INNOVATIVE: Journal Of Social Science Research
Volume 4 Nomor 2 Tahun 2024 Page 7891-7906
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Pengembangan Aplikasi Aman Di Cloud Untuk Lean Startup

Purnaresa Yuliartanto[1✉], Benfano Soewito[2]
Computer Science Department BINUS Graduate Program – Master of Computer Science
Bina Nusantara University, Jakarta, Indonesia, 11380
Email: purnaresa.yuliartanto@binus.ac.id[1✉]

Abstrak

Intisari—Dua pertiga usaha kecil dan menengah atau startup mengalami serangan siber pada tahun 2018. Dari seluruh serangan tersebut, insiden siber pada aplikasi termasuk dalam tiga peristiwa paling merugikan. Hal ini menimbulkan pertanyaan tentang bagaimana startup mengembangkan aplikasinya. Saat mengembangkan suatu produk, startup selalu fokus pada peluncuran produk, dan mereka menggunakan komputasi awan untuk itu. Meskipun penyedia cloud bertanggung jawab atas infrastruktur keamanan cloud, aplikasi yang diterapkan oleh startup di cloud adalah tanggung jawab mereka untuk mengamankannya. Startup perlu mengamankan pengembangan aplikasi mereka. Namun, kerangka keamanan yang ada seperti NIST mencakup topik luas yang lebih cocok untuk perusahaan dibandingkan startup dengan tim dan portofolio produk yang lebih kecil. Dalam karya ini, kami menyajikan kerangka NIST SSDF yang dimodifikasi untuk startup untuk mengimplementasikan pengembangan aplikasi yang aman di cloud. Metodologi kami adalah menganalisis aspek keamanan apa yang penting bagi startup. Hilangkan praktik keamanan non prioritas dari kerangka awal. Kemudian memanfaatkan sebanyak mungkin kemampuan cloud publik untuk mengurangi risiko yang perlu dikelola oleh sebuah startup. Jadi startup bisa mendapatkan pengembangan aplikasi yang aman dengan upaya sesedikit mungkin agar mereka bisa fokus pada peluncuran produk.

Kata kunci: *keamanan aplikasi, pengembangan aman, keamanan cloud*

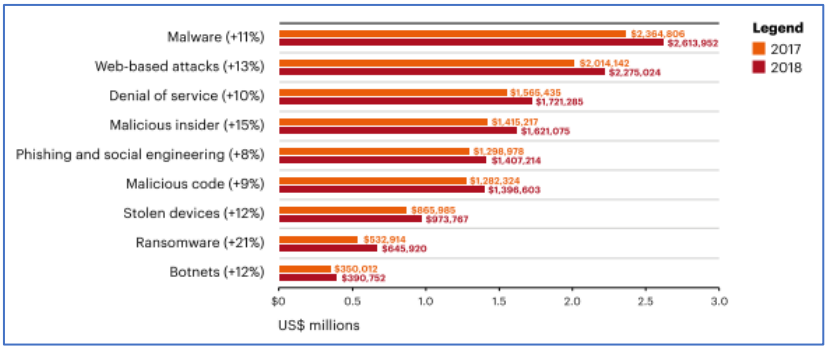
Abstract

Two-thirds of small and medium businesses or startups experienced cyberattacks in 2018. Of all those attacks,cyber incidents on the application are among the top three most damaging events. It raisesquestionsabout how startup develop their application. When developing a product, startups always focus on product release, and they use cloud computing for that. Whilethe cloud provider is responsible for the security infrastructure of the cloud, the applicationthata startup deploys in the cloud is its responsibility to secure. Startups need to secure their application development. However, the existingsecurity framework like NISTcovers broad topic which fit more toenterprise than a startup with a smaller team and product portfolio.In thiswork, we present a modified NIST SSDF framework for a startup to implement secure application development in the cloud. Our methodology is to analyze what's security aspect vital to the startups. Eliminate non priority security practice from the original framework. Then leveraging as much public cloud capability to reduce the risk that a startup needs to manage. So startups can gain secure application development with as little effort as possible to allow them to focus on product release.

Keywords: *application security, secure development, cloud security*

PENDAHULUAN

Pada tahun 2018, serangan siber berdampak pada 67% usaha kecil dan menengah (UKM) [1]. Perusahaan konsultan global, Accenture, menerbitkan laporan bahwa jumlah serangan siber terus meningkat, mencapai peningkatan 50% pada tahun 2021 [2]. Jika melihat lebih dekat jenis serangan keamanan, tiga serangan teratas berkaitan dengan aplikasi. Tiga serangan teratas adalah malware, serangan berbasis web, dan penolakan layanan. Contoh terbaru dari serangan berbasis web adalah kerentanan Log4j yang menyebabkan gangguan bisnis di seluruh dunia [3]. Gambar 1.1 menunjukkan biaya serangan siber berdasarkan jenis serangannya. Saat ini, mengembangkan aplikasi dengan kerentanan minimum adalah investasi yang berharga.



Gambar 1. Kerugian akibat kejahatan dunia maya menurut jenis serangannya

Banyaknya kejadian insiden tersebut terjadi karena 60% UKM atau startup tidak memiliki rencana peningkatan keamanan siber[1]. Menurut definisinya, startup adalah organisasi non-IPO baru dengan jumlah karyawan kurang dari 500 orang [4], [5]. Sebagian

besar startup mengadopsi prinsip lean startup [6]. Inti dari lean startup adalah fokus pada pengembangan produk kecil dan secara aktif mengumpulkan masukan untuk perbaikan. Berdasarkan pendekatan tersebut, startup sering kali tidak memprioritaskan aspek pengembangan produk lainnya, seperti pencegahan terhadap serangan siber.

Untuk mempercepat pengembangan produk dan mengurangi biaya di muka, startup menggunakan layanan komputasi awan. Penyedia Layanan Cloud (CSP) seperti Amazon Web Service (AWS), Google Cloud, dan Microsoft Azure menawarkan berbagai layanan untuk mendukung bisnis startup [7]. Namun, meskipun komputasi awan dapat membantu startup mengembangkan bisnisnya, hal ini tidak secara otomatis mengamankan beban kerja mereka. CSP mempromosikan Model Tanggung Jawab Bersama untuk menjelaskan konsep tanggung jawab keamanan saat menggunakan CSP [8]. Ini adalah model untuk menentukan area mana yang akan diamankan oleh penyedia cloud, yang dikenal sebagai Keamanan "dari" cloud. CSP akan mengamankan lokasi pusat data, keamanan perangkat keras, dan jaringan yang mendasarinya. Keamanan "di" cloud adalah area yang harus dikelola oleh pengguna cloud. Area tersebut meliputi aplikasi, data, dan identitas. Artinya, startup bertanggung jawab untuk melindungi aplikasi mereka sendiri.

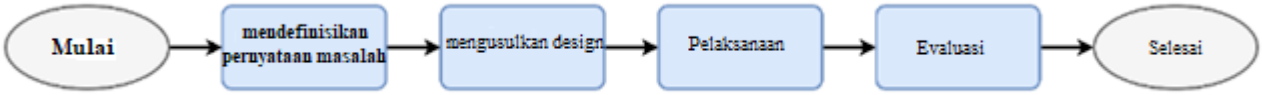
Ada beberapa kerangka keamanan yang dapat digunakan organisasi di cloud untuk membangun praktik pengembangan aplikasi yang kuat dan aman dan melindungi dari ancaman dunia maya. Beberapa opsinya antara lain: NIST Cybersecurity Framework, ISO 27001, CIS Control dan OWASP [9], [10]. Organisasi di cloud harus memilih kerangka keamanan yang sesuai dengan kebutuhan dan sumber daya spesifik mereka. Namun, kerangka kerja tersebut mencakup topik luas yang mungkin kurang dihargai oleh startup dibandingkan organisasi perusahaan. Misalnya, rencana pemulihan bencana dan manajemen perangkat pengguna akhir. Meskipun topiknya secara obyektif penting dari sudut pandang keamanan siber, sebuah startup mungkin tidak dapat menerapkan praktik tersebut karena keterbatasan anggaran dan staf organisasi. Untuk mengatasi masalah tersebut, peneliti dalam karya ini akan memodifikasi framework yang ada agar lebih efisien bagi startup yang menjalankan pengembangan aplikasi di cloud.

Metodologi pekerjaan ini menghilangkan praktik keamanan dari kerangka kerja asli, yang tidak penting untuk startup. Tahap pertama adalah menganalisis aspek keamanan apa saja yang penting bagi startup melalui riset literatur yang didukung dengan wawancara. Berdasarkan analisis, framework disaring dan diurutkan untuk hanya menerapkan kontrol yang prioritas startupnya. Pekerjaan ini akan mengusulkan rencana implementasi membangun lingkungan pengembangan aplikasi yang aman di cloud. Untuk mengevaluasi kerangka kerja, pekerjaan ini juga akan mengembangkan aplikasi pengujian pada

lingkungan pengembangan. Tahap terakhir adalah menjalankan simulasi serangan siber terhadap aplikasi pengujian untuk melihat efektivitas lingkungan pengembangan yang aman.

METODE PENELITIAN

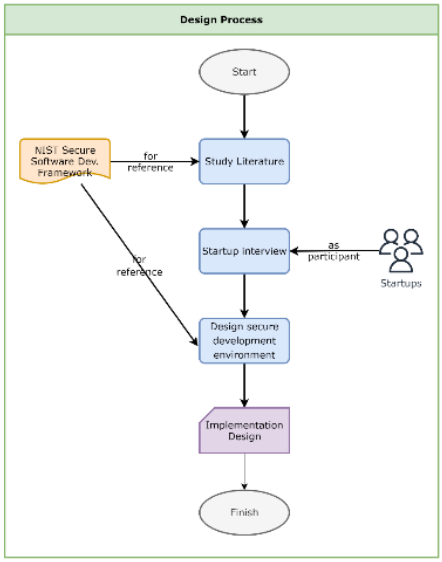
Rumusan masalah dari penelitian ini adalah bagaimana startup dapat mengembangkan aplikasi yang aman di cloud dan menguji efektivitasnya. Kerangka kerja keamanan industri yang ada seperti NIST dan OWASP sudah tersedia, namun mungkin terlalu rumit untuk startup. Oleh karena itu, penelitian ini akan mewawancarai para startup untuk memahami prioritas mereka dalam mengembangkan aplikasinya. Desain kerangka kerja akan menggabungkan referensi dari kerangka keamanan industri dan data dari wawancara. Proses implementasi akan menggunakan desain untuk mengembangkan aplikasi di cloud. Gambar 1 mengilustrasikan proses penelitian—metodologi yang didasarkan pada pengembangan siklus hidup proyek.



Gambar 2. Metodologi

Penelitian perlu mengevaluasi efektivitas kerangka kerja tersebut. Oleh karena itu, penelitian ini akan mengembangkan sistem multi-tier untuk mensimulasikan sistem pada organisasi startup. Setelah selesai pengembangan sistem, langkah terakhir adalah menjalankan proses pengujian keamanan web. Proses pengujiannya menggunakan framework OWASP Top Ten sebagai baseline.

A. Usulan Desain



Gambar 3. Proses desain

Gambar 3 mengilustrasikan proses perancangan. Penelitian ini akan mengimplementasikan kerangka aplikasi yang aman untuk startup. Oleh karena itu perancangannya akan dimulai dengan memahami apa itu pengembangan aplikasi yang aman. Penelitian ini akan menggunakan NIST Secure Software Development Framework (SSDF) untuk memahami praktik yang diperlukan dalam pengembangan aplikasi yang aman. Setelah itu, tindakan berikut memvalidasi startup jika ada praktik keamanan yang dijelaskan dalam kerangka kerja tidak sesuai dengan organisasi. Tabel1 menunjukkan semua praktik yang dijelaskan dalam NIST SSDF.

Kode	Praktik
PO	Mempersiapkan Organisasi
PO.1	Menentukan Persyaratan Keamanan untuk Pengembangan Perangkat Lunak
PO.2	Melaksanakan Peran dan Tanggung Jawab
PO.3	Menerapkan Rantai Alat Pendukung
PO.4	Menentukan dan Menggunakan Kriteria untuk Pemeriksaan Keamanan Perangkat Lunak
PO.5	Menerapkan dan Memelihara Lingkungan Aman untuk Pengembangan Perangkat Lunak
PS	Lindungi Perangkat Lunak
PS.1	Lindungi Segala Bentuk Kode dari Akses Tidak Sah dan Gangguan
PS.2	Menyediakan Mekanisme untuk Memverifikasi Integritas Rilis Perangkat Lunak
PS.3	Arsipkan dan Lindungi Setiap Rilis Perangkat Lunak
PW	Menghasilkan Perangkat Lunak yang Aman (PW)
PW.1	Merancang Perangkat Lunak untuk Memenuhi Persyaratan Keamanan dan Mengurangi Risiko Keamanan
PW.2	Meninjau Desain Perangkat Lunak untuk Memverifikasi Kepatuhan terhadap Persyaratan Keamanan dan Informasi Risiko
PW.4	Menggunakan Kembali Perangkat Lunak yang Ada dan Diamankan dengan Baik Jika

	Memungkinkan Daripada Menduplikasi Fungsionalitas
PW.5	Membuat Kode Sumber dengan Mengikuti Praktik Pengkodean yang Aman
PW.6	Konfigurasikan Proses Kompilasi, Interpreter, dan Build untuk Meningkatkan Keamanan yang Dapat Dieksekusi
PW.7	Meninjau dan/atau Menganalisis Kode yang Dapat Dibaca Manusia untuk Mengidentifikasi Kerentanan dan Memverifikasi Kepatuhan terhadap Persyaratan Keamanan
PW.8	Uji Kode yang Dapat Dieksekusi untuk Mengidentifikasi Kerentanan dan Memverifikasi Kepatuhan terhadap Persyaratan Keamanan
PW.9	Konfigurasikan Perangkat Lunak agar Memiliki Pengaturan Aman secara Default
RV	Menanggapi Kerentanan
RV.1	Identifikasi dan Konfirmasi Kerentanan Secara Berkelanjutan
RV.2	Menilai, Memprioritaskan, dan Memperbaiki Kerentanan
RV.3	Menganalisis Kerentanan untuk Mengidentifikasi Akar Penyebabnya

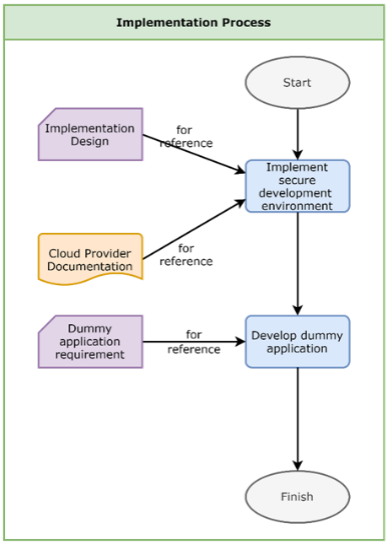
Penelitian ini menggunakan proses wawancara untuk memvalidasi praktik mana yang sesuai dengan startup. Prosesnya dimulai dengan mengundang manajemen startup untuk wawancara. Namun definisi startup harus jelas untuk memastikan keakuratan poin data. Ada banyak definisi startup dari berbagai sumber seperti universitas [27], perusahaan analis [28], dan pemerintah [29]. Tabel 2 merangkum identitas umum sebuah startup.

Tabel 3 Kriteria startup

Kriteria	Parameter
Umur perusahaan	< 10 tahun
Tipe perusahaan	Perseroan terbatas swasta

Pendapatan berulang tahunan	< $50 juta
Ukuran perusahaan	< 500 karyawan

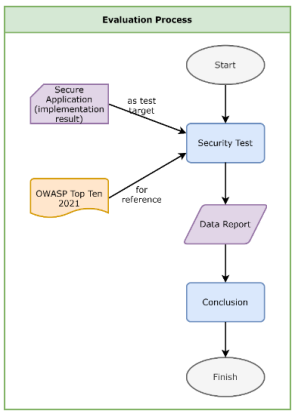
Peneliti akan mengirimkan undangan wawancara ke perusahaan yang sesuai dengan kriteria startup. Selain undangan langsung, peneliti akan mengumumkan media sosial seperti LinkedIn untuk mengumpulkan peserta wawancara. Tujuannya adalah untuk memiliki setidaknya sepuluh peserta wawancara. Angka tersebut mewakili praktik pengembangan aplikasi startup karena karakteristik budaya organisasinya harus serupa. Rencana Implementasi



Gambar 4. Proses pelaksanaan

Gambar 4 mengilustrasikan rencana implementasi setelah desain dari tahap sebelumnya tersedia. Implementasinya akan berjalan di cloud dan menggunakan dokumentasi penyedia cloud sebagai referensi. Tujuannya adalah untuk memiliki kerangka pengembangan aplikasi yang aman dan mengevaluasi efektivitasnya. Oleh karena itu implementasinya harus menerapkan semua praktik dari desain yang diusulkan dengan benar. Selaras dengan kerangka dasar, NIST SSDF, pelaksanaan praktiknya dibagi menjadi empat kategori. Penelitian ini akan mengimplementasikan semua praktik di cloud. Cloud yang dipilih untuk implementasi adalah AWS karena AWS mewakili pangsa pasar cloud terbesar di industri. Hasil wawancara awal akan mempengaruhi desain sebenarnya pada saat implementasi.

B. Evaluasi



Gambar 5. Proses evaluasi

Setelah lingkungan pengembangan yang aman dan pengembangan aplikasi dummy selesai, tahap terakhir adalah tahap evaluasi. Gambar 5 mengilustrasikan metode evaluasi penelitian ini. Tahap evaluasi akan menggunakan dokumen OWASP Top Ten 2021 sebagai referensi. Dokumen tersebut berisi daftar risiko paling kritis terhadap aplikasi web. Tabel 4 menunjukkan daftar risiko dan contoh skenario serangan.

Tabel 4 OWASP 10 teratas 2021

Resiko	Contoh skenario serangan
A01 Kontrol Akses Rusak	Aplikasi ini menggunakan data yang belum diverifikasi dalam panggilan SQL untuk mengakses informasi akun.
	Penyerang hanya memaksa penjelajahan ke URL target tanpa autentikasi yang tepat.
A02 Kegagalan Kriptografi	Situs tidak menggunakan atau menerapkan TLS untuk semua halaman atau mendukung enkripsi yang lemah.
	Basis data kata sandi menggunakan hash sederhana atau sederhana untuk menyimpan kata sandi semua orang.
A03 Injeksi	Aplikasi menggunakan data yang tidak tepercaya untuk membuat panggilan SQL rentan berikut.
	Kepercayaan buta suatu aplikasi terhadap kerangka kerja dapat menghasilkan pertanyaan yang masih rentan.
A04 Desain Tidak Aman	Situs web e-niaga jaringan ritel tidak memiliki perlindungan terhadap bot.
	Alur kerja pemulihan kredensial mungkin mencakup "pertanyaan dan jawaban",

A05 Kesalahan Konfigurasi Keamanan	Konfigurasi server aplikasi memungkinkan pesan kesalahan terperinci, misalnya jejak tumpukan, dikembalikan ke pengguna.
	Penyedia layanan cloud (CSP) memiliki izin berbagi default yang terbuka ke Internet oleh pengguna CSP lainnya.
A06 Komponen Rentan dan Kedaluwarsa	Eksploitasi melalui ketergantungan aplikasi yang rentan
	Komponen biasanya dijalankan dengan hak istimewa yang sama dengan aplikasi itu sendiri, sehingga kelemahan pada komponen mana pun dapat menimbulkan dampak yang parah.
A07 Kegagalan Identifikasi dan Otentikasi	Pengisian kredensial, menggunakan daftar kata sandi yang diketahui, adalah serangan standar.
	Batas waktu sesi aplikasi tidak diatur dengan benar.
A08 Kegagalan Integritas Perangkat Lunak dan Data	Aplikasi, firmware perangkat, dan lainnya tidak memverifikasi pembaruan melalui firmware yang ditandatangani.
	Penyerang memperhatikan tanda tangan objek Java "rO0" (di base64) dan menggunakan alat Java Serial Killer untuk mendapatkan eksekusi kode jarak jauh.
A09 Kegagalan Pencatatan dan Pemantauan Keamanan	Pelanggaran log aplikasi yang berisi data penumpang, termasuk data paspor dan kartu kredit.
	Tinjauan pasca-insiden terhadap situs web rumah sakit menemukan bahwa pengembang belum mengatasi kerentanan yang signifikan. Tidak ada sistem pencatatan atau pemantauan.
A10 Pemalsuan Permintaan Sisi Server (SSRF)	Pemindaian port pada server internal
	Akses penyimpanan metadata layanan cloud untuk mendapatkan informasi sensitif

Skenario pengujian keamanan akan dilakukan terhadap aplikasi dummy menggunakan contoh skenario serangan dari OWASP Top Ten. Pengukuran pertama dari penelitian ini adalah menghitung seberapa efektif praktik tersebut dalam memitigasi risiko. Variabel yang terlibat dalam pengukuran adalah countCategoryPass untuk menggambarkan jumlah kategori yang lulus uji keamanan dan totalCategory untuk jumlah kategori risiko OWASP Top Ten. Rumus untuk mengukur keamanan aplikasi terhadap serangan aplikasi web adalah

$$\text{Kemanan aplikasi} = \frac{\text{Kategori lulus uji}}{\text{Kategori total}} X100\%$$

HASIL DAN PEMBAHASAN

A. Kerangka yang Dimodifikasi

Berdasarkan wawancara dengan lima perusahaan yang memenuhi kriteria startup, kami memahami aspek keamanan apa yang relevan dengan startup. Startup yang diwawancarai berasal dari berbagai industri seperti FSI, layanan kesehatan, dan pasar. Tabel 5 menyajikan data hasil wawancara.

Tabel 5 Hasil wawancara

Practice Code	Relevancy	Priority	Total Score
PO			
PO.1	2	1	3
PO.2	3	1	4
PO.3	4	4	8
PO.4	1	1	2
PO.5	3	3	6
PS			
PS.1	4	4	8
PS.2	1	1	2
PS.3	2	2	4
PW			
PW.1	3	2	5
PW.2	2	2	4
PW.4	4	4	8
PW.5	4	4	8
PW.6	4	3	7
PW.7	4	4	8
PW.8	4	3	7
PW.9	4	3	7
RV			
RV.1	4	2	6
RV.2	3	1	4
RV.3	3	1	4

Dari 19 praktik yang dihadirkan NIST SSDF, 10 praktik relevan dan diprioritaskan oleh startup – ditandai dengan warna hijau. Startup dapat menjalankan inisiatif untuk 10 praktik tersebut untuk mendapatkan keamanan yang lebih baik dalam pengembangan aplikasi mereka dengan alokasi biaya dan anggaran yang efektif. Berikut ini adalah inisiatif-inisiatif yang sejalan dengan praktik-praktik yang disoroti.

Tabel 6 Implementasi Praktek

Kode	Inisiatif	Referensi praktis
I.1	Sentralisasi repositori kode	PO.3, PS.1
I.2	Standarisasi kode pengaturan	PO.3, PW.5
I.3	Atur Pemindaian Ketergantungan	PO.3, PW.5, PW.6
I.4	Pengaturan SAST	PO.3, PW.5, PW.6, PW.7
I.5	Terapkan alat CI/CD	PO.3, PW.6
I.6	Siapkan DAST	PO.3, PW.8
I.7	Atur jadwal pembaruan rantai alat	PO.3. RV.1
I.8	Pisahkan lingkungan pengembangan	PO.5
I.9	Buat RBAC untuk semua alat pengembangan	PO.5, PS.1
I.10	Melakukan Pemodelan Ancaman	PW.1
I.11	Impor perpustakaan umum internal	PW.4
I.12	Lakukan tinjauan kode rekan	PW.4, PW.7
I.13	Siapkan penyimpanan kredensial	PW2. PW.9
I.14	Publikasikan program pengungkapan kerentanan	RV.1

B. Lingkungan Lab

Penelitian ini membangun lingkungan laboratorium untuk mengimplementasikan semua inisiatif. Tidak semua inisiatif merupakan implementasi teknologi, melainkan merupakan proses atau kebijakan internal. Kami tidak dapat meniru inisiatif tersebut. Dan untuk inisiatif yang dapat diterapkan, penelitian ini akan memanfaatkan sebanyak mungkin layanan cloud native. Pemikiran tersebut menyimulasikan lingkungan startup di mana mereka harus tetap fokus pada peluncuran produk daripada memelihara rantai alat. Tabel 5 menunjukkan inisiatif mana yang dapat diterapkan di lingkungan laboratorium.

Tabel 7 Inisiatif di laboratorium

Initiative	Cloud Native			Alternatif Open Source	Berbasis proses
	AWS	Azure	GCP		
I.1	•	•	•	gitlab	
I.2	-	-	-	golanglint	
I.3	•	-	-	gosecure	
I.4	•	-	-	gosecure	
I.5	•	•	•	jenkins	
I.6	-	-	-	sqlmap	
I.7	•	•	•		
I.8	•	•	•		
I.9	•	•	•		
I.10	-	-	-		•
I.11	-	-	-		•
I.12	-	-	-		•
I.13	•	•	•	vault	
I.14	-	-	-		•

C. Evaluasi

Setelah lingkungan lab siap, penelitian ini mengevaluasi lingkungan pengembangan terhadap OWASP Top 10. Analisis lab menunjukkan bahwa 13 dari 14 inisiatif berkontribusi terhadap pencegahan OWASP Top 10. Saat menjalankan simulasi uji keamanan, 50% kategori serangan berhasil dicegah. Sisanya tidak berlaku untuk simulasi karena ini merupakan celah keamanan dalam proses dan bukan penerapan teknologi. Tabel 7 menyajikan data evaluasi.

Tabel 8 Data Evaluasi

OWASP Top 10	Inisiatif Pencegahan	Hasil Pengujian
A01	I.1, I.2, I.10	n/a
A02	I.1, I.2, I.4, I.5, I.7, I.13	lulus
A03	I.1, I.2, I.4, I.5, I.6, I.7	lulus
A04	I.1, I.2, I.9, I.10, I.11, I.12, I.13	n/a
A05	I.8, I.9, I.11, I.13	n/a
A06	I.1, I.2, I.3, I.5, I.7	lulus
A07	I.1, I.2, I.10, I.12	n/a
A08	I.1, I.2, I.3, I.5, I.7	lulus
A09	I.1, I.2, I.9, I.10, I.12	n/a
A10	I.1, I.2, I.4, I.5, I.7	lulus

Kategori A02, A03, A06, A08, dan A10 merupakan kategori kerentanan yang dapat dicegah dengan alat. Hasil pengujian menunjukkan hasil yang konsisten bahwa lingkungan laboratorium mampu mencegah terjadinya kerentanan. A01, A04, A07 dan A09 merupakan kerentanan yang terjadi karena praktik yang tidak aman. Penelitian ini tidak mampu mensimulasikan kondisi tersebut. A05 adalah kerentanan akibat kesalahan konfigurasi keamanan, sementara beberapa inisiatif mencegah kategori jenis ini, proses pengembangan dan operasional infrastruktur merupakan kontributor utama kerentanan ini. Oleh karena itu, penelitian ini tidak dapat menguji kategori kerentanan spesifik tersebut.

SIMPULAN

Penelitian ini menunjukkan bahwa startup dapat menggunakan kerangka keamanan yang dimodifikasi untuk membangun lingkungan aplikasi pengembangan yang aman. Lima puluh dua persen praktik NIST SSDF relevan untuk diterapkan oleh startup. Kerangka kerja yang dimodifikasi dapat mencegah kerentanan berdasarkan OWASP Top 10. Setengah dari kategori kerentanan dicegah secara efektif dan otomatis melalui penerapan teknologi. Sementara separuh lainnya bergantung pada bagaimana organisasi startup dapat menerapkan praktik tersebut dalam proses pengembangannya.

A. Karya Masa Depan

Penelitian selanjutnya dapat mengevaluasi kerangka yang dimodifikasi dari perspektif biaya. Oleh karena itu kita dapat melihat efektivitas kerangka kerja dan pengembalian investasi. Startup adalah tim kecil dengan anggaran terbatas. Mengetahui biaya inisiatif dari kerangka kerja ini akan membantu startup memprioritaskan implementasinya.

B. PENGAKUAN

Publikasi penelitian ini didukung penuh oleh Binus University.

DAFTAR PUSTAKA

C. Lurey, "Cyber Mindset Exposed: Keeper Unveils its 2019 SMB Cyberthreat Study," Keeper Security, Inc., 2019. https://www.keepersecurity.com/blog/2019/07/24/cyber-mindset-exposed-keeper-unveils-its-2019-smb-cyberthreat-study/ (accessed Dec. 25, 2021).

M. Leatherbee and R. Katila, "The lean startup method: Early-stage teams and hypothesis-based probing of business ideas," Strateg. Entrep. J., vol. 14, no. 4, pp. 570–593, Dec. 2020, doi: 10.1002/sej.1373.

K. Bissell and L. Ponemon, "Ninth Annual Cost of Cybercrime Study Unlocking the Value of Improved Cybersecurity Protection the Cost of Cybercrime Contents," cost cybercrime. Ninth Annu. Cost Cybercrime Study Unlocking Value Improv. Cybersecurity Prot., p. 18, 2019.

Acunetix, "The True Nature of Web Application Security The Role and Function of Black Box Scanners," 2007.

David C, "Log4j critical vulnerability advice for boards - NCSC.GOV.UK," National Cyber Security Centre, Dec. 17, 2021. https://www.ncsc.gov.uk/blog-post/log4j-vulnerability-what-should-boards-be-asking (accessed Dec. 28, 2021).

T. Hunt, "';--Have I Been Pwned?," Have I Been Pwned, 2019. https://haveibeenpwned.com/About (accessed Dec. 28, 2021).

Amir Karimuddin, "Startup Report 2020," Daily Social Innovate, Mar. 2021. https://dailysocial.id/research/startup-report-2020 (accessed Dec. 28, 2021).

Elva Rini, "AWS Asia Pasifik Jakarta Pacu Pemerataan Teknologi Cloud Berbagai Sektor Usaha," Dec. 20, 2021. https://www.kompas.tv/article/243642/aws-asia-pasifik-jakarta-pacu-pemerataan-teknologi-cloud-berbagai-sektor-usaha?page=all (accessed Dec. 28, 2021).

A. Konrad, "The Cloud 100 2021," Forbes, 2021.

L. Ferri, R. Spanò, and A. Tomo, "Cloud computing in high tech startups: evidence from a case study," Technol. Anal. Strateg. Manag., vol. 32, no. 2, pp. 146–157, Feb. 2020, doi: 10.1080/09537325.2019.1641594.

Amazon.com inc, "Shared Responsibility Model - Amazon Web Services (AWS)," Amazon, 2018. https://aws.amazon.com/compliance/shared-responsibility-model/ (accessed Sep. 08, 2021).

N. T. Le and D. B. Hoang, "Capability maturity model and metrics framework for cyber cloud security," Scalable Comput., vol. 18, no. 4, pp. 277–290, 2017, doi: 10.12694/scpe.v18i4.1329.

R. Kerrigan, "Startup vs. Corporate: Which Is Right for You? | HBS Online," Harvard Business Online, 2018. https://online.hbs.edu/blog/post/startup-vs-corporate-culture (accessed Jan. 20, 2022).

D. Dodson, M. Souppaya, and K. Scarfone, "Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)," Nist. Gaithersburg, MD, pp. 1–24, Apr. 23, 2020, doi: 10.6028/NIST.CSWP.04232020.

Microsoft, "Microsoft Security Development Lifecycle (SDL)," pp. 1–132, 2010.

J. de V. Mohino, J. B. Higuera, J. R. B. Higuera, and J. A. S. Montalvo, "The application of a new secure software development life cycle (S-SDLC) with agile methodologies," Electron., vol. 8, no. 11, 2019, doi: 10.3390/electronics8111218.

M. Souppaya, K. Scarfone, and D. Dodson, "Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities," Feb. 2021, doi: 10.6028/NIST.SP.800-218.

Matthew Chiodi, "4 Practical Steps for 'Shift Left' Security," 2019. https://www.paloaltonetworks.com/blog/2019/07/4-practical-steps-shift-left-security/ (accessed Feb. 11, 2022).

J. Varia and S. Mathew, "Overview of Amazon Web Services (Survey Report)," 2014.

S. Shilpashree, R. R. Patil, and C. Parvathi, "'Cloud computing an overview,'" Int. J. Eng. Technol., vol. 7, no. 4, pp. 2743–2746, 2018, doi: 10.14419/ijet.v7i4.10904.

M. Saraswat and R. C. Tripathi, "Cloud Computing: Comparison and Analysis of Cloud Service Providers-AWs, Microsoft and Google," in Proceedings of the 2020 9th International Conference on System Modeling and Advancement in Research Trends, SMART 2020, 2020, pp. 281–285, doi: 10.1109/SMART50582.2020.9337100.

M. Kara, "Review on Common Criteria as a Secure Software Development Model," Int. J. Comput. Sci. Inf. Technol., vol. 4, no. 2, pp. 83–94, 2012, doi: 10.5121/ijcsit.2012.4207.

M. I. Tariq, S. Tayyaba, M. W. Ashraf, H. Rasheed, and F. Khan, "Analysis of NIST SP 800-53 Rev.3 Controls Effectiveness for Cloud Computing," 1st Natl. Conf. Emerg. Trends Innov. Comput. Technol., pp. 88–92, 2016.

R. Kalaiprasath, R. Elankavi, and R. Udayakumar, "Cloud security and compliance - A semantic approach in end to end security," Int. J. Smart Sens. Intell. Syst., vol. 2017, no. Specialissue, pp. 482–494, 2017, doi: 10.21307/ijssis-2017-265.

B. Knaffl, "Case Study: How CIS Controls Can Limit the Cascading Failures During an Attack GIAC (GSEC) Gold Certification," GIAC Gold Certif., 2016.

P. Kobezak, R. Marchany, D. Raymond, and J. Tront, "Host inventory controls and systems survey: Evaluating the CIS critical security control one in higher education networks," in Proceedings of the Annual Hawaii International Conference on System Sciences, 2018, vol. 2018-January, doi: 10.24251/hicss.2018.597.

University of Sydney, "What is a start-up actually - The University of Sydney," Jan. 16, 2020. https://www.sydney.edu.au/study/why-choose-sydney/student-life/student-news/2017/07/25/what-is-a-start-up-actually.html (accessed Feb. 08, 2022).

A. Wilhelm, "The Definition Of A Startup," Crunchbase News, Sep. 13, 2018. https://news.crunchbase.com/news/the-definition-of-a-startup/ (accessed Feb. 08, 2022).

Startup India Hub, "Startup India Scheme," Jun. 21, 2021. https://www.startupindia.gov.in/content/sih/en/startup-scheme.html (accessed Feb. 08, 2022).