AUDIT KEAMANAN PROGAM APLIKASI E-DOKUMEN KAMPUS DENGAN METODE *CODE REVIEW* DAN *ACTION RESEARCH*

Bili Renaldi[1], Heri Suroyo[2]
Fakultas Ilmu Komputer, Universitas Bina Darma
Email: 161410187@student.binadarma.ac.id[1], herisuroyo@binadarma.ac.id[2]

ABSTRAK

Program aplikasi E-Dokumen dan juga melakukan peningkatan keamaanan sistem E-dokumen. Penelitian ini akan menggunakan metode code reviews dan penetration testing karena di metode ini peneliti dapat dengan mudah untuk melakukan proses peneltitan karena metode ini merupakan salah satu metode yang paling sering digunakan dalam melakukan audit keamananWebsite E-Dokumen merupakan website yang dimiliki oleh Kampus yang digunakan untuk memanajemen dokumen-dokumen yang dimiliki oleh dosen ataupun pegawai Kampus. Audit keamana merupkan penilaian atau evaluasi teknis kemamanan sistem. Dengan dilakukanya penelitian ini maka diharapkan dapat secara langsung untuk menambah atau meningkatkan keamanan pada program aplikasi E-Dokumen Kampus.

Kata Kunci: Sql-Injection,Cross Site Scripting,E-Dokumen,Audit Keamanan.

ABSTRACT

E-Document application program and also improve the security of E-document system. This research will use code reviews and penetration testing methods because in this method researchers can easily carry out the research process because this method is one of the most frequently used methods in conducting security audits. The E-Document website is a website owned by the campus that is used for management documents owned by lecturers or campus employees. A security audit is an assessment or technical evaluation of system security. By doing this research, it is hoped that it can directly add or improve security in the Campus E-Document application program.

Keywords: *Sql-Injection, Cross Site Scripting, E-Documents, Security Audit.*

1. PENDAHULUAN

Sistem manajemen dokumen adalah sistem komputer (atau sekumpulan program komputer) yang digunakan untuk menelusuri dan menyimpan dokumen dan gambar elektronik dalam dokumen. DMS sangat berguna dalam mepermudah dan menyederhanakan proses bisnis. Manfaat utama bagi pengguna adalah mereka dapat dengan cepat menemukan informasi yang mereka butuhkan, yang dapat membuat proses menjadi lebih cepat, lebih baik, dan lebih murah [2]. Sementara itu Suryana [3] meyakini bahwa Document Management System (DMS) adalah sistem manajemen dokumen yang dikembangkan oleh Unikom Center untuk mengatur dan mengelola surat atau dokumen penting sehingga dapat dengan mudah ditemukan dan sistem pengelolaan dokumen yang bermanfaat dapat didaur ulang. Sederhanakan dan sederhanakan proses bisnis. Manfaat utamanya adalah pengguna dapat dengan cepat menemukan informasi yang mereka butuhkan, yang dapat membuat prosesnya lebih cepat, lebih baik, dan lebih murah.

Keamanan merupakan faktor penting dalam sistem, sistem yang baik adalah sistem dengan keamanan yang baik, karena jika keamanan sistem terganggu maka kepercayaan pengguna sistem akan berkurang, dan lebih parah lagi, sistem akan ditinggalkan. Berdasarkan informasi di atas, demi menjaga kenyamanan dan

keamanan pengguna aplikasi dokumen elektronik Kampus maka pengamanan aplikasi dokumen elektronik Kampus sangat diperlukan. Website dokumen elektronik merupakan salah satu aplikasi yang dimiliki oleh Kampus, Dokumen elektronik digunakan untuk mengelola semua dokumen yang ada, seperti pdf, doc, ppt, dll. Dokumen elektronik itu sendiri berada di http://e-doc.binadarma.ac.id. Oleh karena itu untuk menjaga keamanan dokumen dan data pada website E-Document, maka penting untuk meningkatkan keamanan aplikasi E-Document untuk mencegah serangan sql-injection, sehingga aplikasi tersebut sangat penting untuk mendukung pembelajaran. Proses Manajemen Kampus. Hal tersebut dapat diatasi dengan melakukan audit keamanan sistem informasi e-dokumen dengan menggunakan metode *Action Research* dan dengan mennggunakan teknik *Code Review*. *Code Review* bertujuan untuk memastikan kode dapat dimengerti dengan baik, terstruktur rapi, dan tidak adanya kecacatan dalam desain dan pemrograman [1].

2. METODOLOGI PENELITIAN

2.1 Waktu dan Tempat

Penelitian ini dilakukan di Rumah Peneliti sendiri karena *Source Code* Program Aplikasi E-Dokumen sudah peneliti miliki. Penelitian ini dimulai pada tanggal 24 Agustus 2020 sampai dengan selesai.

2.2 Alat dan Bahan Penelitian

Bahan yang digunakan dalam penelitian ini adalah *Source Code* Prorgram Aplikasi E-Dokumen, yang telah dijinkan oleh pembuat Program untuk digunakan dalam proses penelitian. Serta alat yang gunakan dalam proses penelitian ini adalah satu buah laptop Asus dan dua buah *Software Automate code review* yaitu *Visual Code Grepper* dan *RIPS 0.5*. Alasan dipilih dua *tools* karena *open source* dan bebas untuk digunakan.

2.3 Metode Pengumpulan Data

Metode pengumpulan data yang digunakan dalam penelitian ini adalah:

a. Observasi

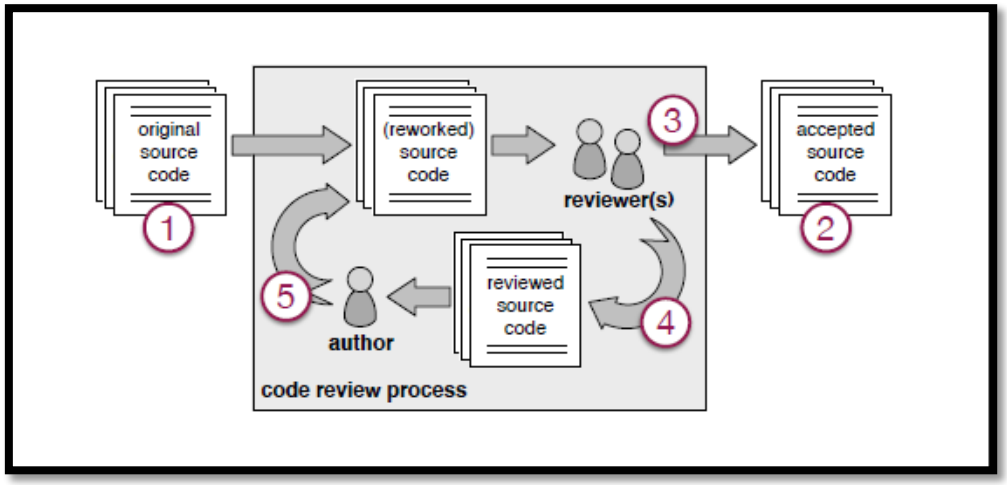
Metode pembuatan observasi atau observasi ini adalah dengan melihat kode-kode yang ada pada sistem file elektronik dan melakukan pengujian langsung pada sistem file elektronik.

b. Studi Literasi.

Peneliti melakukan studi literasi untuk memahami pengetahuan yang ada tentang sistem audit dan pengetahuan yang perlu dipelajari.Kajian literasi ini dilakukan dengan membaca buku dan jurnal yang ada.

2.4 Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah metode penelitian tindakan. Penelitian Tindakan dipilih karena dalam penelitian ini langsung ditujukan untuk tujuan penelitian yaitu meninjau keamanan pada aplikasi dokumen elektronik Universitas Drama Bina. Langkah-langkah yang dilakukan adalah sebagai berikut: 1) mendiagnosis, 2) merencanakan tindakan (action plan), 3) mengevaluasi (mengevaluasi) dan 4) menentukan pembelajaran (pembelajaran) dari hasil penelitian. Peneliti menggunakan teknologi code review untuk mendiagnosis kerentanan keamanan pada aplikasi dokumen elektronik.Teknologi tersebut meliputi tahapan sebagai berikut: 1) perencanaan, 2) penemuan, dan 3) perbaikan. Seluruh tahapan tersebut ditunjukkan pada gambar 1. Selain itu peneliti akan menganalisis hasil diagnosa dan melakukan beberapa perbaikan pada aplikasi dokumen elektronik.



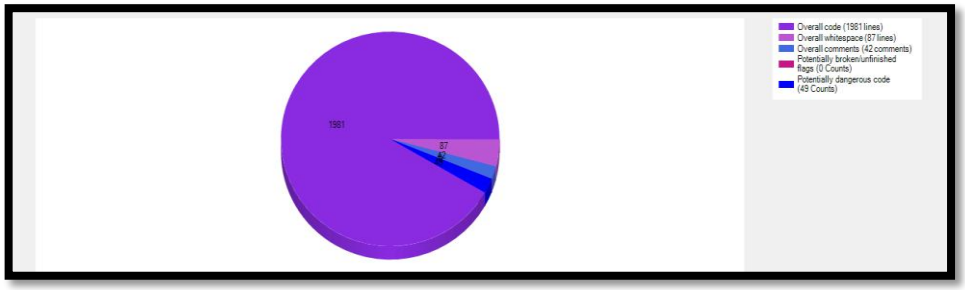
Gambar 1. Tahapan Kode Review

3. HASIL DAN PEMBAHASAN

Setelah dilakukan diagnosa menggunakan *tools rips dan visual code grepper* dapat diketahui hasilnya sebagai berikut:

Gambar 2. Hasil Scanning RIPS

Ada 15 file yang memiliki celah keamanan mulai dari sql-injection , cross site-scripting dan error lainnya, untuk keterangan warnanya adalah sebagai berikut **Hijau** berarti low tisk, **Biru** berarti Medium Risk dan **Puth** berarti Medium Risk



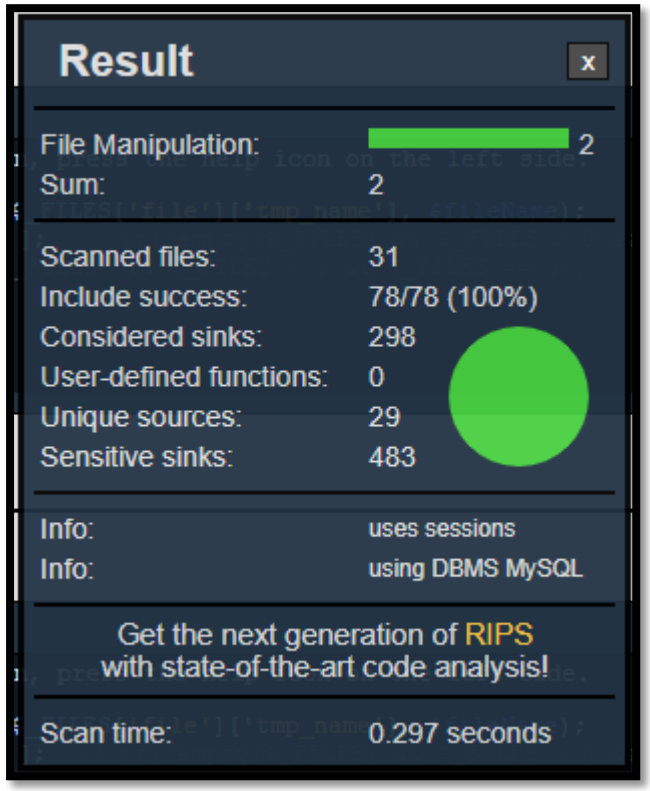
Gambar 3. Hasil Scanning Visual Code Grepper

Dari total 31 file yang di scanning ada 14 file yang memiliki celah seperti sql-injection dan cross site scripting dan ada beberapa error yang tidak terlalu berpengaruh terhadap keamanan sistem. Untuk hasil *scanning* selengkapnya dapat dilihat pada tabel berikut:

Tabel 1. Hasil Keseluruhan

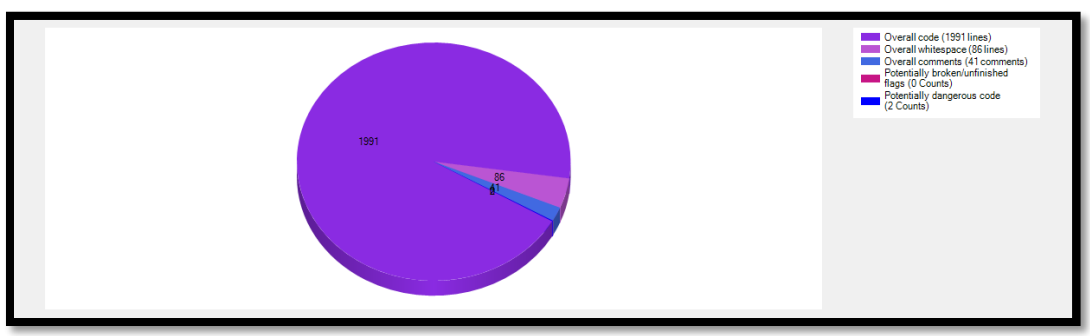
No.	Nama *File*	RIPS	Visual Code Grepper
1	*/admin/index.php*	*SQL-Injection*	*Cross Site Scripting (XSS)* dan *Sql Injection*
2	*/admin/s-e-template.php*	*SQL-Injection*	Tidak Terdeteksi
3	*/admin/save_dok.php*	*SQL-Injection*	*Cross Site Scripting (XSS)*
4	*/admin/save_dok_mou.php*	*SQL-Injection* dan *File Manipulation*	*Cross Site Scripting (XSS)*
5	/admin/save_edit.php	*SQL-Injection*	Tidak Terdeteksi
6	/admin/save_edit_mou.php.	*SQL-Injection*	Tidak Terdeteksi
7	/admin/del_dok.php	*Cross Site Scriping (XSS)*	Tidak Terdeteksi
8	*cek-akses.php*	Tidak Terdeteksi	*Unsafe Code*
9	*index.php*	Tidak Terdeteksi	*Unsafe Code*
10	*login.php*	Tidak Terdeteksi	*Unsafe Code*
11	*register.php*	Tidak Terdeteksi	*Unsafe Code*
12	*\admin \edit-artikel.php*	Tidak Terdeteksi	*Cross Site Scripting (XSS)*
13	*\admin\edit-artikel.php*	Tidak Terdeteksi	*Cross Site Scripting (XSS)*
14	*\admin\edit-mou.php*	Tidak Terdeteksi	*Cross Site Scripting (XSS)*
15	*\edok\admin\save_dok.php*	Tidak Terdeteksi	*Cross Site Scripting (XSS)*
16	*\admin\save_dok_mou.php*	Tidak Terdeteksi	*Cross Site Scripting (XSS)*
17	*\admin\template_std_6.php*	Tidak Terdeteksi	*Cross Site Scripting (XSS)*

Setelah melakukan proses re-diagnosa, terlihat bahwa semua celah yang telah ditambah atau dikurangi hanyalah dua celah yang tidak terlalu mempengaruhi keamanan sistem, bagan berikut dapat melihat jebakan-jebakan tersebut:



Gambar 4. Hasil Diagnosa Ulang dengan RIPS

Setelah dilakukan diagnosa ulang menggunakan RIPS dan Visual Code Grepper sudah tidak ditemukan lagi celah yang memilik potensi mengancam keamanan sistem e-dokumen ini



Gambar 5. Hasil Diagnosa Ulang dengan Visual Code Grepper

Berikut merupakan tabel celah dan cara pencegahannya.

Tabel 2. Celah dan Solusi

No	File	Celah Keamanan	Solusi
1	Admin/inddex.php	*Sql-injection* dan *Cross-Site Scripting (XSS)*	Dengan menambahkan *quotes string* dan melakukan validasi dan sanitasi.
2	Admin/s-e-tempalte.php	*Sql-injection*	Dengan menambahkan *quotes string.*
3	Admin/save_dok.php	*Sql-injection* dan *Cross-Site Scripting (XSS*	Dengan menambahkan *quotes string* dan melakukan validasi dan sanitasi.
4	Admin/save_dok_mou.php	*Sql-injection* dan *Cross-Site Scripting (XSS*	Dengan menambahkan *quotes string* dan melakukan validasi dan sanitasi.
5	Admin/save_edit.php	*Sql-injection*	Dengan menambahkan *quotes string.*
6	Admin/save_edit_mou.php	*Sql-injection*	Dengan menambahkan *quotes string.*
7	Admin/del_dok.php	*Cross-Site Scripting*	melakukan validasi dan sanitasi.
8	Edit-artikel.php	*Cross-Site Scripting*	melakukan validasi dan sanitasi.
9	Admin/edit._mouphp	*Cross-Site Scripting*	melakukan validasi dan sanitasi.
10	Admin/template_std_6.php	*Cross-Site Scripting*	melakukan validasi dan sanitasi.
11	login.php	Penggunaan algoritma md5 saat login	Algoritma MD5 diganti menjadi algoritma *Password_Hash*

4. KESIMPULAN

Kesimpulan yang diambil dari hasil pengujian dan pembahasan dapat ditarik kesimpulan sebagai berikut: Studi ini menemukan bahwa 11 file memiliki kerentanan keamanan, termasuk sql injection, cross-site scripting (xss) dan beberapa kesalahan lain yang tidak terlalu mempengaruhi keamanan sistem. Dilihat dari hasil diagnostik menggunakan Rips 0.5 dan Visual Code Grepper, 36% file memiliki kerentanan keamanan dan kesalahan lainnya. Proses mempersempit kerentanan keamanan menggunakan teknik verifikasi dan sanitasi dan string yang dikutip. Sistem diagnostik dapat diselesaikan sesuai harapan penulis dan menghasilkan sistem yang aman.

DAFTAR PUSTAKA

[1] Holzmann, G. J. (2010*). SCRUB: A tool for code reviews*. Innovations in Systems and Software Engineering, 6(4), 311–318. https://doi.org/10.1007/s11334-010-0136-x

[2] Suroyo, H., & Amin, Z. (2017). *Aplikasi Sistem Manajemen Dokumen Elektronik Berorientasi Standar Borang BAN PT.* Jurnal Sistem Informasi, 8, 11.

[3] Suryana, T. (2013). *Sistem Manajemen Dokumen Komunikasi Internal*. 16.