BAB I PENDAHULUAN

1.1 Latar Belakang

Di era digital yang semakin canggih ini, email menjadi salah satu alat komunikasi utama yang digunakan oleh individu maupun organisasi dalam berbagai kegiatan. Namun, seiring dengan meningkatnya penggunaan email, ancaman siber yang memanfaatkan platform ini juga meningkat secara signifikan. Salah satu ancaman yang paling sering ditemui adalah serangan *phishing*, *phishing* merupakan salah satu ancaman siber paling umum dan berbahaya yang dihadapi oleh pengguna internet saat ini [1]. Serangan *phishing* dilakukan dengan memanipulasi pengguna agar mengungkapkan informasi sensitif seperti kata sandi, nomor kartu kredit, atau data pribadi lainnya, seringkali melalui email yang terlihat sah [2].

Menurut data laporan terbaru, insiden *phishing* terus mengalami peningkatan setiap tahunnya [3]. Serangan *phishing* berdampak besar bagi individu dan organisasi dengan merugikan secara finansial, mencuri identitas, dan merusak reputasi. Dengan meningkatnya kebiasaan *browsing online*, kerentanan terhadap serangan semacam itu juga meningkat, terutama pada pengguna yang menghabiskan lebih banyak waktu *online* tanpa kesadaran keamanan yang memadai [4]. Salah satu alasan mengapa serangan *phishing* sangat efektif, karena pelaku sering memanfaatkan sisi psikologis korban, seperti rasa takut, tekanan waktu, atau kepercayaan terhadap identitas yang tampak sah. Dalam kondisi seperti itu, pengguna cenderung lebih mudah dimanipulasi untuk menyerahkan informasi pribadi [5]. Oleh sebab itu, aspek teknis *phishing*, seperti email palsu dan situs *website* palsu, dapat membahayakan keamanan pengguna [6].

Oleh karena itu dibuatlah aplikasi berbasis *website* PhishProof, yaitu sebuah aplikasi berbasis *website* untuk meningkatkan kesadaran dan kemampuan pengguna dalam mengidentifikasi serangan *phishing*. Kehadiran aplikasi pelatihan anti *phishing* seperti PhishProof memiliki dampak positif dalam menjembatani kesenjangan pemahaman pengguna terkait ancaman *phishing*. Seiring dengan meningkatnya kerumitan serangan *phishing*, diperlukan solusi praktis yang dapat membekali setiap individu yang berinteraksi dengan email, seperti mahasiswa, profesional TI, dan pengguna umum, untuk dapat mengenali tanda-tanda *phishing* secara efektif. Serangan *phishing* modern sering kali tampak sah dan tidak mudah terdeteksi melalui metode konvensional, sehingga membutuhkan pendekatan pelatihan yang lebih interaktif. PhishProof dirancang sebagai aplikasi yang mengarahkan pengguna untuk mengenali email yang berpotensi berbahaya melalui simulasi email dunia nyata dengan tingkat kesulitan dan karakteristik yang bervariasi. Dengan menghadirkan elemen-elemen umum yang digunakan dalam *phishing*, seperti tautan mencurigakan, lampiran tidak dikenal, dan bahasa yang mendesak.

Setelah pengguna merespons setiap simulasi email, PhishProof memberikan umpan balik langsung yang berisi penjelasan terperinci atas keputusan mereka, baik benar maupun salah. Umpan balik ini tidak hanya memberi informasi tentang kebenaran keputusan yang dibuat, tetapi juga memberikan analisis mengenai elemen mencurigakan dalam email tersebut, serta *tips* untuk mengenali *phishing* di masa mendatang. Hal ini membantu pengguna belajar dari kesalahan dan memperkuat pemahaman mereka mengenai ancaman *phishing* yang terus berkembang. Sebagai platform pembelajaran berkelanjutan, PhishProof bertujuan untuk membangun keahlian dan refleks pengguna dalam mengidentifikasi *phishing* secara mandiri, sehingga pengguna bisa menjadi pertahanan pertama dalam keamanan siber untuk diri mereka sendiri maupun lingkungan profesional mereka.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang di atas, maka rumusan masalah yang akan dibahas adalah sebagai berikut:

1. Bagaimana mengembangkan aplikasi berbasis *website* yang dapat mensimulasikan email *phishing* secara realistis?
2. Bagaimana aplikasi dapat menyediakan umpan balik interaktif untuk meningkatkan efektivitas pelatihan dalam mengidentifikasi *phishing*?
3. Bagaimana merancang sebuah aplikasi berbasis *website* yang memudahkan pengguna untuk mendeteksi serangan *phishing*?

1.3 Tujuan

Berdasarkan rumusan masalah yang ada, tujuan yang akan dicapai adalah:

1. Mengembangkan aplikasi yang dapat mensimulasikan email *phishing* secara realistis, dengan menampilkan elemen-elemen *phishing* umum seperti tautan mencurigakan, lampiran berbahaya, serta gaya bahasa yang sering digunakan oleh pelaku *phishing*.
2. Menyediakan fitur umpan balik interaktif dalam aplikasi, sehingga pengguna dapat memahami kesalahan mereka dalam mengidentifikasi *phishing* dan mendapatkan edukasi langsung mengenai pola serangan yang umum digunakan.
3. Menyediakan sistem yang mampu merekam dan menganalisis respons pengguna terhadap simulasi *phishing* untuk menghasilkan evaluasi yang komprehensif.

1.4 Batasan Masalah

Batasan Pengembangan aplikasi berbasis *website* PhishProof memiliki beberapa Batasan yang harus diperhatikan, diantaranya:

1. Aplikasi hanya berfokus pada simulasi serangan *phishing* melalui email.
2. Aplikasi tidak menyediakan analisis lanjutan berbasis kecerdasan buatan atau *machine learning* dalam mengevaluasi perilaku pengguna.
3. Aplikasi tidak menangani jenis ancaman siber lainnya di luar *phishing*.

1.5 Metode Penyelesaian Masalah

Berikut adalah metodologi penyelesaian masalah yang digunakan dalam tugas akhir ini.

1. Studi Literatur

   Melakukan pencarian referensi mengenai serangan *phishing* dan metode edukasi keamanan siber yang efektif. Sumber-sumber yang digunakan meliputi buku, artikel jurnal, dan laporan terkini tentang *phishing* untuk memahami bagaimana serangan ini bekerja serta dampaknya terhadap pengguna. Selain itu, dipelajari cara-cara pelatihan berbasis simulasi yang bertujuan meningkatkan kesadaran dan kewaspadaan pengguna dalam mengidentifikasi email yang berpotensi berbahaya. Studi ini membantu merancang aplikasi berbasis *website* PhishProof dengan fitur simulasi yang mampu menampilkan elemen-elemen khas dalam email *phishing*, sehingga aplikasi dapat memberikan pengalaman belajar yang realistis dan mendidik.

2. Analisis Kebutuhan

   Melakukan survei atau wawancara untuk memahami kebutuhan pengguna, khususnya dalam hal fitur, desain antarmuka, dan jenis-jenis pelatihan yang paling membantu dalam mengenali ancaman *phishing*. Pengguna yang menjadi fokus adalah mereka yang sering berinteraksi dengan email, seperti mahasiswa, profesional, dan pengguna umum.

3. Perancangan Aplikasi

   Berdasarkan hasil dari studi literatur dan analisis kebutuhan, dilakukan perancangan aplikasi berbasis *website* PhishProof. Pada tahap ini, ditentukan fitur-fitur yang akan diimplementasikan dalam aplikasi, seperti mekanisme simulasi email *phishing*, autentikasi pengguna, pelacakan performa, dan pembuatan laporan. Rancangan antarmuka aplikasi juga dibuat, termasuk desain *dashboard* untuk pengguna dan *admin*. Struktur basis data yang

mendukung pengelolaan pengguna, simulasi email, respons, dan laporan juga dirancang pada tahap ini. *Framework* Laravel digunakan sebagai basis pengembangan aplikasi dengan mengadopsi arsitektur MVC.

4. Pembuatan Aplikasi

   Setelah perancangan selesai, tahap ini melibatkan pembuatan aplikasi berbasis *website* PhishProof dengan menggunakan Laravel. Proses pengembangan dilakukan sesuai dengan rancangan yang telah dibuat. *Tools* dan teknologi yang digunakan meliputi Laravel sebagai *framework* utama, MySQL untuk *database*, dan JavaScript (*Blade templating*) untuk antarmuka pengguna. Pembuatan fitur-fitur seperti simulasi email *phishing*, autentikasi pengguna, pelacakan respons, umpan balik, dan *dashboard admin* dilakukan pada tahap ini.

5. Pengujian Aplikasi

   Setelah aplikasi selesai dibuat, dilakukan pengujian untuk memastikan bahwa aplikasi berjalan sesuai dengan yang diharapkan. Pengujian dilakukan dalam dua tahap. Pertama, pengujian internal oleh tim pengembang aplikasi untuk mendeteksi dan memperbaiki kesalahan teknis (*bug*). Kedua, pengujian dilakukan dengan melibatkan pengguna target, baik individu maupun *admin*, untuk memastikan bahwa aplikasi dapat digunakan dengan mudah dan sesuai dengan kebutuhan pengguna. Pengujian ini juga membantu dalam memberikan umpan balik untuk pengembangan lebih lanjut.

6. Analisis dan Evaluasi

   Setelah tahap pengujian selesai, dilakukan analisis dan evaluasi terhadap hasil pengujian. Langkah ini bertujuan untuk mengidentifikasi dan memperbaiki kesalahan atau kekurangan yang ditemukan selama pengujian. Misalnya, jika ditemukan *bug* teknis atau fitur yang tidak sesuai dengan kebutuhan pengguna, dilakukan pembenahan secara mendetail. Umpan balik dari pengguna target juga menjadi bahan evaluasi untuk meningkatkan fungsionalitas aplikasi. Selain itu, dilakukan revisi terhadap elemen antarmuka pengguna dan performa aplikasi untuk memastikan pengalaman pengguna yang lebih optimal. Evaluasi ini memastikan bahwa aplikasi berbasis *website* PhishProof memenuhi standar kualitas dan kebutuhan pengguna yang telah ditetapkan.

1.6 Pembagian Tugas Anggota

Berikut adalah pembagian tugas tim tugas akhir:

a. Aufar Hadni Azzakky

Peran : *Front-end developer*, *Back-end developer*

Tanggung Jawab :

1. Merancang alur aplikasi
2. Membuat fungsi aplikasi
3. Membuat rancangan *database*
4. Membuat poster
5. Membuat dokumen

b. M. Faishal Rafid

Peran : *Front-end Developer*, *UI/UX Designer*

Tanggung Jawab :

1. Membuat *mockup* aplikasi
2. Membuat antarmuka aplikasi
3. Membuat poster
4. Membuat video promosi
5. Membuat dokumen