6(2017) support
- A modern web browser that can incorporate chart.js.

VI. PROBLEM DEFINITION

To create a website by using which security analysts and penetration testers will be able to analyze the severity of the risk of a particular vulnerability depending on the security posture of an organization and also based on the skill of the hacker or a hacking group.

VII. EXISTING SYSTEM

1) FAIR (Factor Analysis of Information Risk): This is a widely used framework for cyber risk calculation. It uses a variety of factors, such as the asset value, the likelihood of a threat, and the impact of a breach, to calculate the overall risk.

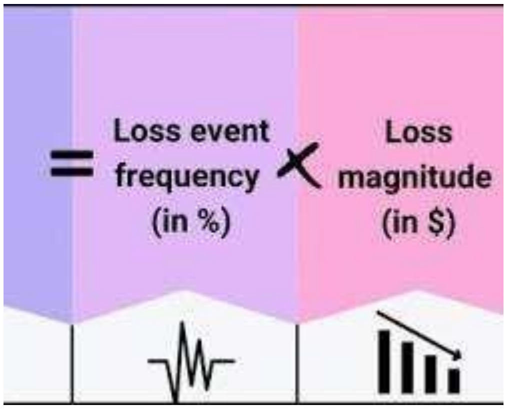


Fig-2 FAIR risk calculation

2) ISO 27005: This is an international standard for information security risk management. It provides a framework for organizations to identify, assess, and manage cyber risks.

3) NIST Cybersecurity Framework: This is a framework developed by the National Institute of Standards and Technology (NIST) for managing cyber risk. It provides a set of best practices that organizations can follow to improve their cyber security posture.

4) COSO ERM: This is a framework developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) for enterprise risk management. It provides a holistic approach to managing risk across an organization.

VIII. LIMITATIONS OF EXISTING SYSTEM

1) Contextual Relevance: Other risk calculators may not be specifically designed for web application security or may not consider the unique characteristics and vulnerabilities associated with web applications. The OWASP Risk Calculator is tailored to web application security risks, making it more contextually relevant for this domain.

2) Industry Expertise: OWASP's risk assessment methodologies are developed and maintained by a community of security experts, ensuring that they reflect the latest industry knowledge and best practices. Other calculators may lack this level of expertise and community-driven input.

3) Open Source and Transparency: The OWASP Risk Calculator is an open-source tool, which means it's transparent and can be reviewed and audited by the community. Some other calculators may not provide the same level of transparency, making it difficult to assess the underlying methodologies and assumptions.

4) Continuous Updates: OWASP regularly updates its risk calculator and other security resources to stay current with emerging threats and vulnerabilities. Other calculators may not receive the same level of ongoing maintenance and updates.

5) Community Support: The OWASP community provides support and guidance to users of the Risk Calculator, which can be valuable for organizations looking for assistance in understanding and applying the tool. Other calculators may not have a similar level of community support.

6) Customization and Flexibility: The OWASP Risk Calculator allows for customization to fit the specific needs and risk appetite of an organization. Other calculators may have limited flexibility and may not adapt well to unique organizational requirements.

7) Documentation and Guidance: OWASP typically provides detailed documentation and guidance on how to use its tools effectively. Other calculators may lack comprehensive documentation or user-friendly guides.

8) Recognized Industry Standard: The OWASP Top Ten list and its associated risk calculator are widely recognized as industry standards for web application security risk assessment. Other calculators may not have the same level of recognition or adoption in the security community.

9) Education and Awareness: OWASP's resources often serve an educational purpose, helping organizations and developers understand the underlying security principles and best practices. Other calculators may focus solely on risk assessment without providing educational value.

IX. ARCHITECTURE

1) This calculator has mainly two properties for calculating they are “likelihood score” and “impact” and the total severity of risk is the product of both.

2) Both the likelihood and impact have parameters and sub-parameters and some pre-defined score will be assigned to them.

3) Based on the selected options by the user the score will be assigned which in turn adds up to the complete score of the Likelihood and Impact.

4) Finally, a chart will be displayed with the help of chart.js based on the score from each parameter.

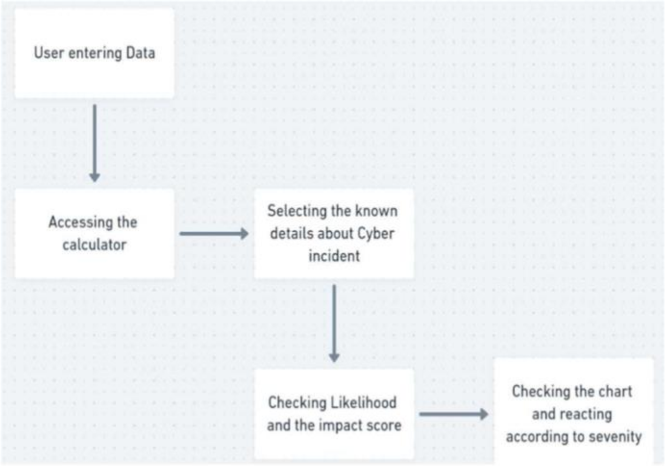

User entering Data
Accessing the calculator
Selecting the known details about Cyber incident
Checking Likelihood and the impact score
Checking the chart and reacting according to severity

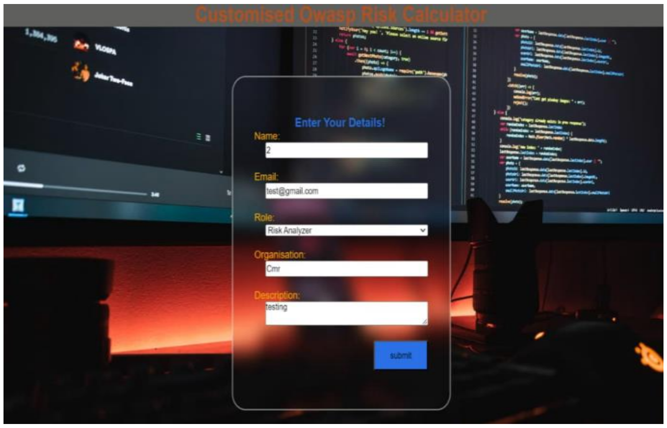
Fig-2 Block Diagram

X. CONCLUSION

The OWASP Risk Calculator is a valuable and well- regarded tool for assessing and prioritizing security risks in web applications. It offers several advantages, including its focus on web application security, integration with other OWASP resources, community- driven expertise, transparency, and the ability to adapt to the specific needs of organizations. By utilizing the OWASP Risk Calculator, organizations can enhance their web application security posture, make informed risk management decisions, and stay aligned with industry best practices. However, it's important to recognize that the choice of a risk assessment tool should be based on an organization's unique requirements and objectives and that the OWASP Risk Calculator is one among several options available in the field of risk assessment and management.

XI. RESULTS

The result of the OWASP Risk Calculator varies based on individual web applications and their characteristics. This tool assesses security risks by analyzing factors like vulnerabilities, potential impact, and likelihood of occurrence. After inputting specific information about the web application, it generates a report with risk scores and recommendations for mitigating vulnerabilities. The outcome provides insights into potential security threats and serves as a basis for prioritizing security measures and best practices. Ultimately, the exact result and recommendations are application-specific, and addressing identified risks is crucial for enhancing web application security.



Customised Owasp Risk Calculator

Enter Your Details!

Name: 2

Email: test@gmail.com

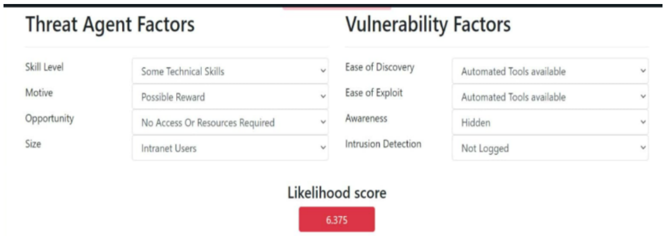
Role: Risk Analyzer

Organisation: Cmr

Description: testing

Fig-3 Home Page

1. The project report aims to explain how the project works in different scenarios of user interaction with the application.
2. The project has two main options: Likelihood and Impact factors. The user can select the option from the drop-down menu of each factor.



Threat Agent Factors

Skill Level	Some Technical Skills
Motive	Possible Reward
Opportunity	No Access Or Resources Required
Size	Intranet Users

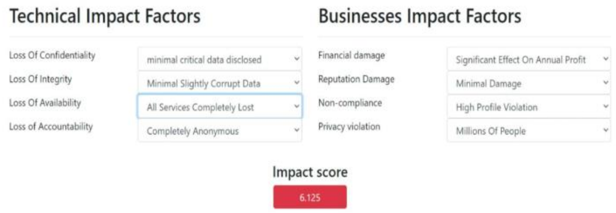
Vulnerability Factors

Ease of Discovery	Automated Tools available
Ease of Exploit	Automated Tools available
Awareness	Hidden
Intrusion Detection	Not Logged

Likelihood score

6.375

Fig-4 Likelihood Factors



Technical Impact Factors

Loss Of Confidentiality	minimal critical data disclosed
Loss Of Integrity	Minimal Slightly Corrupt Data
Loss Of Availability	All Services Completely Lost
Loss of Accountability	Completely Anonymous

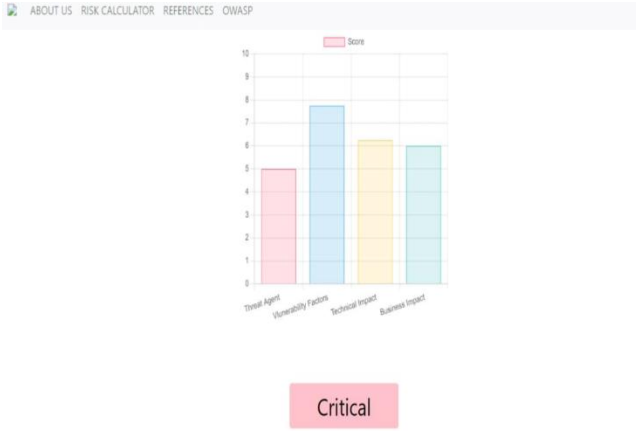
Businesses Impact Factors

Financial damage	Significant Effect On Annual Profit
Reputation Damage	Minimal Damage
Non-compliance	High Profile Violation
Privacy violation	Millions Of People

Impact score

6.125

Fig-5 Impact Factors



Critical

Fig-6 Output Chart

This Chart is generated with the help of the chart.js framework of JavaScript.

XII. REFERENCES

Websites:

[1] https://owasp.org/www-community/Threat_Modeling.
[2] https://owasp.org/wwwcommunity/Application_Threat_ Modeling.
[3] https://owasp.org/Top/A06 Vulnerable and Outdated Components -OWASP Top 10:2021
[4] https://owasp.org/Top/A07 Identification and Authentication Failures - OWASP Top 10:2021

Books:

[1] "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws" by Dafydd Stuttard and Marcus Pinto.
[2] "Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis" by Tony UcedaVélez and Marco M. Morana.

[3] "Security Metrics: A Beginner's Guide" by Caroline Wong.
[4] "OWASP Testing Guide v4" by OWASP