



Penerapan Vulnerability Assessment dan Penetration Test Bagi Pelaksanaan Audit Keamanan Informasi Sektor Pemerintah

BADAN SIBER DAN SANDI NEGARA

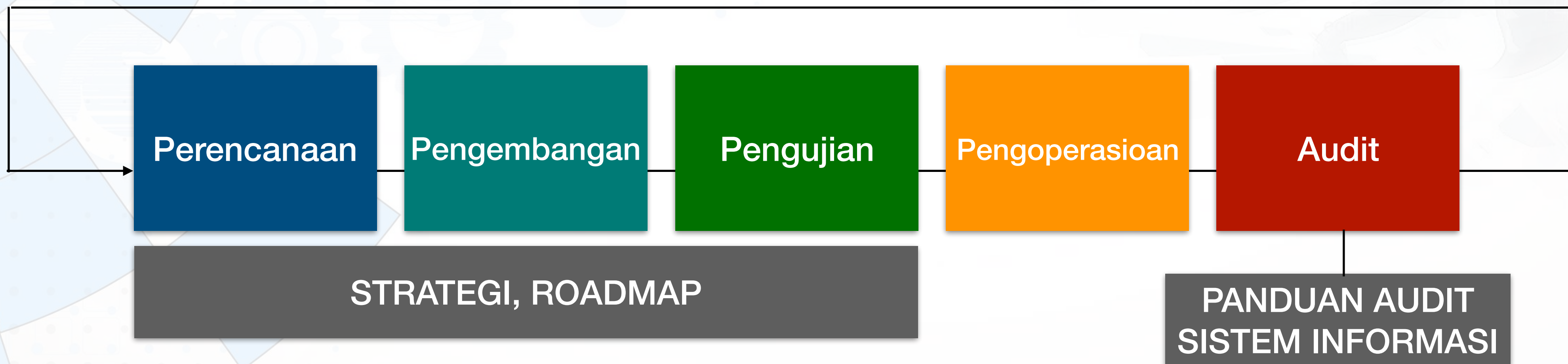
Anggrahito, S.ST., S.T.

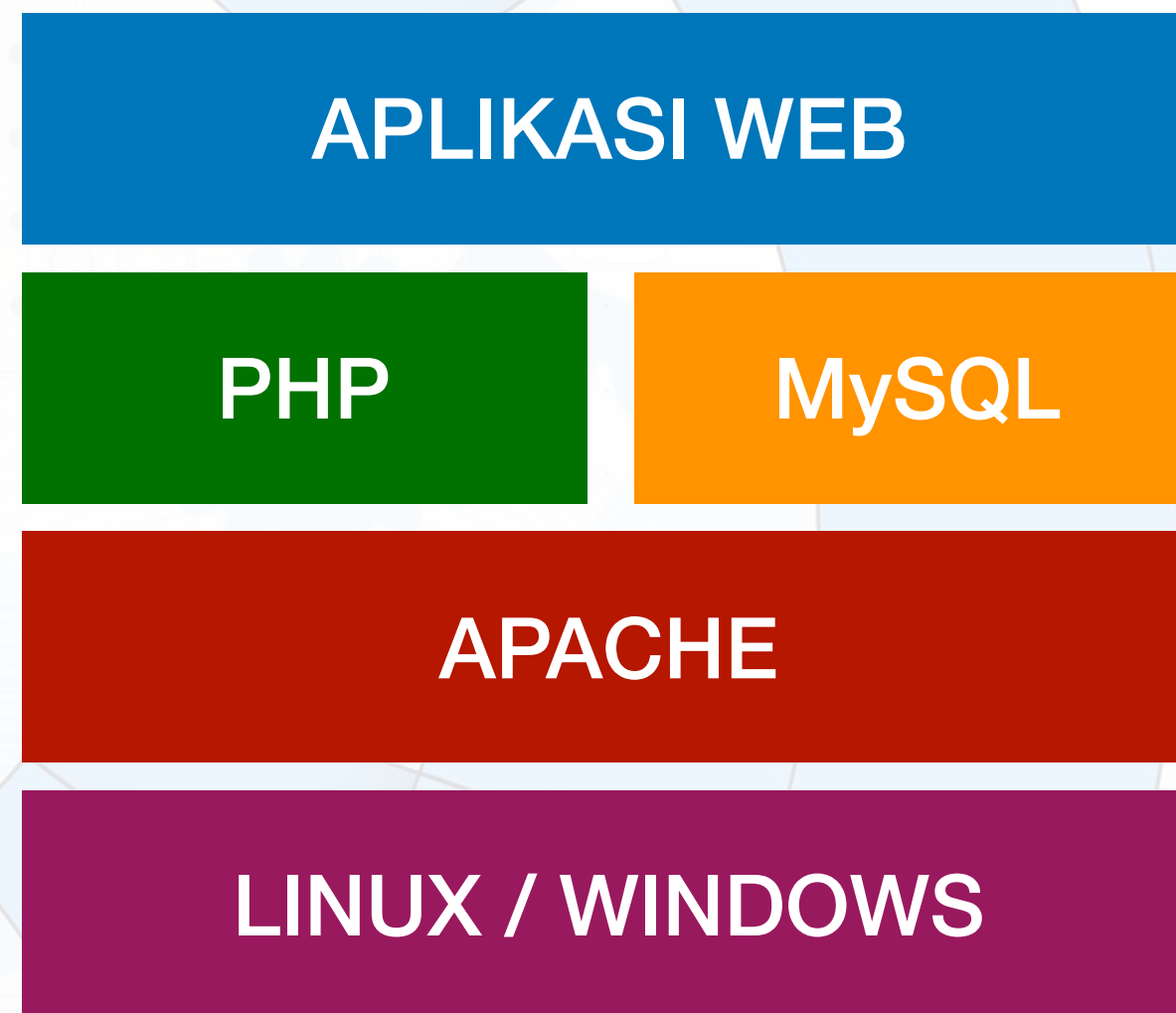
Sandiman Muda pada Pusat Pengkajian dan Pengembangan Teknologi Keamanan Siber dan Sandi

Jakarta, 10 Agustus 2018

- Tidak Berkesinambungan antara pengembangan sistem secara multiyear
- Tidak Mampu Bertukar Data
- Beragam Sistem :
 - Beragam metode pengembangan dari pihak ke-3
 - Beragam jenis Teknologi
 - Beragam Jenis Format Data
 - Beragam Jenis Program
- Kurangnya Dukungan Organisasi dan SDM
- Tidak Terverifikasi ;
 - Sistem yang dikembangkan dan kebutuhan pengguna tidak sesuai
 - Rendahnya kinerja sistem dikarenakan tidak adanya tahapan ujicoba yang telah ditetapkan







Apakah struktur tersebut cukup aman?

- Kesalahan terbanyak terjadi di aplikasi web (SQL injection, XSS, Denial of Service dan sebagainya)
- Bila aplikasi web (misal CMS, menggunakan aplikasi populer yang “Free” apakah tidak beresiko?)
- Kebanyakan situs pemerintah down karena request besar



Celah kerawanan pada file :

- /js/lookup.js
- /js/common.js

Celah kerawanan dengan merequest file tersebut sebesar 18446744073709551615 Bytes Maka Windows Server akan Crash (DOS)

Vulnerability Name:	HTTP.sys Allows Remote Code Execution (MS15-034, Network Check)
Test ID:	17622
Risk:	High
Category:	Web servers
Type:	Attack
Summary:	HTTP.sys in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 allows remote attackers to execute arbitrary code via crafted HTTP requests, aka "HTTP.sys Remote Code Execution Vulnerability."
Impact:	A remote attacker can exploit this to execute arbitrary code with SYSTEM privileges.
Solution:	https://technet.microsoft.com/en-us/library/security/ms15-034
CVE:	CVE-2015-1635
More Information:	https://technet.microsoft.com/en-us/library/security/ms15-034
Nist NVD (CVSS):	AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS Score:	10.0

Microsoft Patch : <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2015/ms15-034>

Masih banyak Website Pemerintah menggunakan Framework gratis yang belum dilakukan verifikasi dalam membuat Sistem Informasi, sebagai contoh penggunaan Framework Lokomedia CMS

Penggunaan Lokomedia CMS pada website Pemerintah perlu diantisipasi karena memiliki celah kerawanan yang critical

```
view-source:http://[redacted].go.id/[redacted]union
1 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-t
2 <html xmlns="http://www.w3.org/1999/xhtml">
3 <head>
4 <title>admin 43347a112 [redacted] </title>
5
6 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
7 <meta name="robots" content="index, follow">
8 <meta name="description" content="admin 43347a [redacted]">
9 <meta name="keywords" content="admin 43347a [redacted]">
10 <meta http-equiv="Copyright" content="lokomedia">
11 <meta name="author" content="[redacted]">
12 <meta http-equiv="imagetoolbar" content="no">
13 <meta name="language" content="Indonesia">
14 <meta name="revisit-after" content="7">
15 <meta name="webcrawlers" content="all">
16 <meta name="rating" content="general">
17 <meta name="spiders" content="all">
18
19 <link rel="shortcut icon" href="favicon.ico" />
20 <link rel="alternate" type="application/rss+xml" title="RSS 2.0" href="rss.xml" />
21 <link rel="stylesheet" href="templates/elfquery-yahoo/css/style.css" type="text/css" />
22 <link rel="stylesheet" href="templates/elfquery-yahoo/css/ticker.css" type="text/css" />
23 <link rel="stylesheet" href="templates/elfquery-yahoo/themes/base.css" type="text/css" />
24 <link rel="stylesheet" href="templates/elfquery-yahoo/themes/default/theme.css" type="text/css" />
25 <link rel="stylesheet" href="templates/elfquery2/css/style.css" type="text/css" />
26
27 <script src="templates/elfquery-yahoo/js/jquery-1.4.min.js" type="text/javascript"></script>
28 <script type="text/javascript" src="templates/elfquery-yahoo/js/flowplayer-3.2.4.min.js"></script>
29 <script src="templates/elfquery-yahoo/js/superfish.js" type="text/javascript"></script>
30 <script src="templates/elfquery-yahoo/js/hoverIntent.js" type="text/javascript"></script>
31
32 <script src="templates/elfquery2/js/jquery-1.4.js" type="text/javascript"></script>
33 <script src="templates/elfquery2/js/jquery.tipsy.js" type="text/javascript"></script>
```



Home Setting Web Setting Menu Manajemen Berita Hubungi Kami Interaksi Media Banner View Web Logout

Hai admin, selamat datang di halaman Administrator. Silahkan klik menu pilihan yang berada di bagian header untuk mengelola content website.

Senin, 05 Agustus 2018, 16:25:13 WIB

Komentar Terbaru				Hubungi Kami Terbaru			
Nama	Isi Komentar	Tanggal	Aksi	Nama	Email	Tanggal	Aksi
Agen SBOBET	I always spent my half an hour to read this weblog's content every day along with a mug of coffee.	2018-08-04	edit	Hamos	[redacted]	2017-10-04	balas
Agen SBOBET	It's amazing to pay a visit this web page and reading the views of all colleagues regarding this post, while I am also eager of getting knowledge.	2018-08-03	edit	lukman	[redacted]	2010-05-16	balas

Control Panel

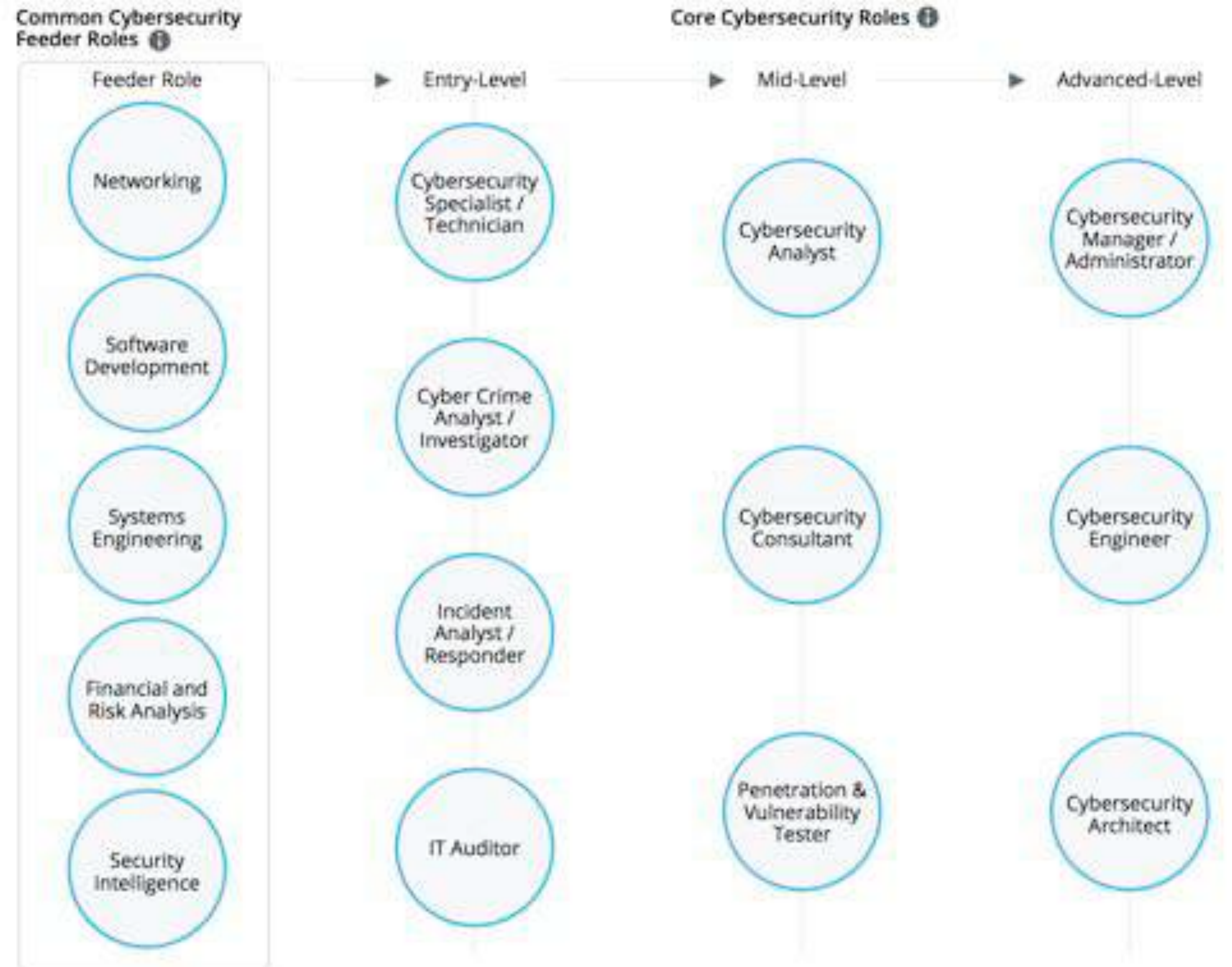
- Manajemen User
- Manajemen Modul
- Berita
- Komentar
- Download
- Agenda
- Banner
- Galeri Foto
- Poling
- Hubungi Kami

Copyright © 2009 by CMS Lokomedia. All rights reserved. [admin theme edited by wabiyu]



CYBERSECURITY CAREER PATHWAY

Pada gambar disamping memperlihatkan jenjang karir yang ideal dibidang keamanan siber. Terdapat beberapa tingkat yaitu mulai dari Feeder Role - Entry Level - Mid Level - Advanced Level



Sumber : <https://www.cyberseek.org/pathway.html>
di akses Tanggal : 18 Juli 2018



Peraturan Menteri Kominfo No. 4 Tahun 2016 Tentang Sistem Manajemen Pengamanan Informasi

Sistem Elektronik	Definisi (draft)	Tenaga Ahli	Penerapan	Penyelenggaraan
SE Strategis	sistem elektronik yang berdampak serius terhadap kepentingan umum, pelayanan publik, kelancaran penyelenggaraan negara, atau pertahanan dan keamanan negara.	Internal/ Eksternal WNI	SNI 27001	Wajib Sertifikasi SNI 27001 oleh Lembaga Sertifikasi
SE beresiko Tinggi	Sistem elektronik yang berdampak terhadap tercapainya tujuan organisasi.	Internal/Eksternal	SNI 27001	Wajib Sertifikasi SNI 27001 oleh Lembaga Sertifikasi
SE beresiko Rendah	Sistem Elektronik yang tidak termasuk Sistem Elektronik Strategis dan Sistem Elektronik Tinggi.	Internal/ Eksternal	Indeks KAMI	Dapat dilakukan

Elements of IT Security Program

- Good Planning
- Good Operations
- Continous Assessment
- Good Management Oversight





ISO 27001 Control Objective A12.6 (Technical Vulnerability Management) menyatakan bahwa “informasi tentang kerentanan teknis dari sistem informasi yang digunakan harus diperoleh secara tepat waktu, paparan organisasi terhadap kerentanan tersebut dievaluasi dan tindakan yang tepat diambil untuk mengatasi risiko terkait”.

Penetration testing membantu mengidentifikasi celah kerawanan dan memberikan detail tentang celah kerawanan atau ancaman yang terdapat pada sistem, serta memberikan panduan bagaimana cara mengatasinya. Serangan dan celah kerawanan yang teridentifikasi sebagai input *risk assessment*, dan menjadi informasi bagi tindakan perbaikan pada kontrol audit.

- Proses Pentest akan memberikan kontribusi signifikan terhadap proses audit ISMS sebagai bagian dari analisis resiko. Kerentanan aplikasi web, sistem internal dan aplikasi dapat diidentifikasi terkait dengan ancamannya;
- Sebagai bagian dari rencana perawatan resiko yang memungkinkan untuk memastikan semua tindakan yang dilaksanakan berfungsi sebagai mana mestinya;
- Sebagai bagian dari perbaikan terus menerus dari proses untuk memastikan bahwa langkah-langkahnya berfungsi dengan baik dan bahwa ancaman serta kerentanan baru yang muncul diidentifikasi dan diperbaiki.

WHY..?

Penetration Test is one of the most effective ways to identify weakness and deficiencies in these Programs

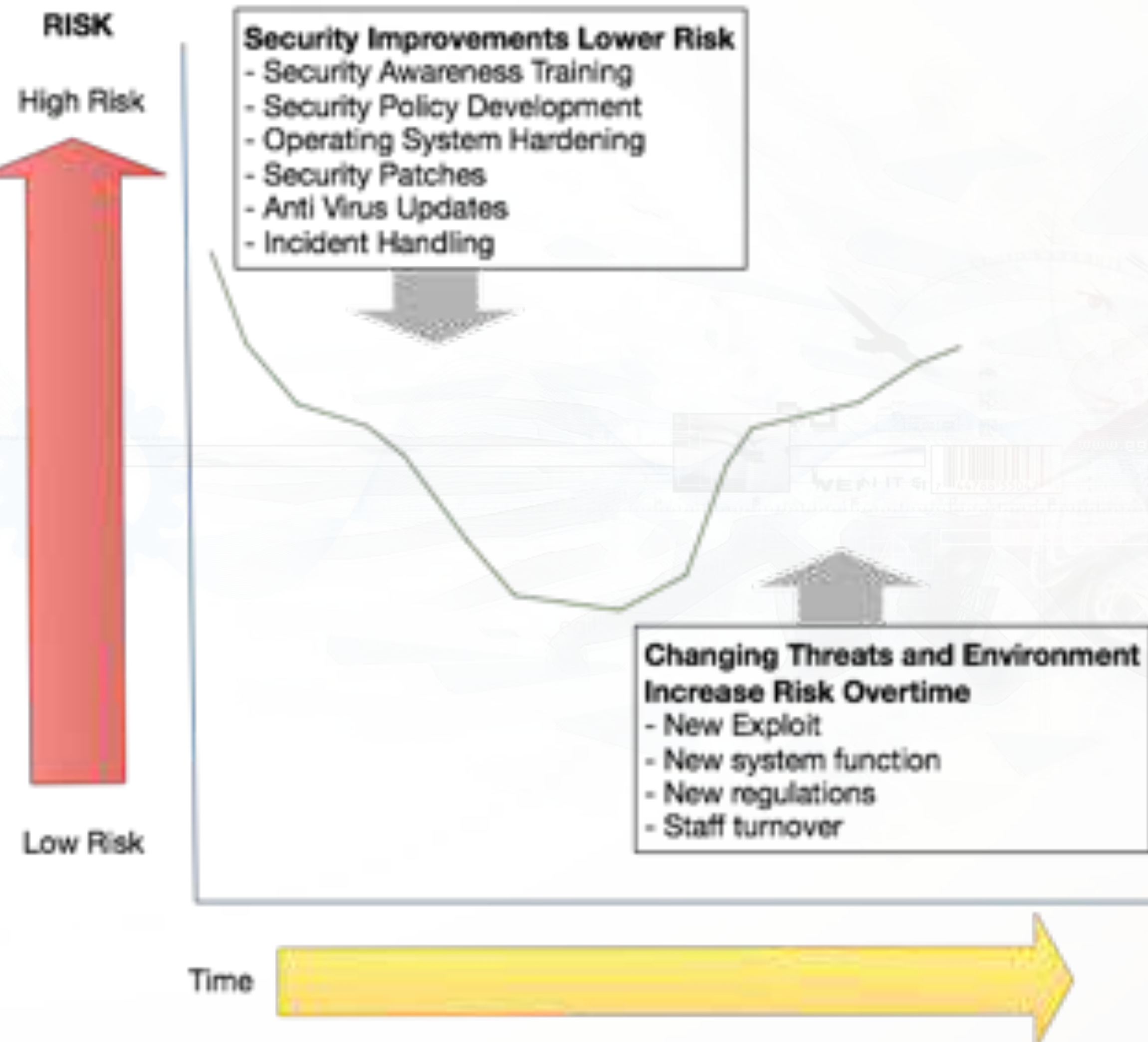
KENAPA DIBUTUHKAN IT SECURITY ASSESSMENT (PENTEST)

Information Assurance (IA) is information operations (IO) that protect and defend information and information systems by ensuring their

availability, integrity, authentication, confidentiality and nonrepudiation.

This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities (U.S. DoD 3600-1). (Boyce, 2002)

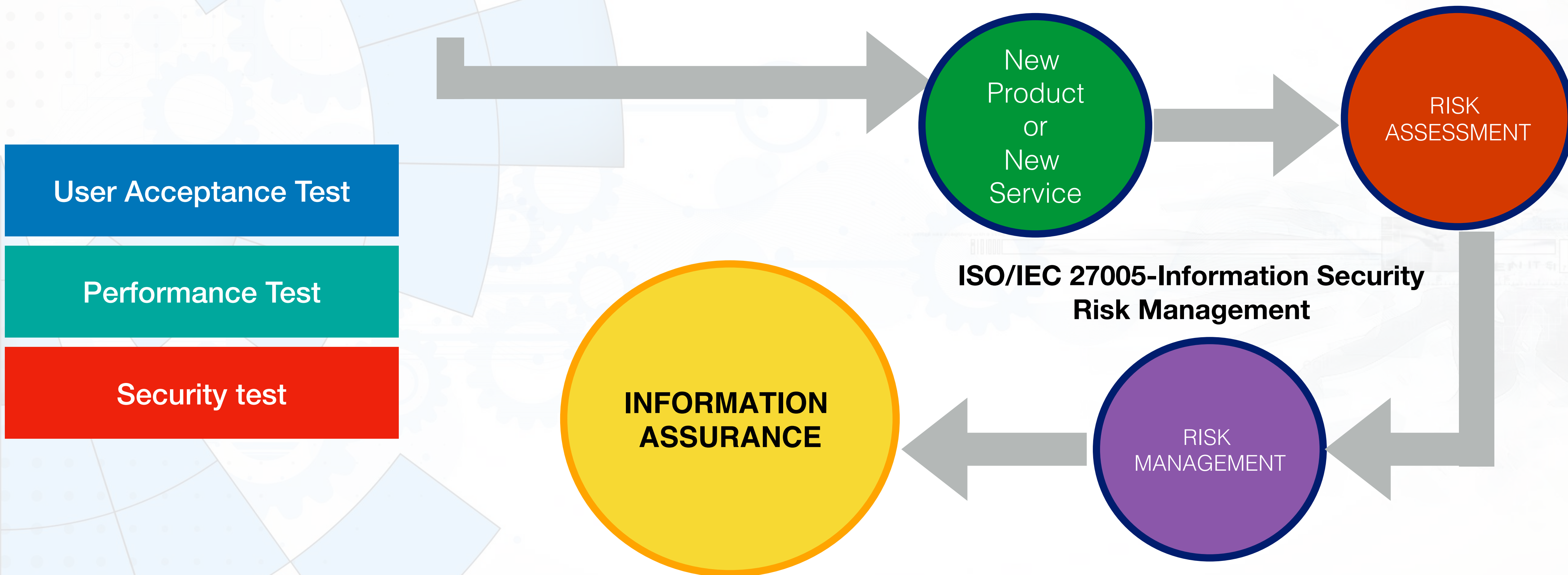
RISK ASSESSMENT





WHEN – KAPAN DILAKUKAN IT SECURITY ASSESSMENT (PENTEST)

Standar Penilaian IT Sec. Assessment Lemsaneg :
TOP 10 OWASP & Risk Rating OWASP





OWASP Top 10 - 2013	➔	OWASP Top 10 - 2017
A1 – Injection	➔	A1:2017-Injection
A2 – Broken Authentication and Session Management	➔	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	➔	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]



RISK = LIKELIHOOD * IMPACT

STEP 1 : Identifying 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



Sumber : 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	3 - Hundreds of people
Overall technical impact: 4.250				Overall business impact: 3.000			
Overall impact: 3.625				MEDIUM			
Overall Risk Severity = Likelihood x Impact				Likelihood and Impact Levels			
Impact	HIGH	Medium	High	Critical	0 to <3	LOW	
	MEDIUM	Low	Medium	High	3 to <6	MEDIUM	
	LOW	None	Low	Medium	6 to 9	HIGH	
		LOW	MEDIUM	HIGH			
		Likelihood					



Sumber : <https://gist.github.com/ErosLever/f72bc0750af4d2e75c3a>

Likelihood

Threat Agent Factors

Skill Level	Motive	Opportunity	Size
3 - Some technicals	4 - Double reward	3 - No access or req	4 - Intranet users

Vulnerability Factors

Ease of Discovery	Ease of Exploit	Awareness	Intrusion Detection
2 - Easy	1 - Theoretical	4 - Hidden	3 - Logged without

Impact

Technical Impact

Loss of Confidentiality	Loss of Integrity	Loss of Availability	Loss of Accountability
3 - All data exposed	1 - Minimal/slightly	3 - Minimal primary	1 - Fully traceable

Business Impact

Financial Damage	Reputation Damage	Non-Compliance	Privacy Violation
3 - Bankrupt	3 - Loss of goodwill	2 - High public profile	3 - Hundreds of people

Scores

Intermediate

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

Final Score

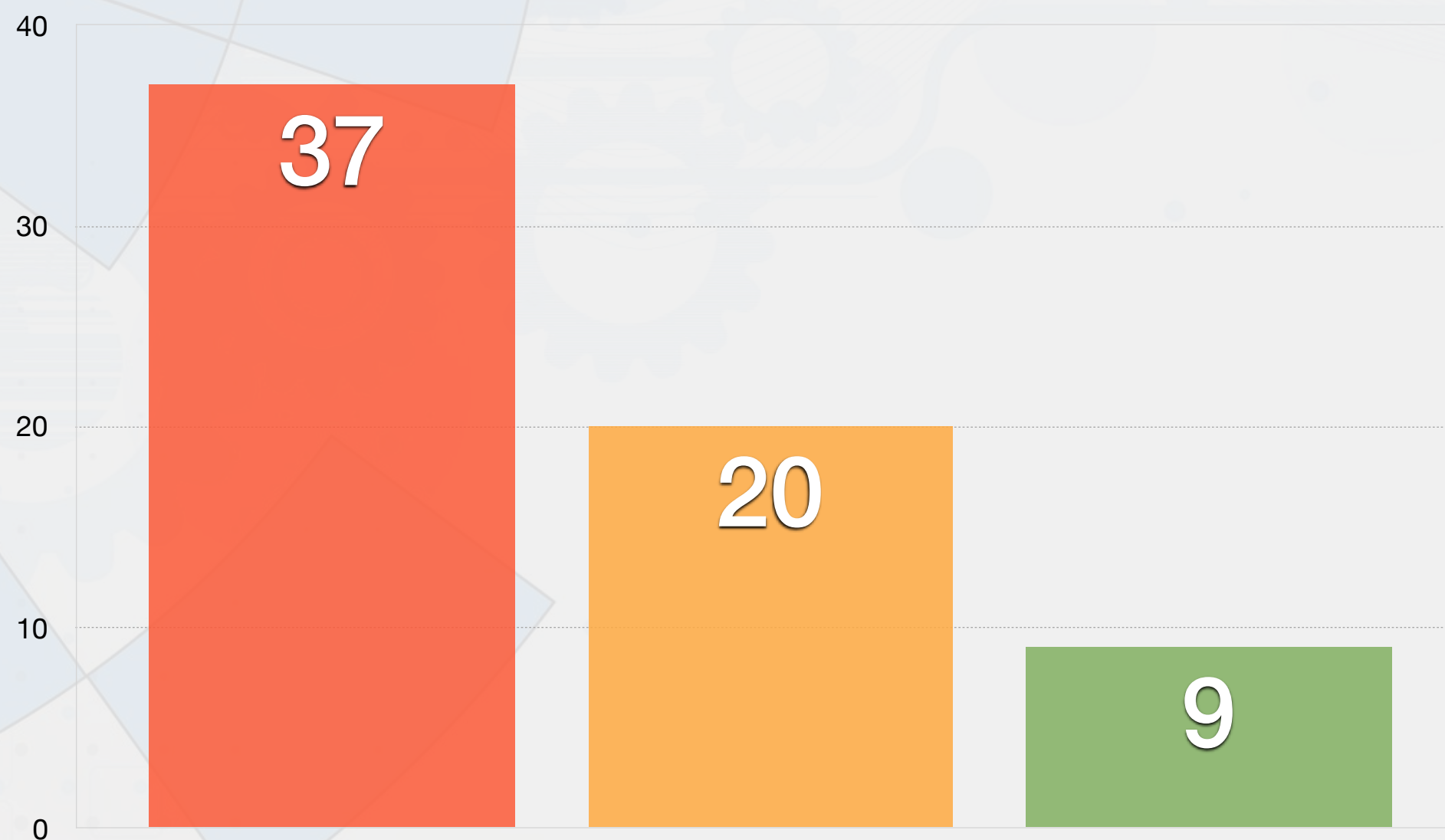
Adjust score	Risk
Technical Business	MEDIUM



Rekapitulasi Risk Level Tahun 2016

- 1. **66 Sistem Informasi**
- 2. **16 Instansi Pemerintah**
- 3. Hasil yang didapatkan dalam presentase yaitu **56 % High Risk**, **30 % Medium Risk**, dan **14% Low Risk**

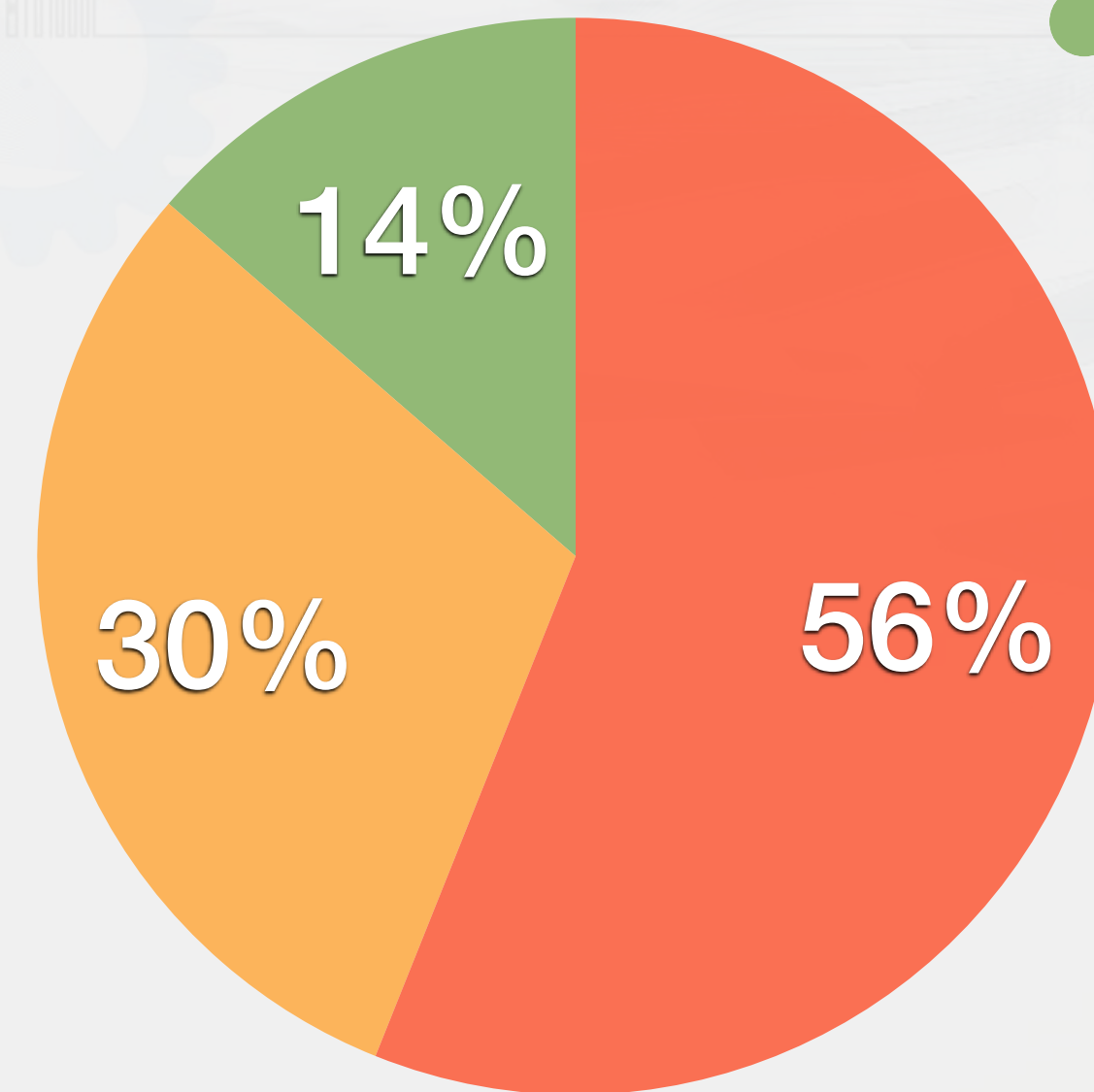
Column Chart



RISK LEVEL

Level	Jumlah Sistem Web
High	37
Medium	20
Low	9
Total	66

Pie Chart



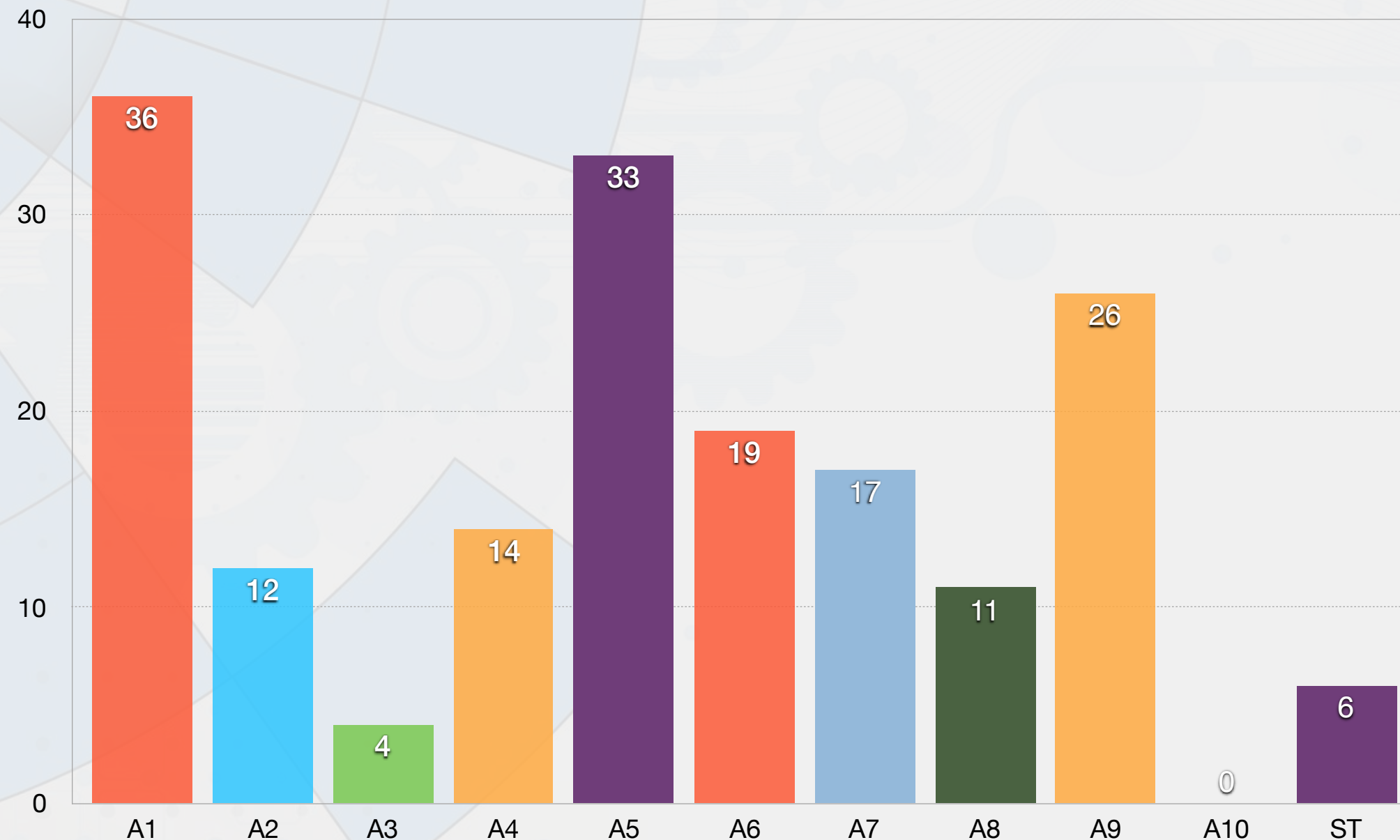
- High
- Medium
- Low



Rekapitulasi OWASP VULNERABILITIES Tahun 2016

- Hasil tertinggi dari celah kerawanan yang ditemukan dalam bentuk presentase yaitu **Database SQL Injection sebesar 20 %.**

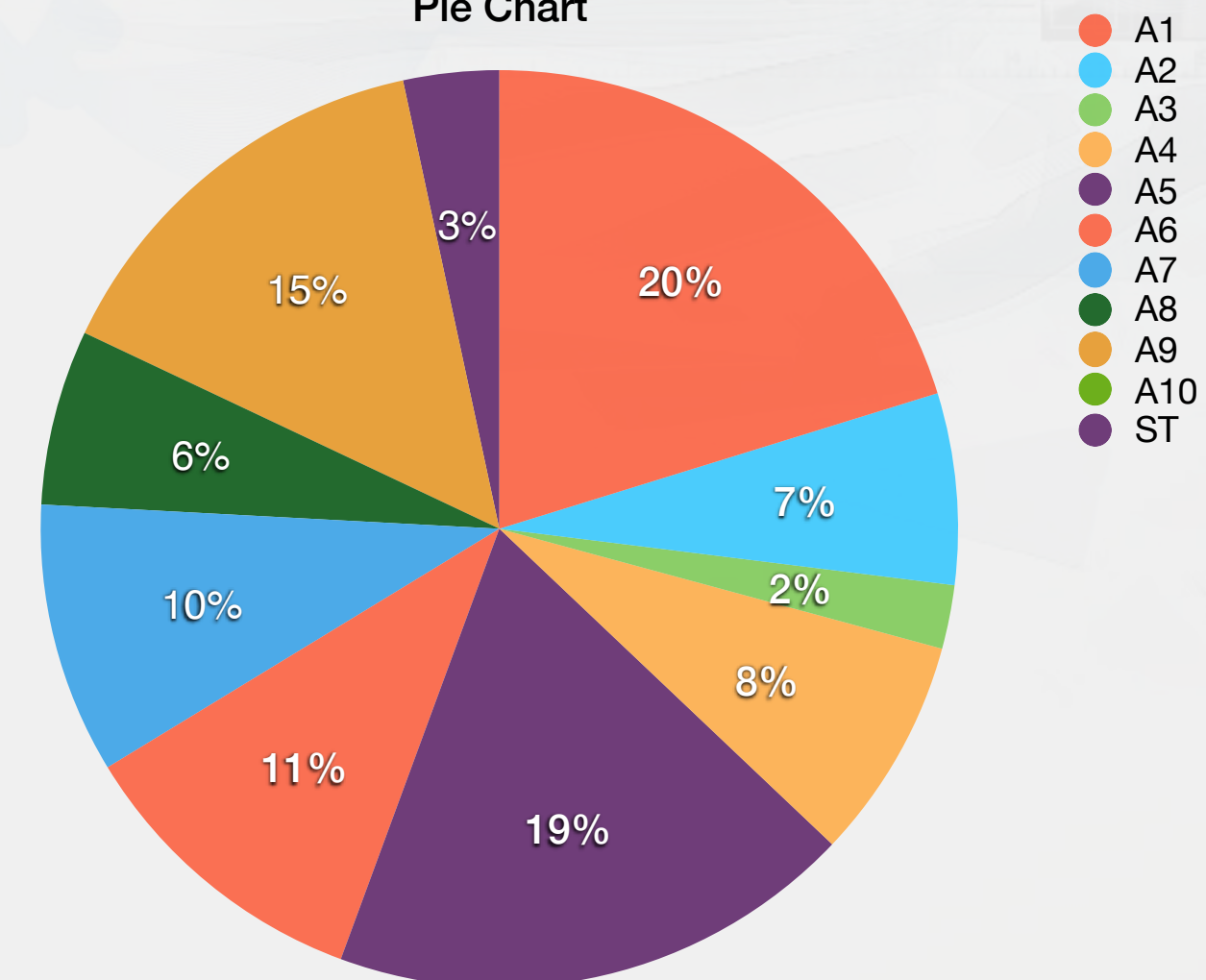
Column Chart



OWASP VULNERABILITES

VULNERABILITY POINTS	JUMLAH
A1 Database SQL Injection	36
A2 Improper Session Management	12
A3 Cross Site Scripting (XSS)	4
A4 Insecure Direct Object Reference	14
A5 Security Misconfiguration	33
A6 Sensitive Data Exposure	19
A7 Missing Function Level Access Control	17
A8 Cross Site Request Forgery (CSRF)	11
A9 Using Known Vulnerable Control	26
A10 Unvalidated Redirects & Forwards	0
ST DOS	6

Pie Chart

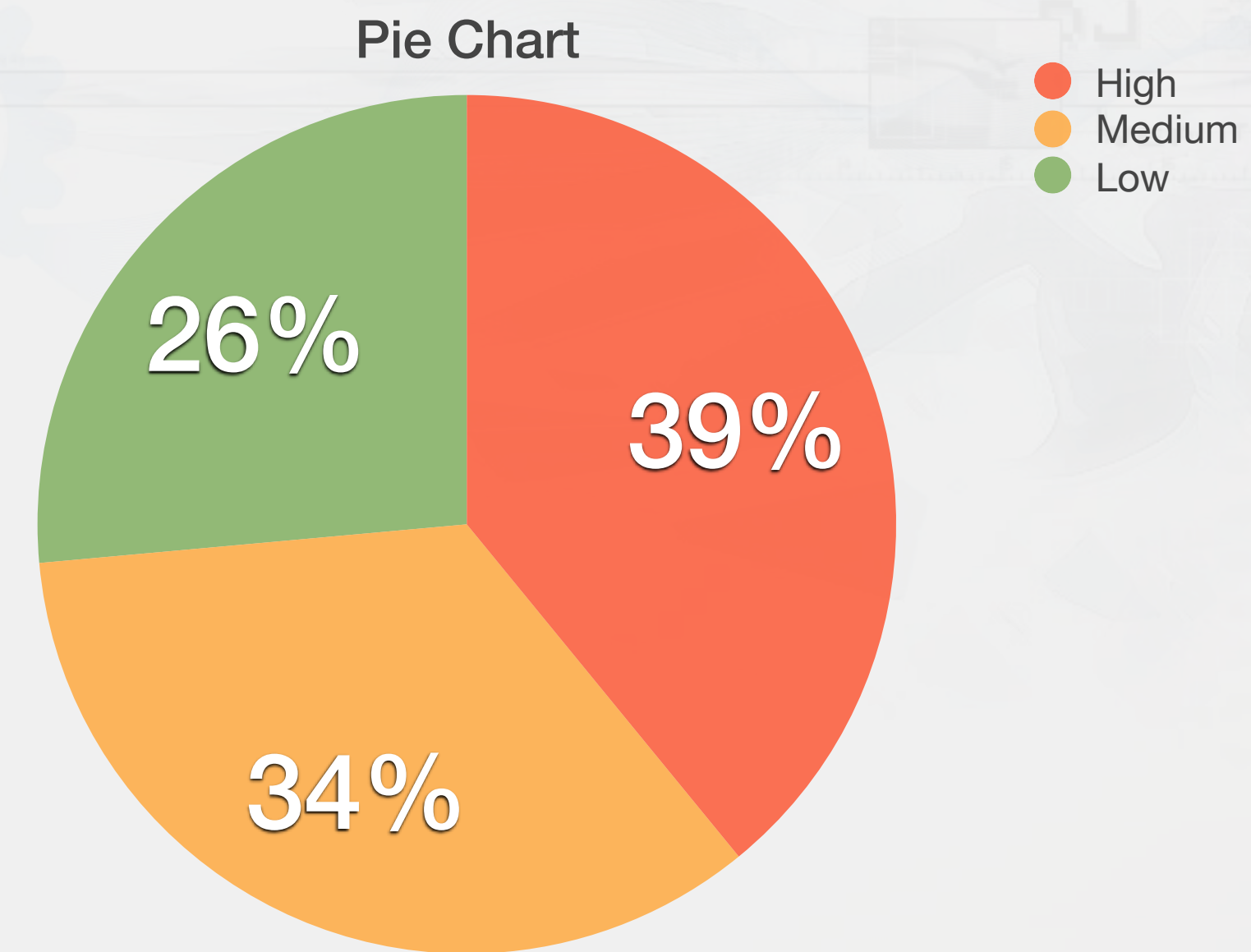
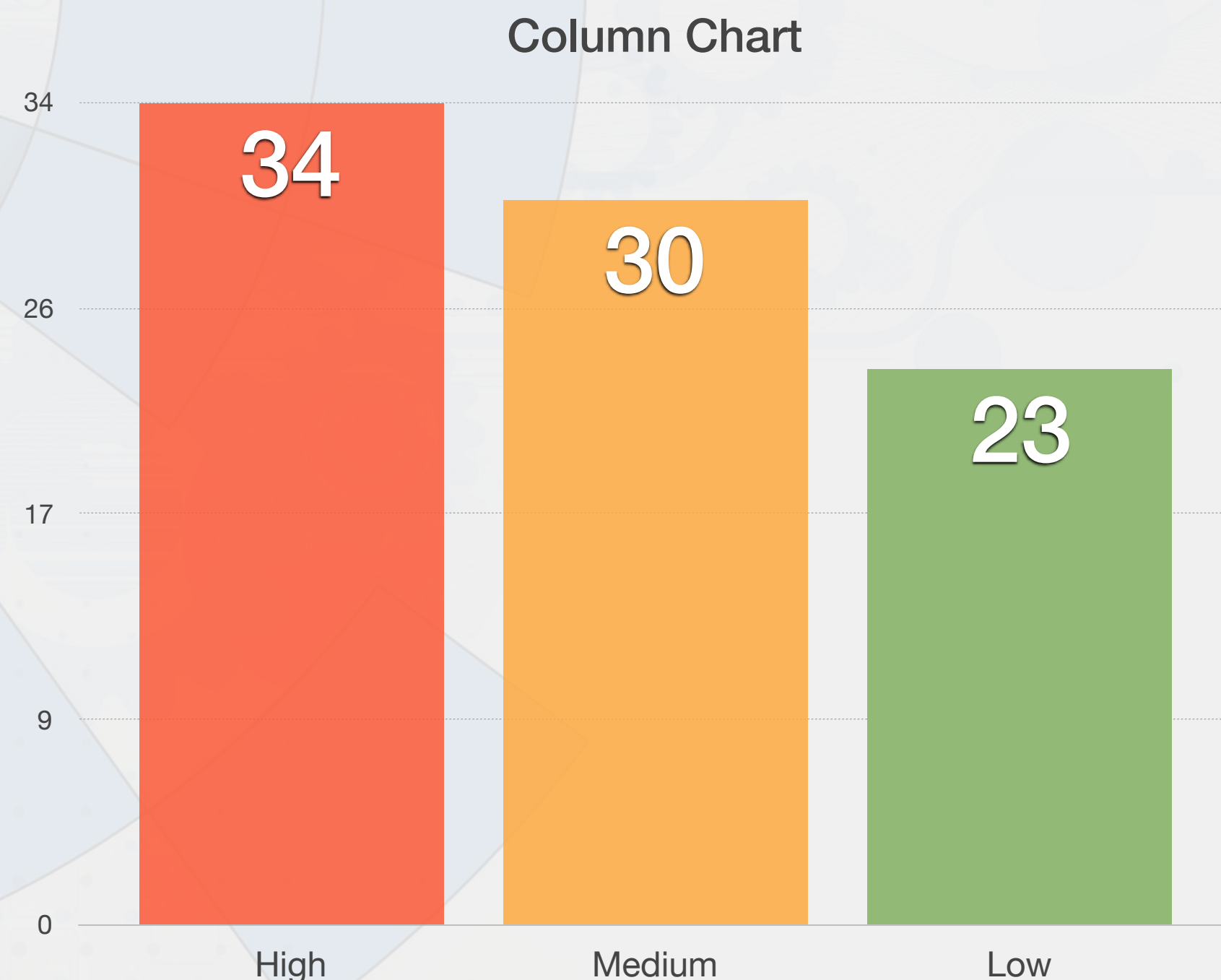




Rekapitulasi Risk Level Tahun 2017

1. 87 Sistem Informasi
2. 21 Instansi Pemerintah.
3. Hasil yang didapatkan dalam presentase yaitu **35% High Risk**, **34 % Medium Risk**, dan **26 % Low Risk**

Level	Jumlah Sistem Web
High	34
Medium	30
Low	23
Total	87

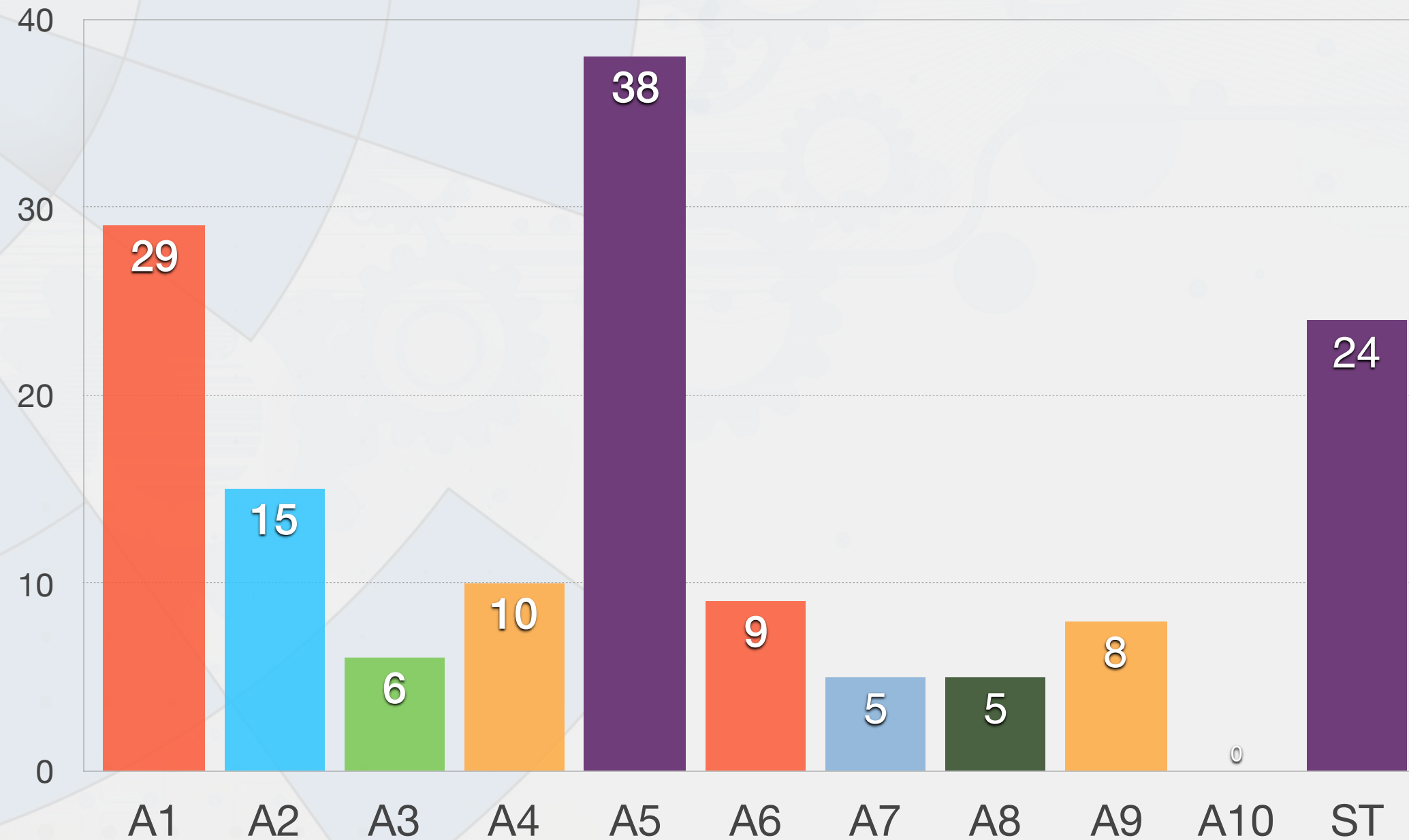




Rekapitulasi OWASP VULNERABILITIES Tahun 2017

- Hasil tertinggi dari celah kerawanan yang ditemukan dalam bentuk presentase yaitu **26 % Kesalahan Konfigurasi Keamanan, dan 19 % Kerawanan SQL Injection.**

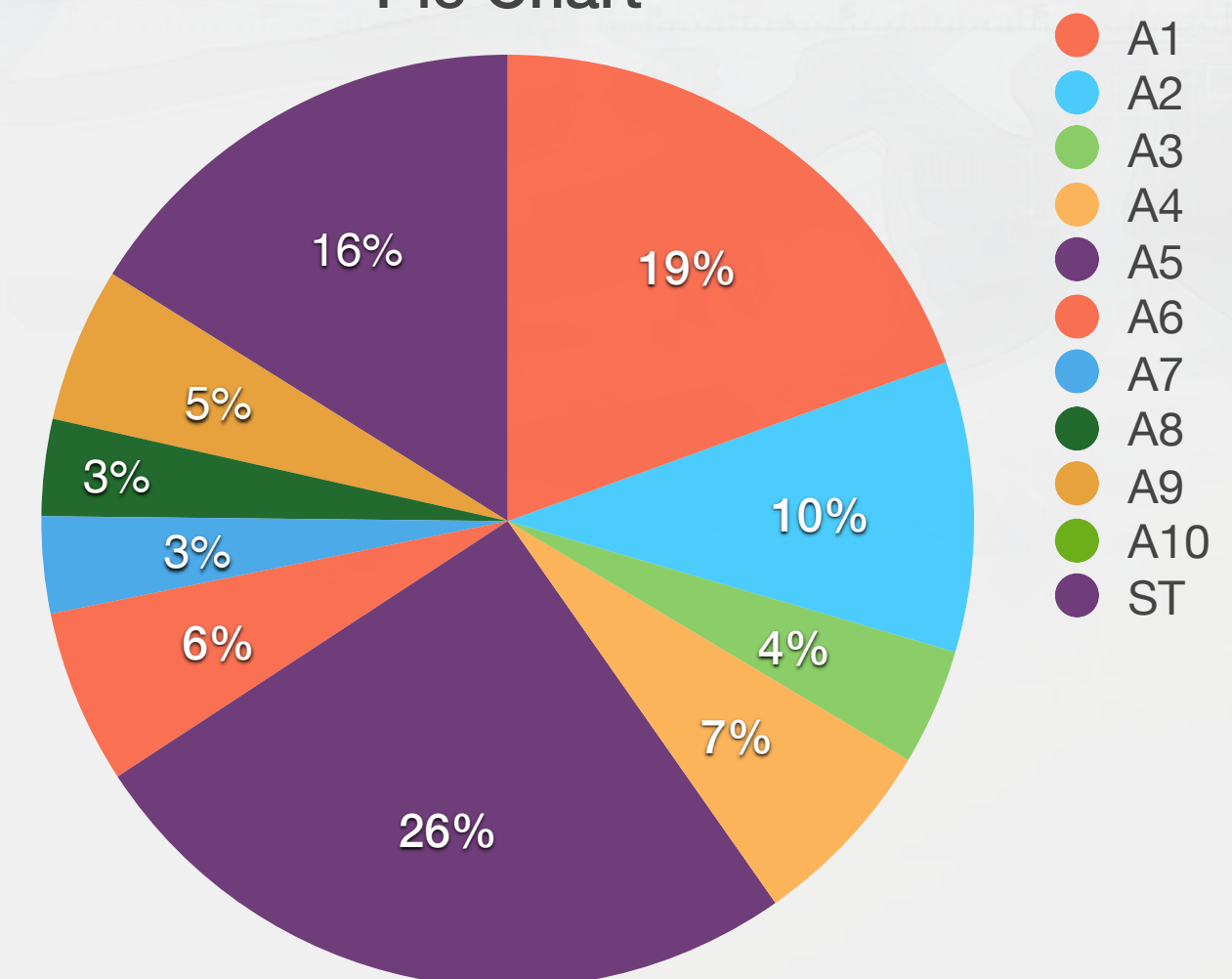
Column Chart



OWASP VULNERABILITES

VULNERABILITY POINTS		JUMLAH
A1	Injection	29
A2	Broken Authentication and Session Management	15
A3	Cross Site Request Forgery (XSS)	6
A4	Insecure Direct Object References	10
A5	Security Misconfiguration	38
A6	Sensitive Data Exposure	9
A7	Missing Function Level Access Control	5
A8	Cross Site Request Forgery (CSRF)	5
A9	Using Component With Known Vulnerabilities	8
A10	Unvaildated Redirects and Forwards	0
ST	Denial of Service (DOS)	24

Pie Chart



- Nothing is a 100% secure
- Never trust user input
- Defense in depth is the only defense
- Simple is easier to secure
- Peer review is critical to security