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


: mohammadfebriramadlan


: mohammadfebri.r


: 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:

Risk = Likelihood * 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

Likelihood and Impact Levels	
0 to < 3	low
3 to < 6	medium
6 to 9	high

#Step 4: Determining the Severity of the Risk (2)

- Repeatable Method

Likelihood							
Skill level	**Motive**	**Opportunity**	**Size**	**Ease of discovery**	**Ease of exploit**	**Awareness**	**Intrusion detection**
5	9	4	9	3	3	4	8
Overall Likelihood				**5.625**	Medium		

#Step 4: Determining the Severity of the Risk (2)

- Repeatable Method

Likelihood							
Skill level	**Motive**	**Opportunity**	**Size**	**Ease of discovery**	**Ease of exploit**	**Awareness**	**Intrusion detection**
5	9	4	9	3	3	4	8
Overall Likelihood				**5.625**	Medium		

#Step 4: Determining the Severity of the Risk (2)

- Repeatable Method (2)

Impact							
Loss of confidenti-ality	**Loss of integrity**	**Loss of availability**	**Loss of account-ability**	**Financial damage**	**Reputation damage**	**Non-compliance**	**Privacy violation**
5	7	7	7	7	9	7	7
			Overall Impact	**7.0**	High		

#Step 4: Determining the Severity of the Risk (2)

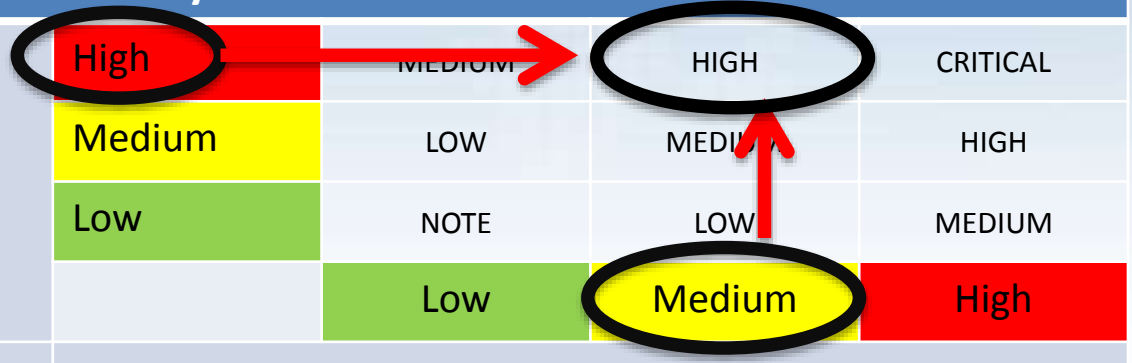
- Repeatable Method (2)

Impact							
Loss of confidenti-ality	**Loss of integrity**	**Loss of availability**	**Loss of account-ability**	**Financial damage**	**Reputation damage**	**Non-compliance**	**Privacy violation**
5	7	7	7	7	9	7	7
			Overall Impact	**7.0**	High		

#Step 4: Determining the Severity of the Risk (3)

- Determining Severity

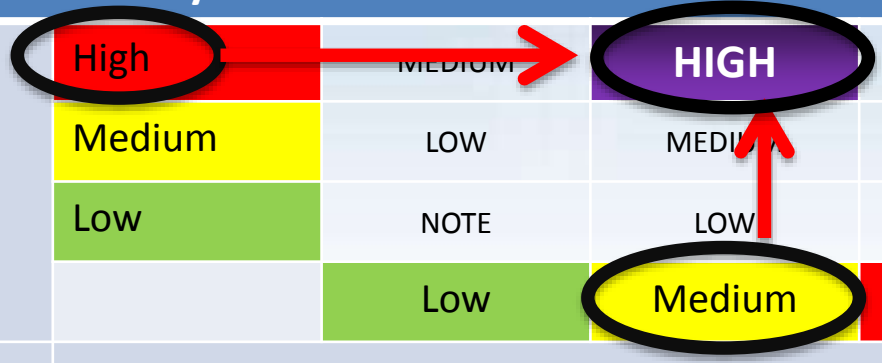
Overall Risk Severity				
IMPACT	High	MEDIUM	HIGH	CRITICAL
	Medium	LOW	MEDIUM	HIGH
	Low	NOTE	LOW	MEDIUM
		Low	Medium	High
	LIKELIHOOD			



#Step 4: Determining the Severity of the Risk (3)

- Determining Severity

Overall Risk Severity				
IMPACT	High	MEDIUM	HIGH	CRITICAL
	Medium	LOW	MEDIUM	HIGH
	Low	NOTE	LOW	MEDIUM
		Low	Medium	High
	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

Likelihood								
Threat agent factors					Vulnerability factors			
Skill level	Motive	Opportunity	Size		Ease of discovery	Ease of exploit	Awareness	Intrusion detection
4 - Advanced computer user	1 - Low or no reward	4 - Special access or resources required	5 - Partners		3 - Difficult	3 - Difficult	4 - Hidden	3 - Logged and reviewed
Overall likelihood: 3,375 MEDIUM								

Technical Impact					Business Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability		Financial damage	Reputation damage	Non-compliance	Privacy violation
2 - Minimal non-sensitive data disclosed	1 - Minimal slightly corrupt data	5 - Minimal primary services interrupted, extensive secondary services interrupted	9 - Completely anonymous		1 - Less than the cost to fix the vulnerability	1 - Minimal damage	5 - Clear violation	5 - Hundreds of people
Overall technical impact: 4,250 MEDIUM					Overall business impact: 3,000 MEDIUM			
Overall impact: 3,625 MEDIUM								

Overall Risk Severity = Likelihood x Impact				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

OWASP
Open Web Application Security Project

2. OWASP Risk Rating Calc (one website/domain)

https://gist.github.com/ErosLever/f72bc0750af4d2e75c3a

Likelihood

Threat Agent Factors

Skill Level	Motive	Opportunity	Size
3 - Some technical s	4 - Possible reward	9 - No access or res	4 - Intranet users

Vulnerability Factors

Ease of Discovery	Ease of Exploit	Awareness	Intrusion Detection
7 - Easy	1 - Theoretical	4 - Hidden	8 - Logged without

Impact

Technical Impact

Loss of Confidentiality	Loss of Integrity	Loss of Availability	Loss of Accountability
9 - All data disclosed	1 - Minimal slightly	5 - Minimal primary	1 - Fully traceable

Business Impact

Financial Damage	Reputation Damage	Non-Compliance	Privacy Violation
9 - Bankruptcy	5 - Loss of goodwill	7 - High profile viola	5 - Hundreds of peo

Scores

Intermediate

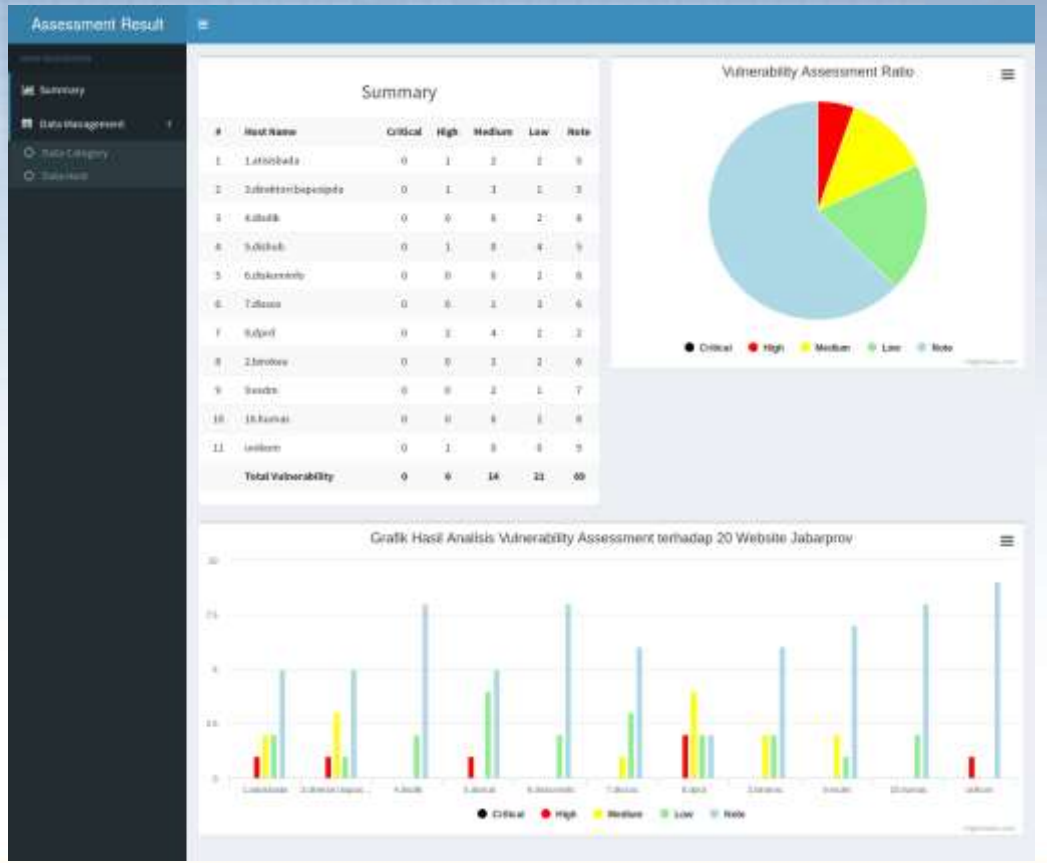
Overall Likelihood		Overall Technical Impact		Overall Business Impact	
5	MEDIUM	4	MEDIUM	6.5	HIGH

Final Score

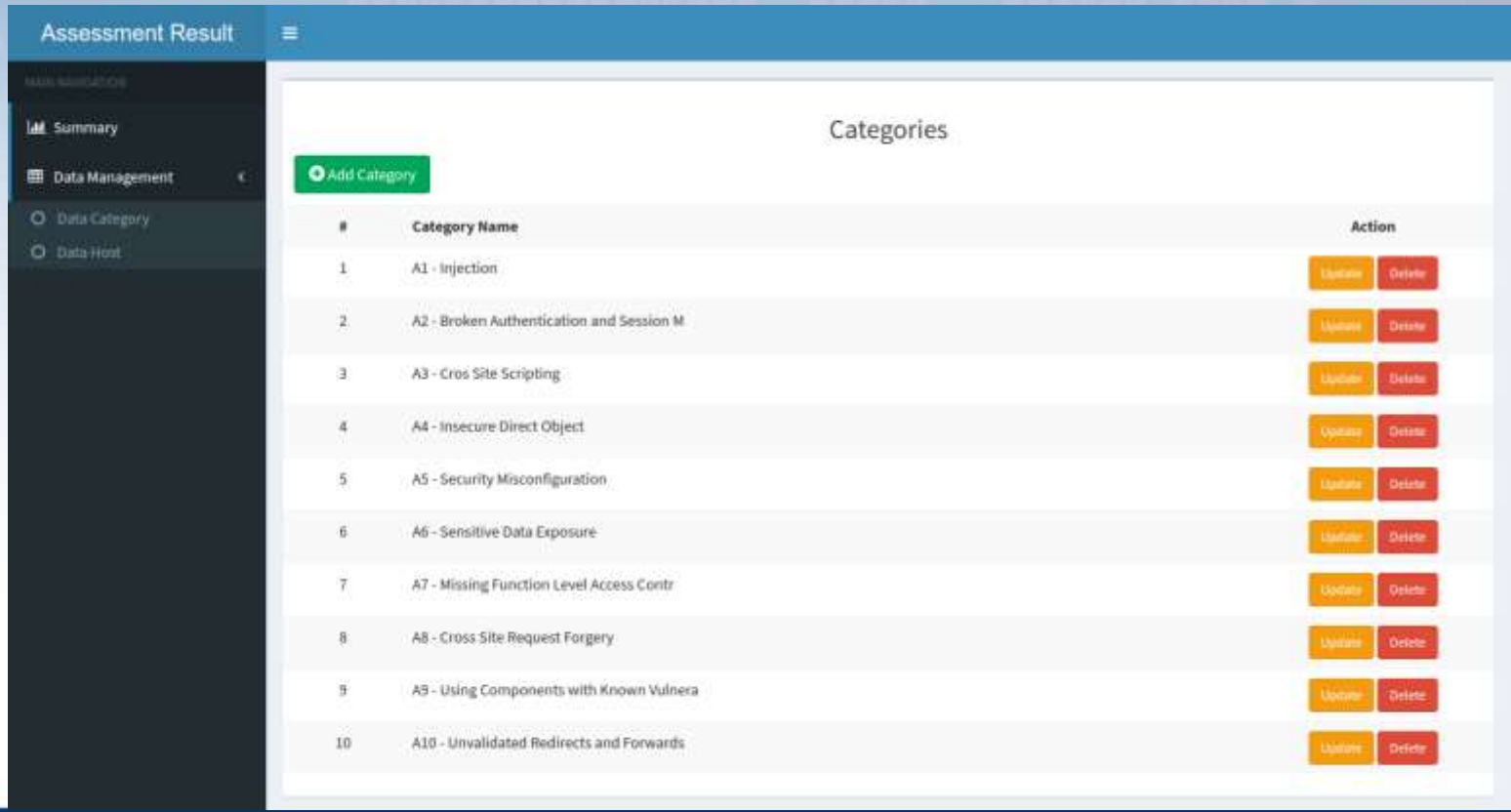
Adjust score	Risk
Technical — Business	MEDIUM

3. OWASP Risk Rating Management (many website/domain)

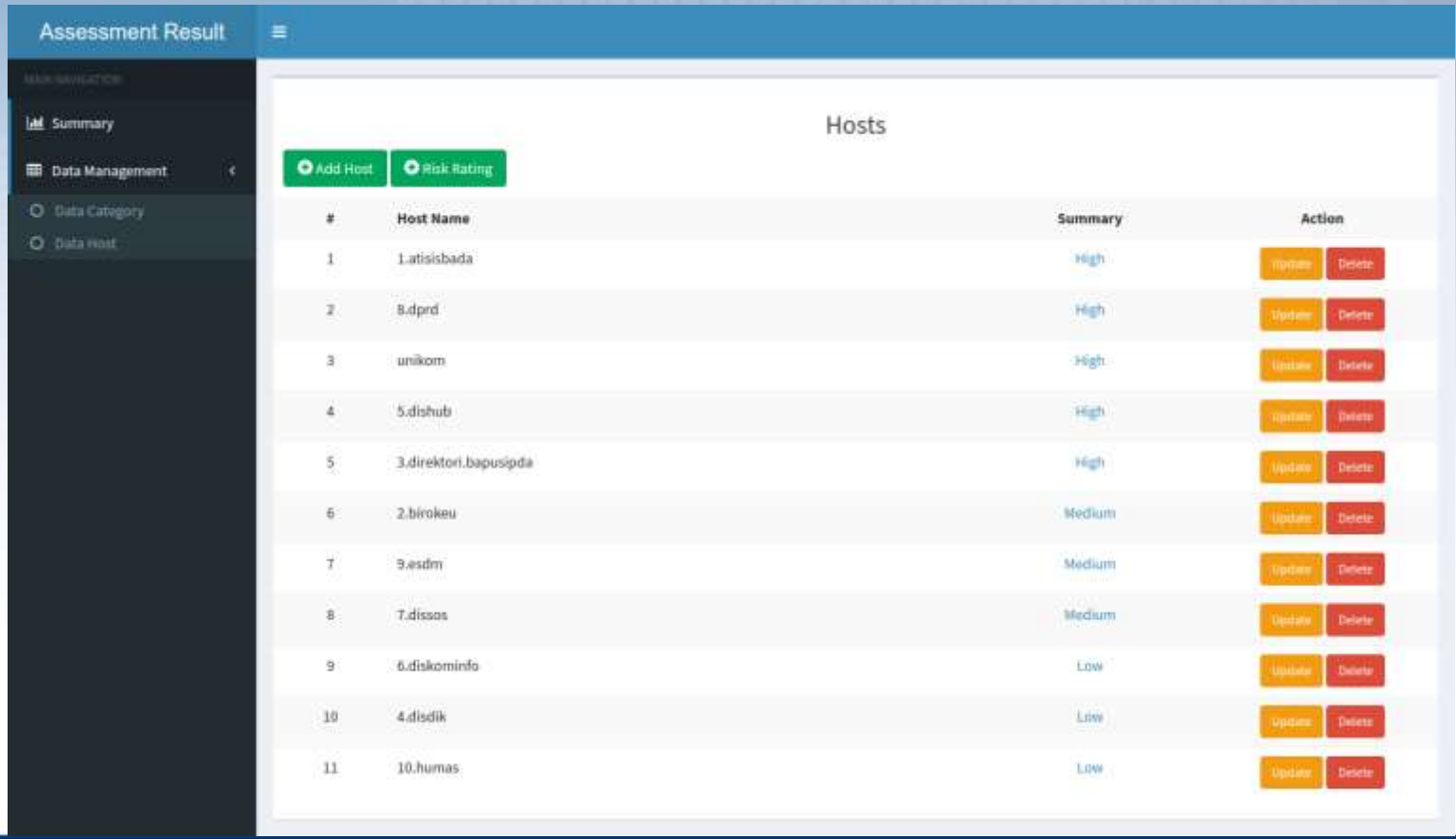
https://github.com/mohammadfebrir/owasp-riskrating



//category set by OWASP Top 10 - 2013



//you can assesst many website as you want (dynamic)



Question?

Thank you..