Implementasi Sistem Kriptografi Hash SHA-256 dan OTP pada Pengembangan Login Page Website Toko Sepatu

Nur Muhammad Kevin[1], Allawy Umar Maula[2] dan Ramadhan Renaldy[3]

[1,2,3]*Jurusan Informatika, Fakultas Teknik dan Informatika, Universitas PGRI Semarang*

Gedung B Lantai 3, Kampus 1 Jl. Sidodadi Timur 24, Semarang

E-mail : nurmkevin532@gmail.com[1], allawyumar37@gmail.com[2], ramadhanrenaldy@upgris.ac.id[3]

Abstrak

Keamanan data pengguna sangat penting saat membuat sistem informasi, terutama pada platform e-commerce seperti situs web toko sepatu, di mana pelanggan melakukan transaksi online dan menyimpan data pribadi mereka. Kegagalan sistem login dapat menyebabkan berbagai risiko keamanan seperti pencurian identitas, akses ilegal, dan penyalahgunaan data pengguna. Tujuan penelitian ini adalah untuk meningkatkan keamanan sistem login dengan menggunakan algoritma Secure Hash Algorithm 256 bit (SHA-256) dan One Time Password (OTP). SHA-256 mengamankan kata sandi melalui proses hashing yang menghasilkan nilai yang unik dan tidak dapat dibalik, sedangkan OTP berfungsi sebagai lapisan autentikasi tambahan yang bersifat dinamis dan sekali pakai.Dengan kombinasi SHA, kedua teknologi ini diharapkan dapat mengurangi serangan seperti brute force, serangan replay, dan penyadapan informasi.

***Kata Kunci*:** Keamanan Data, SHA-256, OTP, Autentikasi, Sistem Login, E-commerce.

I. PENDAHULUAN

1. LATAR BELAKANG

Dalam era digital saat ini, keamanan data pengguna menjadi salah satu aspek yang paling krusial dalam pengembangan sistem informasi, terutama pada platform e-commerce. Website toko sepatu, sebagai salah satu jenis layanan digital yang melibatkan transaksi online dan data pribadi pelanggan, memerlukan sistem autentikasi yang andal untuk melindungi informasi sensitif seperti kata sandi dan detail transaksi. Keamanan yang lemah pada sistem login dapat membuka celah bagi berbagai ancaman keamanan, seperti pencurian identitas, akses ilegal, hingga penyalahgunaan data pengguna.[1] Oleh karena itu, diperlukan pendekatan yang tidak hanya memastikan perlindungan terhadap data pelanggan, tetapi juga mampu meningkatkan kepercayaan pengguna dalam bertransaksi secara online.[2]

Peningkatan keamanan sistem dapat dilakukan dengan menggunakan One Time Password (OTP), yaitu kode sekali pakai yang hanya berlaku dalam waktu yang telah ditentukan. Token adalah kode yang bersifat rahasia atau kunci otentikasi yang digunakan sebagai keamanan yang berupa informasi tentang pemilik.[3] Pada penelitian yang dilakukan memakai algoritma Secure Hash Algorithm 256 bit (SHA-256) yang digunakan untuk hash password dan OTP sebagai verifikasi email. Proses untuk mencari nilai string yang sesuai dihitung secara fleksibel yang

E-ISSN: 2985-3532

menghasilkan menghasilkan message digest dan dapat mencari nilai string yang berbeda dan menghasilkan initisari pesan yang nilainya sama, jadi SHA-256 bisa dikatakan keamanan yang akurat.[4] Asal mulanya algoritma SHA-256 adalah dari algoritma SHA-0 dan SHA-1 yang dikembangkan dan disempurnakan dari algoritma sebelumnya, terdapat berbedaan dari algoritma sebelumnya yaitu nilai blok yang digunakanDesain dari algoritma SHA-256 hampir sama dengan algoritma SHA-2, tetapi berbagai macam serangan tidak dapat dilakukan SHA-256 ini.[5]

Berdasarkan dari latar belakang tersebut, penelitian ini meningkatkan keamanan sistem login menggunakan algoritma SHA-256 dan OTP sebagai verifikasi login, Pendekatan ini diharapkan mampu memberikan perlindungan optimal terhadap ancaman seperti pencurian data, penyadapan informasi, dan akses ilegal.[6] Dengan penerapan algoritma SHA-256, sistem dapat menghasilkan hash yang unik dan tidak dapat dibalik, sehingga kata sandi pengguna lebih aman meskipun terjadi pelanggaran keamanan. Sementara itu, OTP memberikan lapisan autentikasi tambahan yang bersifat dinamis dan tidak dapat digunakan kembali, sehingga risiko serangan replay atau brute force dapat diminimalkan.

Penerapan teknologi ini tidak hanya meningkatkan kepercayaan pelanggan dalam menggunakan layanan toko sepatu online, tetapi juga memperkuat perlindungan terhadap data pribadi dan transaksi. Dengan demikian, pengembangan sistem login berbasis SHA-256 dan OTP memberikan solusi yang efektif dan efisien dalam menciptakan ekosistem e-commerce yang aman, handal, dan ramah pengguna. Penelitian ini juga dapat menjadi acuan bagi pengembang lain dalam mengintegrasikan teknologi kriptografi dan autentikasi modern pada platform digital mereka.

II. METODOLOGI PENELITIAN

1. Metodologi Penelitian

Berikut ini adalah rincian yang digunakan untuk mengamankan data login pengguna agar pengguna dapat yakin bahwa data mereka aman. Sistem ini dirancang menggunakan algoritma SHA-256 untuk melakukan hashing pada password. Hashing dengan SHA-256 menjadikan password tidak dapat dikembalikan ke bentuk aslinya (*one-way function*), sehingga memberikan perlindungan tambahan terhadap serangan seperti *brute force*.[10] Algoritma ini dirancang untuk menghasilkan nilai hash yang unik dan aman, sehingga menjamin kerahasiaan data meskipun terjadi kebocoran basis data. OTP sebagai verifikasi email untuk menambahkan authentikasi keamanan tambahan. Berikut tahapan tahapan dalam pembuatan website Sepatu focus pada login page:

a. Pengumpulan Data

Mengumpulkan data yang dibutuhkan dari keseluruhan elemen sistem yang akan di aplikasikan ke dalam bentuk perangkat lunak, dan mengumpulkan data mengenai Algoritma SHA-256 dan One Time Password (OTP).

b. Desain atau perancangan Aplikasi

Di dalam tahap ini akan dilakukannya proses penulisan kode (coding) dalam bahasa pemrograman yang telah ditentukan, yakni Javascript dengan framework Express.JS dan ReactJS sebagai client server dengan menggunakan database MongoDB serta dijalankan menggunakan web browser.

c. Pengkodean

Pengkodean dilakukan untuk memudahkan dalam mengimplementasikan rancangan login page kedalam algoritma hash SHA-256 dan OTP dengan menggunakan bahasa pemrograman Javascript

E-ISSN: 2985-3532

degan framework ExpressJS dan ReactJS. Kode SHA-256 akan mengenkripsi password ketika register dan OTP sebagai verifikasi tambahan pada email.

d. Implementasi
Rancangan website yang sudah dibuat kemudian diimplementasikan berdasarkan analisismasalahnya.

e. Pengujian
Pengujian dilakukan setelah aplikasi selesai dibuat dengan melakukan beberapa pengujian program dan mencari kesalahan pada program hingga tidak ada lagi kesalahan program dan program sudah berjalan sesuai dengan yang dirancang.

2. Perhitungan

Metode yang kami pakai menggunakan SHA-256 untuk perhitungan hash pada password yang dimana nantinya nilai hash tidak bisa diubah. Berikut penerapan Algoritma SHA-256

Pesan awal (M) = Admin2023-06-05 19:45:45
Input dalam bilangan biner :

01000001	01100100	01101101	01101001	01101110	00110010	00110000	00110010
00110011	00101101	00110000	00110110	00101101	00110000	00110101	00100000
00110001	00111001	00111010	00110100	00110101	00111010	00110100	00110101

1) Penambahan Padding Bit
Penambahan Padding Bit dengan menggunakan rumus
k = l+ 1 = 448 mod 512
k = 192 + 1 = 448 mod 512

01000000	01100100	01101101	01101001	01101110	00110010	00110000	00110010	00110011	00101101
00110000	00110110	00101101	00110000	00110101	00100000	00110001	00111001	00111010	00110100
00110101	00111010	00110100	00110101	10000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000				

k = 193 = 448 mod 512
k =448 –193 = 255, jadi padding bit ‘0’ yang ditambahkan sebanyak 255

2) Panjang Append
Pada Langkah ini panjang data atau pesan dibuat kelipatan 512 bit dari Panjang data atau pesan 64 bit, kemudian hasilnya ditambahkan di hasil akhir.

E-ISSN: 2985-3532

01000001	01100100	01101101	01101001	01101110	00110010	00110010	00110010	00110011	00101101
00110000	00110110	00101101	00110000	00110101	00100000	00110001	00111001	00111010	00110100
00110101	00111010	00110100	00110101	10000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	11000001						

3) Menghitung nilai hash, dengan nilai i=1

$H_0^{(1)} = a + h_0^{(1-1)}$

$= bd0a4laf$

$H_1^{(1)} = b + h_1^{(1-1)}$

$= 69a99bc0 + bb67ae85$

$= 25114a45$

$H_4^{(1)} = e + h_4^{(1-1)}$

$= 7e695ba2 + 510e527f$

$= cf77ae21$

$H_5^{(1)} = f + h_5^{(1-1)}$

$= b07cb434 + 9b05688c$

$= 4b821cc0$

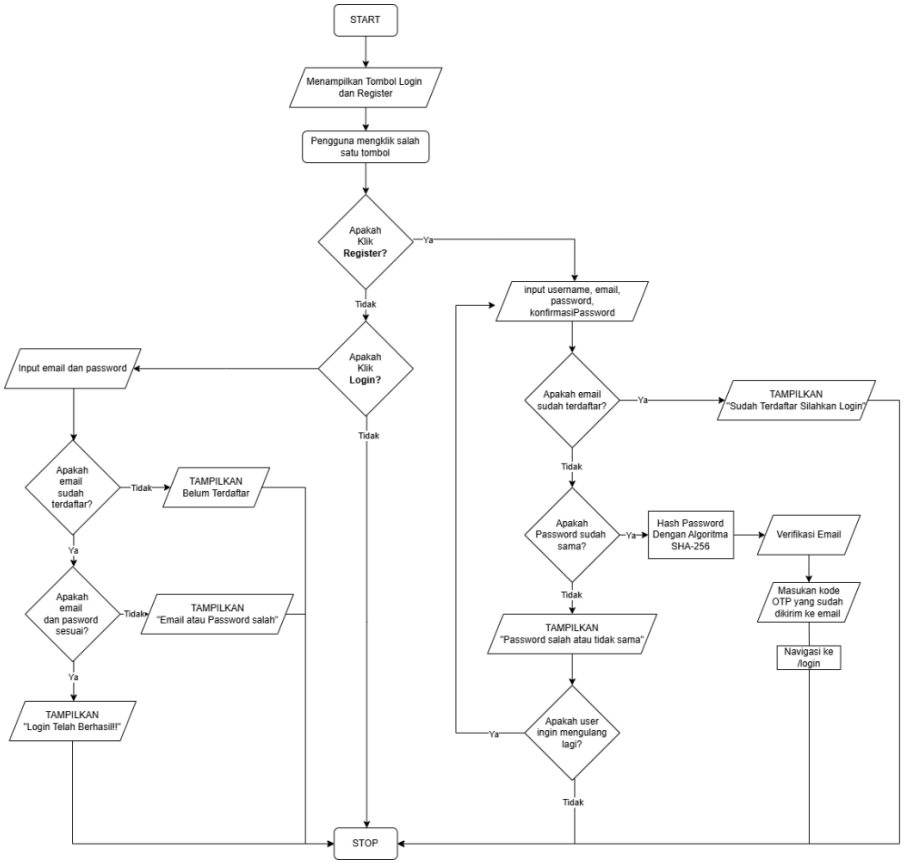
4) Hasil

Tahapan terakhir yaitu hasilakhir dari SHA-256 adalah gabungan dari H0(0) hingga H7(0) adalah: bd0a41af || 25114a45 || b5b23ea0 || c0d29658 || cf77ae21 || 4b821cc0 || 9ef66779 || fdf0f5cb

3. Flowchart

Berikut adalah flowchart untuk sistem register dan login fokus pada bagian register yang dimana keamanan hash SHA-256 dan OTP diimplementasikan

E-ISSN: 2985-3532



Gambar 10 Flowchart Register dan Login

4. Implementasi

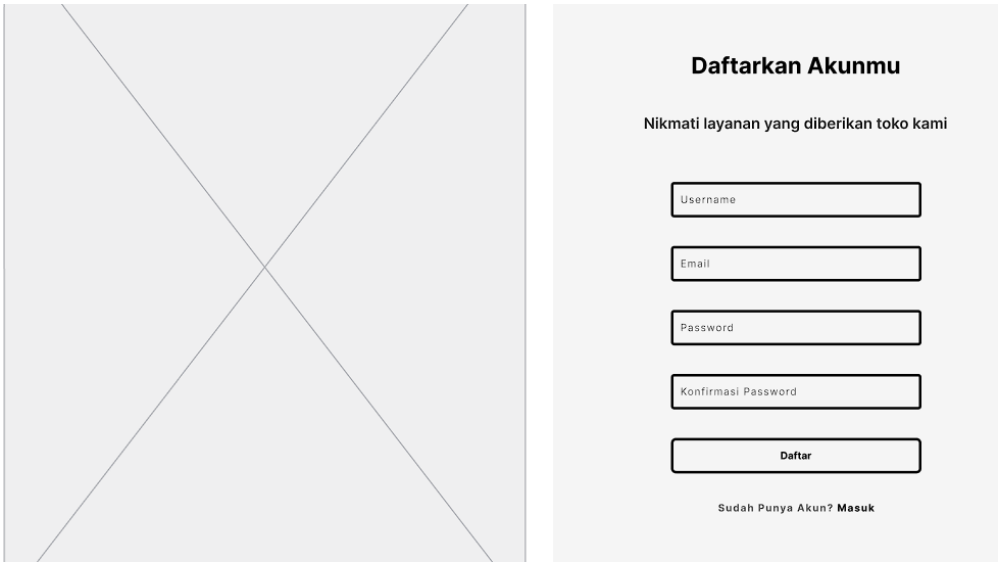
Berikut ini mockup design toko septau yang bernama "**Footware**"

4.1. Login

Gambar 11. Mockup desain Login

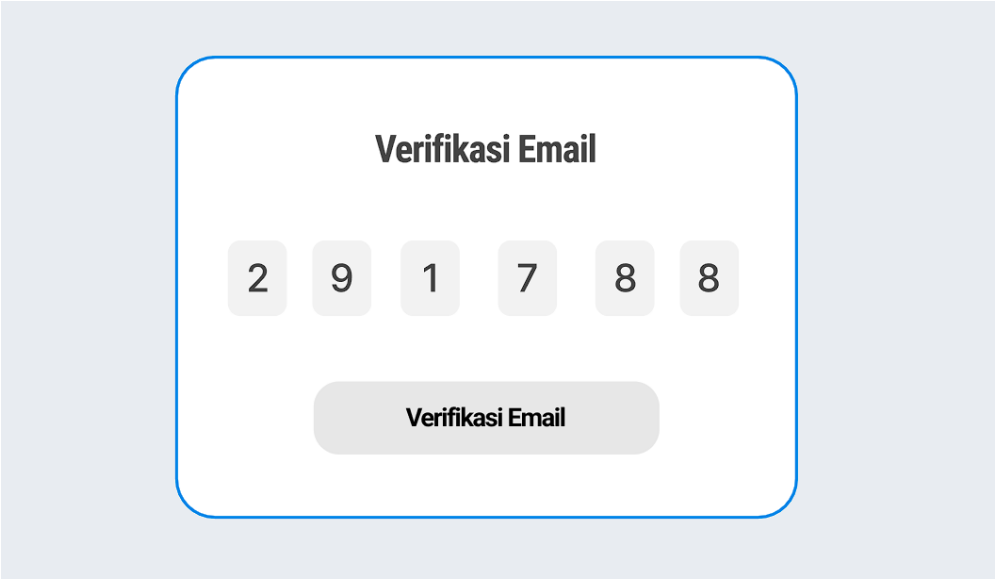
E-ISSN: 2985-3532

4.2. Register



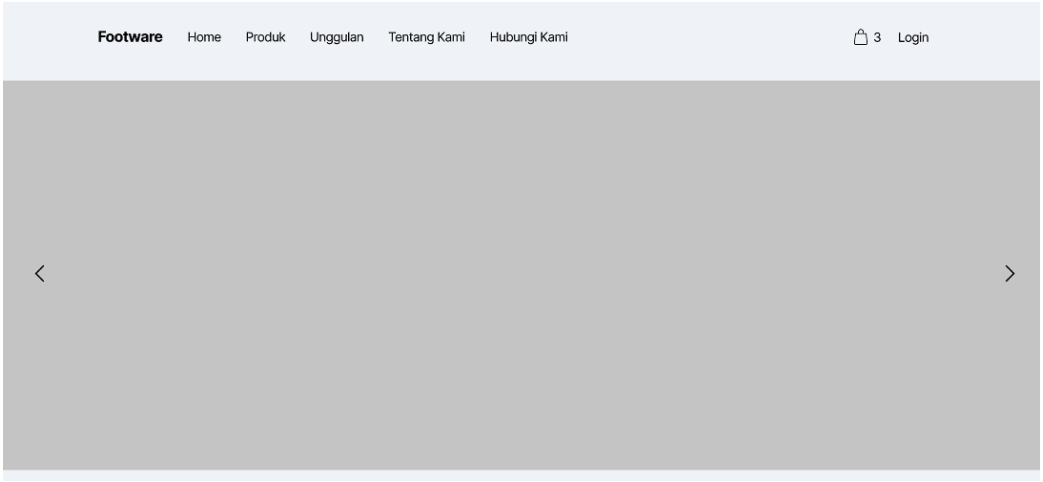
Gambar 12. Mockup design Register

4.3. Verifikasi OTP



Gambar 13. Mockup design OTP

4.4. Halaman Utama



Gambar 14. Mockup design Halaman Utama Toko Sepatu

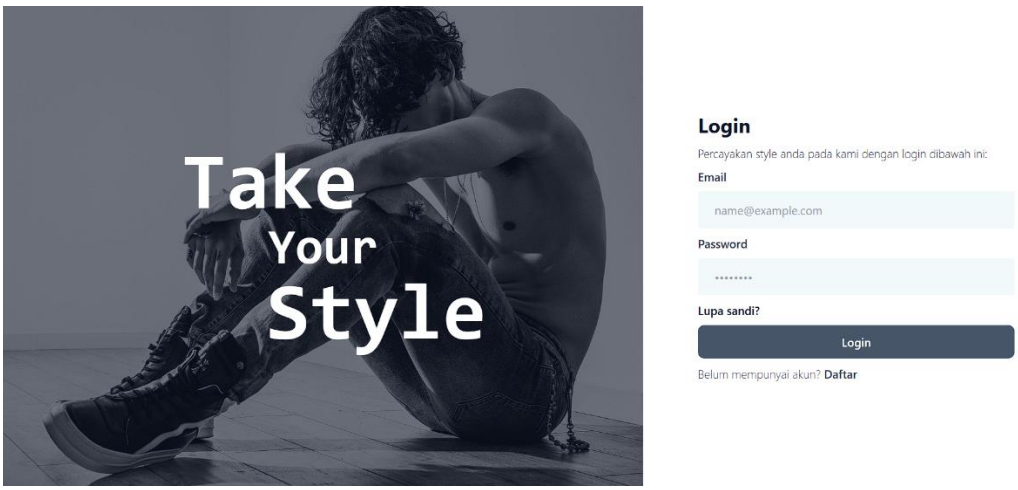
III. HASIL DAN PEMBAHASAN

1. Hasil

Sistem yang telah dikembangkan adalah Website Toko Sepatu yang mengimplementasikan kriptografi hash SHA-256 untuk mengamankan kata sandi pengguna serta OTP (One-Time Password) sebagai verifikasi email untuk meningkatkan keamanan tambahan. Berikut adalah hasil implementasi sistem:

1. Halaman Register
   Tampilan Antarmuka
   - Terdapat input untuk username, email, password dan konfirmasi password
   - Setelah pengguna sudah daftar akun sistem akan diarahkan ke verifikasi email untuk memasukan kode OTP

   Kemanan Kata Sandi
   - Kata sandi pengguna di-hash menggunakan algoritma **SHA-256** sebelum disimpan di basis data. Tidak ada kata sandi yang disimpan dalam bentuk plaintext.

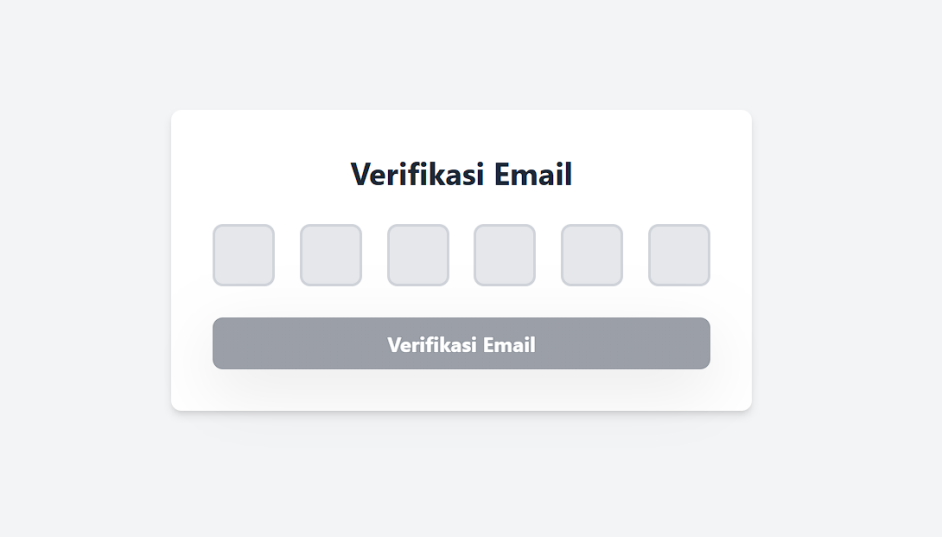


Gambar 15. Login

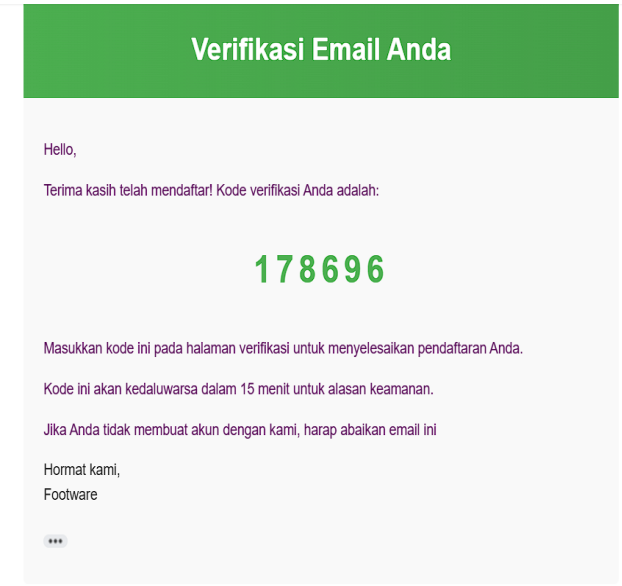
E-ISSN: 2985-3532

Halaman Verifikasi Email dengan OTP

2. Halaman Verifikasi OTP
   Halaman ini akan menampilkan tempat utntuk mengisi kode OTP yang sudah dikirimkan ke dalam email yang sudah diregister



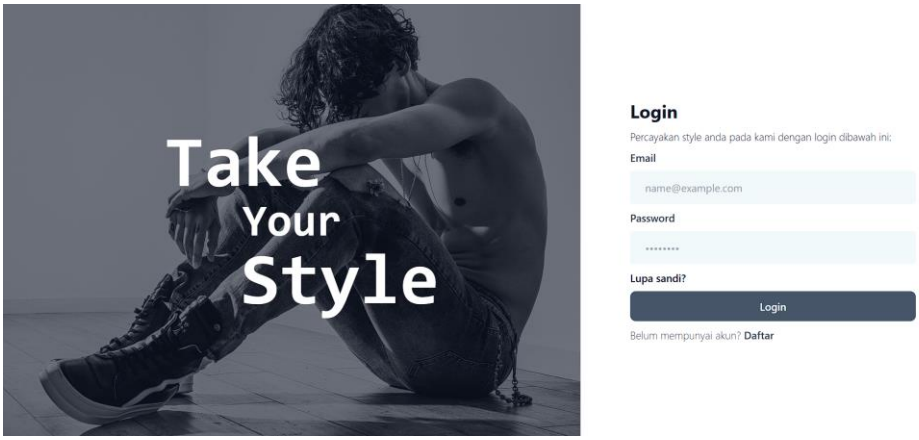
Gambar 16. Halaman Verifikasi Kode OTP



Gambar 17. Kode OTP

3. Halaman Login
   Pada halaman login pengguna bisa memasukan email dan password yang sudah dibuat, didalam sistem password akan di cocokan dengan password yang dihash dan nantinya apabila cocok akan terdapat pesan “Berhasil Login” dan di akan diarahkan ke halaman utama website footware toko sepatu

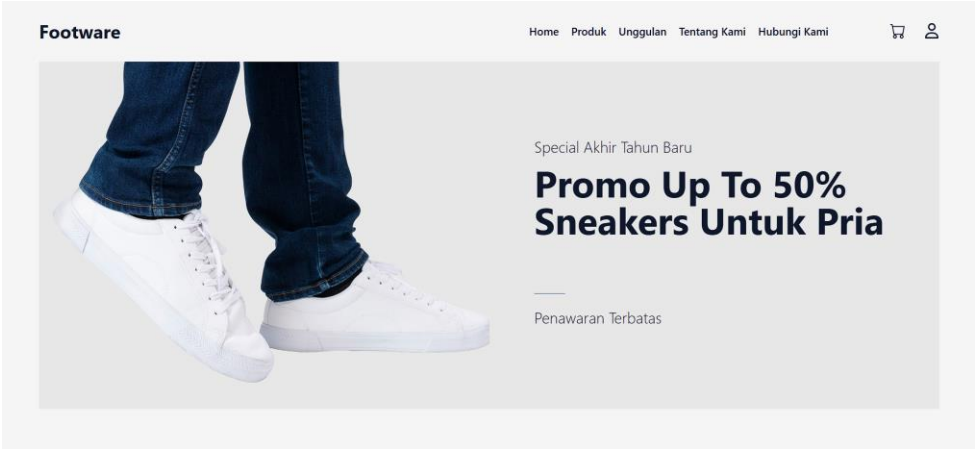
E-ISSN: 2985-3532



4. Basis Data
   Struktur basis data mencakup tabel users untuk menyimpan informasi pengguna, termasuk hash kata sandi,dan kode otp, waktu pembuatan,expired dan statusnya.


```
_id: ObjectId('675e818432e0cab85a072f11')
username: "kevins123"
email: "nurmkevin532@gmail.com"
password: "95c9f6244daf04aed0b8ae294e0372843e643cc28ddab1e936373c68543d8cc6"
role: "user"
isVerified: false
verificationToken: "832678"
verificationTokenExpiresAt: 2024-12-16T07:13:08.436+00:00
lastLogin: 2024-12-15T07:13:08.439+00:00
createdAt: 2024-12-15T07:13:08.443+00:00
updatedAt: 2024-12-15T07:13:08.443+00:00
__v: 0
```


5. Halaman Toko Sepatu "**Footware**"
   Disinilah halaman utama yang bisa diakses untuk berbelanja Sepatu dengan aneka ragam diskon yang diberikan.



Gambar 18. Halam Utama Footware

E-ISSN: 2985-3532

2. Pembahasan

Implementasi Sistem

1. **Kriptografi Hash SHA-256**
   Langkah Kerja**:**
   1. Ketika pengguna mendaftar, kata sandi di-hash menggunakan algoritma SHA-256.
   2. Hasil hash disimpan di basis data.
   3. Saat pengguna login, kata sandi yang dimasukkan di-hash dan dibandingkan dengan nilai hash di basis data.

   Keunggulan

   SHA-256 memberikan keamanan tinggi karena bersifat one-way dan sulit direversi.

2. **One-Time Password (OTP)**
   Langkah Kerja:
   1. Sistem menghasilkan kode OTP 6 digit acak menggunakan pustaka seperti pyotp atau algoritma serupa.
   2. Kode dikirimkan ke email pengguna menggunakan layanan pengiriman email seperti SMTP atau API pihak ketiga.
   3. OTP disimpan di basis data dengan timestamp untuk validasi masa berlaku.

   Keunggulan:

   Menambah lapisan keamanan dan mencegah akses tidak sah meskipun kredensial pengguna bocor.

IV. KESIMPULAN

Kesimpulan dari pengembangan sistem login pada Website Toko Sepatu menunjukkan bahwa penerapan metode kriptografi hash SHA-256 dan One-Time Password (OTP) berhasil meningkatkan keamanan sistem secara signifikan. Masalah keamanan, seperti risiko pencurian data akibat penyimpanan kata sandi dalam bentuk plaintext, dapat diatasi melalui penerapan SHA-256 yang mengubah kata sandi menjadi hash bersifat one-way. Hal ini memastikan bahwa data kata sandi tetap aman meskipun terjadi pelanggaran pada basis data. Selain itu, penggunaan OTP sebagai lapisan autentikasi tambahan mampu mencegah akses tidak sah, meskipun kredensial utama pengguna telah diketahui pihak lain.

Proses pengembangan sistem ini tidak hanya berfokus pada keamanan, tetapi juga menjaga kenyamanan pengguna. Dengan integrasi layanan pengiriman email yang andal dan validasi kode OTP yang efisien, sistem mampu memberikan pengalaman login yang aman dan user-friendly. Secara keseluruhan, implementasi metode ini menjadi solusi yang efektif untuk memenuhi kebutuhan keamanan modern dalam aplikasi berbasis web. Sistem ini dapat dikembangkan lebih lanjut dengan menambahkan fitur keamanan tambahan, seperti enkripsi end-to-end atau deteksi anomali pada aktivitas pengguna, untuk meningkatkan perlindungan data dan pengalaman pengguna.

VI. REFERENSI

[1] Azhar, Arkarni Wais, and Atthariq, “Sistem Keamanan Pada Halaman Login

E-ISSN: 2985-3532

Menggunakan One Time Password," *J. Embed. Syst. Secur. Intell. Syst.*, vol. 01, no. 2, pp. 106–113, 2020.

[2] H. S. W. Mujianto, Nur Iswatun Khasanah Ahmad, "Peningkatan Sistem Keamanan One Time Password(Otp) Pada Token Aplikasi Computer Based Test (Cbt) Menggunakan Algoritma Sha-256," vol. 01, pp. 1–23, 2023.

[3] H. Setiawan, D. Sartika, and B. G. Ramadhan, "Implementasi Time-Based One Time Password (Totp) Pada Sistem Two Factor Authentication (2Fa)," *J. Teknol.*, vol. 13, no. 1, pp. 63–68, 2020.

[4] E. al. Manish Rana, "Enhancing Data Security: A Comprehensive Study on the Efficacy of JSON Web Token (JWT) and HMAC SHA-256 Algorithm for Web Application Security," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 11, no. 9, pp. 4409–4416, 2023, doi: 10.17762/ijritcc.v11i9.9930.

[5] F. Basya, M. Hardjanto, and I. Permana Putra, "SHA512 and MD5 Algorithm Vulnerability Testing Using Common Vulnerability Scoring System (CVSS)," *Buana Inf. Technol. Comput. Sci. (BIT CS)*, vol. 3, no. 1, pp. 1–4, 2022, doi: 10.36805/bit-cs.v3i1.2046.

[6] R. Rizki and S. Mulyati, "Implementasi One Time Password Menggunakan Algoritma SHA-512 Pada Aplikasi Penagihan Hutang PT. XHT," *Edumatic J. Pendidik. Inform.*, vol. 4, no. 1, pp. 111–120, 2020, doi: 10.29408/edumatic.v4i1.2158.

[7] A. Prayogo and M. A. Rony, "Implementasi One Time Password pada Sistem Login dengan Algoritma SHA-256 dan DES pada Aplikasi EO Blucampus Berbasis Client Server," *Skanika*, vol. 1, no. 2, pp. 146–152, 2018.

[8] J. P. Yapo, I. Wahidah, and Fahdan, "Analisis Sistem Autentikasi Otp Data Medis Dengan Menggunakan Teknik Embbeded Symmetric Key," *e-Proceeding Eng.*, vol. 9, no. 2, pp. 388–395, 2022.

[9] M. Anwar Fauzi, A. Id Hadiana, and F. Rakhmat Umbara, "Penambahan Fitur Multi-Factor Authentication Dalam Studi Kasus Sistem Informasi Rekam Medis Rumah Sakit," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 7, no. 4, pp. 2938–2944, 2024, doi: 10.36040/jati.v7i4.7305.

[10] N. Khairiyah, Y. Hendriyani, A. Hadi, and L. Mursyida, "Hash-Based Authentication Code Algorithm for Quick Response (QR) Code as Digital Signature," pp. 7–12, 2023, doi: 10.24036/int.j.emerg.technol.eng.educ..v1i1.2.