BAB III
METODE PENELITIAN

3.1 Pendekatan Penelitian

Penelitian ini menggunakan model Waterfall dalam pengembangan perangkat lunak serta pendekatan Penetration Testing Execution Standard (PTES) untuk pengujian keamanan sistem. Setiap tahap dalam PTES akan diintegrasikan ke dalam proses Waterfall guna memastikan evaluasi keamanan dilakukan secara sistematis. PTES terdiri dari tujuh tahap, yaitu Pre-Engagement Interaction, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post-Exploitation, dan Reporting. Implementasi tahapan ini akan dilakukan secara berurutan sesuai dengan tahapan dalam model Waterfall, dimulai dari tahap pertama yang dibahas pada subbab 3.2.

3.2 Requirements

3.2.1 Pre-Engagement Interactions

Pada bagian pertama dari sikulus waterfal ini bagian dari PTES yang dimasukkan adalah pre-engagement interactions. Langkah awal adalah melibatkan diskusi dan kesepakatan dengan Operator desa dan pengembang DevOps pertama website desa untuk mendefinisikan ruang lingkup pengujian. Izin untuk melakukan observasi pada website juga diperoleh pada tahap ini dengan menggunakan Akun Admin Desa XYZ. Wawancara dilakukan untuk memahami proses pemberian akun, pemberian kebijakan kepada operator desa dan memahami pengetahuan sistem keamanan maupun fitur yang dimiliki oleh Website Desa. Hasil wawancara yang diperoleh akan dijelaskan lebih lanjut pada Tabel 3.2.1 dan Tabel 3.2.2.

Tabel 3.2.1 Wawancara dengan Operator Desa

Responden : Bapak ABC

Jabatan : Operator Desa XYZ

Metode Wawancara : Wawancara langsung

Waktu : 9 Desember 2024

No.	Pertanyaan	Jawaban
1.	Apakah ada arahan untuk email level di bawah superadmin?	Tidak ada arahan khusus, hanya diberikan akses admin login dan pelatihan fitur (Manajemen Administrasi Desa).
2.	Apakah diberikan buku Panduan dalam penggunaan Website Desa?	Tidak ada, hanya sosialisasi dan pelatihan mengenai Fitur MAD saja.
3.	Apakah ada kebijakan atau arahan terkait penggantian password?	Tidak ada arahan untuk ganti password.
4.	Siapa saja yang boleh menggunakan akun superadmin?	Tidak ada arahan khusus mengenai siapa saja yang boleh menggunakan akun superadmin.
5.	Apakah ada pembatasan terkait sistem login?	Tidak ada pembatasan pada sistem login.
6.	Apakah email desa digunakan untuk verifikasi?	Tidak, email desa tidak digunakan untuk verifikasi.
7.	Apakah operator desa pernah membuat akun email level di bawah admin?	Ya, operator desa pernah membuat email level di bawah admin untuk eksperimen.
8.	Apakah operator desa mengetahui mengenai username dan password yang diberikan oleh pihak Website Desa memiliki format khusus?	Ya, pihak desa mengetahui adanya format khusus yang dimiliki oleh akun Website Desa yang diberikan.

9.	Apakah pada akun Website Desa bisa melakukan reset password apabila user atau operator desa lupa password tersebut?	Ya, namun proses reset password hanya bisa dilakukan dengan menghubungi pihak Website Desa untuk mereset secara manual dan memerlukan waktu yang lama.
10.	Apakah terdapat fitur pada Halaman Pengelola Layanan yang tidak pernah dipergunakan?	Ya, terdapat 1 fitur Checklist yang hanya berfungsi sebagai penanda dan tidak memiliki arti penting dalam pengelolaan Akun.
11.	Apakah penerapan pengembangan sistem keamanan Website Desa penting bagi pengelolaan data Masyarakat?	Ya, penerapan pengembangan sistem keamanan Website Desa sangat penting untuk melindungi data dan informasi desa.
12.	Apa harapan pihak desa terkait pengembangan sistem keamanan Website Desa?	Pihak desa mengharapkan adanya pengembangan sistem keamanan untuk melindungi data lebih baik.

Berdasarkan hasil wawancara yang dirangkum dalam tabel 3.2.1, terdapat beberapa kelemahan dalam pengelolaan sistem keamanan pada level administrasi desa. Tidak adanya arahan khusus terkait penggunaan akun Admin Desa, kebijakan penggantian kata sandi, dan pembatasan sistem login menunjukkan kurangnya kontrol akses dan perlindungan terhadap serangan siber seperti brute force dan dictionary attack. Selain itu, email desa belum digunakan untuk proses verifikasi, sehingga meningkatkan risiko keamanan. Meski demikian, pihak desa memiliki kesadaran terhadap potensi ancaman keamanan dan berharap adanya pengembangan sistem keamanan yang lebih baik untuk melindungi data desa. Fungsi checklist dalam pengaturan MAD juga dinilai tidak efektif, karena tidak memiliki pengaruh apapun pada sistem. Dengan demikian, diperlukan kebijakan dan fitur yang lebih terstruktur, seperti pengelolaan akses akun,

pembatasan login, penggunaan email untuk verifikasi, serta peningkatan fungsi sistem untuk meningkatkan keamanan data dan informasi desa secara keseluruhan.

Tabel 3.2.2 Wawancara dengan Mantan DevOps Website

Responden : *Anonym*

Jabatan : Mantan DevOps Website Desa

Metode Wawancara : Wawancara daring menggunakan aplikasi percakapan WhatsApp

Waktu : 27 November 2024

No.	Pertanyaan	Jawaban
1.	Apa peran Anda dalam pengembangan dan pengelolaan sistem Website Desa?	Narasumber terlibat di bagian DevOps, bertanggung jawab pada infrastruktur dan cloud.
2.	Apakah pembuatan user ID, password, dan mekanisme login termasuk tanggung jawab Anda?	Ya, termasuk dalam cakupan.
3.	Dari observasi yang peneliti lakukan, Apa pendapat Anda tentang celah keamanan yang mungkin ada pada Website Desa?	Celah pada Website Desa sudah pasti ada, dan diperlukan Pengembangan sistem keamanan, namun Fokus saja dengan celah yang berdampak besar, apabila akan diberikan rekomendasi mitigasinya.
4.	Apakah ada pembatasan pada sistem login, seperti pemblokiran IP atau percobaan login?	Tidak ada pembatasan, seperti pemblokiran IP atau pembatasan percobaan login.
5.	Apakah Anda berkontribusi dalam pembuatan pola atau struktur khusus pada password dan nama pengguna di Website Desa?	Ya, saya berkontribusi pada pembuatan pola username dan password yang sama di berbagai desa untuk mempermudah Akses Akun oleh Operator Desa.

6.	Menurut Anda, bagaimana kebijakan penggantian password bisa diterapkan lebih baik?	Kewajiban ganti password diperlukan untuk meningkatkan keamanan.
7.	Apakah aman untuk melakukan brute force testing langsung pada server asli?	Server bisa down jika dilakukan brute force testing langsung.
8.	Apakah Anda ingin menjaga kerahasiaan informasi atau identitas terkait proyek ini?	Ya, mohon rahasiakan nama saya.

Tabel 3.2.2 menyajikan hasil wawancara dengan narasumber yang terlibat dalam pengelolaan sistem Website Desa. Narasumber menjelaskan perannya dalam aspek infrastruktur dan cloud serta memberikan wawasan penting terkait potensi celah keamanan sistem, meskipun tidak terlibat langsung dalam pengembangan. Ditemukan bahwa tidak ada pembatasan pada sistem login, sehingga rentan terhadap *Brute Force Attack*, sementara pola password seragam di berbagai desa meningkatkan risiko *Dictionary Attack* dan *Hybrid Attack*. Narasumber juga menekankan bahwa pengujian langsung menggunakan *brute force* pada server asli dapat menyebabkan kerusakan dan lebih baik dilakukan pada server terpisah atau mockup. Hasil wawancara ini menunjukkan pentingnya memperbaiki mekanisme login dan memperketat kebijakan penggantian password untuk meningkatkan keamanan sistem Website Desa.

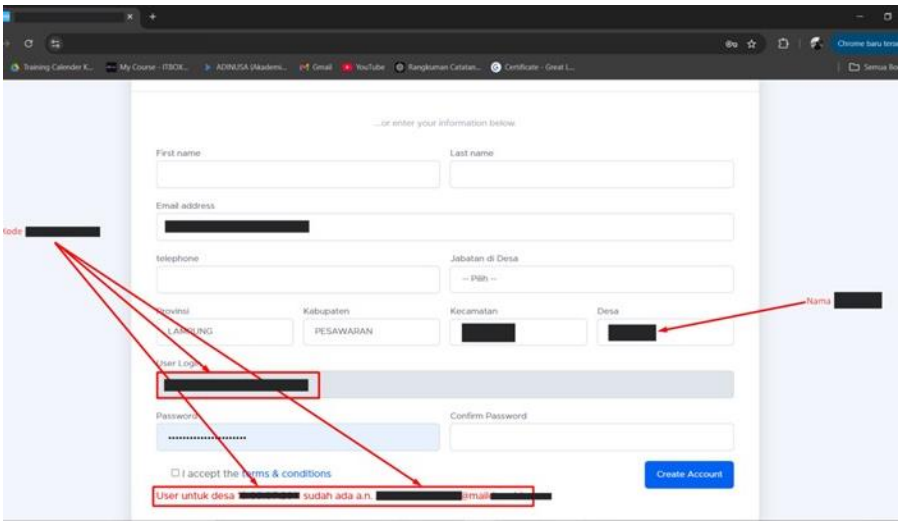
3.3 Design

Pada bagian ke dua tahapan waterfall adalah perancangan atau design, maka tahapan PTES di bagian ini adalah intelligence gathering yaitu observasi terhadap wesbite yang saat ini berjalan.

3.3.1 Intelligence Gathering

1. Observasi Halaman Pendaftaran

Observasi langsung dilakukan terhadap halaman "Pendaftaran" pada website desa di alamat xxy.websitedesa.com/pendaftaran.xyz. Seperti pada gambar 3.3.1, ditemukan bahwa format username mengikuti pola yang konsisten, yaitu nama<kode>@mailxxxx.id, yang digunakan untuk semua akun admin desa yang terdaftar. Pola username ini mudah dikenali dan tidak memberikan variasi yang cukup untuk menghindari potensi serangan. Selain itu, tabel 3.3.1 juga menunjukkan bahwa pola password default yang digunakan pada akun baru adalah pengelola<nama>@456. Pola password ini mengandung elemen standar yang sama di setiap akun, menjadikannya rentan terhadap serangan dictionary attack, di mana kata-kata atau frasa umum yang digunakan dalam kombinasi tersebut dapat dengan mudah ditebak oleh alat otomatis yang digunakan dalam serangan tersebut.



Gambar 3.3.1 Kerentanan pada halaman Pendaftaran

2. Temuan Pola Password

Temuan pola password ini diperoleh selama masa Praktik Kerja, di mana mahasiswa diberi akses sebagai admin untuk keperluan pengelolaan data desa. Akses tersebut memungkinkan mahasiswa atau pihak lain yang berkontribusi untuk mengidentifikasi pola password yang diterapkan di akun desa lainnya. Pengamatan ini menunjukkan adanya pola yang konsisten dalam format username dan password yang digunakan, yang berpotensi meningkatkan kerentanannya terhadap serangan. Pola ini dapat dilihat lebih rinci pada Tabel 3.3.1, yang menyajikan sampel format username dan password yang diterapkan pada akun-akun desa.

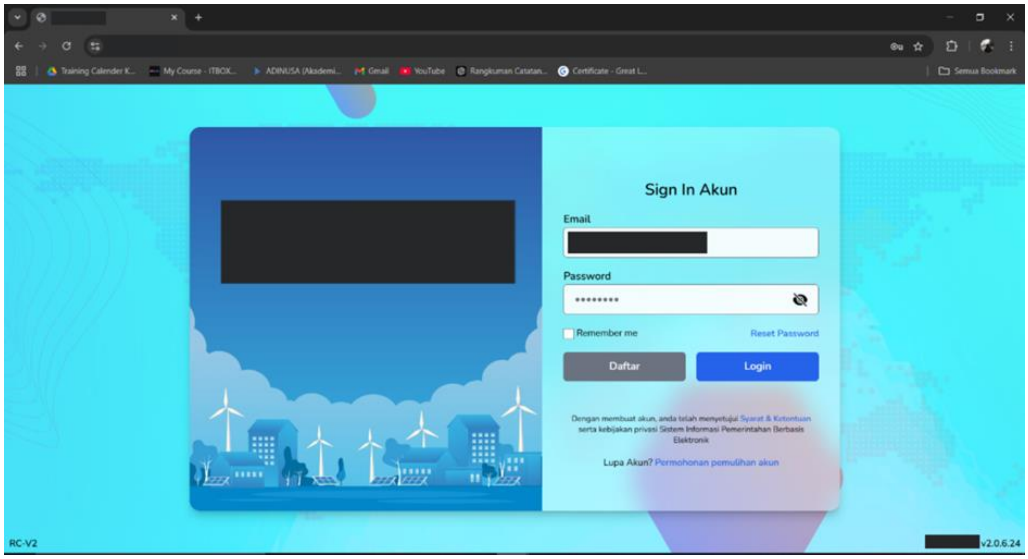
Tabel 3.3.1 Observasi Sampel Format Username dan Password

No.	Username	Password
1.	nama<kode>@mailxxxx.id	pengelola<nama>@456
2.	nama1234567891@mailxxxx.id	pengeloladesajambu@456
3.	nama1234567892@mailxxxx.id	pengeloladesamangga@456
4.	nama1234567893@mailxxxx.id	pengeloladesakedondong@456
5.	nama1234567894@mailxxxx.id	pengeloladesaapel@456
6.	nama1234567895@mailxxxx.id	pengeloladesajeruk@456

3. Ketiadaan Autentikasi Multi Faktor

Gambar 3.3.2 ditunjukkan halaman login yang dapat diakses melalui https://xxy.websitedesa.com/masuk.xyz, ditemukan bahwa pemrosesan login akun tidak menerapkan sistem *Multi-Factor Authentication* (MFA), seperti yang teridentifikasi pada Gambar 3.3.2. Ketiadaan MFA ini meningkatkan risiko keamanan, karena tanpa adanya lapisan tambahan untuk verifikasi identitas pengguna, akun-akun tersebut menjadi lebih rentan terhadap akses tidak sah. Tanpa perlindungan ekstra, penyerang yang berhasil menebak atau mencuri kredensial login dapat dengan mudah mendapatkan akses ke akun admin, yang

tentunya dapat menimbulkan kerusakan pada sistem. Penerapan MFA dapat membantu mengurangi risiko ini dengan menambahkan langkah verifikasi tambahan yang sulit dilewati oleh pihak yang tidak berwenang.



Gambar 3.3.2 Halaman Login Akun Admin Website Desa

4. Ketidakfungsian Fitur Reset Password

Selain itu, fitur "Reset Password" pada halaman login yang terlihat pada Gambar 3.3.2 tidak berjalan atau tidak dapat dipergunakan. Hal ini mengakibatkan pengguna tidak dapat mengatur ulang password mereka jika lupa. Maka dari itu sesuai dengan hasil yang didapat dari tahap *Pre-Engagement Interaction* untuk melakukan reset password, pihak desa melakukan konfirmasi kepada pihak Website Desa dan memerlukan waktu yang lama Tanpa kemampuan untuk mereset password, pengguna yang kehilangan akses ke akun mereka tidak memiliki cara untuk memulihkan akses. Hal ini dapat dimanfaatkan oleh penyerang untuk mengunci pengguna dari akun mereka atau untuk melakukan manipulasi lebih lanjut pada sistem. Fitur reset password yang berfungsi dengan baik adalah elemen penting untuk memastikan bahwa pengguna dapat memulihkan akses mereka dengan cara yang aman dan terkontrol.

3.3.2 Threat Modeling

Berdasarkan hasil observasi (*Pre-Engagement Interactions* & *Intellegence Gathering*), ditemukan potensi ancaman berupa brute force attack akibat tidak adanya *Loging Attempt Throttling* pada halaman login. Simulasi serangan dilakukan pada mockup untuk menguji dampaknya terhadap keamanan data. Temuan ini dirangkum lebih lanjut dalam Tabel 3.4.1 yang memuat Threat Modeling terkait potensi ancaman yang ada.

Tabel 3.3.2 Threat Modeling

	Ancaman	**Keterangan**	**CIA Triad**
1.	Insider Attack	Tidak adanya masa expire Akun	Confidentiality, Integrity
2.	Dictionary Attack	Password mudah ditebak	Confidentiality, Integrity, Availability
3.	Brute Force	Tidak ada pembatasan login (*Login Attempt Throttling*)	Availability, Confidentiality
4.	Hybrid Attack	Perpaduan beberapa serangan seperti Insider Attack dan Dictionary Attack	Confidentiality, Integrity, Availability
5.	Account Lockout Risk	Fitur “Reset Password” yang tidak berfungsi	Availability, Confidentiality

Tabel 3.4.1 memuat Threat Modeling yang mengidentifikasi ancaman terhadap kerahasiaan, integritas, dan ketersediaan sistem, seperti *Insider Attack*, *Dictionary Attack*, *Brute Force Attack*, *Hybrid Attack*, dan *Account Lockout Risk*. Ancaman-ancaman ini mencakup kelemahan pada pengelolaan password, ketiadaan pembatasan login, dan fitur pemulihan akun yang tidak berfungsi. Penjelasan rinci mengenai masing-masing ancaman disajikan pada bagian berikut:

1. **Insider Attack:** Akses yang diberikan kepada pihak eksternal desa dengan password yang masih valid memungkinkan mereka untuk tetap mengakses sistem,

meskipun mereka sudah tidak terlibat dalam pengelolaan data desa. Hal ini menciptakan risiko keamanan, karena pihak yang tidak berwenang dapat memanfaatkan akses tersebut untuk melakukan tindakan yang merugikan, seperti mengubah atau menghapus data penting.

2. **Dictionary Attack:** Akses yang diberikan kepada pihak eksternal dalam pengelolaan data desa melibatkan penggunaan password. Berdasarkan wawancara dengan operator desa, diketahui bahwa password yang diberikan mengikuti pola tertentu dan merupakan password default. Hal ini memungkinkan terjadinya serangan dictionary attack, di mana penyerang dapat dengan mudah menebak password yang lemah dan umum digunakan, sehingga dapat mengakses akun-akun yang seharusnya dilindungi.
3. **Brute Force Attack:** Tanpa adanya pembatasan pada jumlah percobaan login dan/atau *Multi-Factor Authentication* (MFA), penyerang dapat mencoba berbagai kombinasi password secara berulang. Jika ancaman ini diimplementasikan dengan menggunakan alat otomatisasi, penyerang dapat memanfaatkan data username dan password yang telah diperoleh sebelumnya untuk meningkatkan peluang keberhasilan serangan. Dengan demikian, risiko akses tidak sah ke akun admin menjadi semakin tinggi, yang dapat mengakibatkan kebocoran data dan kerugian bagi sistem.
4. **Hybrid Attack:** Hybrid Attack menggabungkan teknik dari serangan dictionary dan brute force untuk meningkatkan efektivitasnya. Dalam konteks pengelolaan data desa, penyerang dapat memanfaatkan pola password yang lemah dan umum, seperti yang ditemukan dalam serangan dictionary, sambil juga mencoba variasi kombinasi karakter yang lebih kompleks dari brute force. Dengan cara ini, penyerang dapat menyesuaikan pendekatan mereka berdasarkan informasi yang diperoleh, sehingga meningkatkan kemungkinan untuk berhasil mendapatkan akses ke akun yang dilindungi. Pendekatan ini membuatnya lebih sulit untuk mendeteksi serangan, karena penyerang dapat beradaptasi dengan cepat terhadap langkah-langkah keamanan yang ada.

5. **Account Lockout Risk:** Ketiadaan fitur reset password dapat menyebabkan pengguna yang sah tidak dapat mengakses akun mereka jika lupa password. Hal ini menciptakan risiko bahwa penyerang dapat mengunci pengguna dari akun mereka, yang dapat mengakibatkan kehilangan data dan kontrol atas sistem.

3.3.3 Vulnerability Analysis

1. Kerentanan Akun Admin

Akses yang diberikan kepada pihak eksternal desa dengan password yang masih valid menciptakan kerentanan, karena meskipun pihak tersebut sudah tidak terlibat dalam pengelolaan data desa, mereka masih dapat mengakses sistem.

Hal ini dapat mengakibatkan penyalahgunaan akses, di mana pihak yang tidak berwenang dapat mengubah atau menghapus data penting, yang berdampak pada Confidentiality dan Integrity data.

2. Kerentanan Password

Penggunaan password default yang mudah ditebak, seperti pengelola<nama>@456, meningkatkan risiko serangan, karena pola password yang sama di berbagai akun admin desa membuatnya rentan terhadap serangan dictionary attack.

Penyerang dapat dengan mudah menebak password dan mendapatkan akses ke akun yang seharusnya dilindungi, yang berdampak pada Confidentiality, Integrity, dan Availability data.

3. Kebocoran Username

Pada halaman Pendaftaran yang terdapat pada gambar 3.3.1, format username yang digunakan mengikuti pola pengelola<nama>@mailxxxx.id, yang dapat diakses oleh pihak luar.

Kebocoran informasi username ini memungkinkan penyerang untuk mengetahui username yang valid, sehingga meningkatkan risiko serangan seperti brute force attack atau dictionary attack, karena penyerang tidak perlu lagi menebak username yang valid, mempercepat proses eksploitasi.

4. Ketiadaan Pembatasan Login

Tidak adanya Login Attempt Throttling pada halaman login memungkinkan penyerang untuk melakukan brute force attack tanpa batasan, di mana mereka dapat mencoba berbagai kombinasi password secara berulang.

Jika penyerang menggunakan alat otomatisasi untuk melakukan serangan ini, mereka dapat memanfaatkan data username dan password yang telah diperoleh sebelumnya, meningkatkan peluang keberhasilan serangan dan mengakibatkan akses tidak sah ke akun admin, yang berdampak pada Availability dan Confidentiality data.

5. Ketiadaan Multi-Faktor Authentication (MFA)

Sistem login yang tidak menerapkan Multi-Factor Authentication (MFA) meningkatkan risiko keamanan, karena tanpa lapisan tambahan untuk verifikasi identitas pengguna, akun-akun tersebut lebih rentan terhadap akses tidak sah.

Penyerang dapat dengan mudah mendapatkan akses ke akun admin jika mereka berhasil menebak atau mencuri kredensial login, yang dapat mengakibatkan kebocoran data dan kerugian bagi sistem.