OWASP Risk Calculator Documentation

What is OWASP?

OWASP (Open Web Application Security Project) is a nonprofit organization focused on improving the security of software.[1] It provides unbiased and practical information about application security risks, tools, and best practices.[2] OWASP's most notable contribution is the OWASP Top 10, which identifies the most critical web application security vulnerabilities.[3]

Why and Where OWASP is Used? OWASP is used in:

1. **Software Development:**
   - Ensuring security is built into applications from the start.
   - Following OWASP guidelines helps developers mitigate common vulnerabilities.[4]
2. **Security Audits:**
   - Assessing web and mobile applications against OWASP standards.[5]
3. **Compliance and Regulation:**
   - Aligning with standards like GDPR, PCI-DSS, and others often references OWASP.[6]
4. **Risk Assessment Tools:**
   - Automating security risk assessments in incident management and vulnerability prioritization workflows.

OWASP standards are applicable across industries such as banking, healthcare, e-commerce, and any domain reliant on secure web applications.

Key Features of the OWASP Risk Calculator

1. Aligns with OWASP standards to evaluate and prioritize risks.[7]
2. Automates risk scoring based on likelihood and impact metrics.[8]
3. Supports incident management workflows.
4. Developed using Python, Streamlit, HTML, and JavaScript.
5. Visualizes risk scores and provides actionable mitigation recommendations.[9]

How Likelihood and Impact are Calculated

Likelihood Calculation:

Likelihood is determined by analyzing two main factors:

1. **Threat Agent Factors**:
   - Skill Level
   - Motive
   - Opportunity
   - Size
2. **Vulnerability Factors**:
   - Ease of Discovery
   - Ease of Exploit
   - Awareness
   - Intrusion Detection

Formula:

```
Likelihood Score = (Threat Agent Score + Vulnerability Score) / 2
```

Impact Calculation:

Impact is derived from:

1. **Technical Impact Factors**:
   - Loss of Confidentiality
   - Loss of Integrity
   - Loss of Availability
   - Loss of Accountability
2. **Business Impact Factors**:
   - Financial Damage
   - Reputation Damage
   - Non-Compliance
   - Privacy Violation

Formula:

```
Impact Score = (Technical Impact Score + Business Impact Score) / 2
```

Overall Risk Calculation:

```
Overall Risk = Likelihood Score * Impact Score
```

Risk Level:

- High Risk: Overall Risk > 70
- Medium Risk: 30 < Overall Risk ≤ 70
- Low Risk: Overall Risk ≤ 30

Scenarios for Risk Levels

Low Risk Example:

- **Scenario:**
  - **Threat Agent Factors:** No technical skills, Low motive, Special access or resource required, Limited to intranet users.
  - **Vulnerability Factors:** Practically impossible to discover, Difficult to exploit, Hidden vulnerability, Active intrusion detection.
  - **Impact Factors:** Minimal non-sensitive data disclosed, Minimal slightly corrupt data, Minimal secondary services interrupted, Fully traceable.
- **Mitigation:**
  - Continue regular security assessments.

Medium Risk Example:

- **Scenario:**
  - **Threat Agent Factors:** Some technical skills, Possible reward, Some access required, Authenticated users.
  - **Vulnerability Factors:** Easy to discover, Easy to exploit, Obvious vulnerability, Logged without review.
  - **Impact Factors:** Extensive non-sensitive data disclosed, Minimal seriously corrupt data, Extensive secondary services interrupted, Possibly traceable.
- **Mitigation:**
  - Perform targeted security improvements and enhance monitoring.

High Risk Example:

- **Scenario:**
  - **Threat Agent Factors:** Network and programming skills, High reward, No access required, Anonymous internet users.
  - **Vulnerability Factors:** Automated tools available for discovery and exploitation, Public knowledge, Not logged.
  - **Impact Factors:** All data disclosed, All data totally corrupt, All services completely lost, Completely anonymous.
- **Mitigation:**
  - Implement urgent fixes, allocate resources for a security overhaul, and develop a response

plan

Explaining the Project to Others/Interviewers

1. **Objective:** "The OWASP Risk Calculator is a web-based tool developed to assess and prioritize software vulnerabilities using OWASP's risk assessment model."[10]
2. **Purpose:**
   - Helps organizations understand and mitigate risks effectively.[11]
   - Automates complex risk calculations, saving time and improving accuracy.
3. **How It Works:**
   - Users select risk factors through an interactive interface.
   - The tool calculates likelihood and impact scores to determine overall risk.[12]
   - Visualizations and recommendations guide users in mitigating risks.[13]
4. **Tech Stack:**
   - Built using Python (logic), Streamlit (interface), Plotly (visualizations), and JavaScript/HTML (enhanced functionality).
5. **Value Added:**
   - Improves incident management workflows.
   - Enhances decision-making with clear risk prioritization.

Determining the Impact of Each Aspect

1. Threat Agent Factors:

```
- Influence the **Likelihood** by considering who might exploit the vulnerability and their motivations, resources, and capabilities.
```

2. Vulnerability Factors:

```
- Affect the **Likelihood** by assessing the ease of discovery and exploitation of vulnerabilities.
```

3. Technical Impact Factors:

```
- Directly impact the **severity of the consequences** on the system's confidentiality, integrity, availability, and accountability.
```

4. Business Impact Factors:

```
- Reflect the broader organizational effects, such as financial loss, reputational damage, and compliance violations.
```

Key Takeaways

- OWASP Risk Calculator empowers teams to assess risks quantitatively and qualitatively.[14]
- It aligns with globally recognized OWASP standards, ensuring credibility and effectiveness.[15]
- The tool provides actionable insights, making it a valuable asset for proactive risk management.

Scenarios

Low-Risk Scenario

- **Threat Agent Factors:**
  - **Skill Level:** No technical skills
  - **Motive:** Low or no reward
  - **Opportunity:** Full access/expensive resource required
  - **Size:** Developer
- **Vulnerability Factors:**
  - **Ease of Discovery:** Practically impossible
  - **Ease of Exploit:** Theoretical
  - **Awareness:** Unknown
  - **Intrusion Detection:** Active detection in application
- **Impact Factors:**
  - **Loss of Confidentiality:** Minimal non-sensitive data disclosed
  - **Loss of Integrity:** Minimal slightly corrupt data
  - **Loss of Availability:** Minimal secondary services interrupted
  - **Loss of Accountability:** Fully traceable
- **Business Impact Factors:**
  - **Financial Damage:** Less than the cost to fix the vulnerability
  - **Reputation Damage:** Minimal damage
  - **Non-Compliance:** Minor violation
  - **Privacy Violation:** One individual

Medium-Risk Scenario

- **Threat Agent Factors:**
  - **Skill Level:** Some technical skills
  - **Motive:** Possible reward
  - **Opportunity:** Some access or resource required
  - **Size:** Authenticated users
- **Vulnerability Factors:**
  - **Ease of Discovery:** Easy
  - **Ease of Exploit:** Easy
  - **Awareness:** Obvious
  - **Intrusion Detection:** Logged without review
- **Impact Factors:**
  - **Loss of Confidentiality:** Extensive non-sensitive data disclosed
  - **Loss of Integrity:** Minimal seriously corrupt data
  - **Loss of Availability:** Extensive secondary services interrupted
  - **Loss of Accountability:** Possibly traceable
- **Business Impact Factors:**
  - **Financial Damage:** Minor effect on annual profit
  - **Reputation Damage:** Loss of major accounts
  - **Non-Compliance:** Clear violation
  - **Privacy Violation:** Hundreds of people

High-Risk Scenario

- **Threat Agent Factors:**
  - **Skill Level:** Security penetration skills
  - **Motive:** High reward
  - **Opportunity:** No access or resource required
  - **Size:** Anonymous internet users
- **Vulnerability Factors:**
  - **Ease of Discovery:** Automated tools available
  - **Ease of Exploit:** Automated tools available
  - **Awareness:** Public knowledge
  - **Intrusion Detection:** Not logged
- **Impact Factors:**
  - **Loss of Confidentiality:** All data disclosed
  - **Loss of Integrity:** All data totally corrupt
  - **Loss of Availability:** All services completely lost
  - **Loss of Accountability:** Completely anonymous
- **Business Impact Factors:**
  - **Financial Damage:** Bankruptcy
  - **Reputation Damage:** Brand damage
  - **Non-Compliance:** High profile violation
  - **Privacy Violation:** Millions of people