



# KEAMANAN APLIKASI WEB

## TES KEBUGARAN SISWA INDONESIA

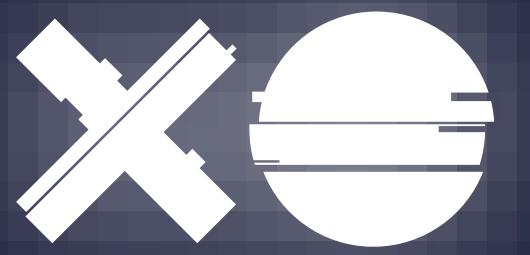
### 2021

P4TK-KEMENDIKBUD

POLTEK SSN-BSSN

START NOW





# ***Donny Seftyanto, S.Tr.TP., M.T.***

Dosen Program Studi Rekayasa Keamanan Siber  
Kepala Unit Pengasuhan, Mental, dan Kedisiplinan  
Politeknik Siber dan Sandi Negara  
Badan Siber dan Sandi Negara

Mail to : [Donny.seftyanto@bssn.go.id](mailto:Donny.seftyanto@bssn.go.id) / [Donny.seftyanto@poltekssn.ac.id](mailto:Donny.seftyanto@poltekssn.ac.id)  
CV : <https://poltekssn.ac.id/rks/donny-seftyanto/>



## Peningkatan

### Penggunaan Mobile, Internet, dan sosial media di Indonesia

Selama Pandemi Covid-19  
Jan 2020 sd Jan 2021





# INFORMASI SERANGAN SIBER

TARGET SERANGAN - [2020-09-17 S/D 2021-09-17]

DUNIA INDONESIA

17 SEPTEMBER 2021

7:49

## PERINGKAT SERANGAN

INDIA	61,129,373
IRELAND	40,491,400
INDONESIA	40,409,907
VIETNAM	27,145,612
RUSSIA	17,871,093



## LIVE FEED

TIME COUNTRY PORT



0 70,866,651

FROM: 2020-09-17

TO: 2021-09-17

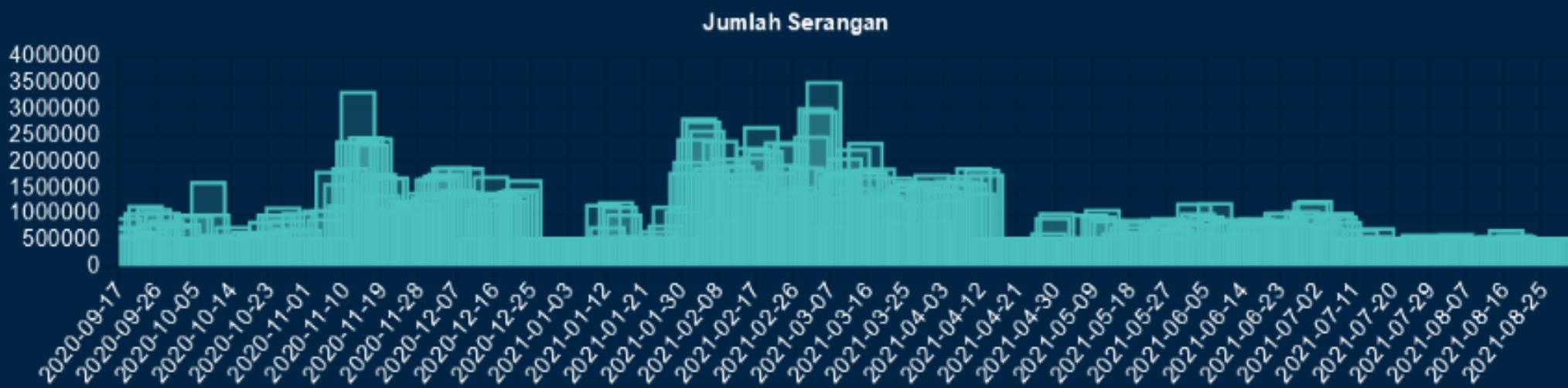
1 MONTH

3 MONTH

6 MONTH

1 YEAR

YTD

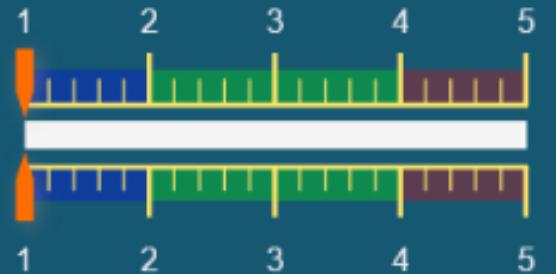


VIRTUAL ASSISTANT

## TREN MALWARE

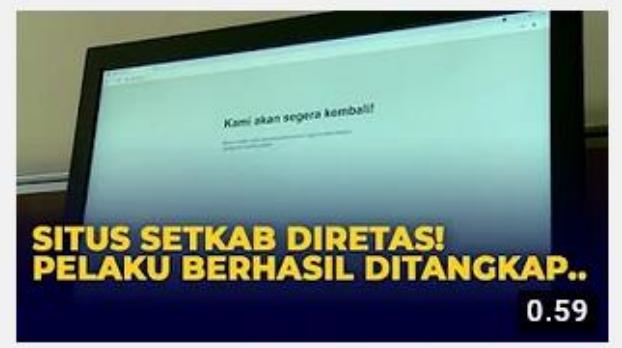
...7D9 (TROJANDOWNLOADER:WIN32/SMALL)	LOW	JUMLAH SERANGAN: 168,858
...CD8 (TROJANDOWNLOADER:WIN32/ZOMBIEBOY.ABIT)	LOW	JUMLAH SERANGAN: 61,626
...D9E (TROJANDOWNLOADER:WIN32/SMALL)	HIGH	JUMLAH SERANGAN: 19,793
...F5E (RANSOM:WIN32/CVE-2017-0147.A)	LOW	JUMLAH SERANGAN: 5,931
...4C1 (TROJANDOWNLOADER:WIN32/SMALL)	LOW	JUMLAH SERANGAN: 5,422

## Risk Low



Indonesia  
Honeynet  
Project

# SERANGAN SIBER SELAMA 1 TAHUN



# CYBER SECURITY



SUDAH SAATNYA KEAMANAN MENJADI PRIORITAS



# **BAGAIMANA SISTEM ELEKTRONIK SEHARUSNYA?**



Penyelenggara Sistem Elektronik harus  
memenuhi PERSYARATAN KEAMANAN sesuai

UU ITE

Undang Undang No. 11 Tahun 2008 tentang  
Informasi dan Transaksi Elektronik  
sebagaimana telah diubah dengan UU No.19  
tahun 2016. (cth: Pasal 16)

Peraturan Pemerintah No. 71 Tahun 2019  
tentang Penyelenggaraan Sistem dan  
Transaksi Elektronik. (cth: Pasal 26)

Peraturan Presiden No. 95 Tahun 2018 Tentang  
Sistem Pemerintah Berbasis Elektronik. (cth:  
Pasal 40)

# **BAGAIMANA SISTEM ELEKTRONIK SEHARUSNYA?**

✗ ✗ ✗



Aspek Ekstra:

## **NIR PENYANGKALAN**

Proteksi Informasi terhadap penyangkalan dari salah satu pihak yang membuat informasi atau terlibat dalam komunikasi. Seperti dengan Tanda Tangan Digital

## **DAPAT DITELUSURINYA INFORMASI**

Seperti dengan adanya log/ pencatatan aktifitas.

PERSYARATAN MINIMUM sesuai UU ITE, melindungi aspek:

## **KETERSEDIAAN**

Kepastian data dan layanan selalu tersedia. Seperti dengan pencadangan dan pemulihan.

## **KEUTUHAN**

Kepastian data persis sama dengan data yang dibuat atau dikirimkan pihak yang sah. Seperti dengan pendekripsi modifikasi via fungsi hash.

## **KEAUTENTIKAN**

Kepastian data yang ada berasal dari pihak yang sah. Seperti dengan mekanisme verifikasi dan validasi.

## **KERAHASIAAN**

Perlindungan data agar tidak diketahui oleh pihak yang tidak berhak. Seperti dengan enkripsi.

## **KETERAKSESAN**

Pencegahan pihak yang tidak berhak untuk menggunakan data atau layanan melalui kontrol akses.



# SANKSI

Sesuai PP PSTE

Peraturan Pemerintah No. 71 Tahun 2019 tentang  
Penyelenggaraan Sistem dan Transaksi Elektronik

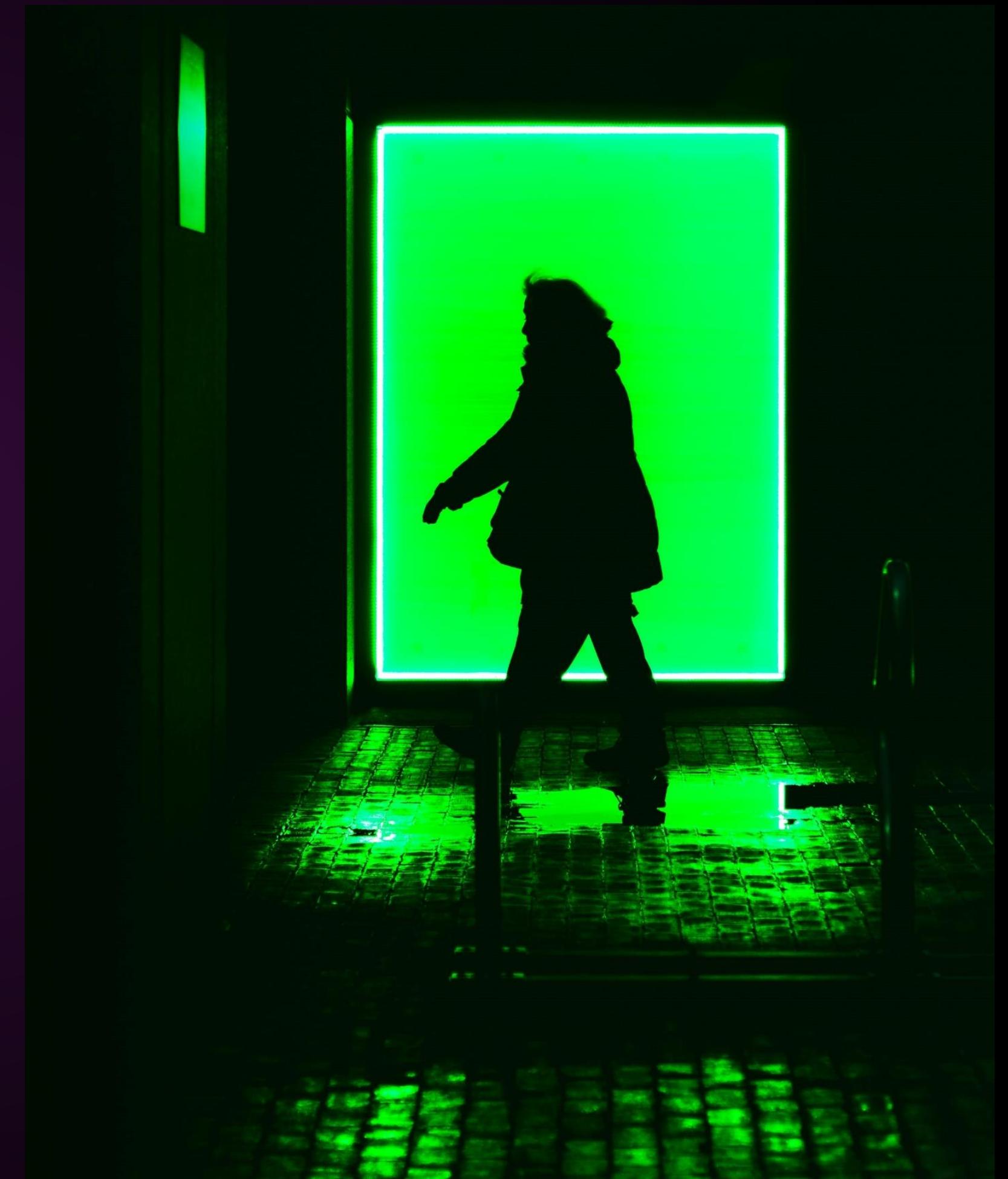
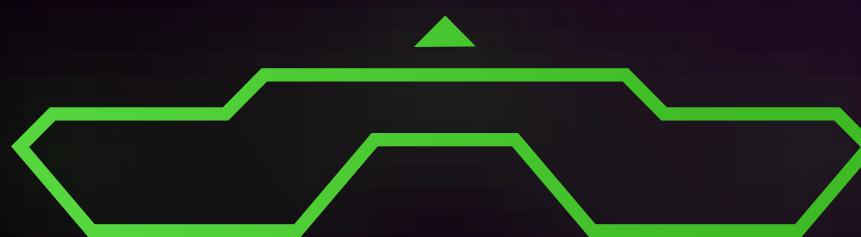
Teguran

Denda Administratif

Penghentian sementara

Pemutusan Akses

Dikeluarkan dari daftar





• • • •

# BAGAIMANA STANDAR KEAMANAN APLIKASI WEB TES KEBUGARAN SISWA INDONESIA

Sebagaimana Amanah Perpres 95 2018 tentang SPBE.  
Tertuang Standar Keamanan Aplikasi Web Pada  
Peraturan BSSN No 4 Tahun 2021  
(Pedoman Manajemen Kemanan Informasi SPBE dan  
Standar Teknis dan Prosedur Keamanan SPBE)



## STANDAR TEKNIS KEAMANAN APLIKASI WEB

Aplikasi perlu memenuhi standar teknis dan prosedur kemanan aplikasi

Terdiri Atas Terpenuhinya Kontrol:

- A. Autentikasi;
- B. Manajemen Sesi
- C. Persyaratan Kontrol Akses
- D. Validasi Input
- E. Kriptografi
- F. Penanganan Eror dan Pencatatan Log
- G. Proteksi Data
- H. Keamanan Komunikasi
- I. Pengendalian Kode Berbahaya
- J. Logika Bisnis
- K. File
- L. Keamanan API dan Web Service
- M. Keamanan Konfigurasi



DASAR : **BAB KETIGA – KEAMANAN APLIKASI SPBE**  
**PERATURAN BSSN NO 4 TAHUN 2021**



# RISIKO KEAMANAN TERTINGGI

## KEAMANAN APLIKASI WEB – VERSI OWASP 2017

Kontrol pada standar digunakan paling sedikit untuk menangani risiko pada aplikasi berbasis web tertinggi.

RISK	Threat Agents	Attack Vectors		Security Weakness		Impacts		Score
		Exploitability	Prevalence	Detectability	Technical	Business		
A1:2017-Injection	App Specific	EASY: 3	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	8.0	
A2:2017-Authentication	App Specific	EASY: 3	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	7.0	
A3:2017-Sens. Data Exposure	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	SEVERE: 3	App Specific	7.0	
A4:2017-XML External Entities (XXE)	App Specific	AVERAGE: 2	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	7.0	
A5:2017-Broken Access Control	App Specific	AVERAGE: 2	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	6.0	
A6:2017-Security Misconfiguration	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0	
A7:2017-Cross-Site Scripting (XSS)	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0	
A8:2017-Insecure Deserialization	App Specific	DIFFICULT: 1	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	5.0	
A9:2017-Vulnerable Components	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	MODERATE: 2	App Specific	4.7	
A10:2017-Insufficient Logging&Monitoring	App Specific	AVERAGE: 2	WIDESPREAD: 3	DIFFICULT: 1	MODERATE: 2	App Specific	4.0	

# A. AUTENTIKASI

Pemenuhan kontrol/fungsi ini dilakukan dengan prosedur:

1. menggunakan manajemen kata sandi untuk proses autentikasi;
2. menerapkan verifikasi kata sandi pada sisi server;
3. mengatur jumlah karakter, kombinasi jenis karakter, dan masa berlaku dari kata sandi;
4. mengatur jumlah maksimum kesalahan dalam pemasukan kata sandi;
5. mengatur mekanisme pemulihan kata sandi;
6. menjaga kerahasiaan kata sandi yang disimpan melalui mekanisme kriptografi; dan
7. menggunakan jalur komunikasi yang diamankan untuk proses autentikasi.

**PROSEDUR**

KEAMANAN SPBE





## B. MANAJEMEN SESI

Pemenuhan kontrol/fungsi ini dilakukan dengan prosedur:

1. menggunakan pengendali sesi untuk proses manajemen sesi;
2. menggunakan pengendali sesi yang disediakan oleh kerangka kerja aplikasi;
3. mengatur pembuatan dan keacakan token sesi yang dihasilkan oleh pengendali sesi;
4. mengatur kondisi dan jangka waktu habis sesi;
5. validasi dan pencantuman session id;
6. pelindungan terhadap lokasi dan pengiriman token untuk sesi terautentikasi; dan
7. pelindungan terhadap duplikasi dan mekanisme persetujuan pengguna.

**PROSEDUR**

KEAMANAN APLIKASI

# C. PERSYARATAN KONTROL AKSES

Pemenuhan kontrol/fungsi ini dilakukan dengan prosedur:

1. menetapkan otorisasi pengguna untuk membatasi kontrol akses;
2. mengatur peringatan terhadap bahaya serangan otomatis apabila terjadi akses yang bersamaan atau akses yang terus-menerus pada fungsi;
3. mengatur antarmuka pada sisi administrator; dan
4. mengatur verifikasi kebenaran token ketika mengakses data dan informasi yang dikecualikan.



**PROSEDUR**

KEAMANAN APLIKASI



# D. VALIDASI INPUT

Pemenuhan kontrol/fungsi ini dilakukan dengan prosedur:

1. menerapkan fungsi validasi input pada sisi server;
2. menerapkan mekanisme penolakan input jika terjadi kesalahan validasi;
3. memastikan runtime environment aplikasi tidak rentan terhadap serangan validasi input;
4. melakukan validasi positif pada seluruh input;
5. melakukan filter terhadap data yang tidak dipercaya;
6. menggunakan fitur kode dinamis;
7. melakukan pelindungan terhadap akses yang mengandung konten skrip; dan
8. melakukan pelindungan dari serangan injeksi basis data.

**PROSEDUR**

KEAMANAN APLIKASI

# E. KRIPTOGRAFI

Pemenuhan kontrol/fungsi ini dilakukan dengan prosedur:

1. menggunakan algoritma kriptografi, modul kriptografi, protokol kriptografi, dan kunci kriptografi sesuai dengan ketentuan peraturan perundang-undangan;
2. melakukan autentikasi data yang dienkripsi;
3. menerapkan manajemen kunci kriptografi; dan
4. membuat angka acak yang menggunakan generator angka acak kriptografi.



**PROSEDUR**

KEAMANAN APLIKASI



## F. PENANGANAN EROR DAN PENCATATAN LOG

Pemenuhan kontrol/fungsi ini dilakukan dengan prosedur:

1. mengatur konten pesan yang ditampilkan ketika terjadi kesalahan;
2. menggunakan metode penanganan eror untuk mencegah kesalahan terprediksi dan tidak terduga serta menangani seluruh pengecualian yang tidak ditangani;
3. tidak mencantumkan informasi yang dikecualikan dalam pencatatan log;
4. mengatur cakupan log yang dicatat untuk mendukung upaya penyelidikan ketika terjadi insiden;
5. mengatur pelindungan log aplikasi dari akses dan modifikasi yang tidak sah;
6. melakukan enkripsi pada data yang disimpan untuk mencegah injeksi log; dan
7. melakukan sinkronisasi sumber waktu sesuai dengan zona waktu dan waktu yang benar.

**PROSEDUR**

KEAMANAN APLIKASI

# G. PROTEKSI DATA

Pemenuhan kontrol/fungsi ini dilakukan dengan prosedur:

1. melakukan identifikasi dan penyimpanan salinan informasi yang dikecualikan;
2. melakukan pelindungan dari akses yang tidak sah terhadap informasi yang dikecualikan yang disimpan sementara dalam aplikasi;
3. melakukan pertukaran, penghapusan, dan audit informasi yang dikecualikan;
4. melakukan penentuan jumlah parameter;
5. memastikan data disimpan dengan aman;
6. menentukan metode untuk menghapus dan mengekspor data sesuai permintaan pengguna; dan
7. membersihkan memori setelah tidak diperlukan.



**PROSEDUR**

**KEAMANAN APLIKASI**

## H. KEAMANAN KOMUNIKASI

Pemenuhan kontrol/fungsi ini dilakukan dengan prosedur:

1. menggunakan komunikasi terenkripsi;
2. mengatur koneksi masuk dan keluar yang aman dan terenkripsi dari sisi pengguna;
3. mengatur jenis algoritma yang digunakan dan alat pengujiannya; dan
4. mengatur aktivasi dan konfigurasi sertifikat elektronik yang diterbitkan oleh penyelenggara sertifikasi elektronik.



**PROSEDUR**

KEAMANAN APLIKASI

# I. KODE BERBAHAYA

Pemenuhan kontrol/fungsi ini dilakukan dengan prosedur:

1. menggunakan analisis kode dalam kontrol kode berbahaya;
2. memastikan kode sumber aplikasi dan pustaka tidak mengandung kode berbahaya dan fungsionalitas lain yang tidak diinginkan;
3. mengatur izin terkait fitur atau sensor terkait privasi;
4. mengatur pelindungan integritas; dan
5. mengatur mekanisme fitur pembaruan



**PROSEDUR**

KEAMANAN APLIKASI

# J. LOGIKA BISNIS

Pemenuhan kontrol/fungsi ini dilakukan dengan prosedur:

1. memproses alur logika bisnis dalam urutan langkah dan waktu yang realistik;
2. memastikan logika bisnis memiliki batasan dan validasi;
3. memonitor aktivitas yang tidak biasa;
4. membantu dalam kontrol antiotomatisasi; dan
5. memberikan peringatan ketika terjadi serangan otomatis atau aktivitas yang tidak biasa.



**PROSEDUR**

KEAMANAN APLIKASI

# K. FILE

Pemenuhan kontrol/fungsi ini dilakukan dengan prosedur:

1. mengatur jumlah file untuk setiap pengguna dan kuota ukuran file yang diunggah;
2. melakukan validasi file sesuai dengan tipe konten yang diharapkan;
3. melakukan pelindungan terhadap metadata input dan metadata file;
4. melakukan pemindaian file yang diperoleh dari sumber yang tidak dipercaya; dan
5. melakukan konfigurasi server untuk mengunduh file sesuai ekstensi yang ditentukan.

**PROSEDUR**

KEAMANAN APLIKASI



# L. API & WEB SERVICE

Pemenuhan kontrol/fungsi ini dilakukan dengan prosedur:

1. melakukan konfigurasi layanan web;
2. memverifikasi uniform resource identifier API tidak menampilkan informasi yang berpotensi sebagai celah keamanan;
3. membuat keputusan otorisasi;
4. menampilkan metode RESTful hypertext transfer protocol apabila input pengguna dinyatakan valid;
5. menggunakan validasi skema dan verifikasi sebelum menerima input;
6. menggunakan metode pelindungan layanan berbasis web; dan
7. menerapkan kontrol antiotomatisasi.

**PROSEDUR**

KEAMANAN APLIKASI



# M. KEAMANAN KONFIGURASI

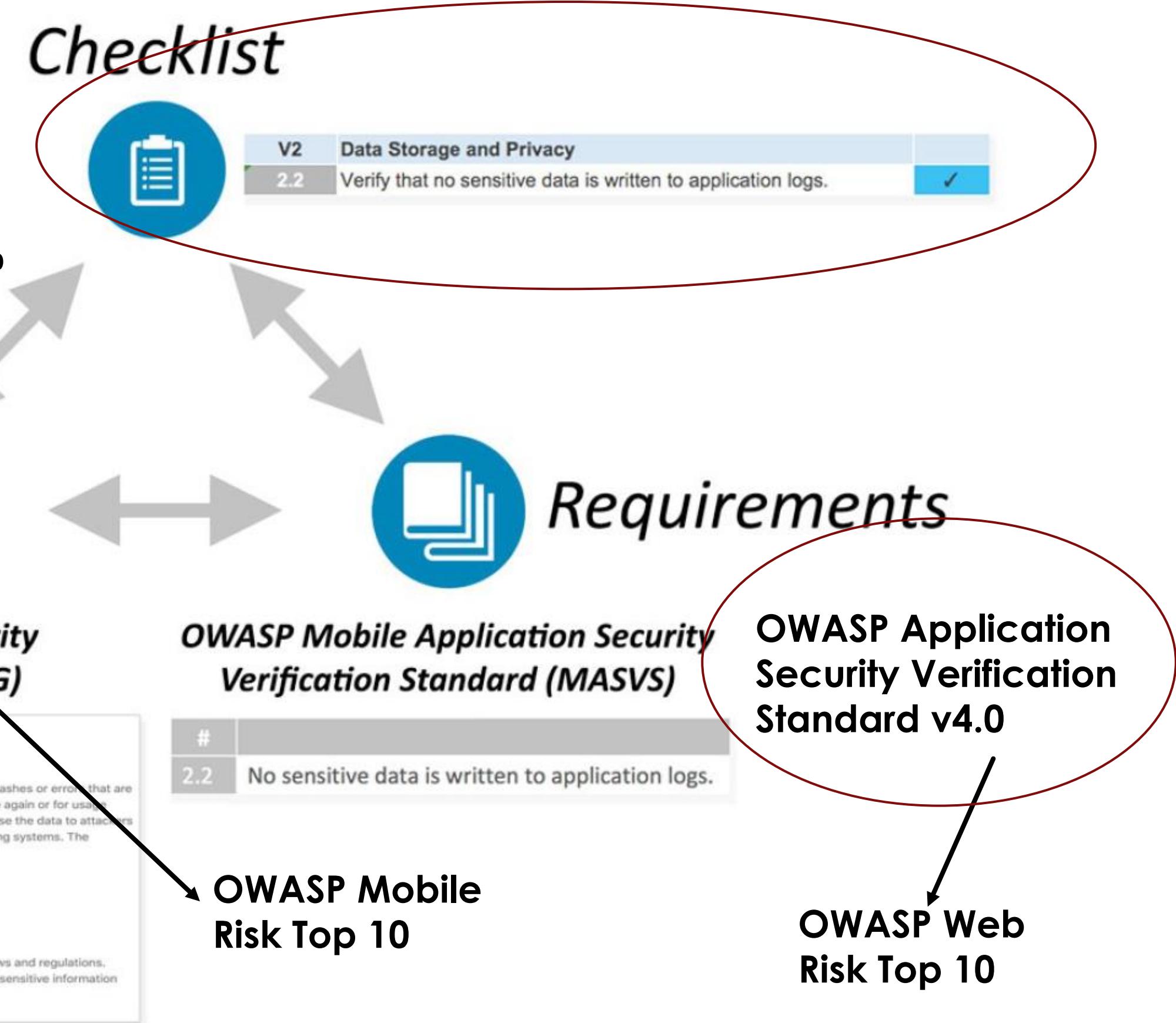
Pemenuhan kontrol/fungsi ini dilakukan dengan prosedur:

1. mengonfigurasi server sesuai rekomendasi server aplikasi dan kerangka kerja aplikasi yang digunakan;
2. mendokumentasi, menyalin konfigurasi, dan semua dependensi;
3. menghapus fitur, dokumentasi, sampel, dan konfigurasi yang tidak diperlukan;
4. memvalidasi integritas asset jika asset aplikasi diakses secara eksternal; dan
5. menggunakan respons aplikasi dan konten yang aman.

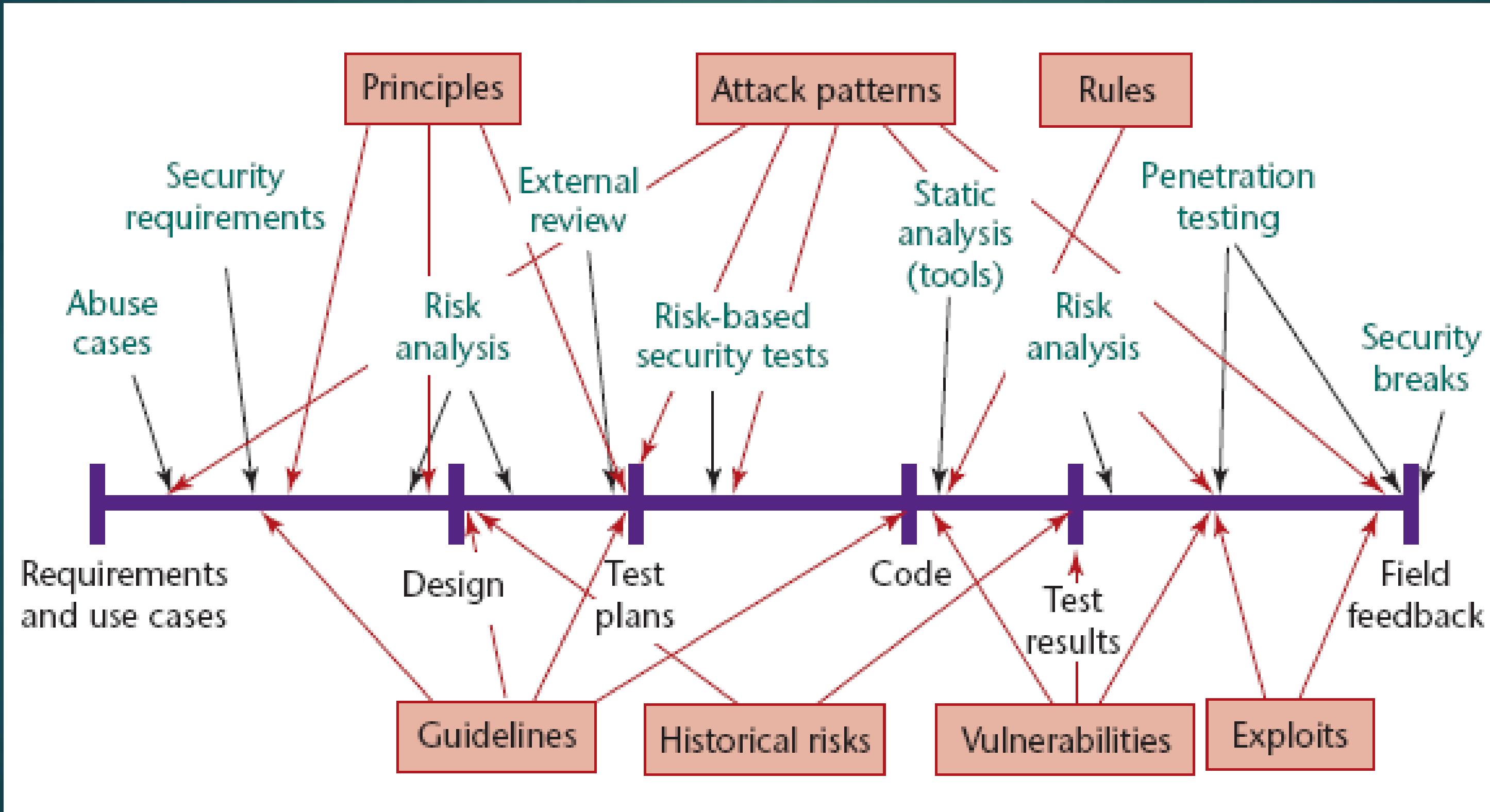


KEAMANAN APLIKASI

**Standar Teknis dan Prosedur Keamanan Aplikasi Pada Peraturan BSSN No 4 Tahun 2021 Mengacu Pada Best Practice OWASP**  
Terdapat level standar verifikasi keamanan aplikasi



# Perlu membangun aplikasi dengan menerapkan Siklus Hidup Pengembangan Software yang aman Secure Software Development Life Cycle (SSDLC)



# JENIS PENGUJIAN KEAMANAN APLIKASI

## Vulnerability Assessment

kegiatan uji yang memiliki karakteristik yang berkaitan erat dengan penggunaan suatu automation vulnerability scanner. kegiatan uji ini tidak dapat menjadi tolak ukur utama karena dianggap kurang dapat mengidentifikasi suatu risiko secara maksimal.

## Penetration Test

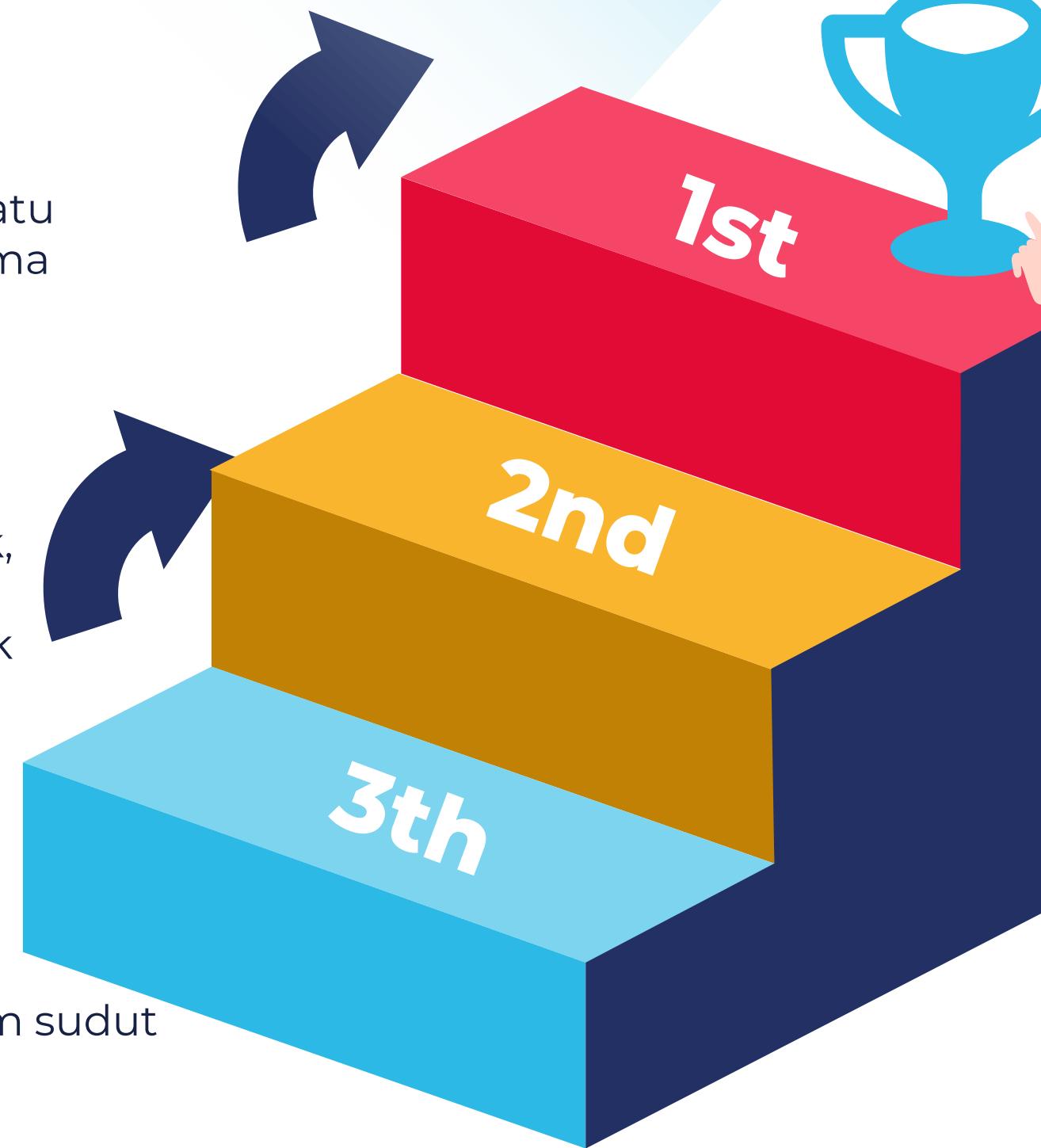
kegiatan penetration test lebih cenderung untuk memiliki suatu tujuan yang spesifik, misalnya seperti dapat tidaknya suatu target diambil alih. Kegiatan uji ini akan mencoba mensimulasikan berbagai jenis serangan yang umumnya digunakan untuk masuk ke dalam suatu sistem.

kegiatan uji ini juga dianggap tidak dapat menjadi acuan utama bila suatu instansi/organisasi hendak melihat risiko yang ada pada dirinya lebih dalam.

## Security Assessment

penguji akan mencoba untuk memaksimalkan suatu pengujian dari berbagai macam sudut pandang untuk dapat mengidentifikasi potensi risiko yang dapat muncul.

Sangat **direkomendasikan untuk melakukan Security Assessment** pada tahap pengujian aplikasi untuk memastikan standar keamanan terpenuhi dan mencegah risiko yang dapat terjadi.



# SUDUT PANDANG PENGUJIAN KEAMANAN APLIKASI

Setidaknya sudut pandang pengujian keamanan aplikasi adalah Grey Box Testing, sehingga penguji dapat menguji semua modul yang ada pada aplikasi

- **Black Box:** Memiliki makna bahwa suatu pengujian dilakukan dalam situasi seorang penguji yang **tidak memiliki akun** untuk masuk ke dalam aplikasi ataupun **tidak memiliki akses** ke dalam suatu jaringan atau asset yang diuji selain yang dimiliki oleh seorang pengunjung (seperti aplikasi) ataupun tamu secara umum.
- **Grey Box:** Memiliki makna bahwa suatu pengujian dilakukan dengan situasi seorang penguji **telah memiliki sedikit akses** yang tidak diperoleh para pengunjung secara umum. Sebagai contoh yaitu ketika seorang pengunjung telah memiliki akses sebagai pengguna (customer / nasabah).
- **White Box:** Memiliki makna bahwa suatu pengujian dilakukan dengan akses tertinggi di masing-masing wilayah. Sebagai contoh yaitu seperti menguji dari sudut pandang server administrator (dengan hak akses administrator), sudut pandang application administrator (dengan hak akses seperti super administrator), dan sudut pandang database administrator (dengan hak akses masuk ke dalam database). Inti sederhananya adalah, memastikan bahwa setiap layer tidak dapat masuk ke layer lain tanpa adanya keperluan yang dituangkan dengan benar sesuai ketentuan.



# PERLU PERLINDUNGAN PADA LAPISAN LAINNYA

PERLU BERKOLABORASI DENGAN UNIT LAINNYA UNTUK MENJAMIN KEAMANAN SISTEM ELEKTRONIK  
PADA LAPISAN SELAIN APLIKASI

## OSI model

Layer	Name	Example protocols
7	Application Layer	HTTP, FTP, DNS, SNMP, Telnet
6	Presentation Layer	SSL, TLS
5	Session Layer	NetBIOS, PPTP
4	Transport Layer	TCP, UDP
3	Network Layer	IP, ARP, ICMP, IPSec
2	Data Link Layer	PPP, ATM, Ethernet
1	Physical Layer	Ethernet, USB, Bluetooth, IEEE802.11



# KOLABORASI KEAMANAN SIBER

PERLU DIBENTUK GOV-CSIRT (TIM RESPON INSIDEN KEAMANAN SIBER PEMERINTAH) BERSAMA BSSN

DAPAT MEMINTA LAYANAN PROAKTIF (LAYANAN SECURITY ASSESSMENT, SECURITY AUDIT, SECURITY DRILL TEST, PEMBENTUKAN CSIRT) DAN

PENANGANAN INSIDEN SIBER (ADUAN SIBER TRIASE INSIDEN, KOORDINASI INSIDEN, DAN RESOLUSI INSIDEN)

# ALUR ADUAN INSIDEN SIBER

Segera laporkan !!!

apabila anda menemukan insiden siber

Terjadi insiden siber

Aduan segera kami tangani

Kumpulkan bukti **insiden** berupa foto / screenshot **insiden** / log file yang ditemukan

Hubungi (021) 78833610  
Laporkan & Kirimkan bukti ke bantuan70@bssn.go.id atau pusopskamsinas@bssn.go.id

PUSAT KONTAK SIBER

Pusat Operasi Keamanan Siber Nasional BSSN

# **PERBUATAN TERLARANG**

Berdasarkan UU ITE

- MENGAKSES sistem dengan sengaja dan tanpa hak  
Sanksi 6 tahun penjara & atau denda Rp600 juta
- MENYADAP data dengan sengaja dan tanpa hak  
Sanksi 10 tahun penjara & atau denda Rp800 juta
- MEMODIFIKASI data dengan sengaja dan tanpa hak  
Sanksi 8 tahun penjara & atau denda Rp2 miliar
- MENGGANGGU sistem dengan sengaja dan tanpa hak  
Sanksi 10 tahun penjara & atau denda Rp 10 miliar
- MEMALSUKAN data dengan sengaja dan tanpa hak  
Sanksi 12 tahun penjara & atau denda Rp12 miliar



A photograph of a person with dark hair and glasses, wearing a blue shirt, looking down at an open book. The background is blurred.

# REFERENSI

<https://honeynet.bssn.go.id/>, diakses pada 17 September 2021

<https://datareportal.com/reports/digital-2021-indonesia>, diakses pada 18 September 2021

UU ITE (Informasi dan Transaksi Elektronik)

PP PSTE (Penyelenggaraan Sistem dan Transaksi Elektronik)

ITU Recommendation X.800

PERATURAN BSSN NO 4 TAHUN 2021

OWASP TOP 10





THANKS  
FOR ATTENTION

