PEMINDAIAN KEAMANAN WEB UNTUK PENINGKATAN KESADARAN KERENTANAN KEAMANAN WEB MENGGUNAKAN NUCLEI

Oleh: Marcello Singadji, S.Kom., M.T.[1], **Augury El Rayeb, S.Kom., M.MSI**[2], **Muhammad Dary Azhari**[3]
Program Studi Sistem Informasi[1, 2, 3]
Universitas Pembangunan Jaya[1, 2, 3]
E-Mail: marcello.singadji@upj.ac.id[1], augury.elrayeb@upj.ac.id[2], muhammad.dary@student.upj.ac.id[3]

Abstrak

Ditengah zaman berkembang pesatnya era digital ini sangat mudah sekali dalam membuat web dari yang sederhana seperti membuat company profile hingga membuat aplikasi berbasis web yang kompleks. Karena kemudahan ini dicapai dengan kehadiran banyak *tools/framework/library* yang membuat kita tidak perlu repot-repot membuat semua dari awal, contohnya kehadiran Bootstrap, Wordpress dan juga tidak lupa untuk disebutkan ialah ReactJS sebuah Javascript library yang memudahkan kita untuk membangun aplikasi kompleks berbasis web. Namun ditengah kemudahan itu semua, banyak dari kita dalam pengembangan website hanya fokus pada tampilan dan "yang penting jalan" saja sehingga melupakan aspek yang juga tidak kalah penting yaitu keamanan pada website. Jika aspek ini diabaikan, dapat menimbulkan dampak negatif yaitu peretasan pada suatu website khususnya data yang diakibatkan dari keamanan website yang rentan dari berbagai macam celah contohnya seperti masih menggunakan protokol HTTP yang dimana data pada protokol ini tidak dienkripsi. Maka dari itu penulis ingin meningkatkan kesadaran dalam pentingnya keamanan dalam membangun website dengan merancang sebuah aplikasi berbasis website dimana memiliki sebuah fitur utama yaitu memindai kerentanan keamanan suatu website dan memberikan sebuah output berupa laporan sebuah daftar masalah kerentanan keamanan website yang harus diperbaiki dari berbagai macam tingkat masalah. Hal ini dapat dicapai dengan adanya tools CLI bernama Nuclei, adalah sebuah alat pemindai kerentanan keamanan web yang biasa digunakan oleh *Security Engineer* untuk memudahkan pekerjaan dalam mendeteksi celah keamanan pada suatu halaman web.

Kata Kunci: Kerentanan Web, Keamanan Web, Nuclei, Pemindaian.

PENDAHULUAN

Perkembangan teknologi web yang begitu pesat memudahkan proses merancang dan membangun sebuah web. Dengan web perusahaan, organisasi, juga perseorangan dengan mudah memperkenalkan usaha dan bisnisnya hingga memasarkan produk dan jasa. Kemudahan merancang dan membangun didukung oleh hadirnya *tools/ framework/ library* yang mudah didapatkan dan gratis.

Kehadiran Bootstrap sebuah framework CSS memudahkan dalam pembuatan tampilan website yang ciamik dengan komponen-komponen *user interface* nya, Wordpress sebuah CMS (*Content Management System*) yang memudahkan untuk membangun *company profile* hingga *e-commerce* tanpa *coding* sama sekali, serta juga tidak lupa untuk disebutkan ialah React JS sebuah Javascript *library* yang memudahkan kita untuk membangun aplikasi kompleks berbasis web. Dari kemudahan itu semua karena perkembangan teknologi sekarang yang sangat pesat ini, juga menimbulkan dampak negatif yaitu maraknya peretasan sebuah data yang diakibatkan dari keamanan website yang rentan diretas dari berbagai macam celah. Hingga menimbulkan dampak kerugian dari skala kecil hingga skala kebocoran data yang sangat besar, yaitu skala nasional.

Selain daripada itu hal ini dapat terjadi karena banyak dari kita dalam melakukan pengembangan sistem informasi berbasis web hanya fokus pada tampilan dan "yang penting jalan" saja sehingga melupakan aspek yang juga tidak kalah penting yaitu keamanan pada website.

Jika aspek ini diabaikan, dapat menimbulkan dampak negatif yaitu peretasan pada suatu website khususnya data yang diakibatkan dari keamanan website yang rentan dari berbagai macam celah seperti contohnya masih menggunakan protokol HTTP yang dimana data pada protokol ini tidak dienkripsi dan hal lainnya seperti *Cross-site scripting*, SQL *Injection*, *Command Injection*, *Path Traversal and insecure server configuration*.

Terdapat sebuah organisasi non-profit yang berfokus dalam mengurus standar keamanan web app dunia bernama OWASP (*Open Web Application Security Project*) yang memberikan informasi, edukasi dan assesmen dalam mengatasi celah-cleah kerentanan keamanan web. Sumber referensi, informasi dari OWASP yang dapat membantu mengatasai kerentanan keamanan web antara lain bernama OWASP *Developer Guide*, OWASP *Application Security Verification Standard*, *Security Knowledge Framework*, *Developer Cheat Sheet Series*. Namun dalam memahami informasi yang OWASP berikan, dibutuhkan dedikasi juga pengalaman dalam bidang kerentanan keamanan sistem informasi khususnya keamanan web (*Web Security Engineering*). Dan juga membutuhkan waktu dalam mengetahui celah-celah kerentanan web yang terjadi misal dengan melalui assesmen OWASP *Developer Cheat Series*.

Dengan demikian untuk mengetahuai tingkat keamanan sebuah halaman web, dibangunlah sebuah aplikasi sederhana berbasis web dengan memanfaatkan *tools* CLI NUCLEI. Dimana setiap pengguna dapat dengan mudah memindai halaman web untuk mengetahui celah-celah kerentanan keamanan pada halaman web.

IDENTIFIKASI MASALAH

Dari latar belakang yang telah dijabarkan, daftar masalah yang berhasil diidentifikai oleh penulis antara lain:

1. Ketidaktahuan keamanan web dalam membangun website.
2. Ketidaktahuan pada bagian mana saja yang menyebabkan suatu website memiliki celah untuk diretas, contohnya SQL *Injection*, menggunakan protokol http yang tidak aman.
3. Dibutuhkannya dedikasi dalam bidang web security engineering untuk memahami informasi yang dapaat dijadikanrefernesi untuk mengatasi celan kerentanan web.
4. Jikapun sudah mempunyai dedikasi dalam bidang tersebut, dibutuhkan waktu mengerjakan assesmen dari OWASP dalam mendapati celah kerentanan keamanan web yang sedang di audit secara manual.

RUMUSAN MASALAH

Dari latar belakang yang telah dijelaskan pada sebelumnya, rumusan masalah yang berhasil diidentifikasi oleh penulis antara lain:

1. Bagaimana cara memberikan kesadaran mengenai pentingnya aspek keamanan dalam membangun website?

2. Bagaimana cara supaya pengguna awam pada umumnya dapat lebih mudah mengerti dalam mengakses dan memahami mengenai informasi berkaitan dengan kerentanan keamanan website yang diberikan, khususnya celah-celah keamanan web yang rentan?

3. Apakah rancangan aplikasi pemindaian ini dapat membantu memindai website target pengguna (individu/korporat) dan memberikan sebuah action list untuk meningkatkan keamanan website?

4. Bagaimana cara membangun perancangan aplikasi pemindaian yang mudah dipahami untuk awam dan tanpa terbatasi oleh spesifik platform?

TUJUAN PENELITIAN

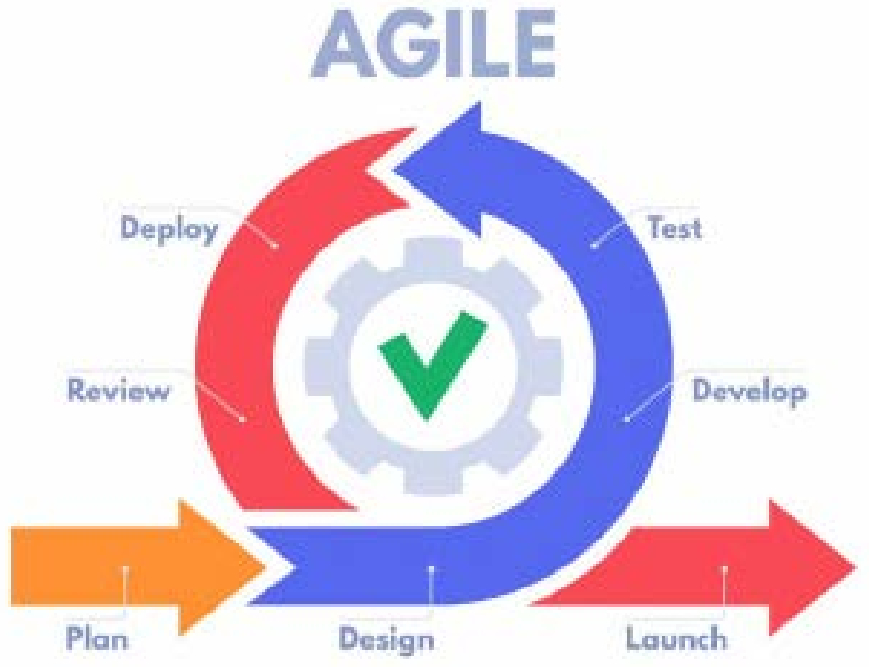
Tujuan dari penelitan ini adalah:

1. Pengguna dapat mengetahui kerentanan bagian mana saja yang harus diperbaiki berdasarkan laporan pemindaian yang dilakukan.

2. Pengguna melakukan perbaikan kerentanan keamanan website yang dapat dilakukan oleh diri sendiri jika memiliki pengetahuan dalam melakukan perbaikan atau dengan merekrut tenaga ahli *(Security Engineer*) yang melakukan daftar pekerjaan berdasarkan laporan pemindaian yang didapatkan dari percangan pengembangan aplikasi ini.

METODE PENGEMBAGAN

Model Agile merupakan model pengembangan cepat yang memerlukan adaptasi cepat dan pengembangan terhadap perubahan dalam bentuk apapun, sehingga jika terjadi perubahan ditengah pengembangan modul akan dengan cepat dilakukan penyesuaian dan pengetesan.



Gambar 1. Metode SDLC (*Software Development Life Cycle*) Agile.

PEMBAHASAN

1. NUCLEI

Nuclei adalah sebuah *tools* dalam bentuk *Command Line Interface* (CLI) di desktop yang biasa digunakan oleh para profesional dibidangnya seperti *Security Engineer*, *Bug Bounty Hunters*, *Penetration Testers* dalam mempermudah pekerjaannya pemindaian/pencarian kerentanan (*vulnerability*) sistem keamanan website yang menjadi target. (Projectdiscovery.io, 2022).

Cara kerja Nuclei yaitu Nuclei mengirimkan *requests* (permintaan) ke alamat web url yang ditarget untuk melakukan pemindaian kerentanan skala besar dan cepat, yang dapat memindai protokol termasuk TCP, SSH, DNS, HTTP, SSL, dan lainnya.

Nuclei memliki klasifikasi tingkatan kekerasan/ keparahan (*severity*) dalam kerentanan pada suatu website, antara lain dimulai yang paling lemah:

- *Info*
- *Low*
- *Medium*
- *High*
- *Critical*

Gambar 2. Cara Kerja NUCLEI (sumber: Amazon AWS).

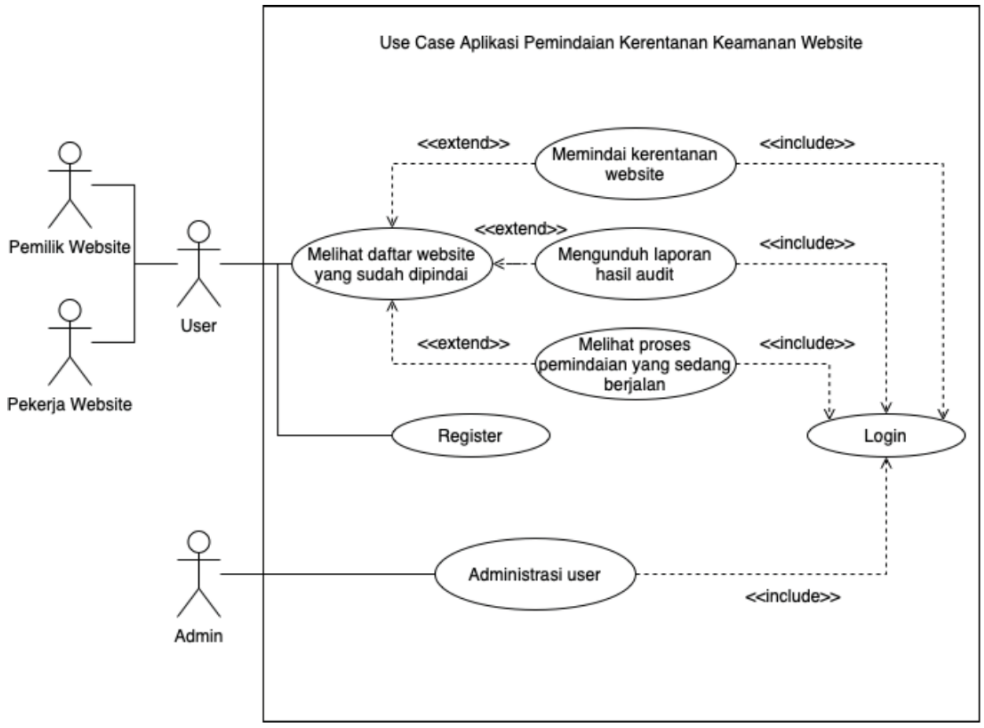
Nuclei dapat ditanamkan didalam service Backend Python yang menjadi engine utama sebagai pemindaian dalam perancangan aplikasi web penyedia pemindaian kerentanan keamanan web.

2. Perancan Aplikasi Pemindaian

Use Case Diagram

Menggambarkan aplikasi modul yang ada pada pemindaian web, dimana yang menjadi pengguna (*user*) pada aplikasi ini adalah pemilik dan pekerja web. Setiap pengguna dapat melakuan beberapa proses, yaitu:

a. Melihat daftar halaman web yang sudah di pindai.
b. Melakukan pemindaian baru terhadap kerentanan keamanan halaman web dari url yang dimasukkan.
c. Melihat proses pemindaian yang sedang berjalan.
d. Mengunduh laporan hasil audit dari pemindaian kerentanan keamanan halaman web yang telah selesai dipindai.



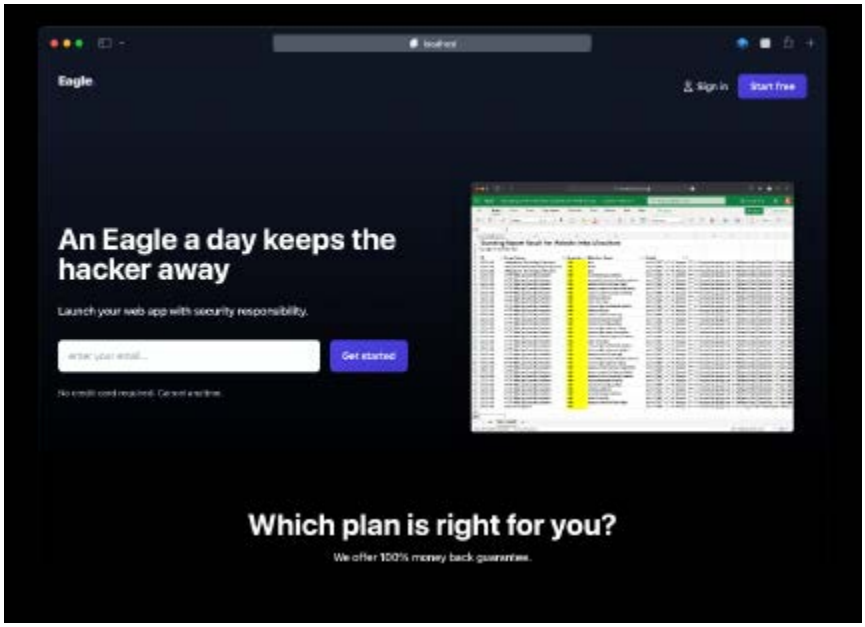
Gambar 3. *Use Case Diagram* Aplikasi Pemindaian Kerentanan Keamanan Web.

Antar Muka Pengguna

Perancangan antar muka pengguna menjelaskan tentang bagaimana tampilan dari setiap modul yang ada pada aplikasi tersebut.

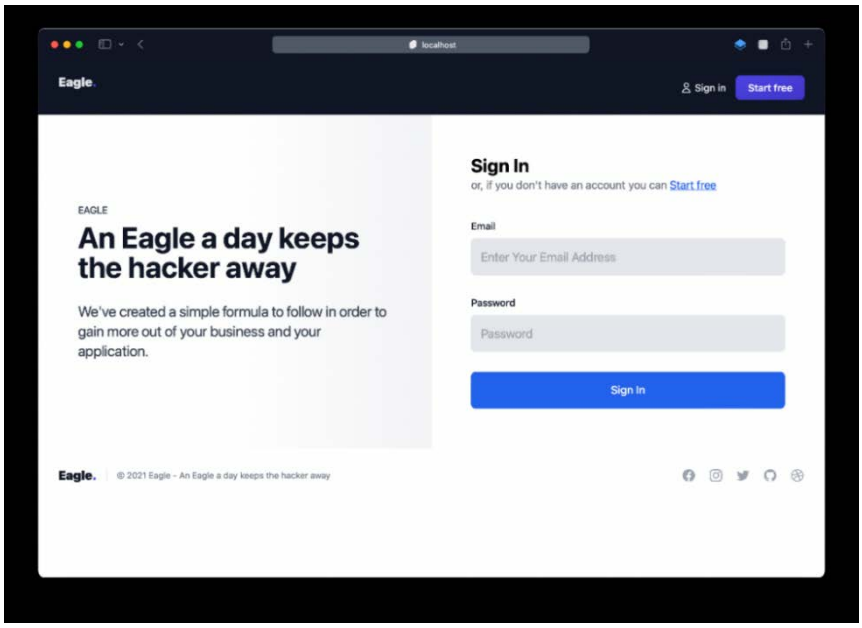
Pada perancangan aplikasi pemindain kerentanan keamanan website ini, penulis menamakan aplikasi ini bernama *Eagle* atau Bahasa Indonesianya adalah Elang. Kenapa dinamakan *Eagle*, karena burung elang terkenal mempunyai mata yang sangat tajam sehingga pada penamaan aplikasi ini ditujukan pemindaian kerentanan keamanan website seperti mata elang yang sangat tajam.

a. Halaman utama (*landing page*)
Tampilan utama atau *landing page* terdapat bagian pengenalan mengenai produk pemindaian kerentanan keamanan web dari *Eagle* ini beserta gambar output dari hasil laporan audit dan menyediakan halaman untuk login dan membuat akun.



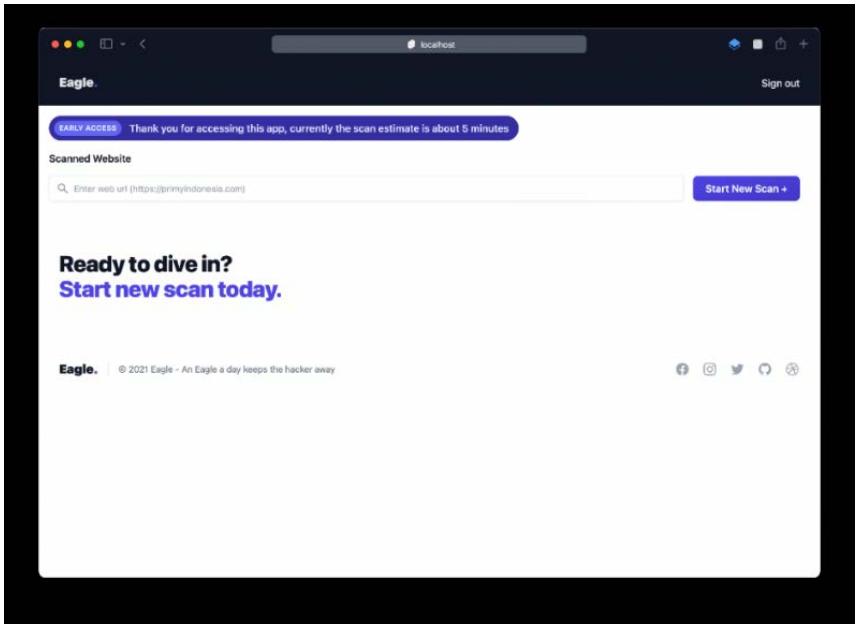
Gambar 4. Tampilan Halaman Utama (*Landing page*) Aplikasi.

b. Halaman login
Menampilkan form login yang dapat diisi dengan username, dan password untuk dapat diarahkan masuk ke dalam dashboard aplikasi jika data yang dimasukkan valid.



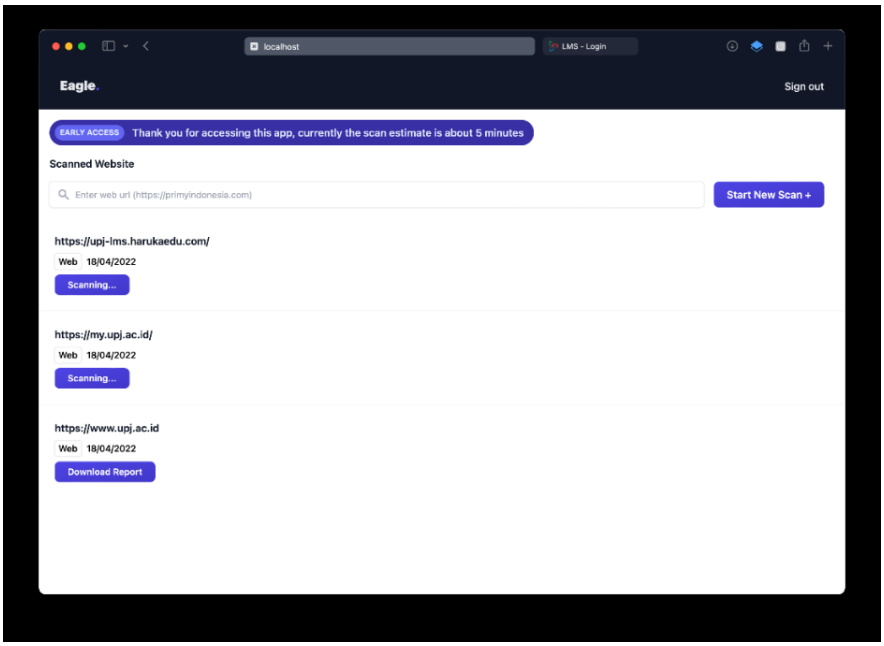
Gambar 5. Tampilan Halaman Login.

c. Halaman *dashboard*
Pada tampilan *dashboard* terdapat fitur utama yaitu pemindaian kerentanan keamanan website berdasarkan input web url yang dimasukkan user pada bagian atas halaman *dashboard*. Serta jika user belum pernah melakukan pemindaian, maka diarahkan untuk melakukan pemindaian baru dengan kalimat memulai pemindaian baru. Jika user sudah melakukan pemindaian sebelumnya, maka akan ditampilkan daftar website yang telah dipindai beserta status proses pemindaian yang sedang berlangsung.



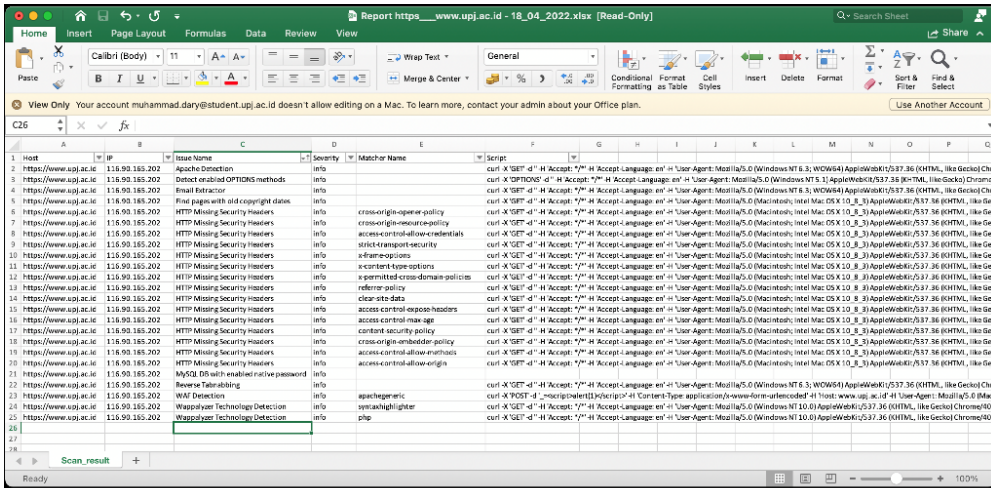
Gambar 6. Tampilan Halaman *Dashboard*.

d. Proses pemindaian
Pengguna mengisi alamat web yang menjadi target untuk pengecekan keamanan web.



Gambar 7. Tampilan Halaman Proses Pemindaian Halaman Web.

e. Report hasil pemindaian
Report hasil pemindaian dapat dilihat melalui file yang didownload melalui menu yang disediakan.



Gambar 8. Report Hasil Pemindaian Web.

KESIMPULAN

Kesimpulan dari penelitian mengenai perancangan aplikasi web pemindaian kerentanan keamanan web yang dapat penulis simpulkan adalah sebagai berikut:

1. Pentingnya atas kesadaran dalam peran krusial keamanan dalam mengembangkan suatu sistem/website agar terhindari dari hal-hal yang tidak diinginkan seperti peretasan yang merugikan kedua belah pihak, pihak konsumen/pengguna yang dirugikan atas kebocoran data dan datanya disalahgunakan. Dan juga pihak yang mempunyai sistem, diminta pertanggungjawaban mengenai perlindungan data pribadi.

2. Kehadiran aplikasi pemindaian web terhadap kerentanan keamanan dapat mempermudah individu/kelompok dalam meningkatkan kesadaran kerentanan keamanan web yang dimilikinya dengan aplikasi pemindaian kerentanan keamanan web ini.

DAFTAR PUSTAKA

Ghozali, B., Kusrini, K., & Sudarmawan, S. (2019). Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating. Creative Information Technology Journal, 4(4), 264. https://doi.org/10.24076/citec.2017v4i4.119.

Ahmed Ali, Abdullah & Zamri Murah, Mohammad. (2018). *Security Assessment of Libyan Government Websites*, 9(12), 583-590.

Dewaweb.com. (2021). OWASP: Standar Keamanan Web App Dunia. https://www.dewaweb.com/blog/owasp-standar-keamanan-web-app-dunia/

Projectdiscovery.io. (2022). Nuclei – Community Powered Vulnerability Scanner. https://nuclei.projectdiscovery.io/

KBBI.web.id. (2022). Kamus Besar Bahasa Indonesia. https://kbbi.web.id/pindai