# Evaluasi Keamanan Sistem E-Government menggunakan Security Development Lifecycle (SDL) Threat Modelling Tool

Said Akmala
17917129

*Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer*
*Konsentrasi Forensika Digital*
*Program Studi Informatika Program Magister*
*Fakultas Teknologi Industri*
*Universitas Islam Indonesia*
2021

# Lembar Pengesahan Pembimbing

**Evaluasi Keamanan Sistem E-Government menggunakan Security Development Lifecycle (SDL) Threat Modelling Tool**

Said Akmala
17917129

Yogyakarta, Juni, 2021

| Pembimbing I | Pembimbing II |
| --- | --- |
| Dr. Imam Riadi, S.Pd., M.Kom. | Dr. Yudi Prayudi, S.Si., M.Kom. |

# Lembar Pengesahan Penguji

**Evaluasi Keamanan Sistem E-Government menggunakan Security Development Lifecycle (SDL) Threat Modelling Tool**

Said Akmala

17917129

Yogyakarta, Juni, 2021

Tim Penguji,

Dr. Imam Riadi, S.Pd., M.Kom.

Ketua

Dr. Yudi Prayudi., S.Si., M.Kom.

Anggota I

Dr. Ir. Bambang Sugiantoro, S.Si., M.T.

Anggota II

Mengetahui,

Ketua Program Studi Informatika Program Magister

Universitas Islam Indonesia

Izzati Muhimmah, S.T., M.Sc., Ph.D.

# Abstrak

**Evaluasi Keamanan Sistem E-Government menggunakan Security Development Lifecycle (SDL) Threat Modelling Tool**

Sistem Sistem informasi berupa pelayanan publik saat ini mulai berkembang cukup pesat di Indonesia, kini banyak penyajian informasi disajikan secara digital atau yang dikenal dengan *electronic government* (*e-government*). Konsep *e-government* sendiri adalah penggunakan teknologi informasi sebagai salah satu alat pemerintah untuk meningkatkan pelayanan pemerintah kepada warga negara, lembaga swasta dan lembaga pemerintah lain yang saling berinteraksi. Namun dalam penggunaan sistem egovernment sendiri memungkinkan banyak terjadinya risiko ancaman oleh karena itu diperlukan evaluasi keamanan sistem. Penelitian ini membahas mengenai tahapan dalam melakukan evaluasi keamanan sistem menggunakan metode Security Development Lifecycle (SDL) yang memiliki 6 tahapan yaitu *Define, Diagram, Identify, Mitigate dan Validate*. Hasil uji menggunakan SDL dalam evaluasi sistem e-government menghasilkan suatu nilai tingkat risiko ancaman dengan menggunakan penilaian berbasis STRIDE dan DREAD dengan potensi ancaman yaitu : spoofing sebesar 4, tampering sebesar 11, elevation of privilege sebesar 8, Danial of Service sebesar 1 dan information disclosure sebesar 1. Hasil potensi ancaman tersebut kemudian dianalisis sehingga menghasilkan sebuah kesimpulan bahwa dalam sistem memerlukan langkah pencegahan dengan membuat TLS (Transport Layer Security) menggunakan mekanisme autentifikasi yang baik, melaukan enkripsi pada database, menggunakan Spam Filter dan update rutin sandi secara berkala. Kelebihan SDL yaitu bersifat pengulangan sehingga dalam pengujiannya memungkinkan untuk selalu mengevaluasi dan menguji ulang sistem untuk melakukan langkah prioritas dalam melakukan mitigasi terhadap potensi ancaman.

**Kata kunci**

**E-government, Modelling, Security Development Lifecycle (SDL), STRIDE, DREAD.**

# Abstract

**E-Government System Security Evaluation using the Security Development Lifecycle (SDL) Threat Modeling Tool**

Information systems in the form of public services are currently starting to develop quite rapidly in Indonesia, now many information presentations are presented digitally or known as electronic government (e-government). The concept of e-government itself is the use of information technology as a government tool to improve government services to citizens, private institutions and other government agencies that interact with each other. However, the use of the e-government sistem itself allows a lot of threat risks, therefore it is necessary to evaluate the security of the sistem. This study discusses the stages in evaluating sistem security using the Security Development Lifecycle (SDL) method which has 6 stages, namely Define, Diagram, Identify, Mitigate and Validate. The test results using SDL in evaluating the e-government sistem produce a threat risk level value using STRIDE and DREAD-based assessments with potential threats, namely: 4 threats of spoofing, 11 threats of tampering, 8 threats of elevation of privilege, 1 threat of Danial of Service and 1 threats of information disclosure. The results of the potential threats then analyzed to produce a conclusion that the sistem requires preventive measures by making TLS (Transport Layer Security), using a good authentication mechanism, encrypting the database, using Spam Filters and updating passwords regularly. The advantage of SDL is that it is iterative so that in its testing it is possible to always evaluate and retest the sistem to take priority steps in mitigating potential threats.

**Keywords**

E-government, Modelling, Security Development Lifecycle (SDL), STRIDE, DREAD.

# Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, Juni 2021


Said Akmala

# Daftar Publikasi

**Publikasi yang menjadi bagian dari tesis**

Publikasi berikut menjadi bagian dalam penulisan tesis ini

- Akmala, S., Riadi, I., & Prayudi, Y. (2021). Evaluasi Kemanan Sistem E-Government menggunakan Security Development Lifecycle (SDL) Threat Modelling Tool; http://jurnal.unmuhjember.ac.id/JUSTINDO.vol6(2)

| Kontributor | Jenis Kontribusi |
|---|---|
| Said Akmala | Mendesain eksperimen (70%)<br>Menulis *paper* (100%) |
| Imam Riadi | Memberi ide dan saran (30%)<br>Mereview artikel |
| Yudi Prayudi | Memberi ide dan saran (30%)<br>Mereview artikel |

# Halaman Kontribusi

Penelitian ini merupakan hasil dari saran dan bimbingan dari berbagai pihak baik saat sedang seminar proposal, seminar kemajuan, hingga seminar pendadaran. Pihak-pihak tersebut antara lain adalah Dr. Imam Riadi, S.Pd., M.Kom., Dr. Yudi Prayudi, S.Si., M.Kom., dan Dr. Ir. Bambang Sugiantoro, S.Si., M.T.

# Halaman Persembahan

Alhamdulillah, puji syukur penulis panjatkan kepada Allah SWT yang telah memberikan banyak sekali rahmat dalam kehidupan. Selanjutnya penelitian ini penulis persembahkan kepada orang-orang yang telah mendukung dan memberikan semangat serta motivasi kepada penulis untuk dapat menyelesaikan pendidikan Pascasarjana di Universitas Islam Indonesia, Yogyakarta. Persembahan secara khusus saya berikan kepada :

1. Kedua orang tua penulis yang tak kenal lelah memberikan motivasi, doa dan harapan untuk terus menjadi lebih baik dalam kehidupan.
2. Teman-teman Magister Teknik Informatika Konsentrasi Forensika Digital yang telah banyak memberikan bantuan dan kebersamaannya selama ini.
3. Teman-teman Pengurus Karang Taruna Dharma Surya Kelurahan Purwokerto Wetan, Pengelola Perpustakaan Segara Ilmu Kelurahan Purwokerto Wetan dan Remaja Masjid Baitul Hikmah Purwokerto Wetan yang telah memberikan motivasi selama ini.

# Kata Pengantar

Alhamdulillah puji syukur penulis panjatkan kepada Allah SWT yang telah memberikan banyak sekali rahmat dalam kehidupan penulis sehingga dapat menyelesaikan laporan tesis dengan judul "Evaluasi Keamanan Sistem E-Government menggunakan Security Development Lifecycle (SDL) Threat Modelling Tool". Penulis sampaikan ucapan terimakasih kepada pihak-pihak yang telah membantu dalam terselesainya penyusunan laporan tesis ini yaitu :

1. Bapak Fathul Wahid, S.T., M.Sc., Ph.D., selaku Rektor Universitas Islam Indonesia yang memberikan kesempatan kepada penulis untuk berkembang bersama di Universitas Islam Indonesia.
2. Bapak Prof. Hari Purnomo, M.T selaku Dekan Fakultas Teknologi Industri Universitas Islam Indonesia yang memberikan fasilitas dan bantuan untuk belajar.
3. Ibu Izzati Muhimmah, ST., M.Sc., Ph.D., selaku Ketua Program Studi Informatika Program Magister Fakultas Teknologi Industri Universitas Islam Indonesia, yang selalu memberikan semangat kepada setiap mahasiswa agar segera menyelesaikan tesis.
4. Bapak Dr. Imam Riadi, S.Pd., M.Kom. selaku dosen pembimbing I yang selalu memberikan masukan dan saran selama proses pembuatan tesis ini.
5. Bapak Dr. Yudi Prayudi, S.Si., M.Kom., selaku dosen pembimbing II yang selalu memberikan movitasi dan saran dalam penelitian tesis ini.
6. Bapak Dr. Ir. Bambang Sugiantoro, S.Si., M.T., selaku Dosen Penguji Ujian Tesis yang telah memberikan berbagai saran perbaikan untuk penelitian ini.
7. Seluruh dosen, staff administrasi dan civitas Magister Informatika Universitas Islam Indonesia, baik secara langsung maupun tidak langsung telah membantu penulis selama studi.
8. Semua pihak yang telah membantu dalam penyusunan tesis ini.

Dalam penulisan tesis ini penulis menyadari bahwa penelitian ini masih perlu banyak masukan dan saran yang membangun dari pembaca untuk pengembangannya. Akhir kata penulis sampaikan terimakasih, semoga laporan tesis ini dapat bermanfaat bagi pembaca.

Yogyakarta, Juli 2021

Penulis

# Daftar Isi

# Daftar Tabel

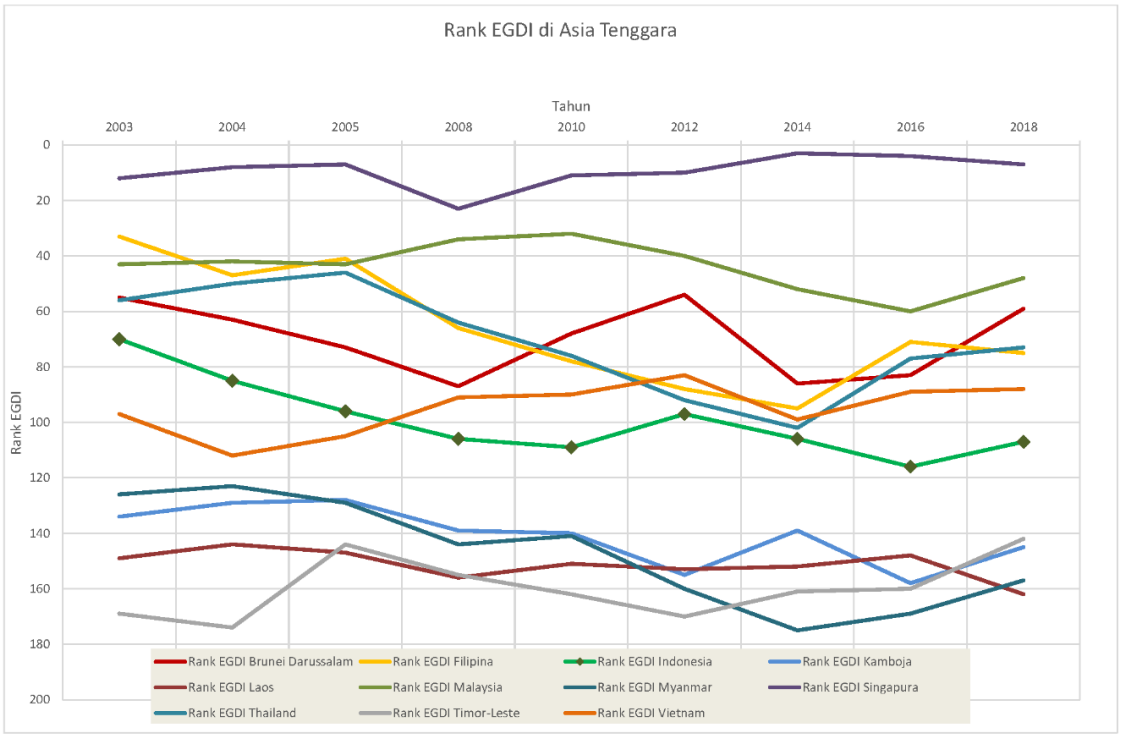
# Daftar Gambar

# BAB I

# Pendahuluan

## 1.1 Latar Belakang

Sistem penyajian informasi berupa pelayanan publik saat ini mulai berkembang cukup pesat baik pada sector pemerintah maupun swasta (Ali et al., 2016). Banyak penyajian informasi dari pemerintah yang disajikan secara digital atau yang dikenal dengan electronic government (e-government). Konsep e-government sendiri adalah penggunakan teknologi informasi sebagai salah satu alat pemerintah untuk meningkatkan pelayanan pemerintah kepada warga negara, lembaga swasta dan lembaga pemerintah lain yang saling berinteraksi (Hayati, 2018)(Salsabila & Purnomo, 2017). Selain itu E-Government adalah wujud aplikasi dalam pelayanan public agar membantu mempermudah dalam segala kegiatan dan urusan pemerintah sesuai dengan landasan hukum yang berlaku untuk meningkatkan tranparansi dan kepercayaan masyarakat (Kim et al., 2020). Pada tahun 2018 negera Indonesia naik 9 peringkat dibandingkan tahun 2016 dalam penggunaan e-government dan menempati peringkat ke-7 di ASEAN[1]. Hal ini seharusnya mendorong pemerintah untuk semakin meningkatkan kualitas pelayanan e-government di Indonesia.




Gambar 0.1 Peringkat E-Government Development Index (EGDI) di Asia Tenggara

[1] https://bpptik.kominfo.go.id/2018/08/23/5938/survei-pbb-2018-peringkat-e-government-indonesia/

Penggunaan teknologi informasi disatu sisi banyak memberikan kemudahan bagi para penggunanya, namun disisi yang lain bisa menjadi ancaman yang bisa dating dari berbagai macam sumber yang dapat menyebabkan berbagai macam kerugian (Jouini et al., 2014). Di Indonesia sendiri banyak sekali serangan siber yang menyerang, menurut Laporan Tahunan Honeynet Project tahun 2018 setidaknya ada 12.895.554 serangan yang terpantau pada 21 sensor yang terpasang[2]. Hal ini tentu perlu menjadi sebuah perhatian yang lebih dalam meningkatkan sistem keamanan informasi agar pelayanan publik dapat diakses secara cepat, tepat dan memberikan hasil yang akurat serta terpercaya dengan penuh pertanggung jawaban. Karena dalam dunia digital, kemanan informasi adalah kunci keberhasilan implementasi sebuah system e-government (Pandya & Patel, 2017). Disisi lain system e-government juga harus dievaluasi dampaknya dalam hal manfaat, biaya dan risiko agar dapat dirasakan manfaatnya secara baik (Irani et al., 2008).

Dalam melakukan pengamanan terhadap sebuah sistem terdapat berbagai macam cara salah satunya adalah dengan menggunakan *Threat Modelling*. Teknik penerapan *Threat Modelling* merupakan salah satu elemen kunci untuk mengintegrasikan keamanan system perangkat lunak. Konsep keamanan siber sendiri merupakan perlindungan dari pencurian atau kerusakan pada perangkat keras, perangkat lunak, dan data yang tersimpan pada system (Lezzi et al., 2018). Hal tersebut memungkinkan untuk mengidentifikasi area kritis yang perlu dilindungi dalam sebuah system (Pandya & Patel, 2017). *Threat Modelling* sendiri ada begitu banyak metodologi dan teknik yang bisa dilakukan diantaranya STRIDE, Abuser, Attack Tress, Fuzzy Logic, CORAS, Security Development Lifecycle (SDL) dan lain-lain (Hussain et al., 2014).

Metode dan teknik *Threat Modelling* tentu memiliki kelebihan dan kekurangannya masing-masing, dalam penelitian yang dilakukan oleh (Abomhara et al., 2015) tentang A STRIDE-Based Threat Model for Telehealth Systems dipilihlah metode berbasis STRIDE dengan tahapan yang dilakukan yaitu (1) identifying assets and access points, (2) listing all potential threats and (3). Berdasarkan latar belakang diatas, kami memilih *Threat Modelling* dengan menggunakan metode dan teknik Security Development Lifecycle (SDL) yang menggabungkan antara metode STRIDE dan DREAD sebagai bahan untuk melakukan pemodelan ancaman sebagai bahan untuk mengetahui ancaman-ancaman yang ada khususnya pada system e-government.

[2] https://bssn.go.id/mengenali-serangan-siber-global-dan-nasional-melalui-laporan-tahunan-honeynet-project-bssn-ihp-tahun-2018/

## 1.2 Rumusan Masalah

Berdasarkan latar belakang diatas maka yang menjadi rumusan masalah adalah sebagai berikut:

a. Bagaimana menerapkan metode Security Development Lifecycle (SDL) dalam melakukan pemodelan pada system e-government.
b. Bagaimana menganalisis ancaman yang didapatkan berdasarkan pemodelan SDL pada system e-government.
c. Bagaimana membuat langkah mitigasi pada system e-government.

## 1.3 Tujuan Penelitian

Berdasarkan rumusan masalah diatas, maka tujuan penelitian ini adalah sebagai berikut:

a. Untuk mengetahui karakteristik system e-government dan membuat pemodelan system e-government.
b. Untuk mengetahui jenis dan tingkat ancaman pada sebuah system e-government.
c. Untuk menentukan langkah mitigasi pada system e-government.

## 1.4 Batasan Masalah

Batasan masalah dalam penelitian ini meliputi:

a. Penelitian ini dilakukan untuk mengetahui ancaman yang ada dalam system e-government pada website e-monitoring Kabupaten Purbalingga.
b. Tidak menyangkut pengujian ancaman/ Paintest.

## 1.5 Manfaat Penelitian

Manfaat yang dihasilkan dari penelitian ini antara lain:

a. Dengan adanya penelitian ini, diharapkan dapat melakukan analisa terhadap karakteristik system e-goverment.
b. Menghasilkan sebuah *treat modelling* pada system e-government.
c. Mengetahui jenis-jenis ancaman yang ada pada system e-goverment.
d. Dengan adanya penelitian ini juga diharapkan dapat memberikan kontribusi bagi penelitian selanjutnya.

## 1.6 Literatur Review

Electronic Government merupakan pemanfaatan teknologi informasi sebagai salah satu alat pemerintah untuk meningkatkan pelayanan pemerintah kepada warga negara, lembaga swasta dan lembaga pemerintah lain yang saling berinteraksi. Namun dalam e-government sendiri membutuhkan banyak peningkatan kualitas khususnya dibidang keamanan agar dapat menjadi sebuah system yang terpercaya dan dapat diakses dengan baik. Ada beberapa penelitian yang membahas mengenai keamaan sebuah system e-government khususnya pada metode threat modelling salah satunya adalah (Harrison et al., 2016) menjelaskan mengenai evaluasi Latarkeamanan terhadap framework terhadap layanan e-government yang mengacu pada Infosec Model dan melakukan analisa terhadap G-Cloud, M-Gov, Biometrics System yang didalamnya terdapat sub-sistem berupa E-voting, E-Passport, E-Transaction. Langkah-langkah yang dilakukan adalah dengan menentukan teknikal model, non-teknikal model dan infransturture system e-government. Hasil dari penelitian ini yaitu penggabungan kombinasi model dapat menjadi peran penting dalam mengamankan sebuah system e-government.

Pembahasan isu keamanan system e-government pada penelitian yang dilakukan oleh (G. Hassan & O. Khalifa, 2016) meliputi: Confidentiality/Privacy/ Accessibility, Integrity, Accountability/Non-repudiation, Authentication, Trust. Penelitian ini melakukan beberapa framework terkai dengan isu keamanan system e-government diatas. Adapun Teknik yang dilakukan meliputi pemodelan teknis, pemodelan non-teknis dan menyiapkan infrastuktur aplikasi e-government. Pemodelan teknis meliputi: Lambrinoudakis security framework dan infosec model. Sedang non-teknis menggunakan UTAUT (Unified Theory of Acceptance and Use of Technology).

Penelitian yang dilakukan oleh (Pete, 2019) merupakan penelitian yang sangat luas karena meneliti banyak aspek yang ada dalam cyber. Hasil penelitian yang dilakukan adalah focus pada risiko tingkat keamanan suatu sistem baik secara human ataupun sistem error sehingga dipilihlah beberapa model seperti: Systems-Theoretic Accident Model and Process (STAMP), The Open Group Architectural Framework (TOGAF), Open Dependency Modelling (O-DM), SABSA. Sedangkan penelitian yang dilakukan oleh (Venkatasen & Mani, 2018) adalah sebagai upaya dalam membuat defensive architecture terhadap sebuah serangan yang didasarkan pada standar Common Attack Pattern Enumeration And Classification (CAPEC). Hasil dari penelitian ini yaitu implementasi model secara web-based RFID Technology untuk mengumpulkan jenis-jenis serangan pada network dan langkah terbaik dalam melakukan mitigasi.

Tabel 0.1 Rangkuman Review Penelitian

| Peneliti | Analisa Kasus | Metode | Target |
|---|---|---|---|
| (G. Hassan & O. Khalifa, 2016) | Melakukan analisis perspektif terhadap kemanan informasi yang ada pada system e-government | • Lambrinoudakis security framework<br>• Infosec Model | Melakukan pengamanan terhadap:<br>• Authentification of user<br>• Availability<br>• Integrity<br>• Confidentiality of information |
| (Harrison et al., 2016) | Melakukan evaluasi keamanan terhadap framework terhadap layanan e-government | • Waterfall<br>• OWASP Application Security Verification Standard (ASVS) | Melakukan evaluasi terhadap:<br>• Scrum<br>• Sprint<br>• Government Service Design Manual |
| (Pandya & Patel, 2017) | Melakukan analisis keamanan informasi (infosec) pada e-governance | • Artificial Neural Network (ANN)<br>• Genetic Algorithm<br>• Bayesian Network<br>• Fuzzy System | Melakukan sebuah penilaian risiko terhadap system |
| (Venkatasen & Mani, 2018) | Melakukan pengamanan terhadap risiko ancaman dengan sebuah pemodelan pada system e-government | • Common Attack Pattern Enumeration And Classification (CAPEC)<br>• Security Development Lifecycle (SDLC)<br>• Building Security In Maturity Model (BSIMM) | Melakukan pengujian terhadap Radio Frequency Identification (RFID) Network berupa:<br>• relay attacks,<br>• cloning,<br>• spoofing,<br>• impersonation,<br>• eavesdropping, |

| Peneliti | Analisa Kasus | Metode | Target |
|---|---|---|---|
| | | • OWASP Software Assurance Maturity Model (SAMM)<br>• STRIDE | • buffer overflow,<br>• malicious code injection,<br>• denial of service (DOS),<br>• crypto attacks,<br>• desynchronisation attacks,<br>• forward secrecy |
| (Pete, 2019) | Melakukan analisa manajemen risiko dan tata kelola prinsip-prinsip dasar pada cyber. | • Systems-Theoretic Accident Model and Process (STAMP)<br>• The Open Group Architectural Framework (TOGAF)<br>• Open Dependency Modelling (O-DM)<br>• SABSA | Melakukan penelitian berbagai aspek terhadap cyber baik dari threat modelling, framework berdasarkan beberapa metode yang ada. |
| (Hussain et al., 2014) | Melakukan survey terhadap berbagai macam metodologi threat modelling dan tekniknya. | • STRIDE<br>• STRIDE Average Model<br>• Attack Trees<br>• Fuzzy Logic<br>• SDL Threat Modelling Tool<br>• T-MAP<br>• CORAS | Melakukan sebuah Analisa ancaman yang dapat menyebabkan sebuah kerentanan system terhadap target dan aspek yang meliputi :<br>• Desain Keamanan<br>• Tool Support<br>• Web Application |
| (Macher et al., 2016) | Melakukan metodologi penilaian ancaman dan risiko dalam domain dan | • STRIDE<br>• SAHARA DREAD | Melakukan sebuah penilaian evaluasi keamanan system dengan |

| Peneliti | Analisa Kasus | Metode | Target |
|---|---|---|---|
| | menyajikan pendekatan untuk mengklasifikasikan ancaman keamanan siber | | melakukan penggabungan metode Hazard Analysis and Risk Assessment (HARA) dengan STRIDE |
| (Ge et al., 2017) | Melakukan penelitian tentang framework untuk analisis keamanan Internet of Things (IoT) | • HARM<br>• SHARPE<br>• Adaptive Security of Smart Internet of Things (ASSET) | Membuat framework untuk pemodelan dan penilaian keamanan Internet of Things (IoT). Pengujian berupa Security Model for the IoT yang terdiri dari security framework dan game-based security modeling. Pengujian kedua berupa Security Model for the non-IoT network yang terdiri dari Tree-based Models dan Graph-based Models |

## 1.7 Metode Penelitian

Langkah-langkah yang ditempuh untuk melakukukan penelitian ini adalah sebagai berikut:


Gambar 0.2 Alur Metode Penelitian

## 1.8 Sistematika Penulisan

Untuk memberikan gambaran dan mempermudah dalam penyusunan penelitian ini, maka dibuat sistematika penulisan sebagai berikut:

**BAB I PENDAHULUAN**

Pendahuluan merupakan pengantar terhadap permasalahan yang akan dibahas. Didalamnya menguraikan tentang gambaran suatu penelitian yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tuuan penelitan, manfaat penelitian, metodologi penelitian serta sistematika penulisan.

**BAB II KAJIAN TEORI**

Pada Bab ini menjelaskan tentang teori-teori dasar yang digunakan untuk memecahkan masalah dalam penelitian ini. Teori yang berkaitan dengan penelitian yang sedang diteliti.

**BAB III METODOLOGI PENELITIAN**

Bab ini membahas tentang langkah-langkah penelitian, kebutuhan perangkat lunak, perangkat keras dan bahan penelitian yang digunakan serta perancangan antar muka aplikasi yang akan dibuat.

**BAB IV PEMBAHASAN**

Pada Bab ini membahas tentang hasil dan pembahasan, terkait dengan pembahasan penyelesaian masalah yang diangkat, penentuan hasil analisis dan evaluasi dari penelitian yang diangkat.

**BAB V PENUTUP**

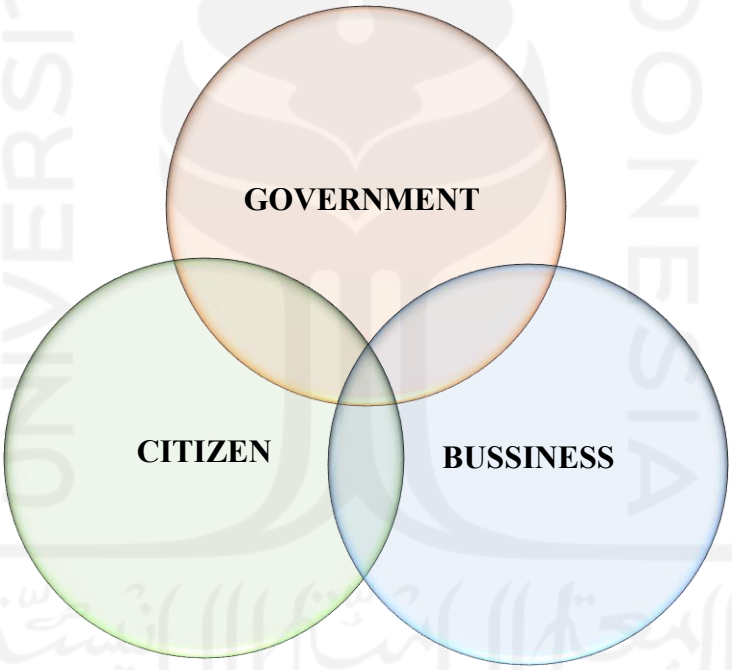
Pada bab ini memuat kesimpulan akhir dari semua proses penelitian sampai kepada hasil implementasi metode dan saran yang perlu diperhatikan karena keterbatasan dalam mendapatkan materi yang dibuat selama melakukan penelitian dan rekomendasi yang dibuat untuk pengembangan penelitian selanjutnya.

# BAB II

# Tinjauan Pustaka

## 2.1 Electronic Government

Electronic Government (e-government) adalah pemerintah yang menggunankan teknologi informasi dan khusunya internet sebagai salah satu alat pemerintah untuk meningkatkan pelayanan pemerintah kepada warga Negara, lembaga swasta dan lembaga pemerintahan lain yang saling berinteraksi (Salsabila & Purnomo, 2017). Selain itu E-Government adalah wujud aplikasi dalam pelayanan public agar membantu mempermudah dalam segala kegiatan dan urusan pemerintah sesuai dengan landasan hukum yang berlaku untuk meningkatkan tranparansi dan kepercayaan masyarakat kepada pemerintahan. Relasi pada system e-government setidaknya meliputi 3 hal yaitu :




Gambar 0.1 Relasi E-Government

1. Government to Citizen (G2C) : dirancang agar mempermudah pemerintah dalam melakukan interkasi dengan masyarakat yang menjadi objek utamanya.
2. Government to Business (G2B) : dalam hal ini diberikan kemudahan pemeritah dalam berinterakasi dengan dunia bisnis dimana membukakan keleluasaan pada dunia bisnis untuk mendapatkan atau mengakses informasi dan perizinan–perizinan yang menyangkut usahanya.

3. Government to Government (G2G) : mempermudah hubungan natra lembaga pemerintahan dalam bekerjasama dan berkomunikasi dengan hal ini menciptakan korelas atau harmoni yang baik antar lembaga pemerintaha dengan begitu akan mempeermudah dalam pemberiaan pelayanan dan penyejahteraan rakyat.

## 2.2 Threat

Threat merupakan suatu ancaman atau bahaya yang dapat menggangu operasi, prosedur, intergritas atau ketersediaan perangkat lunak atau jaringan baik dilakukan secara sengaja maupun tidak. Dengan kata lain, Threat merupakan ancaman yang memungkinkan kondisi yang dapat mengeksploitasi kerentanan dalam menembus system keamanan (Satapathy, 2014).

## 2.3 Vulnerability

Vulnerability dapat didefinisikan sebagai kelemahan bawaan dalam desain, konfigurasi, implementasi atau system jaringan. Vulnerability juga merupakan hal apa saja yang membuat jaringan kehilangan informasi dan downtime, karena setiap jaringan pada dasarnya memiliki suatu celah vulnerability (Satapathy, 2014).

## 2.4 Exploitation

Exploitation adalah cara atau alat yang digunakan penyerang dalam menggunakan celah vulnerability untuk menyebabkan kerusakan pada sebuah system. Exploitation bisa berupa paket kode yang membuat sebuah system berjalan terlalu berat, selain itu exploitation juga bisa berupa skema rekayasa sosial dimana dilakukan pendekatan sosial terhadap admin untuk mendapatkan informasi berharga (Satapathy, 2014).

## 2.5 Attack

Attack atau serangan adalah segala upaya yang dilakukan untuk menghancurkan, mengekspos, mengubah, menonaktifkan, mencuri atau penggunaan akses dan aset secara illegal (Satapathy, 2014).

## 2.6 Threat Modelling

*Treat modelling* merupakan sebuah konsep yang membantu memahami ancaman dan kerentanan keamanan sebuah system dan bagaimana ancaman tersebut berdampak pada pengguna serta untuk menentukan solusi keamanan system yang efektif (Abomhara et al., 2015). Untuk itu pemodelan ancaman merupakan kunci utama untuk mendapatkan potensi ancaman pada sebuah system (Wuyts et al., 2014). Menurut (Hussain et al., 2014) jenis-jenis pendekatan *threat modelling* antara lain: STRIDE, Abuser Stories, STRIDE Average Model, Attack Trees, Fuzy Logic, SDL Threat Modelling Tool, T-MAP dan CORAS.

## 2.7 STRIDE

STRIDE merupakan klasifikasi sebuah ancaman, dalam Microsoft STRIDE Model secara umum jenis serangan dibagi menjadi 6 yaitu : Spoofing, Tampering, Repudiation, Information disclosure, Denial of service dan Elevation of privilege[3]. Berikut ini adalah deskripsi tabel STRIDE :

Tabel 0.1 Deskripsi STRIDE

| No. | Jenis Ancaman | Deskripsi |
|---|---|---|
| 1. | Spoofing | Ancaman dengan cara berusaha mendapatkan akses ke dalam system menggunakan identitas palsu. |
| 2. | Tampering | Ancaman dengan cara melakukan modifikasi data secara tidak sah (illegal). |
| 3. | Repudiation | Ancaman dengan cara melakukan pembuatan database/ aplikasi baik secara sengaja maupun tidak dengan menyisipkan bugs/ virus tanpa pertanggungjawaban. |
| 4. | Information disclosure | Ancaman dengan cara membuka dan membaca sebuah informasi tanpa mempunyai hak otorisasi |
| 5. | Denial of service | Ancaman dengan cara merusak system sehingga menyebabkan sebuah system tidak berjalan atau tidak bisa digunakan oleh orang lain. |
| 6. | Elevation of privilege | Kemungkinan penyalahgunaan wewenang diluar hak aksesnya sehingga menyebabkan dapat diaksesnya hak akses milik orang lain |

## 2.8 DREAD

DREAD merupakan sebuah pemodelan ancaman yang digunakan untuk menilai tingkat keamanan dari sebuah system. Pemodelan DREAD dibagi menjadi lima kategori yaitu: Damage potential, Reproducibility, Exploitability, Affected users dan Discoverability (Macher et al., 2016). Berikut ini adalah deskripsi tabel DREAD:

Tabel 0.2 Deskripsi DREAD

| No. | Dampak Ancaman | Deskripsi |
|---|---|---|
| 1. | Damage Potential | Kerusakan berdiri hanya untuk keseriusan serangan |
| 2. | Reproducibility | Apakah serangan berulang dan betapa mudahnya akan |

[3] https://www.microsoft.com/security/blog/2007/09/11/stride-chart/

| | | |
|---|---|---|
| | | mengulangi serangan |
| 3. | Exploitability | Explotabilitas berarti kemudahan serangan |
| 4. | Affected user | Pengguna yang terpengaruh mewakili semua orang yang terkena dampak serangan |
| 5. | Discoverability | Discoverability berarti betapa mudahnya untuk menemukan mengeksploitasi |

Tahap Rating berdasarkan DREAD digunakan sebagai analisis untuk melakukan penanggulangan ancaman berdasarkan nilai yang didapatkan dari pemodelan pada system sebuah system (Omotosho et al., n.d, 2020). Dalam penyajian data risiko ancaman dikatakan baik apabila disajikan sebagai angka kardinal atau persentase, bukan dengan label kualitatif seperti tinggi, sedang dan rendah (Pete, 2019). Berikut ini adalah tabel Threat Rating dengan metode DREAD :

Tabel 0.3 Threat Rating Table

| | **Rating** | **High (3)** | **Medium (2)** | **Low (1)** |
|---|---|---|---|---|
| D | Damage potential | Penyerang dapat merusak sistem keamanan; dapatkan otorisasi kepercayaan penuh; Jalankan sebagai administrator; unggah konten. | Membocorkan informasi sensitif | Membocorkan informasi sepele |
| R | Reproducibility | Serangan tersebut dapat direproduksi setiap saat dan tidak memerlukan jendela waktu. | Serangan dapat direproduksi, tetapi hanya dengan jendela waktu dan situasi balapan tertentu. | Serangan itu sangat sulit untuk direproduksi, bahkan dengan pengetahuan tentang lubang keamanan. |
| E | Exploitability | Seorang programmer pemula bisa melakukan serangan dalam waktu singkat. | Seorang programmer yang terampil dapat melakukan serangan, lalu mengulangi langkah-langkah tersebut. | Serangan itu membutuhkan orang yang sangat terampil dan pengetahuan yang mendalam setiap saat untuk mengeksploitasinya. |
| A | Affected users | Semua pengguna, konfigurasi default, pelanggan utama | Beberapa pengguna, konfigurasi non-default | Persentase pengguna yang sangat kecil, fitur tidak jelas; |

| | | | | |
|---|---|---|---|---|
| | | | | mempengaruhi pengguna anonim |
| D | Discoverability | Informasi yang dipublikasikan menjelaskan serangan itu. Kerentanan ditemukan di fitur yang paling umum digunakan dan sangat terlihat. | Kerentanan ada di bagian produk yang jarang digunakan, dan hanya sedikit pengguna yang dapat menemukannya. Perlu beberapa pemikiran untuk melihat penggunaan yang jahat. | Bug tidak jelas, dan kecil kemungkinannya pengguna akan mengetahui potensi kerusakan. |

Melakukan DREAD rating dengan menggunakan 2 contoh serangan yaitu :

- Attacker obtains authentication credentials by monitoring the network.
- SQL commands injected into application.

Tabel 0.4 DREAD rating

| Threat | D | R | E | A | D | Total | Rating |
|---|---|---|---|---|---|---|---|
| Attacker obtains authentication credentials by monitoring the network. | 3 | 3 | 2 | 2 | 2 | 12 | High |
| SQL commands injected into application. | 3 | 3 | 3 | 3 | 2 | 14 | High |

Tabel 0.5 Threat 1

| **Threat Description** | **Attacker obtains authentication credentials by monitoring the network** |
|---|---|
| Threat target | Web application user authentication process |
| Risk rating | High |
| Attack techniques | Use of network monitoring software |
| Countermeasures | Use SSL to provide encrypted channel |

## 2.9 SDL Threat Modelling Tool

SDL *(Security Development Lifecycle)* Threat Modelling Tool dan Aplication Threat Modelling (TAM) merupakan pengembangan yang berbasis pada pemodelan STRIDE dan

DREAD. Dalam SDL Tool dan TAM Tool akan menghasilkan laporan yang menggambarkan semua kemungkinan ancaman terhadap system beserta langkah mitigasi yang relevan. Nantinya kombinasi antara STRIDE dan DREAD mampu menghasilkan suatu nilai tingkat risiko ancaman sehingga memudahkan dalam melakukan prioritas perbaikan system (Meimer, 2010). Pada SDL ada 5 tahap pemodelan ancaman yaitu[4] :


Gambar 0.2 Tahap Security Development Lifecycle (SDL)

a. Menentukan kebutuhan keamanan
b. Membuat diagram/ pemodelan
c. Mengidentifikasi ancaman
d. Mitigasi Ancaman
e. Memvalidasi bahwa ancaman telah dimitigasi.

[4] https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling

# BAB III

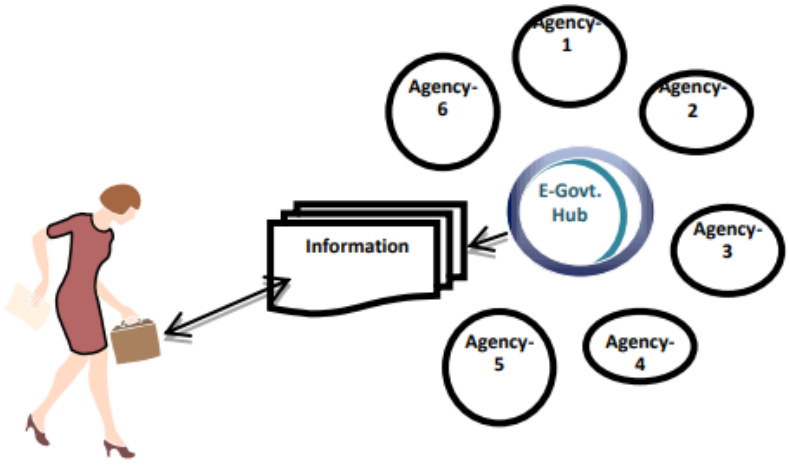
# Metode Penelitian

Bab ini menjelaskan bagaimana cara penelitian dilakukan sehingga dapat diketahui rincian tentang urutan langkah-langkah yang dibuat secara sistematis dan dapat dijadikan pedoman yang jelas dalam menyelesaikan permasalahan, membuat analisis terhadap hasil penelitian, serta kesulitan-kesulitan yang dihadapi. Adapun langkah-langkah atau tahapan-tahapan pada penelitian ini dapat dilihat pada Gambar 3.1.


Gambar 0.1 Metodologi Penelitian

## 3.1 Identifikasi Sistem E-Government

Pada tahap ini dilakukan identifikasi system e-government dengan memberhatikan semua bagian-bagian yang saling berkaitan seperti user, admin, server, jaringan atau objek apapun yang ada. Adapun menurut (G. Hassan & O. Khalifa, 2016) membuat sebuah ilustrasi E-Government Architecture seperti gambar dibawah ini:




Gambar 0.2 Arsitektur E-Government

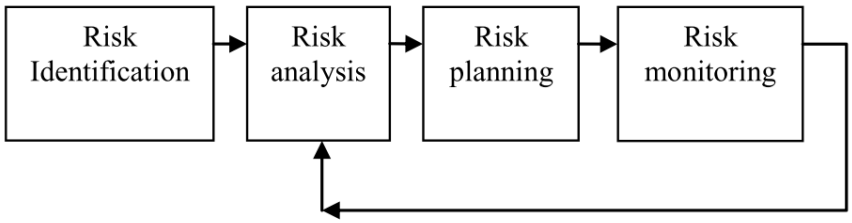
## 3.2 Studi Literatur

Studi literatur dilakukan untuk mengumpulkan bahan-bahan referensi yang terkait dengan penelitian, baik melalui buku, artikel, paper, jurnal, makalah, dan mengunjungi beberapa

situs yang terdapat pada internet terkait dengan *threat modelling* beserta kemungkinan ancaman-ancaman yang ada pada sebuah sistem.

### 3.3 Melakukan Pemodelan Sistem (SDL Based)

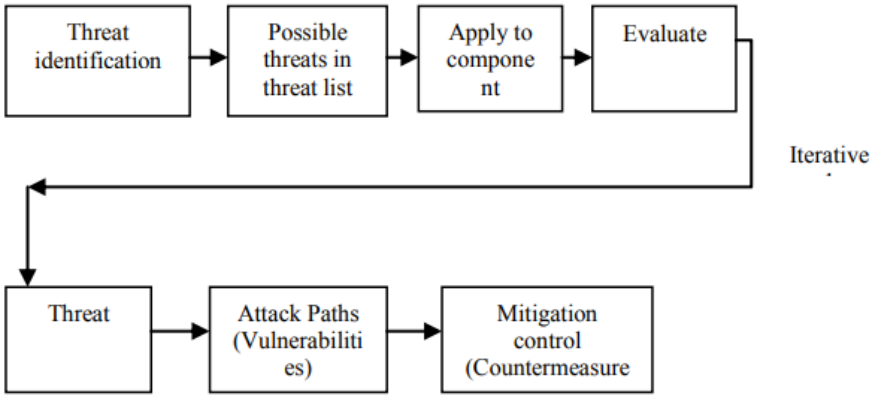
Tahap pertama yang dilakukan pada Security Development Lifecycle (SDL) adalah pendefinisian kebutuhan, atribut dan data pada sebuah system. Kemudian dilakukan identifikasi ancaman dari penyerang seperti proses, aliran data, penyimpanan data dan interaksi dengan pengguna. Kemudian tahap terakhir pada proses ini yaitu dengan penanggulangan serangan yang telah diketahui untuk mengurangi kemungkinan terjadi serangan (Maheshwari & Prasanna, 2017).




Gambar 0.3 Proses Manajemen Risiko pada SDL

### 3.4 Analisis Ancaman

Namun jenis ancaman untuk setiap komponen ditentukan untuk aplikasi dalam bentuk pohon ancaman, kerentanan dan penanggulangan. Proses ini dilakukan berulang untuk melakukan evaluasi terhadap identifikasi ancaman.




Gambar 0.4 Proses identifikasi sebuah Ancaman

Berikut ini adalah jenis jenis ancaman menurut penggunaan medote STRIDE:

Tabel 0.1 Jenis-jenis ancaman pada metode STRIDE

| No. | Jenis Ancaman |
|---|---|
| 1. | Spoofing |

| | |
|---|---|
| 2. | Tampering |
| 3. | Repudiation |
| 4. | Information disclosure |
| 5. | Denial of service |
| 6. | Elevation of privilege |

Setelah mengetahui jenis-jenis ancaman yang ada, kemudian dilakukan pemodelan DREAD, yaitu alat pemodelan untuk mengetahui peringkat pada ancaman-ancaman yang telah ditemukan dengan sekala risiko high, low dan medium.

Tabel 0.2 Analisis Tingkat Ancaman menggunakan DREAD

| Threat | D | R | E | A | D | Grade |
|---|---|---|---|---|---|---|
| T1 | $N_{T1}$ | $N_{T1}$ | $N_{T1}$ | $N_{T1}$ | $N_{T1}$ | $G_{T1}$ |
| T2 | $N_{T2}$ | $N_{T2}$ | $N_{T2}$ | $N_{T2}$ | $N_{T2}$ | $G_{T2}$ |
| T3 | $N_{T3}$ | $N_{T3}$ | $N_{T3}$ | $N_{T3}$ | $N_{T3}$ | $G_{T3}$ |
| T..n | $N_{T..n}$ | $N_{T..n}$ | $N_{T..n}$ | $N_{T..n}$ | $N_{T..n}$ | $G_{T4}$ |

Keterangan:

T = Ancaman N= Nilai Ancaman G= Tingkat Ancaman

Untuk menghitung tingkat ancaman yaitu:

$$\mathbf{G = ( D + R + E + A + D ) / 5}$$

Sedangkan untuk mengetahui Nilai Risiko Ancaman maka digunakan Rumus :

**Risk = Probability * Damage Potential**

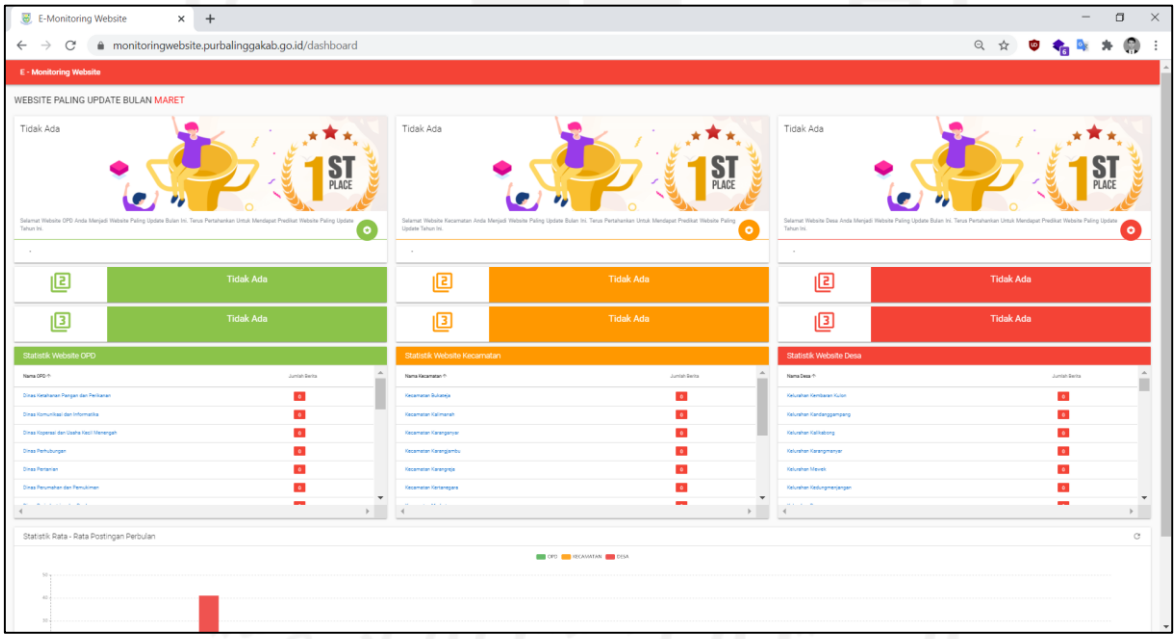
### 3.5 Kesimpulan

Pada tahapan ini adalah tahapan pengambilan kesimpulan dengan memperhatikan pengujian dan implementasi metode Security Development Lifecycle (SDL) yang didalamnya terdapat penerapan metode STRIDE dan DREAD sehingga diketahui jenis ancaman beserta besar risiko ancaman yang ditemukan pada sebuah system e-government berikut dengan langkah mitigasi ancaman tersebut.

# BAB IV
# Hasil dan Pembahasan

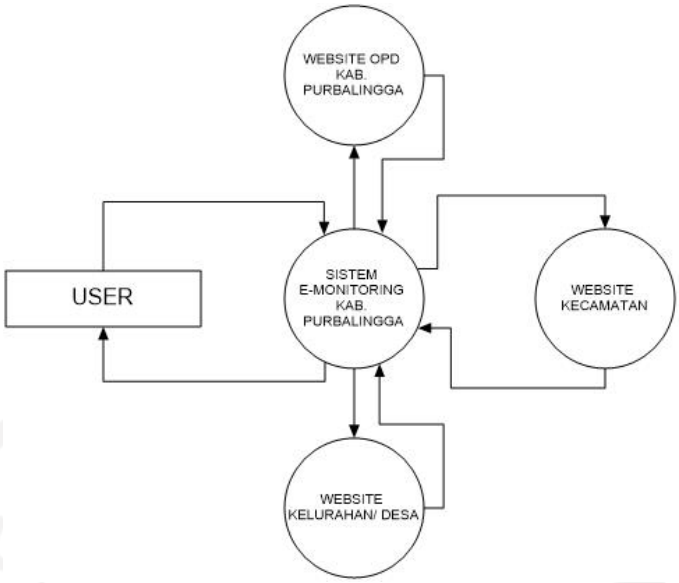
## 4.1 Identifikasi Sistem E-Government

Identifikasi system e-government dilakukan dengan wawancara dan analisis system e-monitoring pada: https://monitoringwebsite.purbalinggakab.go.id/. Web aplikasi tersebut dirancang untuk melakukan monitoring pengelolaan seluruh website di Kabupaten Purbalingga, Jawa Tengah. Dalam web e-monitoring tersebut berisi tentang informasi berita di Kabupaten Purbalingga yang terintegrasi dengan Website Organisasi Perangkat Daerah (OPD), Website Kecamatan dan Website Desa. Berikut ini merupakan home page dari aplikasi e-monitoring yaitu pada Gambar 4.1 :




Gambar 0.1 Tampilan Website e-monitoring

Dalam penggunaan Metode Security Development Lifecycle (SDL) pada system e-monitoring tersebut perlu dilakukan identifikasi terhadap system e-monitoring yang akan digambarkan seperti Gambar 4.2 berikut ini :




Gambar 0.2 Gambaran system e-monitoring

Selanjutnya system e-monitoring Kabupaten Purbalingga setelah dianalisa memiliki manajemen system sebagai berikut:

Tabel 0.1 Manajemen sistem e-monitoring

| | |
|---|---|
| Bahasa Pemrograman | Node.js |
| Web Servers | Nuxt.js |
| Web Framework | Nuxt.js |
| CDN | Cloudflare |
| XmlHttpRequest | stat-opd<br>stat-kecamatan<br>stat-desa<br>stat-year |
| Web API | Available |
| Database | Available |

Berikut ini adalah hasil analisa integrasi yang ada pada website e-monitoring meliputi Website Organisasi Perangkat Desa (OPD) sejumlah 25, Website Kecamatan sejumlah 14, Website Desa sejumlah 121 yang secara lengkap dapat dilihat Tabel 4.2, Tabel 4.3 dan Tabel 4.5 pada Lampiran A.

## 4.2 Pemodelan Sistem (SDL Based)

Pemodelan system dilakukan menggunakan metode Security Development Lifecycle (SDL) dengan menggunakan aplikasi Microsoft Threat Modeling Tool. Setelah melakukan

identifikasi system e-monitoring, selanjutkan adalah melakukan pemodelan system berdasarkan hasil identifikasi system tersebut. Terdapat setidaknya lima komponen utama yaitu: User, Browser, Web Aplication, Web API, Web Service dan Database.

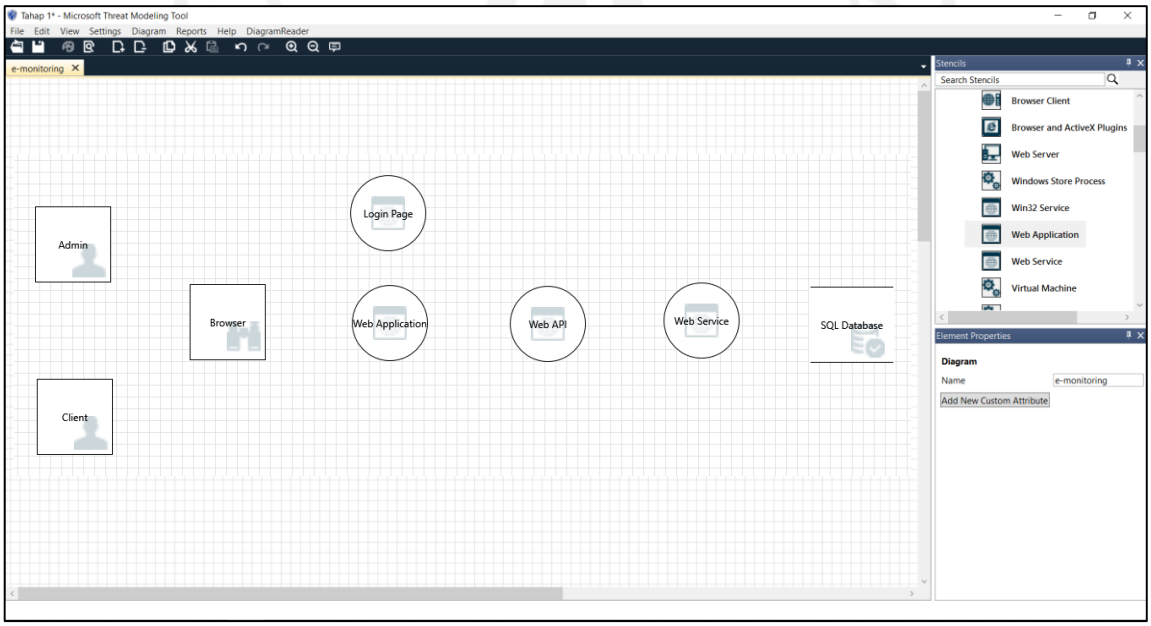
Tabel 0.2 Komponen Pemodelan Sistem

| No. | Komponen | Keterangan |
|---|---|---|
| 1. | User | Terdiri dari admin dan client |
| 2. | Browser | Software yang digunakan untuk mengakses Web |
| 2. | Web Aplication | Web Utama yang akan dianalisis yaitu : https://monitoringwebsite.purbalinggakab.go.id/ |
| 3. | Login Page | Login page for Admin |
| 4. | Web API | Data Hasil dari Web Service, data yang ditampilkan dalam bentuk JSON |
| 5. | Web Service | Jembatan untuk memudahkan mengakses Database |
| 6. | Database | Tempat penyimpanan data, untuk database yang digunakan adalah mongoDB (noSQL Database) |

Tahap Pemodelan menggunakan: Microsoft Threat Modelling Tool meliputi :

### 4.2.1 Membuat Pemodelan Komponen Utama

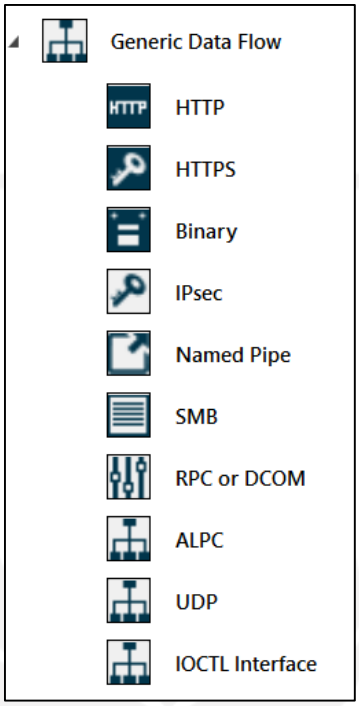
Komponen utama dari web e-monitoring terdiri dari Human User (Admin dan Client), Browser, Web Aplication (e-monitoring), Login Page, Web API, Web Service, SQL Database.




Gambar 0.3 Tahap 1 Pembuatan Komponen Utama

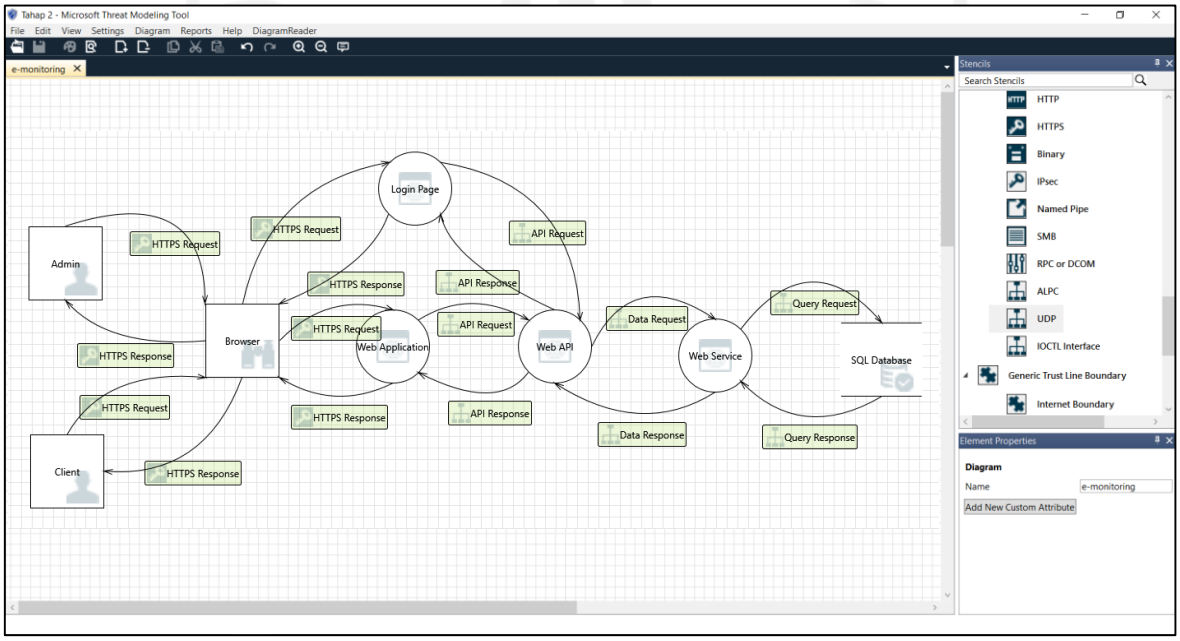
### 4.2.2 Membuat Jenis Generic Data Flow

Membuat jenis generic data flow yang yang saling menghubungkan pada komponen utama yang telah dibuat. Adapun jenis Generic Data Flow yang tersedia pada aplikasi Microsoft Threat Modeling yaitu :




Gambar 0.4 Jenis Generic Data Flow yang tersedia

Generic Data Flow yang digunakan untuk komponen utama pada pemodelan system e-monitoring yaitu : HTTPS, Generic Data Flow dan UDP yang digambarkan request dan response sebagai berikut:




Gambar 0.5 Tahap 2 Pembuatan Jenis Generic Data Flow

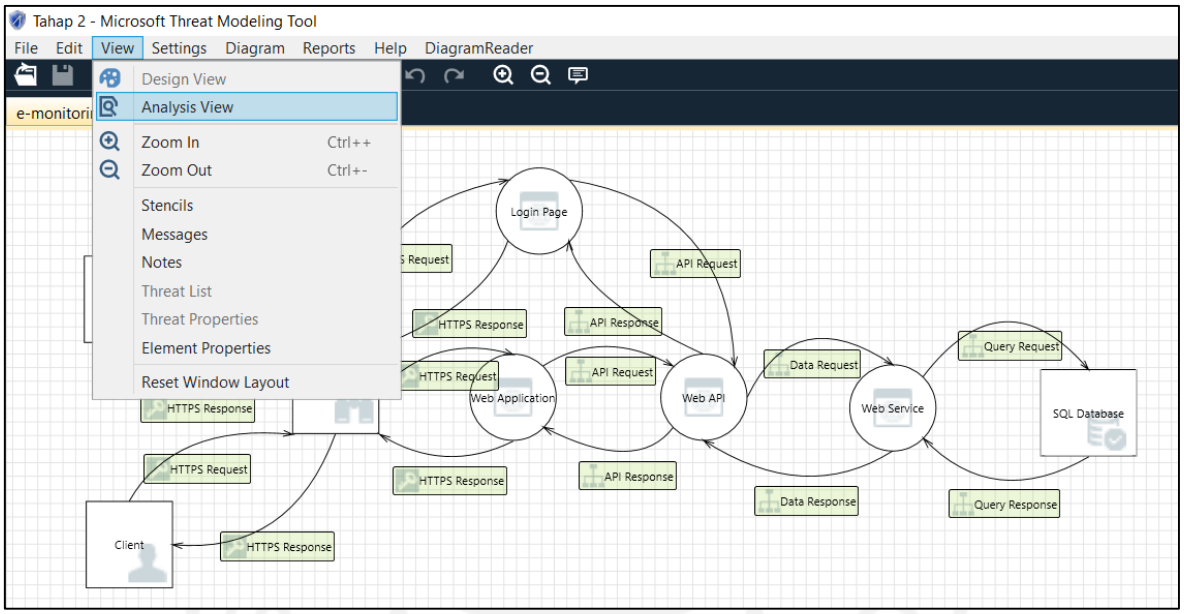
Penjelasan pada Gambar 4.5 dalam Pembuatan Jenis Generic Data Flow adalah sebagai berikut :

Tabel 0.3 Penjelasan Human User

| No. | Human User | Data Flow |
|---|---|---|
| 1. | Admin | 1) Admin melakukan HTTPS Request ke Browser yang diteruskan ke Login Page. Apabila request sebagai Admin tidak berhasil maka akan segera dilakukan response dan tidak bisa melanjutkan ke proses berikutnya. Karena login page berisi tentang hak akses sebagai admin dalam melakukan manajemen/ pengelolaan pada system e-monitoring.<br>2) Dari Login page kemudian melakukan API Request ke Web API<br>3) Dari Web API kemudian melakukan Data Request ke Web Service<br>4) Dari Web Service kemudian melakukan Query Request ke Database yang kemudian akan memberikan response sesuai dengan request yang dilakukan oleh Admin. |
| 2. | Client | 1) Client melakukan HTTPS Request ke Web Application yaitu system e-monitoring. Request tersebut bisa berarti tentang pencarian informasi seperti: informasi Organisasi Perangkat Daerah (OPD), Informasi Kecamatan, Informasi Desa/ Kelurahan, Statistik Rata-rata postingan.<br>2) Dari Web Application tersebut kemudian melakukan API Request ke Web API<br>3) Dari Web API kemudian melakukan Data Request ke Web Service<br>4) Dari Web Service kemudian melakukan Query Request ke Database yang kemudian akan memberikan response sesuai dengan request yang dilakukan oleh Client. |

## 4.3 Hasil Potensi Ancaman

Setelah melakukan tahap Pemodelan, untuk mendapatkan hasil potensi ancaman yaitu dengan melakukan langkah view-analysis view seperti Gambar 4.6




Gambar 0.6 Proses Analysis View

hasil potensi ancaman yang didapatkan berdasarkan pemodelan pada Gambar 4.5 adalah sebagai berikut :

Tabel 0.4 Hasil Potensi Ancaman berdasarkan Pemodelan Sistem

| id | Title | Category |
|---|---|---|
| 1. | Spoofing the Browser External Entity | Spoofing |
| 2. | Cross Site Scripting | Tampering |
| 3. | Elevation Using Impersonation | Elevation Of Privilege |
| 4. | Spoofing the Browser External Entity | Spoofing |
| 5. | Cross Site Scripting | Tampering |
| 6. | Elevation Using Impersonation | Elevation Of Privilege |
| 7. | Login Page Process Memory Tampered | Tampering |
| 8. | Elevation Using Impersonation | Elevation Of Privilege |
| 9. | Web API Process Memory Tampered | Tampering |
| 10. | Cross Site Scripting | Tampering |
| 11. | Elevation Using Impersonation | Elevation Of Privilege |
| 12. | Web Application Process Memory Tampered | Tampering |
| 13. | Elevation Using Impersonation | Elevation Of Privilege |
| 14. | Web API Process Memory Tampered | Tampering |

Tabel 4.7 Hasil Potensi Ancaman berdasarkan Pemodelan Sistem (lanjutan)

| id | Title | Category |
|---|---|---|
| 15. | Cross Site Scripting | Tampering |
| 16. | Elevation Using Impersonation | Elevation Of Privilege |
| 17. | Web API Process Memory Tampered | Tampering |
| 18. | Elevation Using Impersonation | Elevation Of Privilege |
| 19. | Web Service Process Memory Tampered | Tampering |
| 20. | Elevation Using Impersonation | Elevation Of Privilege |
| 21. | Spoofing of Destination Data Store SQL Database | Spoofing |
| 22. | Potential SQL Injection Vulnerability for SQL Database | Tampering |
| 23. | Potential Excessive Resource Consumption for Web Service or SQL Database | Denial Of Service |
| 24. | Spoofing of Source Data Store SQL Database | Spoofing |
| 25. | Weak Access Control for a Resource | Information Disclosure |

## 4.4 Analisis Ancaman

Setelah didapatkan hasil 25 potensi ancaman pada Tabel 4.7 maka selanjutnya dilakukan rating terhadap potensi ancaman tersebut dengan menggunakan metode DREAD. Pemberian nilai pada masing-masing jenis ancaman dengan kategori Damage potential, Reproducibility, Exploitability, Affected user dan Discoveratibility adalah dengan memberikan nilai 3 = High; 2 = Medium; 1 = low. Pemberian nilai tersebut menggunakan standar dari DREAD Rating yang ada di Tabel 2.3 terhadap jenis ancaman yang dihasilkan dari pemodelan website e-monitoring yang kemudian dilakukan konfirmasi dengan pengelola website e-monitoring. Hasil Rating berdasarkan Total nilai yang didapatkan dengan karegori rating yaitu 11 – 15 = High;  6 – 10 = Medium; 1 – 5 = Low. Adapun hasil analisis dan Rekapitulasi DREAD Rating scoring Threat 1 – 25 ada pada Tabel 4.8 dan Tabel 4.9 sebagai berikut :

Tabel 0.5 Hasil Analisis DREAD Rating Scoring

| Threat 1. *Spoofing the Browser External Entity* | | |
|---|---|---|
| Dampak Ancaman | Penjelasan Penilaian | Nilai |
| Damage Potential | Potensi Penyerang dalam melakukan spoofing melalui browser dan login page berupa otorisasi penuh | 3 |

Tabel 4.8 Hasil Analisis DREAD Rating Scoring (lanjutan)

| | | |
|---|---|---|
| Threat 1. *Spoofing the Browser External Entity* | | |
| Reproducibility | Serangan dapat dilakukan dengan jeda waktu tertentu (tidak setiap saat) | 2 |
| Exploitability | Dibutuhkan orang yang sangat terampil dan pengetahun mendalam dalam melakukan serangan karena web sudah dilengkapi firewall dan login page disembunyikan | 1 |
| Affected user | Apabila penyerang berhasil, maka ini menjadi ancaman yang berbahaya karena target usernya bisa semua pengguna dan melakukan konfigurasi default | 3 |
| Discoverability | Tidak terdapat bug yang jelas dalam website, login page disembunyikan | 1 |
| Threat 2. *Cross Site Scripting* | | |
| Dampak Ancaman | Penjelasan Penilaian | Nilai |
| Damage Potential | Potensi Penyerang dalam melakukan Tampering berupa CSS melalui Web Server dan login page | 1 |
| Reproducibility | Serangan dapat dilakukan dengan jeda waktu tertentu (tidak setiap saat) | 2 |
| Exploitability | Dibutuhkan seorang programmer yang terampil untuk melakukan serangan | 2 |
| Affected user | Apabila penyerang berhasil, maka ini menjadi ancaman yang berbahaya karena target usernya bisa semua pengguna dan melakukan konfigurasi default | 3 |
| Discoverability | Tidak terdapat bug yang jelas dalam website, login page disembunyikan | 1 |
| Threat 3. *Elevation Using Impersonation* | | |
| Dampak Ancaman | Penjelasan Penilaian | Nilai |
| Damage Potential | Potensi Penyerang dalam melakukan serangan Elevation Using Impersonation melalui login page berupa informasi sensitive. | 2 |
| Reproducibility | Serangan dapat dilakukan dengan jeda waktu tertentu (tidak setiap saat) | 2 |

Tabel 4.8 Hasil Analisis DREAD Rating Scoring (lanjutan)

| | | |
|---|---|---|
| Threat 3. *Elevation Using Impersonation* | | |
| Exploitability | Dibutuhkan orang yang sangat terampil dan pengetahun mendalam dalam melakukan serangan karena login page disembunyikan | 1 |
| Affected user | Presentase mempengaruhi pengguna sangat kecil | 1 |
| Discoverability | Kerentanan ada di bagian produk yang jarang digunakan, dan hanya sedikit pengguna yang dapat menemukannya. Perlu dilakukan pengujian terus menerus agar bisa melakukan serangan Elevation Using Impersonation. | 2 |
| Threat 4. *Spoofing the Browser External Entity* | | |
| Dampak Ancaman | Penjelasan Penilaian | Nilai |
| Damage Potential | Potensi Penyerang dalam melakukan Spoofing melalui Browser dan Web Application berupa otorisasi penuh | 3 |
| Reproducibility | Serangan dapat dilakukan dengan jeda waktu tertentu (tidak setiap saat) | 2 |
| Exploitability | Dibutuhkan orang yang sangat terampil dan pengetahun mendalam dalam melakukan serangan karena dalam web application beberapa fitur telah disembunyikan seperti login page | 1 |
| Affected user | Apabila penyerang berhasil, maka ini menjadi ancaman yang berbahaya karena target usernya bisa semua pengguna dan melakukan konfigurasi default | 3 |
| Discoverability | Tidak terdapat bug yang jelas dalam website | 1 |
| Threat 5. *Cross Site Scripting* | | |
| Dampak Ancaman | Penjelasan Penilaian | Nilai |
| Damage Potential | Potensi Penyerang dalam melakukan Tampering berupa CSS melalui Web Server dan Web Application | 1 |
| Reproducibility | Serangan dapat dilakukan dengan jeda waktu tertentu (tidak setiap saat) | 2 |
| Exploitability | Dibutuhkan seorang programmer yang terampil untuk melakukan serangan | 2 |

Tabel 4.8 Hasil Analisis DREAD Rating Scoring (lanjutan)

| | | |
|---|---|---|
| Threat 5. *Cross Site Scripting* | | |
| Affected user | Apabila penyerang berhasil, maka ini menjadi ancaman yang berbahaya karena target usernya bisa semua pengguna dan melakukan konfigurasi default | 3 |
| Discoverability | Tidak terdapat bug yang jelas dalam website | 1 |
| Threat 6. *Elevation Using Impersonation* | | |
| Dampak Ancaman | Penjelasan Penilaian | Nilai |
| Damage Potential | Potensi Penyerang dalam melakukan serangan Elevation Using Impersonation melalui Web Application berupa informasi sensitive. | 2 |
| Reproducibility | Serangan dapat dilakukan dengan jeda waktu tertentu (tidak setiap saat) | 2 |
| Exploitability | Dibutuhkan orang yang sangat terampil dan pengetahun mendalam dalam melakukan serangan karena dalam web application beberapa fitur telah disembunyikan seperti login page | 1 |
| Affected user | Presentase mempengaruhi pengguna sangat kecil | 1 |
| Discoverability | Kerentanan ada di bagian produk yang jarang digunakan, dan hanya sedikit pengguna yang dapat menemukannya. Perlu dilakukan pengujian terus menerus agar bisa melakukan serangan Elevation Using Impersonation. | 2 |
| Threat 7. *Login Page Process Memory Tampered* | | |
| Dampak Ancaman | Penjelasan Penilaian | Nilai |
| Damage Potential | Potensi Penyerang dalam melakukan Tampering melalui login page berupa otorisasi penuh | 3 |
| Reproducibility | Serangan sulit untuk direproduksi karena login page disembunyikan | 1 |
| Exploitability | Dibutuhkan orang yang sangat terampil dan pengetahun mendalam dalam melakukan serangan karena login page disembunyikan | 1 |

Tabel 4.8 Hasil Analisis DREAD Rating Scoring (lanjutan)

| | | |
|---|---|---|
| Threat 7. *Login Page Process Memory Tampered* | | |
| Affected user | Apabila penyerang berhasil, maka ini menjadi ancaman yang berbahaya karena target usernya bisa semua pengguna dan melakukan konfigurasi default | 3 |
| Discoverability | Tidak terdapat bug yang jelas dalam website | 1 |
| Threat 8. *Elevation Using Impersonation* | | |
| Dampak Ancaman | Penjelasan Penilaian | Nilai |
| Damage Potential | Potensi Penyerang dalam melakukan serangan Elevation Using Impersonation melalui Web API berupa informasi sensitive. | 2 |
| Reproducibility | Serangan dapat dilakukan dengan jeda waktu tertentu (tidak setiap saat) | 2 |
| Exploitability | Dibutuhkan orang yang sangat terampil dan pengetahun mendalam dalam melakukan serangan | 1 |
| Affected user | Presentase mempengaruhi pengguna sangat kecil | 1 |
| Discoverability | Kerentanan ada di bagian produk yang jarang digunakan, dan hanya sedikit pengguna yang dapat menemukannya. Perlu dilakukan pengujian terus menerus agar bisa melakukan serangan Elevation Using Impersonation pada WEB API. | 2 |
| Threat 9. *Web API Process Memory Tampered* | | |
| Dampak Ancaman | Penjelasan Penilaian | Nilai |
| Damage Potential | Potensi Penyerang dalam melakukan serangan Tampering melalui Web API berupa informasi sensitive. | 2 |
| Reproducibility | Serangan dapat dilakukan dengan jeda waktu tertentu (tidak setiap saat) | 2 |
| Exploitability | Dibutuhkan seorang programmer yang terampil untuk melakukan serangan | 2 |
| Affected user | Apabila penyerang berhasil, maka ini menjadi ancaman yang berbahaya karena target usernya bisa semua pengguna dan melakukan konfigurasi default | 3 |
| Discoverability | Tidak terdapat bug yang jelas dalam website | 1 |

Tabel 4.8 Hasil Analisis DREAD Rating Scoring (lanjutan)

| Threat 10. *Cross Site Scripting* | | |
|---|---|---|
| Dampak Ancaman | Penjelasan Penilaian | Nilai |
| Damage Potential | Potensi Penyerang dalam melakukan Tampering berupa CSS melalui Web Server dan Login page sangat kecil | 1 |
| Reproducibility | Serangan dapat dilakukan dengan jeda waktu tertentu (tidak setiap saat) | 2 |
| Exploitability | Dibutuhkan seorang programmer yang terampil untuk melakukan serangan | 2 |
| Affected user | Apabila penyerang berhasil, maka ini menjadi ancaman yang berbahaya karena target usernya bisa semua pengguna dan melakukan konfigurasi default | 3 |
| Discoverability | Tidak terdapat bug yang jelas dalam website | 1 |
| Threat 11. *Elevation Using Impersonation* | | |
| Dampak Ancaman | Penjelasan Penilaian | Nilai |
| Damage Potential | Potensi Penyerang dalam melakukan serangan Elevation of Privilege melalui Login page berupa informasi sensitive. | 2 |
| Reproducibility | Serangan dapat dilakukan dengan jeda waktu tertentu (tidak setiap saat) | 2 |
| Exploitability | Dibutuhkan orang yang sangat terampil dan pengetahun mendalam dalam melakukan serangan | 1 |
| Affected user | Presentase mempengaruhi pengguna sangat kecil | 1 |
| Discoverability | Kerentanan ada di bagian produk yang jarang digunakan, dan hanya sedikit pengguna yang dapat menemukannya. Perlu dilakukan pengujian terus menerus agar bisa melakukan serangan Elevation Using Impersonation pada Login page. | 2 |
| Threat 12. *Web Application Process Memory Tampered* | | |
| Dampak Ancaman | Penjelasan Penilaian | Nilai |
| Damage Potential | Potensi Penyerang dalam melakukan Tampering melalui Web Application berupa otorisasi penuh | 3 |

Tabel 4.8 Hasil Analisis DREAD Rating Scoring (lanjutan)

| | | |
|---|---|---|
| Threat 12. *Web Application Process Memory Tampered* | | |
| Reproducibility | Serangan dapat dilakukan dengan jeda waktu tertentu (tidak setiap saat) | 2 |
| Exploitability | Dibutuhkan seorang programmer yang terampil untuk melakukan serangan | 2 |
| Affected user | Apabila penyerang berhasil, maka ini menjadi ancaman yang berbahaya karena target usernya bisa semua pengguna dan melakukan konfigurasi default | 3 |
| Discoverability | Tidak terdapat bug yang jelas dalam website | 1 |
| Threat 13. *Elevation Using Impersonation* | | |
| Dampak Ancaman | Penjelasan Penilaian | Nilai |
| Damage Potential | Potensi Penyerang dalam melakukan serangan Elevetion of Privilege melalui WEB API berupa informasi sensitive. | 2 |
| Reproducibility | Serangan dapat dilakukan dengan jeda waktu tertentu (tidak setiap saat) | 2 |
| Exploitability | Dibutuhkan orang yang sangat terampil dan pengetahun mendalam dalam melakukan serangan | 1 |
| Affected user | Presentase mempengaruhi pengguna sangat kecil | 1 |
| Discoverability | Kerentanan ada di bagian produk yang jarang digunakan, dan hanya sedikit pengguna yang dapat menemukannya. Perlu dilakukan pengujian terus menerus agar bisa melakukan serangan Elevation Using Impersonation pada WEB API. | 2 |
| Threat 14. *Web API Process Memory Tampered* | | |
| Dampak Ancaman | Penjelasan Penilaian | Nilai |
| Damage Potential | Potensi Penyerang dalam melakukan serangan Tampering melalui WEB API berupa informasi sensitive. | 2 |
| Reproducibility | Serangan dapat dilakukan dengan jeda waktu tertentu (tidak setiap saat) | 2 |
| Exploitability | Dibutuhkan seorang programmer yang terampil untuk melakukan serangan | 2 |

Tabel 4.8 Hasil Analisis DREAD Rating Scoring (lanjutan)

| | | |
|---|---|---|
| Threat 14. *Web API Process Memory Tampered* | | |
| Affected user | Apabila penyerang berhasil, maka ini menjadi ancaman yang berbahaya karena target usernya bisa semua pengguna dan melakukan konfigurasi default | 3 |
| Discoverability | Kerentanan ada di bagian produk yang jarang digunakan, dan hanya sedikit pengguna yang dapat menemukannya. Perlu dilakukan pengujian terus menerus agar bisa melakukan serangan Tampering pada WEB API. | 2 |
| Threat 15. *Cross Site Scripting* | | |
| Dampak Ancaman | Penjelasan Penilaian | Nilai |
| Damage Potential | Potensi Penyerang dalam melakukan Tampering berupa CSS melalui Web Application | 1 |
| Reproducibility | Serangan dapat dilakukan dengan jeda waktu tertentu (tidak setiap saat) | 2 |
| Exploitability | Dibutuhkan seorang programmer yang terampil untuk melakukan serangan | 2 |
| Affected user | Apabila penyerang berhasil, maka ini menjadi ancaman yang berbahaya karena target usernya bisa semua pengguna dan melakukan konfigurasi default | 3 |
| Discoverability | Tidak terdapat bug yang jelas dalam website | 1 |
| Threat 16. *Elevation Using Impersonation* | | |
| Dampak Ancaman | Penjelasan Penilaian | Nilai |
| Damage Potential | Potensi Penyerang dalam melakukan serangan Elevetion of Privilege melalui WEB Application berupa informasi sensitive. | 2 |
| Reproducibility | Serangan dapat dilakukan dengan jeda waktu tertentu (tidak setiap saat) | 2 |
| Exploitability | Dibutuhkan orang yang sangat terampil dan pengetahun mendalam dalam melakukan serangan | 1 |
| Affected user | Presentase mempengaruhi pengguna sangat kecil | 1 |

Tabel 4.8 Hasil Analisis DREAD Rating Scoring (lanjutan)

| | | |
|---|---|---|
| Threat 16. *Elevation Using Impersonation* | | |
| Discoverability | Kerentanan ada di bagian produk yang jarang digunakan, dan hanya sedikit pengguna yang dapat menemukannya. Perlu dilakukan pengujian terus menerus agar bisa melakukan serangan Elevation of Privilege pada WEB Application. | 2 |
| Threat 17. *Web API Process Memory Tampered* | | |
| Dampak Ancaman | Penjelasan Penilaian | Nilai |
| Damage Potential | Potensi Penyerang dalam melakukan serangan Tampering melalui WEB API berupa informasi sensitive. | 2 |
| Reproducibility | Serangan dapat dilakukan dengan jeda waktu tertentu (tidak setiap saat) | 2 |
| Exploitability | Dibutuhkan seorang programmer yang terampil untuk melakukan serangan | 2 |
| Affected user | Apabila penyerang berhasil, maka ini menjadi ancaman yang berbahaya karena target usernya bisa semua pengguna dan melakukan konfigurasi default | 3 |
| Discoverability | Kerentanan ada di bagian produk yang jarang digunakan, dan hanya sedikit pengguna yang dapat menemukannya. Perlu dilakukan pengujian terus menerus agar bisa melakukan serangan Tampering pada WEB API. | 2 |
| Threat 18. *Elevation Using Impersonation* | | |
| Dampak Ancaman | Penjelasan Penilaian | Nilai |
| Damage Potential | Potensi Penyerang dalam melakukan serangan Elevetion of Privilege melalui WEB Service berupa informasi sensitive. | 2 |
| Reproducibility | Serangan dapat dilakukan dengan jeda waktu tertentu (tidak setiap saat) | 2 |
| Exploitability | Dibutuhkan orang yang sangat terampil dan pengetahun mendalam dalam melakukan serangan | 1 |
| Affected user | Presentase mempengaruhi pengguna sangat kecil | 1 |

Tabel 4.8 Hasil Analisis DREAD Rating Scoring (lanjutan)

| | | |
|---|---|---|
| Threat 18. *Elevation Using Impersonation* | | |
| Discoverability | Kerentanan ada di bagian produk yang jarang digunakan, dan hanya sedikit pengguna yang dapat menemukannya. Perlu dilakukan pengujian terus menerus agar bisa melakukan serangan Elevation of Privilege pada WEB Service. | 2 |
| Threat 19. *Web Service Process Memory Tampered* | | |
| Dampak Ancaman | Penjelasan Penilaian | Nilai |
| Damage Potential | Potensi Penyerang dalam melakukan serangan Tampered melalui WEB Service berupa informasi sensitive. | 2 |
| Reproducibility | Serangan dapat dilakukan dengan jeda waktu tertentu (tidak setiap saat) | 2 |
| Exploitability | Dibutuhkan seorang programmer yang terampil untuk melakukan serangan | 2 |
| Affected user | Apabila penyerang berhasil, maka ini menjadi ancaman yang berbahaya karena target usernya bisa semua pengguna dan melakukan konfigurasi default | 3 |
| Discoverability | Kerentanan ada di bagian produk yang jarang digunakan, dan hanya sedikit pengguna yang dapat menemukannya. Perlu dilakukan pengujian terus menerus agar bisa melakukan serangan Tampered pada WEB Service. | 2 |
| Threat 20. *Elevation Using Impersonation* | | |
| Dampak Ancaman | Penjelasan Penilaian | Nilai |
| Damage Potential | Potensi Penyerang dalam melakukan serangan Elevetion of Privilege melalui WEB API berupa informasi sensitive. | 2 |
| Reproducibility | Serangan dapat dilakukan dengan jeda waktu tertentu (tidak setiap saat) | 2 |
| Exploitability | Dibutuhkan orang yang sangat terampil dan pengetahun mendalam dalam melakukan serangan | 1 |
| Affected user | Presentase mempengaruhi pengguna sangat kecil | 1 |

Tabel 4.8 Hasil Analisis DREAD Rating Scoring (lanjutan)

| | | |
|---|---|---|
| Threat 20. *Elevation Using Impersonation* | | |
| Discoverability | Kerentanan ada di bagian produk yang jarang digunakan, dan hanya sedikit pengguna yang dapat menemukannya. Perlu dilakukan pengujian terus menerus agar bisa melakukan serangan Elevation of Privilege pada WEB API. | 2 |
| Threat 21. *Spoofing of Destination Data Store SQL Database* | | |
| Dampak Ancaman | Penjelasan Penilaian | Nilai |
| Damage Potential | Potensi Penyerang dalam melakukan Spoofing melalui Database berupa otorisasi penuh | 3 |
| Reproducibility | Serangan dapat dilakukan dengan jeda waktu tertentu (tidak setiap saat) | 2 |
| Exploitability | Dibutuhkan orang yang sangat terampil dan pengetahun mendalam dalam melakukan serangan. Karena database telah dienkripsi | 1 |
| Affected user | Apabila penyerang berhasil, maka ini menjadi ancaman yang berbahaya karena target usernya bisa semua pengguna dan melakukan konfigurasi default | 3 |
| Discoverability | Tidak terdapat bug yang jelas dalam website | 1 |
| Threat 22. *Potential SQL Injection Vulnerability for SQL Database* | | |
| Dampak Ancaman | Penjelasan Penilaian | Nilai |
| Damage Potential | Potensi Penyerang dalam melakukan serangan Tampering berupa SQL Injection melalui WEB API berupa informasi sensitive. | 2 |
| Reproducibility | Serangan dapat dilakukan dengan jeda waktu tertentu (tidak setiap saat) | 2 |
| Exploitability | Dibutuhkan orang yang sangat terampil dan pengetahun mendalam dalam melakukan serangan. Karena database telah dienkripsi | 1 |
| Affected user | Presentase mempengaruhi pengguna sangat kecil | 1 |
| Discoverability | Tidak terdapat bug yang jelas dalam website | 1 |

Tabel 4.8 Hasil Analisis DREAD Rating Scoring (lanjutan)

| Threat 23. *Potential Excessive Resource Consumption for Web Service or SQL Database* | | |
|---|---|---|
| Dampak Ancaman | Penjelasan Penilaian | Nilai |
| Damage Potential | Potensi Penyerang dalam melakukan Denial of Service (DoS) pada database sangat kecil | 1 |
| Reproducibility | Serangan sulit untuk direproduksi karena login page disembunyikan dan database telah dienskripsi | 1 |
| Exploitability | Dibutuhkan orang yang sangat terampil dan pengetahun mendalam dalam melakukan serangan. Karena database telah dienkripsi | 1 |
| Affected user | Presentase mempengaruhi pengguna sangat kecil | 1 |
| Discoverability | Tidak terdapat bug yang jelas dalam website | 1 |
| Threat 24. *Spoofing of Source Data Store SQL Database* | | |
| Dampak Ancaman | Penjelasan Penilaian | Nilai |
| Damage Potential | Potensi Penyerang dalam melakukan Spoofing melalui Database berupa otorisasi penuh | 3 |
| Reproducibility | Serangan dapat dilakukan dengan jeda waktu tertentu (tidak setiap saat) | 2 |
| Exploitability | Dibutuhkan orang yang sangat terampil dan pengetahun mendalam dalam melakukan serangan. Karena database telah dienkripsi | 1 |
| Affected user | Apabila penyerang berhasil, maka ini menjadi ancaman yang berbahaya karena target usernya bisa semua pengguna dan melakukan konfigurasi default | 3 |
| Discoverability | Tidak terdapat bug yang jelas dalam website | 1 |
| Threat 25. *Weak Access Control for a Resource* | | |
| Dampak Ancaman | Penjelasan Penilaian | Nilai |
| Damage Potential | Potensi Penyerang dalam melakukan serangan Information Disclosure melalui Database berupa informasi sensitive. | 2 |
| Reproducibility | Serangan dapat dilakukan dengan jeda waktu tertentu (tidak setiap saat) | 2 |

Tabel 4.8 Hasil Analisis DREAD Rating Scoring (lanjutan)

| Threat 25. *Weak Access Control for a Resource* | | |
|---|---|---|
| Exploitability | Dibutuhkan seorang programmer yang terampil untuk melakukan serangan | 2 |
| Affected user | Apabila penyerang berhasil, maka ini menjadi ancaman yang cukup berbahaya karena target usernya hanya Sebagian pengguna dan melakukan konfigurasi non-default | 2 |
| Discoverability | Tidak terdapat bug yang jelas dalam website | 1 |

Tabel 0.6 Rekapitulasi DREAD Rating Scoring

| id | Threat | D | R | E | A | D | Total | Rating |
|---|---|---|---|---|---|---|---|---|
| 1. | Spoofing the Browser External Entity | 3 | 2 | 1 | 3 | 1 | 10 | Medium |
| 2. | Cross Site Scripting | 1 | 2 | 2 | 3 | 1 | 9 | Medium |
| 3. | Elevation Using Impersonation | 2 | 2 | 1 | 1 | 2 | 8 | Medium |
| 4. | Spoofing the Browser External Entity | 3 | 2 | 1 | 3 | 1 | 10 | Medium |
| 5. | Cross Site Scripting | 1 | 2 | 2 | 3 | 1 | 9 | Medium |
| 6. | Elevation Using Impersonation | 2 | 2 | 1 | 1 | 2 | 8 | Medium |
| 7. | Login Page Process Memory Tampered | 3 | 1 | 1 | 3 | 1 | 9 | Medium |
| 8. | Elevation Using Impersonation | 2 | 2 | 1 | 1 | 2 | 8 | Medium |
| 9. | Web API Process Memory Tampered | 2 | 2 | 2 | 3 | 2 | 11 | High |
| 10. | Cross Site Scripting | 1 | 2 | 2 | 3 | 1 | 9 | Medium |
| 11. | Elevation Using Impersonation | 2 | 2 | 1 | 1 | 2 | 8 | Medium |
| 12. | Web Application Process Memory Tampered | 3 | 2 | 2 | 3 | 1 | 11 | High |
| 13. | Elevation Using Impersonation | 2 | 2 | 1 | 1 | 2 | 8 | Medium |
| 14. | Web API Process Memory Tampered | 2 | 2 | 2 | 3 | 2 | 11 | High |
| 15. | Cross Site Scripting | 1 | 2 | 2 | 3 | 1 | 9 | Medium |

Tabel 4.9 Rekapitulasi DREAD Rating Scoring

| id | Threat | D | R | E | A | D | Total | Rating |
|---|---|---|---|---|---|---|---|---|
| 16. | Elevation Using Impersonation | 2 | 2 | 1 | 1 | 2 | 8 | Medium |
| 17. | Web API Process Memory Tampered | 2 | 2 | 2 | 3 | 2 | 11 | High |
| 18. | Elevation Using Impersonation | 2 | 2 | 1 | 1 | 2 | 8 | Medium |
| 19. | Web Service Process Memory Tampered | 2 | 2 | 2 | 3 | 2 | 11 | High |
| 20. | Elevation Using Impersonation | 2 | 2 | 1 | 1 | 2 | 8 | Medium |
| 21. | Spoofing of Destination Data Store SQL Database | 3 | 2 | 1 | 3 | 1 | 10 | Medium |
| 22. | Potential SQL Injection Vulnerability for SQL Database | 2 | 2 | 1 | 1 | 1 | 7 | Medium |
| 23. | Potential Excessive Resource Consumption for Web Service or SQL Database | 1 | 1 | 1 | 1 | 1 | 5 | Low |
| 24. | Spoofing of Source Data Store SQL Database | 3 | 2 | 1 | 3 | 1 | 10 | Medium |
| 25. | Weak Access Control for a Resource | 2 | 2 | 2 | 2 | 1 | 9 | Medium |

Rating : (11-15) High; (6-10) Medium; (1-5) Low.

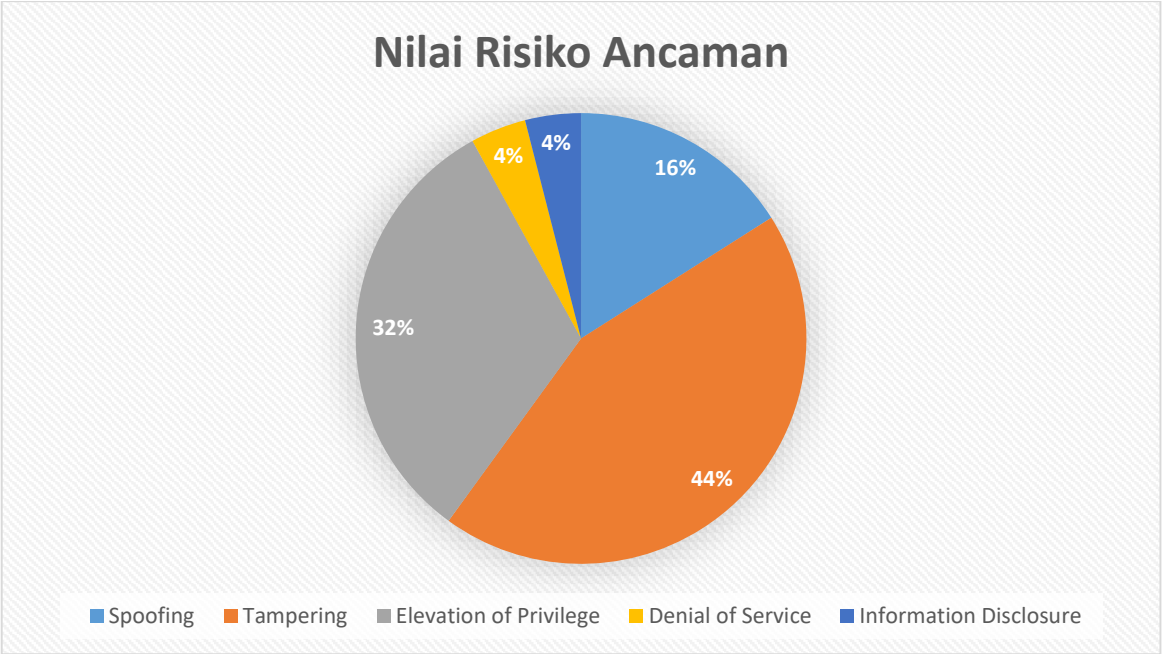
## 4.5 Nilai Risiko Ancaman

Untuk mengetahui Nilai Risiko Ancaman maka digunakan Rumus :

**Risk = Probability * Damage Potential (10)**

Tabel 0.7 Nilai Risiko Ancaman

| No. | Jenis Ancaman | Probability | Damage Potential | Nilai Risiko Ancaman |
|---|---|---|---|---|
| 1. | Spoofing | 4 | 10 | 40 |
| 2. | Tampering | 11 | 10 | 110 |
| 3. | Elevation of Privilege | 8 | 10 | 80 |
| 4. | Denial of Service | 1 | 10 | 10 |
| 5. | Information Disclosure | 1 | 10 | 10 |




Gambar 7 Grafik Nilai Risiko Ancaman

### 4.6 Mitigasi Ancaman

Dalam melakukan mitigasi ancaman dilakukan langkah analisa terhadap 28 serangan yang terbagi kedalam lima jenis serangan yaitu : Spoofing (4), Tampering (11), Elevation of Privilege (8), Denial of Service (1) dan Information Disclosure (1). Mitigasi dilakukan dengan mendeskripsikan satu per satu potensi ancaman dengan beberapa kategori yaitu : deskripsi ancaman, target ancaman, tingkat risiko, teknik serangan dan mitigasi (penanggulangan). Berikut ini adalah mitigasi terhadap risiko ancaman yang ada :

Tabel 0.8 Threat 1

| **Deskripsi Ancaman** | **Spoofing the Browser External Entity** |
|---|---|
| Target Ancaman | Browser, Login Page |
| Tingkat Risiko | Medium |
| Teknik Serangan | Penyerang bisa saja melakukan spoofing melalui browser untuk mendapatkan hak akses terhadap halaman login. |
| Mitigasi (Penanggulangan) | Mempertimbangkan untuk menggunakan standar otentifikasi untuk mengidentifikasi entitas eksternal |

Tabel 0.9 Threat 2

| **Deskripsi Ancaman** | **Cross Site Scripting** |
|---|---|
| Target Ancaman | Web Server, Login Page |

Tabel 4.12 Threat 2 (lanjutan)

| **Deskripsi Ancaman** | **Cross Site Scripting** |
|---|---|
| Tingkat Risiko | Medium |
| Teknik Serangan | web server pada halaman login menjadi sasaran untuk melakukan serangan CSS. |
| Mitigasi (Penanggulangan) | Mengkonfigurasi system input secara baik, menggunakan fitur penanggulangan seperti Global XSS Filtering, validasi input dan output. |

Tabel 0.10 Threat 3

| **Deskripsi Ancaman** | **Elevation Using Impersonation** |
|---|---|
| Target Ancaman | Login Page |
| Tingkat Risiko | Medium |
| Teknik Serangan | Login Page mungkin dapat meniru konteks Browser untuk mendapatkan hak istimewa tambahan. |
| Mitigasi (Penanggulangan) | Melakukan pengamanan data user. |

Tabel 0.11 Threat 4

| **Deskripsi Ancaman** | **Spoofing the Browser External Entity** |
|---|---|
| Target Ancaman | Browser, Web Application |
| Tingkat Risiko | Medium |
| Teknik Serangan | Penyerang bisa saja melakukan spoofing melalui browser untuk mendapatkan hak akses terhadap Web Application |
| Mitigasi (Penanggulangan) | Mempertimbangkan untuk menggunakan standar otentifikasi untuk mengidentifikasi entitas eksternal |

Tabel 0.12 Threat 5

| **Deskripsi Ancaman** | **Cross Site Scripting** |
|---|---|
| Target Ancaman | Web Server, Web Application |
| Tingkat Risiko | Medium |
| Teknik Serangan | Web Application menjadi sasaran untuk melakukan serangan CSS. |

Tabel 4.15 Threat 5 (lanjutan)

| **Deskripsi Ancaman** | **Cross Site Scripting** |
|---|---|
| Mitigasi (Penanggulangan) | Mengkonfigurasi system input secara baik, menggunakan fitur penanggulangan seperti Global XSS Filtering, validasi input dan output. |

Tabel 0.13 Threat 6

| **Deskripsi Ancaman** | **Elevation Using Impersonation** |
|---|---|
| Target Ancaman | Web Application |
| Tingkat Risiko | Medium |
| Teknik Serangan | Web Application mungkin dapat meniru konteks Browser untuk mendapatkan hak istimewa tambahan. |
| Mitigasi (Penanggulangan) | Melakukan pengamanan data user. |

Tabel 0.14 Threat 7

| **Deskripsi Ancaman** | **Login Page Process Memory Tampered** |
|---|---|
| Target Ancaman | Login Page |
| Tingkat Risiko | Medium |
| Teknik Serangan | Jika Halaman Login diberi akses ke memori, seperti memori atau pointer bersama, atau diberi kemampuan untuk mengontrol apa yang dijalankan API Web (misalnya, meneruskan kembali pointer fungsi.), Halaman Login dapat merusak Web API. |
| Mitigasi (Penanggulangan) | Mempertimbangkan apakah fungsi halaman login dapat bekerja dengan lebih sedikit akses ke memori, seperti meneruskan data daripada pointer. Salin data yang disediakan, lalu validasi. |

Tabel 0.15 Threat 8

| **Deskripsi Ancaman** | **Elevation Using Impersonation** |
|---|---|
| Target Ancaman | Web API |
| Tingkat Risiko | Medium |
| Teknik Serangan | Web API mungkin dapat meniru konteks Halaman Login untuk mendapatkan hak istimewa tambahan. |

Tabel 4.18 Threat 8 (lanjutan)

| **Deskripsi Ancaman** | **Elevation Using Impersonation** |
|---|---|
| Mitigasi (Penanggulangan) | Melakukan pengamanan data user dan database. |

Tabel 0.16 Threat 9

| **Deskripsi Ancaman** | **Web API Process Memory Tampered** |
|---|---|
| Target Ancaman | Web API |
| Tingkat Risiko | High |
| Teknik Serangan | Jika Web API diberi akses ke memori, seperti memori atau pointer bersama, atau diberi kemampuan untuk mengontrol apa yang dijalankan Halaman Login (misalnya, meneruskan kembali pointer fungsi.), Web API dapat merusak Halaman Login. |
| Mitigasi (Penanggulangan) | Mempertimbangkan apakah fungsi Web API dapat bekerja dengan lebih sedikit akses ke memori, seperti meneruskan data daripada pointer. Salin data yang disediakan, lalu validasi. |

Tabel 0.17 Threat 10

| **Deskripsi Ancaman** | **Cross Site Scripting** |
|---|---|
| Target Ancaman | Web Server, Login Page |
| Tingkat Risiko | Medium |
| Teknik Serangan | Login Page menjadi sasaran untuk melakukan serangan CSS. |
| Mitigasi (Penanggulangan) | Mengkonfigurasi system input secara baik, menggunakan fitur penanggulangan seperti Global XSS Filtering, validasi input dan output. |

Tabel 0.18 Threat 11

| **Deskripsi Ancaman** | **Elevation Using Impersonation** |
|---|---|
| Target Ancaman | Login Page |
| Tingkat Risiko | Medium |
| Teknik Serangan | Halaman Login mungkin dapat meniru konteks Web API untuk mendapatkan hak istimewa tambahan. |
| Mitigasi (Penanggulangan) | Melakukan pengamanan data user dan database. |

Tabel 0.19 Threat 12

| **Deskripsi Ancaman** | **Web Application Process Memory Tampered** |
|---|---|
| Target Ancaman | Web Application |
| Tingkat Risiko | High |
| Teknik Serangan | Jika Web Application diberi akses ke memori, seperti memori atau pointer bersama, atau diberi kemampuan untuk mengontrol apa yang dijalankan Web API (misalnya, meneruskan kembali penunjuk fungsi.), Web Application dapat merusak Web API. |
| Mitigasi (Penanggulangan) | Mempertimbangkan apakah fungsi Web Application dapat bekerja dengan lebih sedikit akses ke memori, seperti meneruskan data daripada pointer. Salin data yang disediakan, lalu validasi. |

Tabel 0.20 Threat 13

| **Deskripsi Ancaman** | **Elevation Using Impersonation** |
|---|---|
| Target Ancaman | Web API |
| Tingkat Risiko | Medium |
| Teknik Serangan | Web API mungkin dapat meniru konteks Web Application untuk mendapatkan hak istimewa tambahan. |
| Mitigasi (Penanggulangan) | Melakukan pengamanan data user dan database. |

Tabel 0.21 Threat 14

| **Deskripsi Ancaman** | **Web API Process Memory Tampered** |
|---|---|
| Target Ancaman | Web API |
| Tingkat Risiko | High |
| Teknik Serangan | Jika Web API diberi akses ke memori, seperti memori atau pointer bersama, atau diberi kemampuan untuk mengontrol apa yang dijalankan Aplikasi Web (misalnya, meneruskan kembali pointer fungsi.), Web API dapat merusak Web Application. |
| Mitigasi (Penanggulangan) | Mempertimbangkan apakah fungsi Web API dapat bekerja dengan lebih sedikit akses ke memori, seperti meneruskan data daripada pointer. Salin data yang disediakan, lalu validasi. |

Tabel 0.22 Threat 15

| **Deskripsi Ancaman** | **Cross Site Scripting** |
|---|---|
| Target Ancaman | Web Application |
| Tingkat Risiko | Medium |
| Teknik Serangan | Web Application menjadi sasaran untuk melakukan serangan CSS. |
| Mitigasi (Penanggulangan) | Mengkonfigurasi system input secara baik, menggunakan fitur penanggulangan seperti Global XSS Filtering, validasi input dan output. |

Tabel 0.23 Threat 16

| **Deskripsi Ancaman** | **Elevation Using Impersonation** |
|---|---|
| Target Ancaman | Web Application |
| Tingkat Risiko | Medium |
| Teknik Serangan | Web Application mungkin dapat meniru konteks Web API untuk mendapatkan hak istimewa tambahan. |
| Mitigasi (Penanggulangan) | Melakukan pengamanan data user dan database. |

Tabel 0.24 Threat 17

| **Deskripsi Ancaman** | **Web API Process Memory Tampered** |
|---|---|
| Target Ancaman | Web API |
| Tingkat Risiko | High |
| Teknik Serangan | Jika Web API diberi akses ke memori, seperti memori atau pointer bersama, atau diberi kemampuan untuk mengontrol apa yang dijalankan Layanan Web (misalnya, meneruskan kembali penunjuk fungsi.), Web API dapat merusak Layanan Web. |
| Mitigasi (Penanggulangan) | Mempertimbangkan apakah fungsi Web API dapat bekerja dengan lebih sedikit akses ke memori, seperti meneruskan data daripada pointer. Salin data yang disediakan, lalu validasi. |

Tabel 0.25 Threat 18

| **Deskripsi Ancaman** | **Elevation Using Impersonation** |
|---|---|
| Target Ancaman | Web Service |
| Tingkat Risiko | Medium |
| Teknik Serangan | Web Service mungkin dapat meniru konteks Web API untuk mendapatkan hak istimewa tambahan. |
| Mitigasi (Penanggulangan) | Melakukan pengamanan data user dan database. |

Tabel 0.26 Threat 19

| **Deskripsi Ancaman** | **Web Service Process Memory Tampered** |
|---|---|
| Target Ancaman | Web Service |
| Tingkat Risiko | High |
| Teknik Serangan | Jika Web Service diberi akses ke memori, seperti memori atau pointer bersama, atau diberi kemampuan untuk mengontrol apa yang dijalankan Web API (misalnya, meneruskan kembali penunjuk fungsi.), Layanan Web dapat merusak Web API. |
| Mitigasi (Penanggulangan) | Mempertimbangkan apakah fungsi Web Service dapat bekerja dengan lebih sedikit akses ke memori, seperti meneruskan data daripada pointer. Salin data yang disediakan, lalu validasi. |

Tabel 0.27 Threat 20

| **Deskripsi Ancaman** | **Elevation Using Impersonation** |
|---|---|
| Target Ancaman | Web API |
| Tingkat Risiko | Medium |
| Teknik Serangan | Web API mungkin dapat meniru konteks Layanan Web untuk mendapatkan hak istimewa tambahan. |
| Mitigasi (Penanggulangan) | Melakukan pengamanan data user dan database. |

Tabel 0.28 Threat 21

| **Deskripsi Ancaman** | **Spoofing of Destination Data Store SQL Database** |
|---|---|
| Target Ancaman | Database |

Tabel 4.31 Threat 21

| **Deskripsi Ancaman** | **Spoofing of Destination Data Store SQL Database** |
|---|---|
| Tingkat Risiko | Medium |
| Teknik Serangan | Database dapat dipalsukan oleh penyerang dan ini dapat menyebabkan data ditulis ke target penyerang, bukan ke Database. |
| Mitigasi (Penanggulangan) | Pertimbangkan untuk menggunakan mekanisme otentikasi standar untuk mengidentifikasi penyimpanan data tujuan. |

Tabel 0.29 Threat 22

| **Deskripsi Ancaman** | **Potential SQL Injection Vulnerability for SQL Database** |
|---|---|
| Target Ancaman | Database |
| Tingkat Risiko | Medium |
| Teknik Serangan | SQL injection adalah serangan di mana kode berbahaya dimasukkan ke dalam string yang kemudian diteruskan ke contoh SQL Server untuk parsing dan eksekusi. Setiap prosedur yang menyusun pernyataan SQL harus ditinjau untuk kerentanan injeksi karena SQL Server akan menjalankan semua kueri yang valid secara sintaksis yang diterimanya. Bahkan data berparameter dapat dimanipulasi oleh penyerang yang terampil dan gigih. Membuat TLS (Transport Layer Security) untuk mencegah terjadinya serangan SQL injection |
| Mitigasi (Penanggulangan) | Penyesuain input box dan membatasi input seperti pembatasan karakter. Melakukan filter terhadap user (validation input), tidak menggunakan filter standar SQL dan melakukan setting Privilege |

Tabel 0.30 Threat 23

| **Deskripsi Ancaman** | **Potential Excessive Resource Consumption for Web Service or SQL Database** |
|---|---|
| Target Ancaman | Database |
| Tingkat Risiko | Low |

Tabel 4.33 Threat 23

| **Deskripsi Ancaman** | **Potential Excessive Resource Consumption for Web Service or SQL Database** |
|---|---|
| Teknik Serangan | Apakah Layanan Web atau Database SQL mengambil langkah-langkah eksplisit untuk mengontrol konsumsi sumber daya? Serangan konsumsi sumber daya bisa jadi sulit untuk ditangani, dan ada kalanya masuk akal untuk membiarkan OS melakukan pekerjaan itu. |
| Mitigasi (Penanggulangan) | Berhati-hatilah agar permintaan resource tidak mengalami deadlock dan timeout. |

Tabel 0.31 Threat 24

| **Deskripsi Ancaman** | **Spoofing of Source Data Store SQL Database** |
|---|---|
| Target Ancaman | Database |
| Tingkat Risiko | Medium |
| Teknik Serangan | Database dapat dipalsukan oleh penyerang dan ini dapat menyebabkan data yang salah dikirim ke Layanan Web. |
| Mitigasi (Penanggulangan) | Pertimbangkan untuk menggunakan mekanisme otentikasi standar untuk mengidentifikasi penyimpanan data sumber. |

Tabel 0.32 Threat 25

| **Deskripsi Ancaman** | **Weak Access Control for a Resource** |
|---|---|
| Target Ancaman | Database |
| Tingkat Risiko | Medium |
| Teknik Serangan | Perlindungan data yang tidak tepat dari Database SQL dapat memungkinkan penyerang membaca informasi yang tidak dimaksudkan untuk pengungkapan. |
| Mitigasi (Penanggulangan) | Tinjau authorization settings. |

Langkah mitigasi terhadap jenis potensi ancaman dapat dilakukan untuk mencegah terjadinya serangan pada web e-monitoring yaitu dengan :

a. Menggunakan standar otentifikasi untuk mengidentifikasi entitas eksternal dan pengamanan user data.
b. Mengkonfigurasi system input secara baik, menggunakan fitur penanggulangan seperti Global XSS Filtering, validasi input dan output untuk menanggulangi serangan CSS.
c. Mempertimbangkan apakah fungsi Login Page, Web API, Web Application, Web Service dapat bekerja dengan lebih sedikit akses ke memori, seperti meneruskan data daripada pointer. Salin data yang disediakan, lalu validasi.
d. Berhati-hatilah agar permintaan resource tidak mengalami deadlock dan timeout.
e. Penyesuain input box dan membatasi input seperti pembatasan karakter. Melakukan filter terhadap user (validation input), tidak menggunakan filter standar SQL dan melakukan setting Privilege serta menggunaan spam filter.
f. Melakukan pengamanan data user dan database (update sandi secara berkala).

## 4.7 Keterbatasan Penelitian

Penelitian ini memiliki keterbatasan antara lain :

a. Hanya berlaku untuk system e-government yaitu e-monitoring Kabupaten Purbalingga (https://monitoringwebsite.purbalinggakab.go.id/).
b. Evaluasi keamanan system menggukan metode Security Development Lifecycle (SDL) yang didalamnya memiliki tahapan analisis STRIDE dan DREAD.
c. Setiap prespektif peneliti dalam memodelkan sebuah system akan menghasilkan report dan analisis yang berbeda

# BAB V
# Kesimpulan dan Saran

## 5.1 Kesimpulan

Kesimpulan yang dapat diambil berdasarkan hasil evaluasi keamanan sistem e-government yaitu: Karakteristik system e-government dapat dievaluasi keamanan sistemnya menggunakan metode Security Development Lifecycle (SDL) dengan mengikuti tahapan yang ada. Berdasarkan hasil pemodelan dan pengujian system e-government (website e-monitoring) terdapat 5 kategori potensi risiko ancaman, namun hal itu masih bisa dilakukan langkah mitigasi terhadap potensi risiko ancaman yang mungkin akan terjadi. Adapun langkah mitigasi dapat dilakukan prioritas perbaikan system berdasarkan tingkat ancaman tertinggi hingga terkecil. Beberapa langkah mitigasi ancaman juga sudah diterapkan pada web e-monitoring untuk mengamankan data yang ada seperti pencegahan terhadap DDos menggunakan Cloudflare, menyembunyikan login page dan melakukan enkripsi terhadap direktori yang ada. Pada dasarnya potensi ancaman terhadap sebuah system dapat diminimalisir dengan melakukan perbaikan system secara berkala dan selalu dilakukan evaluasi serta pengembangan.

## 5.2 Saran

Dalam melakukan evaluasi keamanan sebuah system khususnya menggunakan Metode Security Development Lifecycle (SDL) yang didalamnya terdapat tahapan analisis menggunakan STRIDE dan DREAD perlu memperhatikan desain pada pemodelan yang sesuai dengan system yang berjalan agar dapat menghasilkan hasil Report yang lebih akurat. Karena masing-masing system memiliki desain yang berbeda dan akan menghasilkan report yang berbeda pula. Dalam melakukan pengembangan evaluasi system disarankan untuk menambah metode yang berbeda seperti OWASP, TAM, ASVS, CWSS serta tools yang berbeda untuk menganalisa keamanan sebuah system e-government.

# Daftar Pustaka


Abomhara, M., Gerdes, M., & Køien, G. M. (2015). A stride-based threat model for telehealth systems. *Norsk Informasjonssikkerhetskonferanse (NISK)*, *8*(1), 82–96.

Ali, O. A., Wahbi, T. M., & Osman, I. M. (2016). E-government Security Models. *International Journal of Computer Applications Technology and Research*, *5*(7), 439–442. https://doi.org/10.7753/ijcatr0507.1004

G. Hassan, R., & O. Khalifa, O. (2016). E-Government - an Information Security Perspective. *International Journal of Computer Trends and Technology*, *36*(1), 1–9. https://doi.org/10.14445/22312803/ijctt-v36p101

Ge, M., Hong, J. B., Guttmann, W., & Kim, D. S. (2017). A framework for automating security analysis of the internet of things. *Journal of Network and Computer Applications*, *83*(November 2016), 12–27. https://doi.org/10.1016/j.jnca.2017.01.033

Harrison, S., Tzounis, A., Maglaras, L., Siewe, F., Smith, R., & Janicke, H. (2016). A Security Evaluation Framework for U.K. E-Government Services Agile Software Development. *International Journal of Network Security & Its Applications*, *8*(2), 51–69. https://doi.org/10.5121/ijnsa.2016.8204

Hayati. (2018). *Implementasi E-Government Pada Pemerintah Daerah Kabupaten Bantul Yogyakarta*. *December*, 1–23.

Hussain, S., Kamal, A., Ahmad, S., Rasool, G., & Iqbal, S. (2014). Threat Modelling Methodologies: a Survey. *Sci.Int.(Lahore)*, *26*(4), 1607–1609.

Irani, Z., Love, P. E. D., & Jones, S. (2008). Learning lessons from evaluating eGovernment: Reflective case experiences that support transformational government. *Journal of Strategic Information Systems*, *17*(2), 155–164. https://doi.org/10.1016/j.jsis.2007.12.005

Jouini, M., Rabai, L. B. A., & Aissa, A. Ben. (2014). Classification of security threats in information systems. *Procedia Computer Science*, *32*, 489–496. https://doi.org/10.1016/j.procs.2014.05.452

Kim, K., Cho, K., Lim, J., Jung, Y. H., Sung, M. S., Kim, S. B., & Kim, H. K. (2020). What's your protocol: Vulnerabilities and security threats related to Z-Wave protocol. *Pervasive and Mobile Computing*, *66*(2018), 101211. https://doi.org/10.1016/j.pmcj.2020.101211

Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current

literature: A reference framework. *Computers in Industry*, *103*, 97–110. https://doi.org/10.1016/j.compind.2018.09.004

Macher, G., Armengaud, E., Brenner, E., & Kreiner, C. (2016). Threat and Risk Assessment Methodologies in the Automotive Domain. *Procedia Computer Science*, *83*, 1288–1294. https://doi.org/10.1016/j.procs.2016.04.268

Maheshwari, V., & Prasanna, M. (2017). Integrating risk assessment and threat modeling within SDLC process. *Proceedings of the International Conference on Inventive Computation Technologies, ICICT 2016*, *1*(March). https://doi.org/10.1109/INVENTIVE.2016.7823275

Meimer, J.D, Mackman, A, Wastell B. (2010). Chapter 3 – Threat Modeling https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648644(v=pandp.10)?redirectedfrom=MSDN (diakses tanggal 4 Januari 2020).

Omotosho, A, … B. A. H.-J. of A. (2019). undefined. (n.d.). Threat modeling of Internet of Things health devices. Taylor & Francis. Retrieved January 6, 2020, from https://www.tandfonline.com/doi/abs/10.1080/19361610.2019.1545278

Pandya, D. C., & Patel, D. N. J. (2017). Study and analysis of E-Governance Information Security (InfoSec) in Indian Context. *IOSR Journal of Computer Engineering*, *19*(01), 04–07. https://doi.org/10.9790/0661-1901040407

Pete, B. (2019). *Risk Management & Governance Knowlaege Area*.

Salsabila, L., & Purnomo, E. P. (2017). Establishing and Implementing Good Practices E-Government (A Case Study : e-Government Implementation between Korea and Indonesia). In *Asean/ Asia Academic Society International Conference (Aasic)* (Vol. 5, pp. 221–229).

Satapathy, S. R. (2014). *Threat Modeling in Web Applications*. *June*, 87. http://ethesis.nitrkl.ac.in/5793/1/E-9.pdf

Venkatasen, M., & Mani, P. (2018). A risk-centric defensive architecture for threat modelling in e-government application. *Electronic Government*, *14*(1), 16–31. https://doi.org/10.1504/EG.2018.089537

Wuyts, K., Scandariato, R., & Joosen, W. (2014). Empirical evaluation of a privacy-focused threat modeling methodology. *Journal of Systems and Software*, *96*, 122–138. https://doi.org/10.1016/j.jss.2014.05.075

# LAMPIRAN A

Tabel 0.1 Website Organisasi Perangkat Daerah (OPD)

| No. | Nama Website | Link |
|---|---|---|
| 1. | Dinas Ketahanan Pangan dan Perikanan | https://dkpp.purbalinggakab.go.id/ |
| 2. | Dinas Komunikasi dan Informatika | https://dinkominfo.purbalinggakab.go.id/ |
| 3. | Dinas Koperasi dan Usaha Kecil Menengah | http://dinkopukm.purbalinggakab.go.id |
| 4. | Dinas Perhubungan | http://dinhub.purbalinggakab.go.id |
| 5. | Dinas Pertanian | http://dinpertan.purbalinggakab.go.id |
| 6. | Dinas Perumahan dan Pemukiman | http://dinrumkim.purbalinggakab.go.id |
| 7. | Dinas Perindustrian dan Perdagangan | http://dinperindag.purbalinggakab.go.id |
| 8. | Inspektorat | https://inspektorat.purbalinggakab.go.id |
| 9. | Sekretariat DPRD | http://sekretariatdprd.purbalinggakab.go.id |
| 10. | Satuan Polisi Pamong Praja | http://satpolpp.purbalinggakab.go.id |
| 11. | Badan Kepegawaian, Pendidikan dan Penelitian Daerah | http://bkppd.purbalinggakab.go.id |
| 12. | Website Bupati | http://bupati.purbalinggakab.go.id |
| 13. | Dinas Kearsipan dan Perpustakaan | http://dinarspus.purbalinggakab.go.id |
| 14. | Dinas Kependudukan dan Catatan Sipil | http://dinpendukcapil.purbalinggakab.go.id |
| 15. | Dinas Kesehatan | http://dinkes.purbalinggakab.go.id |
| 16. | Dinas Lingkungan Hidup | http://dlh.purbalinggakab.go.id |
| 17. | Dinas Pekerjaan Umum dan Penataan Ruang | http://dpupr.purbalinggakab.go.id |
| 18. | Dinas Pemberdayaan Masyarakat dan Desa | http://dinpermasdes.purbalinggakab.go.id |
| 19. | Dinas Pemuda, Olahraga dan Pariwisata | http://dinporapar.purbalinggakab.go.id |
| 20. | Dinas Penerangan Modal dan Pelayanan Terpadu Satu Pintu | http://dpmptsp.purbalinggakab.go.id |
| 21. | Dinas Pendidikan dan Kebudayaan | http://dindikbud.purbalinggakab.go.id |
| 22. | Dinas Sosial, Pengendalian Penduduk dan Keluarga Berencana | http://dinsosdaldukkbp3a.purbalinggakab.go.id |
| 23. | Website PKK | http://pkk.purbalinggakab.go.id |

Tabel 4.2 Website Organisasi Perangkat Daerah (OPD) (lanjutan)

| No. | Nama Website | Link |
|---|---|---|
| 24. | Website RSUD | http://rsud.purbalinggakab.go.id |
| 25. | Badan Keuangan Daerah | http://bakeuda.purbalinggakab.go.id |

Tabel 0.2 Website Kecamatan

| No. | Nama Website | Link |
|---|---|---|
| 1. | Kecamatan Bukateja | https://kecamatanbukateja.purbalinggakab.go.id |
| 2. | Kecamatan Kalimanah | https://kecamatankalimanah.purbalinggakab.go.id |
| 3. | Kecamatan karanganyar | https://kecamatankaranganyar.purbalinggakab.go.id |
| 4. | Kecamatan Karangjambu | https://kecamatankarangreja.purbalinggakab.go.id |
| 5. | Kecamatan Karangreja | https://kecamatankertanegara.purbalinggakab.go.id |
| 6. | Kecamatan Kertanegara | https://kecamatanmrebet.purbalinggakab.go.id |
| 7. | Kecamatan Mrebet | https://kecamatanpadamara.purbalinggakab.go.id |
| 8. | Kecamatan Padamara | https://kecamatanpurbalingga.purbalinggakab.go.id |
| 9. | Kecamatan Purbalingga | https://kecamatanrembang.purbalinggakab.go.id |
| 10. | Kecamatan Rembang | https://kecamatanrembang.purbalinggakab.go.id |
| 11. | Kecamatan Karangmoncol | http://kecamatankarangmoncol.purbalinggakab.go.id |
| 12. | Kecamatan Pandegan | http://kecamatanpengadegan.purbalinggakab.go.id |
| 13. | Kecamatan Kejobong | https://kecamatankejobong.purbalinggakab.go.id |
| 14. | Kecamatan Bojongsari | https://kecamatanbojongsari.purbalinggakab.go.id |

Tabel 0.3 Website Desa

| No. | Nama Website | Link |
|---|---|---|
| 1. | Kelurahan Kembaran Kulon | https://kelurahankembarankulon.purbalinggakab.go.id |
| 2. | Kelurahan Kandanggampang | https://kelurahankandanggampang.purbalinggakab.go.id |
| 3. | Kelurahan Kalikabong | https://kelurahankalikabong.purbalinggakab.go.id |
| 4. | Kelurahan Karangmanyar | https://kelurahankarangmanyar.purbalinggakab.go.id |
| 5. | Kelurahan Mewek | https://kelurahanmewek.purbalinggakab.go.id |
| 6. | Kelurahan Kedungmenjangan | https://kelurahankedungmenjangan.purbalinggakab.go.id |

Tabel 4.4 Website Desa (lanjutan)

| No. | Nama Website | Link |
|---|---|---|
| 7. | Kelurahan Bancar | https://kelurahanbancar.purbalinggakab.go.id |
| 8. | Kelurahan Bojong | https://kelurahanbojong.purbalinggakab.go.id |
| 9. | Kelurahan Karangsentul | https://kelurahankarangsentul.purbalinggakab.go.id |
| 10. | Kelurahan Purbalingga Kulon | https://kelurahangalon.purbalinggakab.go.id/ |
| 11. | Desa Sinduraja | http://sinduraja.desa.id |
| 12. | Desa Kalikajar | http://kalikajar.desa.id |
| 13. | Desa Arenan | http://arenan.desa.id |
| 14. | Desa Sempor Lor | http://semporlor.desa.id |
| 15. | Desa Lamongan | http://lamongan-purbalingga.desa.id |
| 16. | Desa Sidanegara | http://sidanegara.desa.id |
| 17. | Desa Selakambang | http://selakambang.desa.id |
| 18. | Desa Tejasari | http://tejasari.desa.id |
| 19. | Desa Brecek | http://brecek.desa.id |
| 20. | Desa Penaruban | http://penaruban.desa.id |
| 21. | Desa Cilapar | http://cilapar.desa.id |
| 22. | Desa Penolih | http://penolih.desa.id |
| 23. | Desa Kaligondang | http://kaligondang.desa.id |
| 24. | Desa Kembaran Wetan | http://kembaranwetan.desa.id |
| 25. | Desa Gembong | http://gembong.desa.id |
| 26. | Desa Bojongsari | http://bojongsari-purbalingga.desa.id |
| 27. | Desa Kajongan | http://kajongan.desa.id |
| 28. | Desa Brobot | http://brobot.desa.id |
| 29. | Desa Metenggeng | http://metenggeng.desa.id |
| 30. | Desa Galuh | http://galuh.desa.id |
| 31. | Desa Bumisari | http://bumisari-purbalingga.desa.id |
| 32. | Desa Patemon | http://patemon.desa.id |
| 33. | Desa Candiwulan | http://candiwulan.desa.id |
| 34. | Desa Karangjengkol | http://karangjengkol.desa.id |
| 35. | Desa Munjul | http://munjul.desa.id |
| 36. | Desa Cendana | http://cendana.desa.id |

Tabel 4.4 Website Desa (lanjutan)

| No. | Nama Website | Link |
|---|---|---|
| 37. | Desa Limbangan | http://limbangan.desa.id |
| 38. | Desa Karanglewas | http://karanglewas.desa.id |
| 39. | Desa Candinata | http://candinata.desa.id |
| 40. | Desa Karangcegak | http://karangcegak.desa.id |
| 41. | Desa Karangklesem | http://karangklesem.desa.id |
| 42. | Desa Sumingkir | http://sumingkir.desa.id |
| 43. | Desa Dagan | http://dagan.desa.id |
| 44. | Desa Banjarsari | http://banjarsari.desa.id |
| 45. | Desa Karangmalang | http://www.karangmalang.desa.id |
| 46. | Desa Gandasuli | http://gandasuli.desa.id |
| 47. | Desa Limbasari | http://limbasari.desa.id |
| 48. | Desa Karangtalun | http://karangtalun.desa.id |
| 49. | Desa Majapura | http://majapura.desa.id |
| 50. | Desa Karangkemiri | http://karangkemiri.desa.id |
| 51. | Desa Sumilir | http://sumilir.desa.id |
| 52. | Desa Muntang | http://muntang.desa.id |
| 53. | Desa Pelumutan | http://pelumutan.desa.id |
| 54. | Desa Jetis | http://jetis-purbalingga.desa.id |
| 55. | Desa Kedungbenda | http://kedungbenda.desa.id |
| 56. | Desa Toyareka | http://toyareka.desa.id |
| 57. | Desa Tangkisan | http://tangkisan.desa.id |
| 58. | Desa Karangturi | http://karangturi.desa.id |
| 59. | Desa Serayu Larangan | http://serayularangan.desa.id |
| 60. | Desa Selanganggeng | http://selaganggeng.desa.id |
| 61. | Desa Bojong | http://bojong.desa.id |
| 62. | Desa Binangun | http://binangun.desa.id |
| 63. | Desa Mangunegara | http://mangunegara.desa.id |
| 64. | Desa Onje | http://onje.desa.id |
| 65. | Desa Lambur | http://lambur.desa.id |
| 66. | Desa Sangkanayu | http://sangkanayu.desa.id |
| 67. | Desa Campakoah | http://campakoah.desa.id |

Tabel 4.4 Website Desa (lanjutan)

| No. | Nama Website | Link |
|---|---|---|
| 68. | Desa Kaliori | http://kaliori-purbalingga.desa.id |
| 69. | Desa Bungkanel | http://bungkanel.desa.id |
| 70. | Desa Karanganyar | http://karanganyar.desa.id |
| 71. | Desa Desa Karanggedang | http://www.karanggedang.desa.id |
| 72. | Desa Ponjen | http://ponjen.desa.id |
| 73. | Desa Brakas | http://brakas.desa.id |
| 74. | Desa Maribaya | http://maribaya.desa.id |
| 75. | Desa Bantarbarang | http://bantarbarang.desa.id |
| 76. | Desa Panusupan | http://panusupan.desa.id |
| 77. | Desa Makam | http://makam.desa.id |
| 78. | Desa Bodaskarangjati | http://bodaskarangjati.desa.id |
| 79. | Desa Karangbawang | http://karangbawang-purbalingga.desa.id |
| 80. | Desa Gudungwuled | http://gunungwuled.desa.id |
| 81. | Desa Wanogara Kulon | http://wanogarakulon.desa.id |
| 82. | Desa Losari | http://losari-purbalingga.desa.id |
| 83. | Desa Dawuhan | http://dawuhan-purbalingga.desa.id |
| 84. | Desa Karangjambe | http://karangjambe.desa.id |
| 85. | Desa Karangpule | http://karangpule.desa.id |
| 86. | Desa Karanggambas | http://karanggambas.desa.id |
| 87. | Desa Desa Purbayasa | http://purbayasa-purbalingga.desa.id |
| 88. | Desa Karangreja | http://karangreja.desa.id |
| 89. | Desa Tlahablor | http://tlahablor.desa.id |
| 90. | Desa Siwarak | http://siwarak.desa.id |
| 91. | Desa Kadarpan | http://kedarpan.desa.id |
| 92. | Desa Pandansari | http://pandansari-purbalingga.desa.id |
| 93. | Desa Nangkod | http://nangkod.desa.id |
| 94. | Desa Bandingan | http://bandingan-purbalingga.desa.id |
| 95. | Desa Nangkasawit | http://nangkasawit.desa.id |
| 96. | Desa Karangtengah | http://karangtengah.desa.id |
| 97. | Desa Langkap | http://langkap.desa.id |
| 98. | Desa Kertanegara | http://kertanegara-purbalingga.desa.id |

Tabel 4.4 Website Desa (lanjutan)

| No. | Nama Website | Link |
|---|---|---|
| 99. | Desa Krangean | http://krangean.desa.id |
| 100. | Desa Condong | http://condong.desa.id |
| 101. | Desa Adiarsa | http://adiarsa.desa.id |
| 102. | Desa Mergasana | http://mergasana.desa.id |
| 103. | Desa Kasih | http://kasih.desa.id |
| 104. | Desa Kalimanah Wetan | http://kalimanahwetan.desa.id |
| 105. | Desa Blater | http://blater.desa.id |
| 106. | Desa Klapasawit | http://klapasawit.desa.id |
| 107. | Desa Manduraga | http://manduraga.desa.id |
| 108. | Desa Sidakangen | http://sidakangen.desa.id |
| 109. | Desa Rabak | http://rabak.desa.id |
| 110. | Desa Jompo | http://jompo.desa.id |
| 111. | Desa Selabaya | http://selabaya.desa.id |
| 112. | Desa Karangpetir | http://karangpetir.desa.id |
| 113. | Desa Karangjambu | http://karangjambu.desa.id |
| 114. | Desa Tajug | http://tajug.desa.id |
| 115. | Desa Grantung | http://grantung.desa.id |
| 116. | Desa Karangsari | http://karangsari-karangmoncol.desa.id |
| 117. | Desa Bedagas | http://bedagas.desa.id |
| 118. | Desa Tumunggal | http://tumanggal.desa.id |
| 119. | Desa Tegalpingen | http://tegalpingen.desa.id |
| 120. | Desa Kedungjati | http://kedungjati.desa.id |
| 121. | Desa Karangcengis | http://karangcengis.desa.id |