Introduction and implementation
OWASP Risk Rating Management

M. Febri Ramadlan
About Me

Mohammad Febri Ramadlan (Ebi) is open source and information security enthusiast. Currently, He is IT Security Consultant in Indonesia

Ebi also join some community such as OWASP, Code Security, Fowab (Forum Web Anak Bandung)

Last of all, his hobbies is swimming, playing music, blogging, and part time travelling.

Contact Person:

: (+62) 81809809636
: mohammadfebrir@gmail.com
: mohammadfebriramadlan

: mohammadfebrir
Introduction OWASP
Risk Rating Methodology
Risk

- **Risk** is hazards, consequences that may occur as a result of an ongoing process or future event.
- Risk factor:
  1. Intervension
     - bad habit
     - life style
     - bankrupt
  2. Non-Intervension
     - gen
     - age
     - sex
Risk Management

Risk management is management process that encompasses the identification, evaluation and control of risk that may threaten the continuity of a business or a company's activities.

General Objectives: reduce expenditure, prevent companies from failure, increase corporate profits, reduce production costs and many things.
Risk Assessment

**Risk Assessment** is methods performed to determine whether an activity / risk has an acceptable or not.

Good assessment should to be done by a trained team and experienced.

Each company or organization have variety of acceptance level.
Risk Rating Method

Many standard and guidance that will help you:

• Trike
• AS/NZS 4360:2004 Risk Management
• CVSS
• OCTAVE
• OWASP Risk Rating Methodology
OWASP Risk Rating Methodology

Let's start with the standard risk model:

\[
\text{Risk} = \text{Likelihood} \times \text{Impact}
\]

How to use OWASP Risk Rating Methodology:

#Step 1: Identifying a Risk
#Step 2: Factors for Estimating Likelihood
#Step 3: Factors for Estimating Impact
#Step 4: Determining Severity of the Risk
#Step 5: Deciding What to Fix
#Step 6: Customizing Your Risk Rating Model
#Step 1: Identifying a Risk

The first step is:

**to identify a security risk that needs to be rated.**
Step 2: Factors for Estimating Likelihood

There are a number of factors that can help determine the likelihood. The first set of factors are related to the threat agent involved.

- Skill level
- Motive
- Opportunity
- Size
- Ease of discovery
- Ease of exploit
- Awareness
- Intrusion detection
Step 3: Factors for Estimating Impact

Again, each factor has a set of options:

- Loss of confidentiality
- Loss of integrity
- Loss of availability
- Loss of accountability
- Financial damage
- Reputation damage
- Non-compliance
- Privacy violation
#Step 4: Determining the Severity of the Risk (1)

- Informal Method

<table>
<thead>
<tr>
<th>Likelihood and Impact Levels</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0 to &lt; 3</td>
<td>low</td>
</tr>
<tr>
<td>3 to &lt; 6</td>
<td>medium</td>
</tr>
<tr>
<td>6 to 9</td>
<td>high</td>
</tr>
</tbody>
</table>
#Step 4: Determining the Severity of the Risk (2)

- Repeatable Method

<table>
<thead>
<tr>
<th>Skill level</th>
<th>Motive</th>
<th>Opportunity</th>
<th>Size</th>
<th>Ease of discovery</th>
<th>Ease of exploit</th>
<th>Awareness</th>
<th>Intrusion detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>9</td>
<td>4</td>
<td>9</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>8</td>
</tr>
</tbody>
</table>

Overall Likelihood | 5.625 | Medium
### #Step 4: Determining the Severity of the Risk (2)

- Repeatable Method

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Skill level</th>
<th>Motive</th>
<th>Opportunity</th>
<th>Size</th>
<th>Ease of discovery</th>
<th>Ease of exploit</th>
<th>Awareness</th>
<th>Intrusion detection</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5</td>
<td>9</td>
<td>4</td>
<td>9</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>Overall Likelihood</td>
<td>5.625</td>
<td>Medium</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Overall Likelihood: **5.625** Medium
#Step 4: Determining the Severity of the Risk (2)

- Repeatable Method (2)

## Impact

<table>
<thead>
<tr>
<th></th>
<th>Loss of confidentiality</th>
<th>Loss of integrity</th>
<th>Loss of availability</th>
<th>Loss of accountability</th>
<th>Financial damage</th>
<th>Reputation damage</th>
<th>Non-compliance</th>
<th>Privacy violation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall Impact</td>
<td>7.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Overall Impact</td>
<td>7.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
#Step 4: Determining the Severity of the Risk (2)

- Repeatable Method (2)

<table>
<thead>
<tr>
<th>Impact</th>
<th>Loss of confidentiality</th>
<th>Loss of integrity</th>
<th>Loss of availability</th>
<th>Loss of accountability</th>
<th>Financial damage</th>
<th>Reputation damage</th>
<th>Non-compliance</th>
<th>Privacy violation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of confidentiality</td>
<td>5</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>7</td>
<td>9</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Loss of integrity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loss of availability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loss of accountability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial damage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reputation damage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy violation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Overall Impact** 7.0 **High**
#Step 4: Determining the Severity of the Risk (3)

- Determining Severity

<table>
<thead>
<tr>
<th>IMPACT</th>
<th>LOW</th>
<th>MEDIUM</th>
<th>HIGH</th>
<th>CRITICAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>HIGH</td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>NOTE</td>
<td>LOW</td>
<td>MEDIUM</td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td></td>
<td></td>
<td>Medium</td>
<td></td>
</tr>
</tbody>
</table>

NOTE: LOW  MEDIUM  HIGH
#Step 4: Determining the Severity of the Risk (3)

- Determining Severity

<table>
<thead>
<tr>
<th>Impact</th>
<th>Likelihood</th>
<th>Overall Risk Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Medium</td>
<td>HIGH</td>
</tr>
<tr>
<td>Medium</td>
<td>Low</td>
<td>HIGH</td>
</tr>
<tr>
<td>Low</td>
<td>NOTE</td>
<td>MEDIUM</td>
</tr>
<tr>
<td></td>
<td>Low</td>
<td>MEDIUM</td>
</tr>
</tbody>
</table>

**NOTE:**
- **IMPACT**: High, Medium, Low
- **LIKELIHOOD**: Low, Medium, High, CRITICAL

**Impact Levels:**
- **High**: High Impact, Medium Likelihood
- **Medium**: Medium Impact, Medium Likelihood
- **Low**: Low Impact, Low Likelihood

**Likelihood Levels:**
- **Low**: Low Likelihood
- **Medium**: Medium Likelihood
- **High**: High Likelihood
- **CRITICAL**: Critical Likelihood

**Risk Levels:**
- **High**: High Impact, High Likelihood
- **Medium**: Medium Impact, Medium Likelihood
- **Low**: Low Impact, Low Likelihood
- **CRITICAL**: Critical Impact, Critical Likelihood
#Step 5: Deciding What to Fix

After the risks to the application have been classified there will be a prioritized list of what to fix.

As a general rule, the most severe risks should be fixed first. It simply doesn't help the overall risk profile to fix less important risks, even if they're easy or cheap to fix.

*Remember that not all risks are worth fixing, and some loss is not only expected, but justifiable based upon the cost of fixing the issue.*
#Step 6: Customizing the Risk Rating Model

Having a risk ranking framework that is customizable for a business is critical for adoption.

- Adding factors
- Customizing options
- Weighting factors
Tools
1. OWASP Risk Rating Template (excel format)

https://www.owasp.org/images/5/5b/OWASP_Risk_Rating_Template_Example.xlsx
2. OWASP Risk Rating Calc (one website/domain)

https://gist.github.com/ErosLever/f72bc0750af4d2e2e75c3a
3. OWASP Risk Rating Management (many website/domain)

https://github.com/mohammadfebrir/owasp-riskrating
//category set by OWASP Top 10 - 2013

<table>
<thead>
<tr>
<th>#</th>
<th>Category Name</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A1 - Injection</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>A2 - Broken Authentication and Session Management</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>A3 - Cross Site Scripting</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>A4 - Insecure Direct Object</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>A5 - Security Misconfiguration</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>A6 - Sensitive Data Exposure</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>A7 - Missing Function Level Access Contr</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>A8 - Cross Site Request Forgery</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>A9 - Using Components with Known Vulnera</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>A10 - Unvalidated Redirects and Forwards</td>
<td></td>
</tr>
</tbody>
</table>
//you can assess many website as you want (dynamic)
Question?
Thank you..