OWASP

Open Web Application
Security Project

Introduction and implementation OWASP Risk Rating Management

Ade Yoseman Putra

About Me

- Researcher & also a Co-founder of Security Just Illusion (non-profit organization information security).
- more than 5 years' experience in information security,
- experience in cert (computer emergency response team) , IDSIRTII/CC - Present
- Information Security Trainer in Kuala Lumpur, Malaysia and Indonesia.
- speaker at arsenal, blackhat asia singapore 2017.
- Volunteer of Security BSide Indonesia . BSide is open security conference in the world

Lists contributor to owasp

- Trainer in OWASP KL DAY 2016, University Kuala Lumpur Malaysia
- OWASP Indonesia (Jakarta) Chapter Leader
- Help organize owasp risk rating management @owasp summit london england 2017 through remotely
- OWASP volunteer (owasp risk rating management project lead)

OWASP
Open Web Application
Security Project

Introduction OWASP
Risk Rating Methodology

OWASP
Open Web Application
Security Project

Risk

- **Risk is** hazards, consequences that may occur as a result of an ongoing process or future event.
- Risk factor:
  1. Intervention
     - bad habit
     - life style
     - bankrupt
  2. Non-Intervention
     - 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 confidentiality	**Loss of integrity**	**Loss of availability**	**Loss of accountability**	**Financial damage**	**Reputation damage**	**Non-compliance**	**Privacy violation**
5	7	7	7	7	9	7	7
			Overall Impact	**7.0**	High		

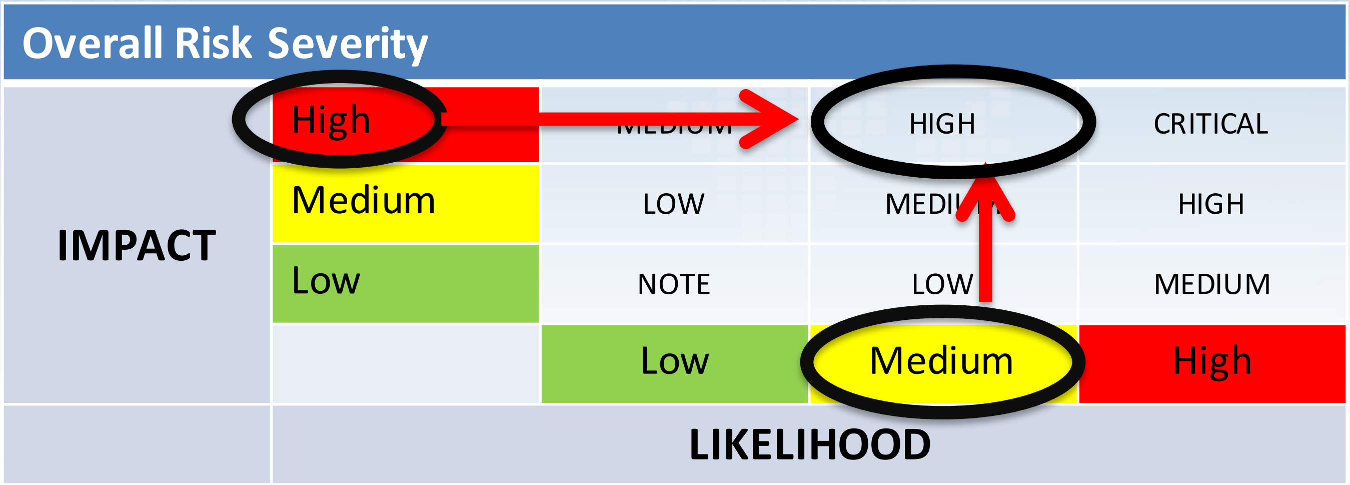
#Step 4: Determining the Severity of the Risk (2)

- Repeatable Method (2)

Impact							
Loss of confidentiality	**Loss of integrity**	**Loss of availability**	**Loss of accountability**	**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.

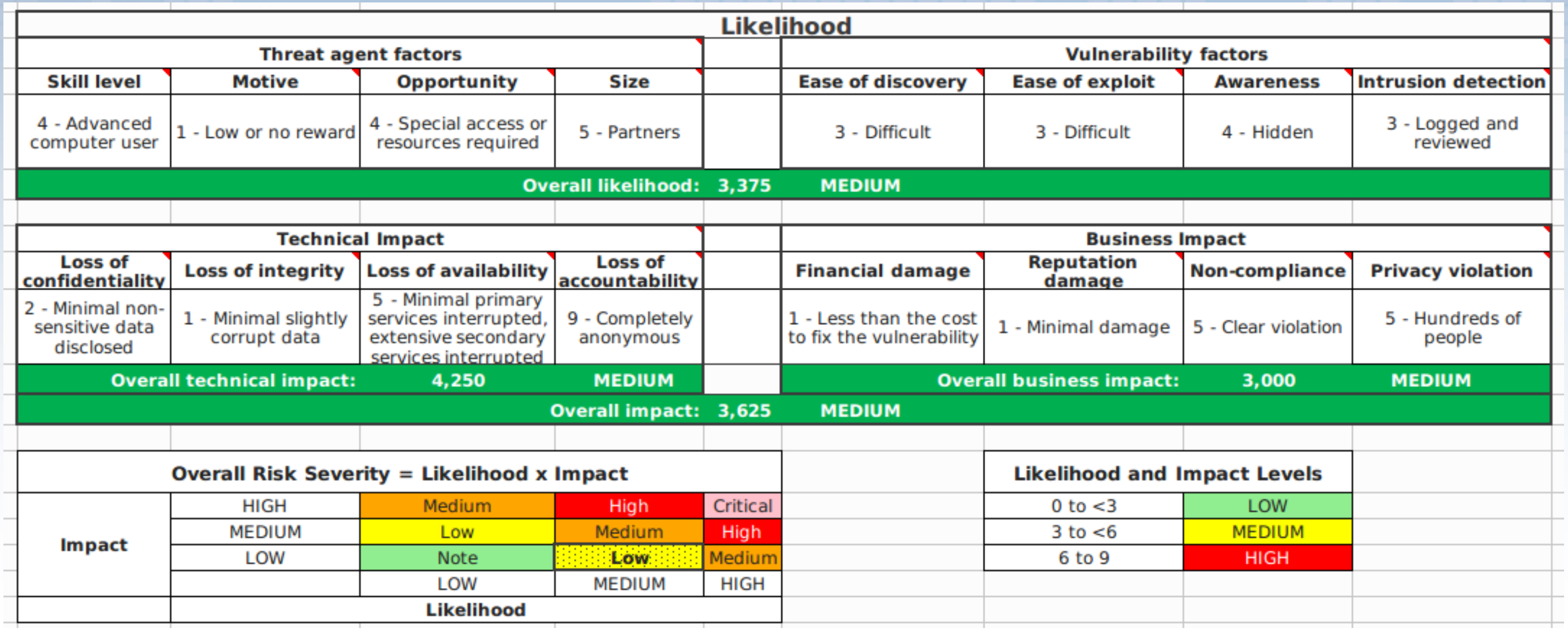
- Adding factors
- Customizing options
- Weighting factors

Tools

Open Web Application
Security Project

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			

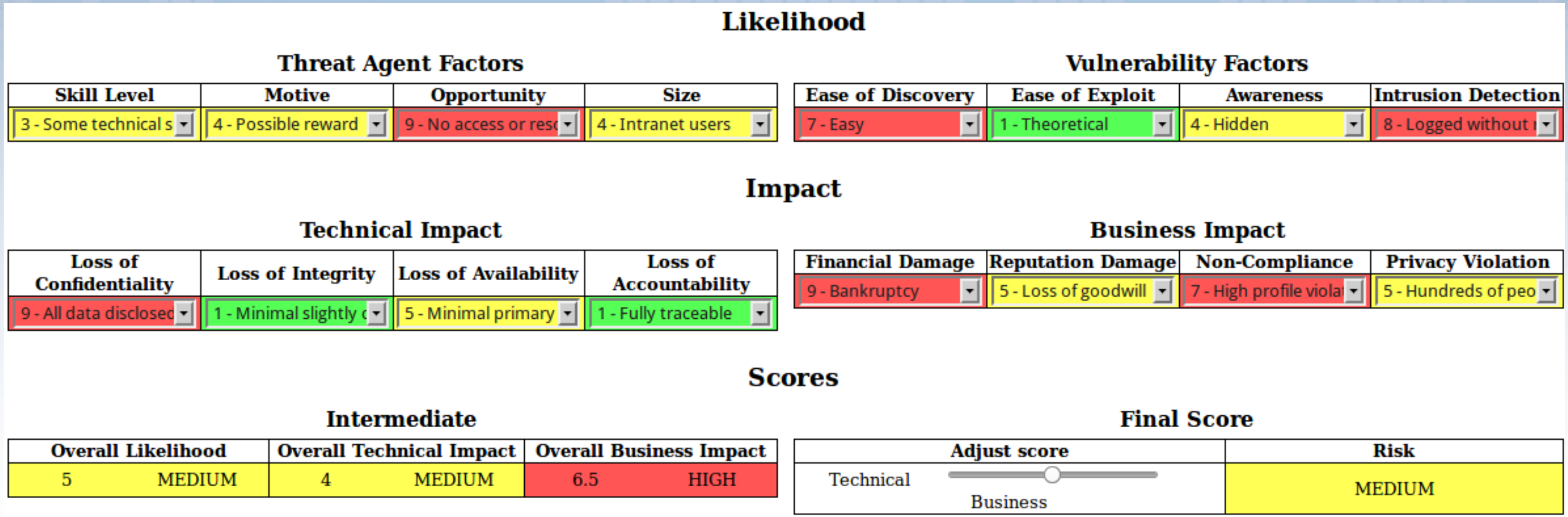
Overall Risk Severity = Likelihood x Impact				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

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 resc	4 - Intranet users

Vulnerability Factors

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

Impact

Technical Impact

Loss of Confidentiality	Loss of Integrity	Loss of Availability	Loss of Accountability
9 - All data disclosec	1 - Minimal slightly c	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

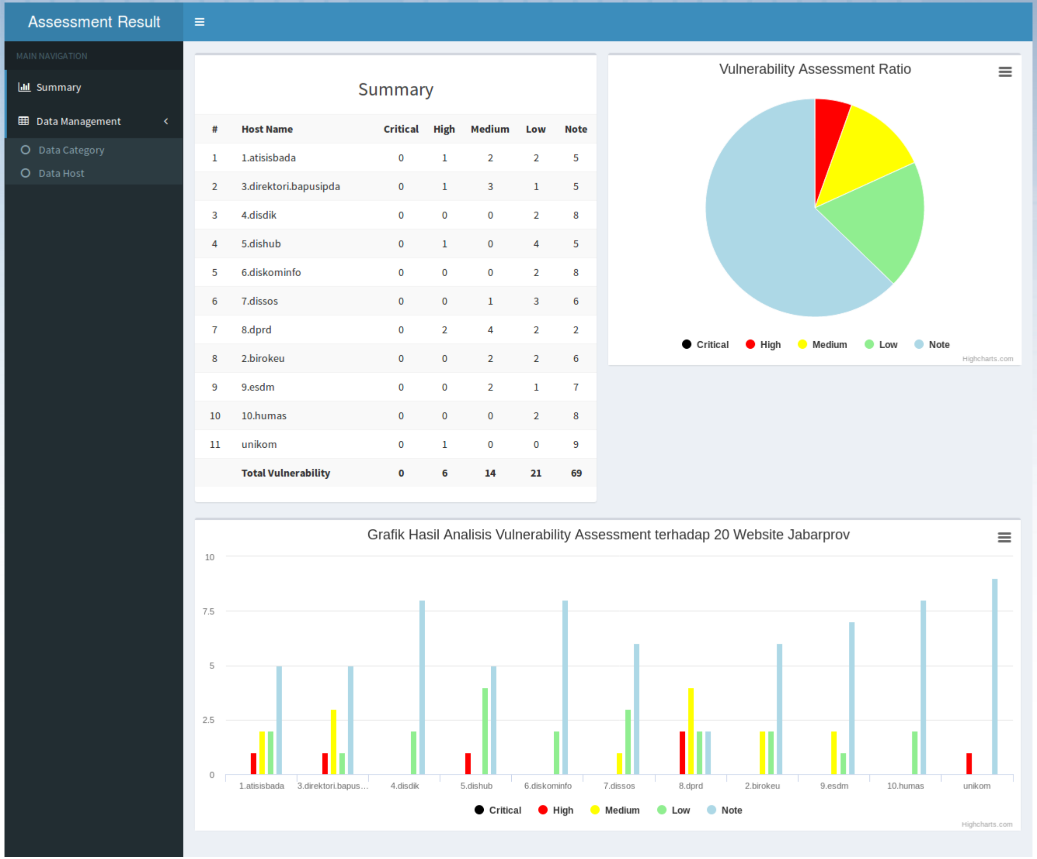
Overall Likelihood		Overall Technical Impact		Overall Business Impact	
5	MEDIUM	4	MEDIUM	6.5	HIGH

Final Score

Adjust score	Risk
Technical Business	MEDIUM

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

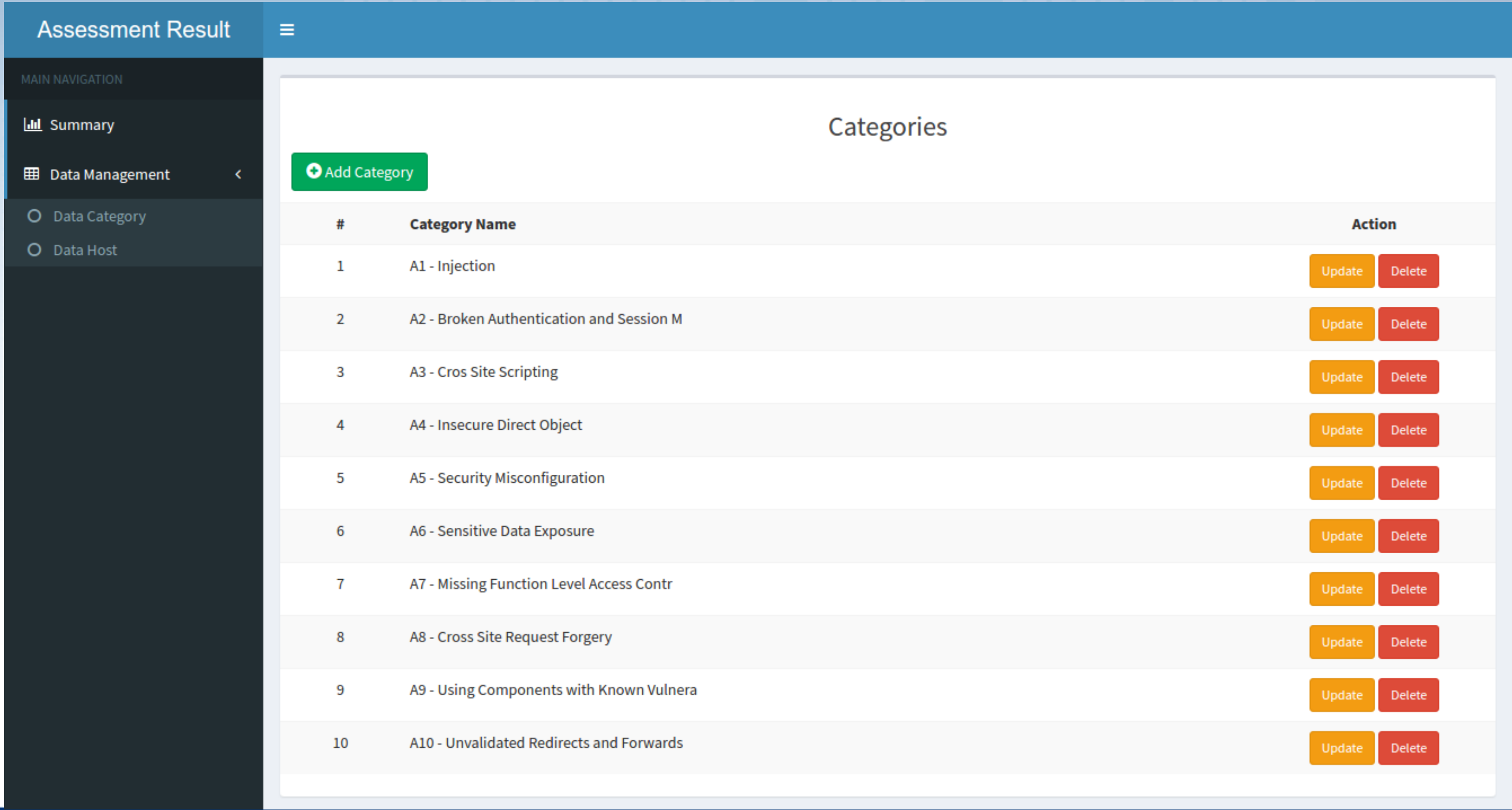
https://github.com/mohammadfebrir/owasp-riskrating



Summary

#	Host Name	Critical	High	Medium	Low	Note
1	1.atisisbada	0	1	2	2	5
2	3.direktori.bapusipda	0	1	3	1	5
3	4.disdik	0	0	0	2	8
4	5.dishub	0	1	0	4	5
5	6.diskominfo	0	0	0	2	8
6	7.dissos	0	0	1	3	6
7	8.dprd	0	2	4	2	2
8	2.birokeu	0	0	2	2	6
9	9.esdm	0	0	2	1	7
10	10.humas	0	0	0	2	8
11	unikom	0	1	0	0	9
	Total Vulnerability	**0**	**6**	**14**	**21**	**69**

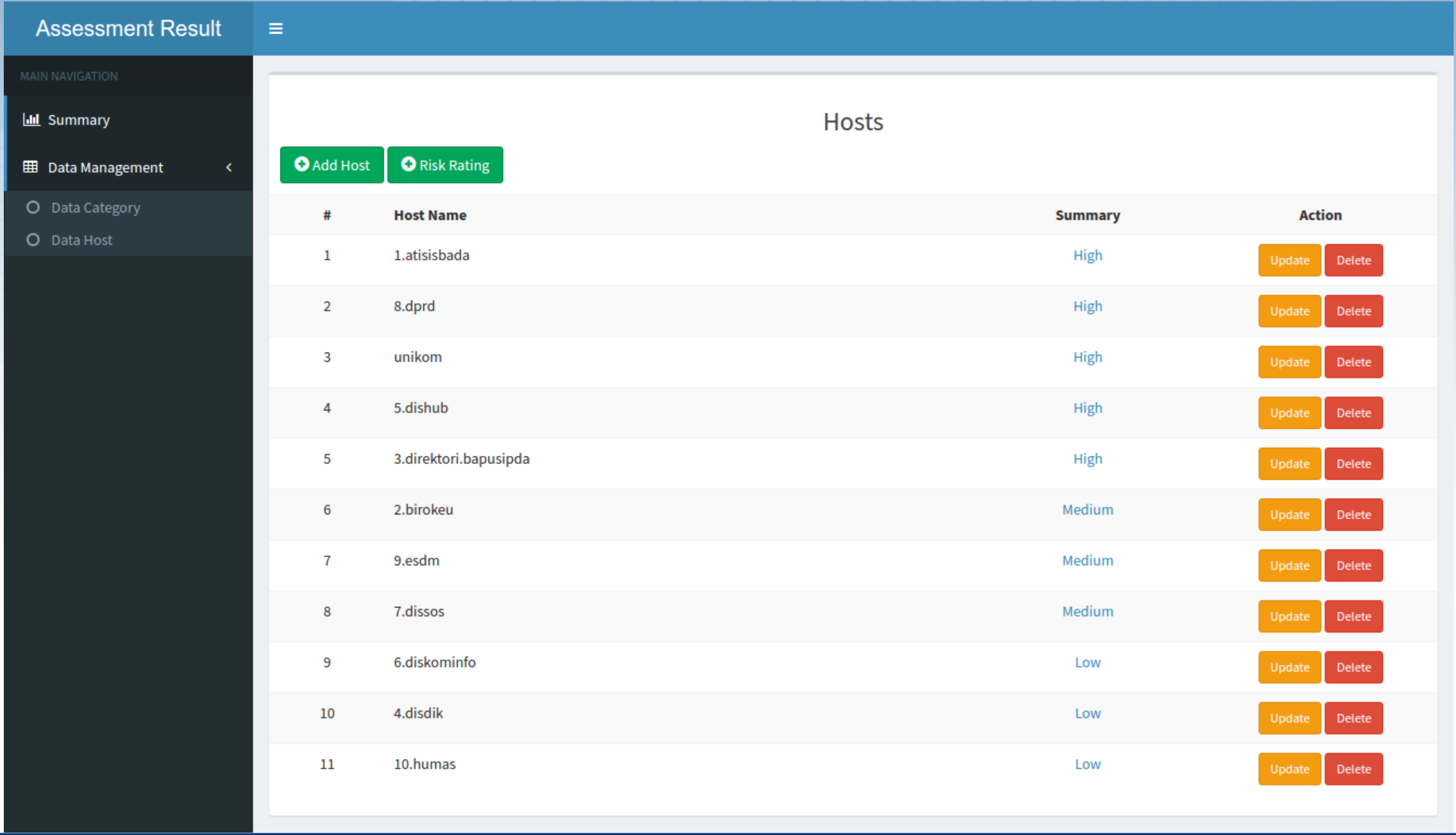
//category set by OWASP Top 10 - 2013



Categories

#	Category Name	Action
1	A1 - Injection	Update Delete
2	A2 - Broken Authentication and Session M	Update Delete
3	A3 - Cros Site Scripting	Update Delete
4	A4 - Insecure Direct Object	Update Delete
5	A5 - Security Misconfiguration	Update Delete
6	A6 - Sensitive Data Exposure	Update Delete
7	A7 - Missing Function Level Access Contr	Update Delete
8	A8 - Cross Site Request Forgery	Update Delete
9	A9 - Using Components with Known Vulnera	Update Delete
10	A10 - Unvalidated Redirects and Forwards	Update Delete

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



Hosts

#	Host Name	Summary	Action
1	1.atisisbada	High	Update Delete
2	8.dprd	High	Update Delete
3	unikom	High	Update Delete
4	5.dishub	High	Update Delete
5	3.direktori.bapusipda	High	Update Delete
6	2.birokeu	Medium	Update Delete
7	9.esdm	Medium	Update Delete
8	7.dissos	Medium	Update Delete
9	6.diskominfo	Low	Update Delete
10	4.disdik	Low	Update Delete
11	10.humas	Low	Update Delete

Question?

OWASP
Open Web Application
Security Project

Thank you..

OWASP
Open Web Application
Security Project