

Audit Keamanan Aplikasi Web: Studi Kasus pada Website E-Commerce Warung Ayam Goreng Selimut Griya Cirebon

Sisca Amalia Putri¹, Nadila Amelia², Khairul Ihwan³, Muhammad Amin⁴

^{1,2}Sistem Informasi, Fakultas Teknik dan Ilmu Komputer, Universitas Islam Indragiri

Email: siskaputri1203@gmail.com¹, amelianadila34@gmail.com,
ihwanp5@gmail.com³, ma618152@gmail.com⁴

ABSTRAK

Keamanan aplikasi web menjadi aspek yang sangat penting dalam era digital saat ini, terutama bagi situs e-commerce yang menangani transaksi keuangan dan data pribadi pelanggan. Penelitian ini bertujuan untuk melakukan audit keamanan pada website e-commerce ayam goreng selimut[1]. Metodologi yang digunakan dalam audit ini adalah analisis risiko, dan evaluasi terhadap standar keamanan web seperti SiteCheck by Sucuri. Hasil penelitian menunjukkan adanya beberapa kerentanan pada aplikasi web ayam goreng selimut yang perlu segera ditangani untuk menghindari potensi ancaman keamanan[2].

Kata Kunci: Aplikasi Web, Audit, E-Commerce, Keamanan Web

ABSTRACT

Web application security is a very important aspect in today's digital era, especially for e-commerce sites that handle financial transactions and customer personal data. This research aims to conduct a security audit on the ayam goreng selimut e-commerce website. The methodology used in this audit is risk analysis, and evaluation against SiteCheck by Sucuri. The results showed that there are several vulnerabilities in the ayam goreng selimut web application that need to be addressed immediately to avoid potential security threats.

Keywords: Web Application, Audit, E-Commerce, Web Security

1 PENDAHULUAN

Keamanan aplikasi web merupakan prioritas utama bagi perusahaan e-commerce yang beroperasi secara online. Website e-commerce ayam goreng selimut merupakan salah satu platform yang digunakan oleh banyak pengguna untuk melakukan transaksi jual beli secara digital. Oleh karena itu, penting untuk memastikan bahwa website ini aman dari berbagai ancaman siber. Tujuan dari penelitian ini adalah untuk mengidentifikasi dan mengevaluasi kerentanan keamanan pada website e-commerce ayam goreng selimut serta memberikan rekomendasi perbaikan.

Website e-commerce ayam goreng selimut, sebagai platform yang digunakan untuk transaksi jual beli online, menyimpan berbagai informasi sensitif pelanggan, seperti data pribadi dan rincian pembayaran, yang menjadikannya target potensial bagi para penyerang.

Audit secara umum adalah proses terpadu dalam pengumpulan dan penilaian terhadap informasi sebagai satu kesatuan organisasi oleh seorang ahli. Pengertian audit sistem informasi adalah proses pengumpulan dan evaluasi bukti-bukti untuk menentukan apakah sistem komputer yang digunakan telah dapat melindungi aset milik organisasi, mampu menjaga integritas data, dapat membantu pencapaian tujuan organisasi secara efektif, serta menggunakan sumber daya yang dimiliki secara efisien[3]. Dalam konteks website e-commerce, audit keamanan membantu dalam mendeteksi kelemahan yang dapat dieksploitasi dan memberikan rekomendasi untuk perbaikan demi melindungi data pengguna dan menjaga integritas sistem.

Metodologi yang digunakan dalam audit ini mencakup analisis SWOT (Strengths, Weaknesses, Opportunities, Threats) dan pengujian penetrasi menggunakan alat-alat otomatis

seperti SiteCheck by Sucuri. Analisis SWOT memberikan gambaran menyeluruh mengenai kekuatan dan kelemahan internal serta peluang dan ancaman eksternal yang dihadapi oleh website e-commerce ayam goreng selimut. Pengujian penetrasi bertujuan untuk mensimulasikan serangan siber guna mengidentifikasi kerentanan yang mungkin tidak terlihat dalam pengujian biasa.

Penelitian ini berfokus pada evaluasi keamanan website e-commerce ayam goreng selimut dengan tujuan untuk:

1. Mengidentifikasi kekuatan dan kelemahan dalam sistem keamanan yang ada.
2. Mengevaluasi peluang untuk perbaikan keamanan.
3. Mengidentifikasi ancaman yang dihadapi oleh website.
4. Menyusun rekomendasi perbaikan berdasarkan temuan audit.

Dengan demikian, penelitian ini diharapkan dapat memberikan wawasan yang berguna bagi pengelola website e-commerce ayam goreng selimut dalam meningkatkan keamanan aplikasi web mereka, serta memberikan kontribusi dalam literatur mengenai audit keamanan aplikasi web di era digital.

Menurut Mc Load dalam Darmawan dan Fauzi (2013:04), "Sistem adalah sekelompok elemen elemen yang terintegrasi dengan tujuan yang sama untuk mencapai tujuan". Sedangkan menurut Sutabri (2012:06) "Sistem adalah sekelompok unsur yang erat hubungannya satu dengan yang lain, yang berfungsi bersama-sama untuk mencapai tujuan tertentu"[4].

Pengertian informasi menurut (Martin Halomoan Lumbangaol, 2020) informasi adalah hasil dari pemrosesan data yang relevan dan memiliki manfaat bagi penggunanya[2].

Pengertian sistem informasi menurut (Jonny Seah, 2020) sistem informasi merupakan gabungan dari berbagai komponen teknologi informasi yang saling bekerjasama dan menghasilkan suatu informasi guna untuk memperoleh satu jalur komunikasi dalam suatu organisasi atau kelompok[2].

Pengertian audit sistem informasi menurut (Ron Weber, 1999) adalah proses mengumpulkan dan mengavaluasi fakta untuk memutuskan apakah sistem komputer yang merupakan aset perusahaan terlindungi, integritas data terpelihara, sesuai dengan tujuan organisasi untuk mencapai efektifitas dan efisiensi dalam penggunaan sumber daya[5].

E-Commerce merupakan suatu transaksi saling tukar menukar barang antar satu dengan yang lainnya untuk memenuhi kebutuhan sehari-hari secara digital[6].

2 METODE PENELITIAN

Metode penelitian yang digunakan dalam audit keamanan aplikasi web pada website e-commerce Ayam Goreng Selimut ini melibatkan beberapa langkah utama, yaitu :

1. Pengumpulan Data: Mengumpulkan dan mempelajari dokumentasi teknis yang ada, termasuk diagram arsitektur, kode sumber, dan kebijakan keamanan.
2. Pengujian Penetrasi: melakukan pengujian penetrasi manual pada modul-modul kritis, seperti pencarian produk dan komentar pengguna, untuk mendeteksi kerentanan seperti SQL Injection dan XSS.
3. Pendekatan Penelitian
Penelitian ini menggunakan pendekatan deskriptif kualitatif untuk menganalisis keamanan aplikasi web pada website e-commerce ayam goreng selimut. Metode ini dipilih karena memungkinkan peneliti untuk menggambarkan situasi saat ini dan memberikan rekomendasi yang dapat diterapkan berdasarkan temuan yang ada.
4. Pengumpulan Data
Pengumpulan data dilakukan melalui dua tahap utama: analisis SWOT dan audit keamanan menggunakan alat SiteCheck by Sucuri.
 - a. Analisis SWOT

Analisis SWOT digunakan untuk mengidentifikasi Strengths (Kekuatan), Weaknesses (Kelemahan), Opportunities (Peluang), dan Threats (Ancaman) dari sistem keamanan aplikasi web e-commerce ayam goreng selimut. Data untuk analisis SWOT dikumpulkan melalui Observasi langsung dengan cara Mengamati proses pengembangan dan penerapan kebijakan keamanan di lingkungan kerja[7].

b. Audit Keamanan dengan SiteCheck by Sucuri

SiteCheck by Sucuri adalah server penyedia jasa scanner online gratis yang bisa digunakan oleh umum untuk melakukan testing terhadap kerentanan keamanan yang bisa juga digunakan untuk melakukan pemindaian keamanan pada website e-commerce ayam goreng selimut[8]. Langkah-langkah audit menggunakan SiteCheck by Sucuri adalah sebagai berikut:

- Pemindaian Awal: Menjalankan SiteCheck by Sucuri pada website e-commerce ayam goreng selimut untuk mendeteksi adanya malware, kesalahan konfigurasi, dan kerentanan keamanan lainnya.
- Analisis Hasil Pemindaian: Mengkaji hasil pemindaian untuk mengidentifikasi area-area yang memerlukan perbaikan dan potensi ancaman keamanan.
- Dokumentasi Temuan: Mencatat semua temuan dari pemindaian untuk dianalisis lebih lanjut dalam konteks analisis SWOT.

5. Analisis Data

Data yang dikumpulkan dari analisis SWOT dan pemindaian keamanan menggunakan SiteCheck by Sucuri dianalisis dengan langkah-langkah berikut:

- Kategorisasi Temuan: Mengelompokkan temuan dari pemindaian SiteCheck by Sucuri ke dalam kategori SWOT (Strengths, Weaknesses, Opportunities, Threats).
- Evaluasi Keamanan: Menilai dampak dan signifikansi setiap temuan terhadap keamanan aplikasi web.
- Sintesis Informasi: Menggabungkan hasil analisis SWOT dengan temuan pemindaian untuk memberikan gambaran komprehensif tentang kondisi keamanan website e-commerce ayam goreng selimut.
- Rekomendasi: Menyusun rekomendasi berdasarkan hasil analisis untuk meningkatkan keamanan aplikasi web.

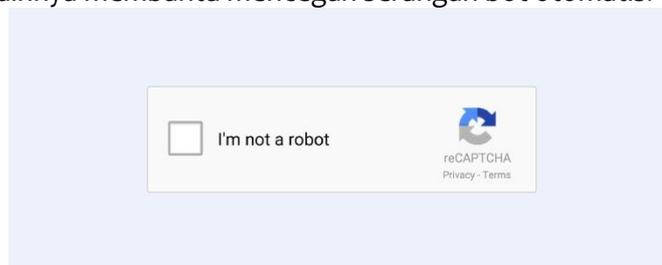
3 HASIL DAN PEMBAHASAN

Hasil:

1. Hasil Analisis SWOT

a. Strengths (Kekuatan):

- Keamanan SSL/TLS: Website e-commerce ayam goreng selimut menggunakan protokol SSL/TLS yang kuat untuk mengenkripsi data yang dikirimkan antara pengguna dan server. Ini membantu melindungi informasi pribadi dan transaksi keuangan pelanggan.
- Penggunaan CAPTCHA: Implementasi CAPTCHA pada halaman login dan formulir lainnya membantu mencegah serangan bot otomatis.



Gambar 1 contoh Captcha

- Pembaruan Berkala: Tim pengembang secara rutin memperbarui sistem dan aplikasi untuk mengatasi kerentanan keamanan yang baru ditemukan.
 - b. Weaknesses (Kelemahan):
 - Validasi Input yang Lemah: Ditemukan bahwa beberapa formulir input tidak memiliki validasi yang memadai, membuka peluang untuk serangan injeksi SQL dan XSS.
 - Konfigurasi Server yang Rentan: Beberapa konfigurasi server, seperti direktori yang dapat diindeks, masih terbuka, memungkinkan potensi eksploitasi.
 - Pengelolaan Patch yang Lambat: Terdapat jeda waktu yang signifikan antara rilis patch keamanan dan implementasinya di sistem produksi, meningkatkan risiko terhadap serangan yang memanfaatkan kerentanan yang diketahui.
 - c. Opportunities (Peluang):
 - Implementasi Sistem Keamanan Tambahan: Penerapan solusi keamanan tambahan seperti firewall aplikasi web (WAF) dapat lebih meningkatkan perlindungan terhadap serangan.
 - Edukasi Keamanan Karyawan: Pelatihan rutin tentang praktik keamanan terbaik dapat meningkatkan kesadaran dan kemampuan karyawan dalam menjaga keamanan sistem.
 - Integrasi dengan Sistem Keamanan Pihak Ketiga: Menggunakan layanan keamanan dari pihak ketiga seperti Cloudflare untuk mitigasi serangan DDoS dapat memberikan perlindungan ekstra.
 - d. Threats (Ancaman):
 - Serangan DDoS: Ancaman serangan DDoS yang dapat menyebabkan downtime dan gangguan layanan, merugikan bisnis dan pengalaman pelanggan.
 - Eksploitasi Kerentanan Zero-Day: Ancaman dari kerentanan zero-day yang belum memiliki patch tersedia, dapat dieksploitasi oleh penyerang yang canggih.
 - Phishing: Ancaman serangan phishing yang menargetkan pelanggan, berpotensi mencuri informasi pribadi dan finansial.
2. Hasil Pemindaian Keamanan Menggunakan SiteCheck by Sucuri
- Pemindaian menggunakan SiteCheck by Sucuri mengungkapkan beberapa temuan penting:
- Malware: Tidak ditemukan adanya malware yang terdeteksi pada website e-commerce ayam goreng selimut.
 - Blacklist: Website tidak masuk dalam daftar hitam (blacklist) mesin pencari atau layanan keamanan lainnya.
 - Kerentanan Keamanan: SiteCheck mendeteksi beberapa kerentanan keamanan terkait plugin dan tema yang digunakan pada platform website, yang perlu segera diperbarui.
 - HTTPS: Sertifikat SSL/TLS terpasang dengan benar dan tidak ada masalah terkait HTTPS.
 - Pengaturan Keamanan: Beberapa pengaturan keamanan seperti header keamanan HTTP (Content Security Policy, X-Frame-Options) belum diimplementasikan dengan baik.

Pembahasan:

1. Keamanan SSL/TLS dan Penggunaan CAPTCHA:

Kekuatan utama website e-commerce ayam goreng selimut adalah penggunaan SSL/TLS yang memastikan keamanan transmisi data dan CAPTCHA yang membantu mencegah serangan otomatis. Kedua elemen ini sangat penting dalam menjaga keamanan data pelanggan dan mencegah akses tidak sah.

2. Kelemahan dalam Validasi Input dan Konfigurasi Server

Analisis mengungkapkan bahwa validasi input yang lemah dan konfigurasi server yang rentan menjadi titik lemah utama dalam sistem. Ini membuka peluang bagi penyerang untuk melakukan serangan injeksi dan eksploitasi lainnya. Diperlukan pengetatan validasi input dan penyesuaian konfigurasi server untuk mengurangi risiko ini.

3. Peluang untuk Meningkatkan Keamanan:

Peluang untuk meningkatkan keamanan termasuk implementasi firewall aplikasi web (WAF), edukasi keamanan karyawan, dan integrasi dengan sistem keamanan pihak ketiga. Langkah-langkah ini dapat memberikan lapisan perlindungan tambahan terhadap berbagai ancaman.

4. Ancaman yang Dihadapi:

Serangan DDoS, kerentanan zero-day, dan phishing adalah ancaman yang signifikan. Menggunakan layanan mitigasi DDoS dan meningkatkan kesadaran pelanggan tentang phishing dapat membantu mengurangi dampak dari ancaman ini.

5. Hasil Pemindaian SiteCheck by Sucuri:

Pemindaian SiteCheck menunjukkan bahwa meskipun tidak ada malware yang ditemukan, masih ada beberapa kerentanan yang perlu ditangani, terutama terkait plugin dan tema yang digunakan. Pengaturan keamanan HTTP yang lebih baik juga perlu diimplementasikan untuk meningkatkan perlindungan.

4 KESIMPULAN

Penelitian ini telah mengevaluasi keamanan aplikasi web pada website e-commerce ayam goreng selimut dengan menggunakan metode analisis SWOT dan alat pemindai keamanan SiteCheck by Sucuri. Hasil analisis menunjukkan bahwa website e-commerce ayam goreng selimut memiliki beberapa kekuatan, seperti penggunaan protokol SSL/TLS yang kuat dan implementasi CAPTCHA yang efektif dalam mencegah serangan bot otomatis. Namun, terdapat kelemahan signifikan, terutama dalam validasi input yang lemah dan konfigurasi server yang rentan, yang dapat menjadi titik masuk bagi penyerang untuk melakukan berbagai eksploitasi.

Pemindaian dengan SiteCheck by Sucuri menunjukkan bahwa tidak ada malware yang ditemukan dan website tidak masuk dalam daftar hitam. Namun, beberapa kerentanan terkait plugin dan tema yang digunakan ditemukan, yang memerlukan perhatian dan pembaruan segera. Selain itu, pengaturan keamanan HTTP perlu diperbaiki untuk meningkatkan perlindungan secara keseluruhan.

Untuk meningkatkan keamanan, terdapat beberapa peluang yang dapat dimanfaatkan, seperti penerapan firewall aplikasi web (WAF), pelatihan keamanan bagi karyawan, dan integrasi dengan layanan keamanan pihak ketiga. Ancaman seperti serangan DDoS, eksploitasi kerentanan zero-day, dan serangan phishing harus diantisipasi dengan langkah-langkah proaktif, termasuk mitigasi serangan DDoS dan edukasi pelanggan mengenai phishing.

Secara keseluruhan, meskipun website e-commerce ayam goreng selimut memiliki dasar keamanan yang baik, ada beberapa area kritis yang memerlukan perbaikan dan peningkatan. Dengan mengimplementasikan rekomendasi yang dihasilkan dari analisis ini, website e-commerce Ayam Goreng Selimut dapat meningkatkan keamanan dan keandalannya, memberikan perlindungan yang lebih baik bagi pengguna dan data mereka.

REFERENSI

- [1] S. Y. Awibi Nazhicol Amin, Eva Ana Rianti, Pramodya Hanggarany, "Wps_Lid." 2023.
- [2] W. C. Pamungkas and F. T. Saputra, "Evaluasi Keamanan Informasi Pada SMA N 1 Sentolo Berdasarkan Indeks Keamanan Informasi (KAMI) ISO/IEC 27001:2013," *J. Sist. Komput. dan Inform.*, vol. 1, no. 2, p. 101, 2020, doi: 10.30865/json.v1i2.1924.
- [3] G. A. Hanindito, "Analisis dan Audit Sistem Manajemen Keamanan Informasi (SMKI) pada Instansi Perpustakaan dan Arsip Daerah Kota Salatiga," *J. Nas. Teknol. dan Sist. Inf.*, vol. 3, no. 2, pp. 279–284, 2017, doi: 10.25077/teknosi.v3i2.2017.279-284.
- [4] Riswandi, "Transaksi On-Line (E-Commerce) : Peluang dan Tantangan Dalam Perspektif Ekonomi Islam," *Angew. Chemie Int. Ed.* 6(11), 951–952., vol. 13, no. April, pp. 15–38, 2019.
- [5] F. Hidayatullah and F. Komputer, "Audit Sistem Informasi Menurut Para Ahli".

- [6] M. Mashuri and D. Nurjannah, “Analisis SWOT Sebagai Strategi Meningkatkan Daya Saing,” *JPS (Jurnal Perbank. Syariah)*, vol. 1, no. 1, pp. 97–112, 2020, doi: 10.46367/jps.v1i1.205.
- [7] Purwantoro, “Implementasi Metode Online Scanner Untuk Mencari Kerentanan Keamanan (Vulnerability) Server (Studi Kasus: Website www.unsika.ac.id),” *J. Rekayasa Inf.*, vol. 6, no. 1, pp. 25–37, 2017.
- [8] M. P. Mokodompit and N. Nurlaela, “Evaluasi Keamanan Sistem Informasi Akademik Menggunakan ISO 17799:2000 (Studi Kasus Pada Peguruan Tinggi X),” *J. Sist. Inf. Bisnis*, vol. 6, no. 2, p. 97, 2017, doi: 10.21456/vol6iss2pp97-104.