Jurnal MANDIRI

ILMU PENGETAHUAN, SENI, DAN TEKNOLOGI

www.jurnalmandiri.com

ISSN : 2580-3220, E-ISSN : 2580-4588
J. Mandiri., Vol. 3, No. 1, Juni 2019 (116 - 131)

Jurnal MANDIRI™
ILMU PENGETAHUAN, SENI, DAN TEKNOLOGI

ANALISIS DAN PENGUJIAN KERENTANAN SISTEM INFORMASI PERPUSTAKAAN

Achmad Nur Sholeh
Fakultas Ekonomi, Universitas Pamulang
dosen01531@unpam.ac.id

Muhammad Subagja Sastra Wardaya
Fakultas Sains dan Teknologi, UIN Syarif Hidayatullah Jakarta
muh.subagja@live.com

Abstrak

Tujuan dari penelitian ini adalah Melakukan pengujian kerentanan dengan menggunakan penetration testing tools, Melakukan analisis terhadap kerentanan yang ada dalam website tulis.uinjkt.ac.id, Memberikan rekomendasi untuk memperbaiki keamanan yang ada dalam website tulis. uinjkt.ac.id berdasarkan hasil laporan pengujian. Metode pengumpulan data dilakukan dengan cara yaitu observasi, wawancara dan studi literature yang berkaitan dengan perpustakaan UIN Syarif Hidayatullah Jakarta. Adapun metodologi dalam penelitian ini yang digunakan untuk menganalisis keamanan sistem informasi yaitu Zero Entry Hacking (ZEH). Setelah melakukan pengujian kerentanan atas aplikasi TULIS yang merupakan Sistem Informasi Perpustakaan pada Pusat Perpustakaan dan berdasarkan hasil pemindaian kerentanan, TULIS memiliki kerentanan mulai dari level sedang (XSS Reflected, Security, Apache Jserv protocol service, Login page password guessing attack dan HTML form without CSRF protection) sampai dengan level berat (Sensitive Data Exposure bagian web server robots.txt information disclosure). Setelah dilakukan eksploitasi kerentanan yang mengacu pada hasil pemindaian sebelumnya, ada kerentanan level berat yang tidak dapat dieksploitasi atau salah pendeteksian (false positive) yaitu buffer overflow dan SQL injection.

Kata Kunci : *Kerentanan, Sistem Informasi, Zero Entry Hacking, TULIS*

Abstract

The purpose of this study is to conduct vulnerability testing on the write.uinjkt.ac.id website using penetration testing tools, analyze the vulnerabilities found on the website write.uinjkt.ac.id, provide recommendations to improve security on the written website. uinjkt.ac.id based on the results of the test report. The method of data collection is done by means of observation, interviews and literature related to the library website of Uin Syarif Hidayatullah Jakarta. The methodology used in research and analysis in this study is Zero Entry Hacking (ZEH). After testing the vulnerability of the TULIS application which is the Library Information System at the Library Center, based on the results of vulnerability scanning, TULIS has a vulnerability starting from the medium level (XSS Reflected, Security, Apache Jserv protocol service, Login page password guessing attacks and HTML form without CSRF protection) up to weight (robots.txt information disclosure Sensitive Data

Exposure section, After exploiting vulnerabilities that refer to the results of previous scanning, there are heavy level vulnerabilities that do not really exist or false positives, namely buffer overflow and SQL injection.

***Keywords** : Vulnerability, Systems Information, Zero Entry Hacking, TULIS*

PENDAHULUAN

Latar Belakang

Peranan sistem informasi dalam suatu organisasi tidak diragukan lagi karena dukungannya dapat membuat sebuah organisasi memiliki keunggulan yang kompetitif, yang berarti suatu organisasi dapat bersaing menggunakan sistem informasi (Kadir, 2014). Salah satu organisasi yang banyak menerapkan sistem informasi sebagai penunjang aktivitasnya yaitu lembaga pendidikan, mulai dari jenjang Sekolah Dasar hingga Perguruan Tinggi.

UIN Syarif Hidayatullah Jakarta sebagai Perguruan Tinggi telah menerapkan sistem informasi yang mana adalah sistem informasi perpustakaan dapat membantu kegiatan perpustakaan yang dikelola oleh Pusat Perpustakaan dan perpustakaan yang tersebar di tiap fakultas. Pusat Perpustakaan yang sebagai sentral dari perpustakaan tiap fakultas telah menerapkan sistem informasi yang beragam, misalnya otomatisasi sistem untuk mempercepat transaksi peminjaman dan pengembalian, penerapan sistem keamanan koleksi buku dengan *sensormatic* sehingga perangkat tersebut akan berbunyi ketika ada pencurian, *Close Circuit Television* (CCTV) sebagai pengawasan tambahan serta katalog *online* menggunakan TULIS *(Technology of UIN Library and Information System)* yang memberikan akses OPAC *(Online Public Access Catalogue)*. OPAC sendiri merupakan sistem katalog yang dapat membantu pengguna mengakses basis data karya ilmiah. Basis data yang disediakan dalam OPAC ini meliputi basis data buku, skripsi, tesis, dan disertasi, majalah, dan laporan penelitian. (Anonim, 2015, Layanan Penelusuran OPAC, http://uinjkt.ac.id/katalog, diakses tanggal 22 Desember 2016). Selain pemberian akses karya ilmiah, TULIS juga memberikan pelayanan dalam kegiatan perpustakaan seperti keanggotan perpustakaan, pencatatan kunjungan, pengkategorian buku, penginputan, transaksi peminjaman dan pengembalian dan lain-lain. Bahkan dalam penelitian salah satu mahasiswa dijelaskan bahwa keberadaan sistem sangat membantu pekerjaan atau studi mahasiswa/i serta tingkat kepuasan pengguna sistem berdasarkan persepsi pengguna saat ini berada pada tingkat yang cukup baik. (Yunita, 2016).

Dengan berbagai manfaat yang diberikan oleh TULIS, perlu maka TULIS perlu dijaga keamanannya agar terus dapat diakses dan dapat memberikan informasi yang akurat, namun keamanan seringkali menjadi prioritas kesekian dalam sebuah institusi. (Anjar, 2006) sehingga aplikasi-aplikasi berbasis web menjadi rentan untuk mengalami peretasan. Dalam wawancara dengan salah satu staf otomasi Pusat Perpustakaan, dijelaskan bahwa belum pernah dilaksanakannya pengujian keamanan pada TULIS, sehingga TULIS pernah mengalami keretasan, berikut detail dalam tabel 1.1

Tabel 1.1 Serangan yang Terjadi Pada Pusat Perpustakaan

Waktu Terjadi	Insiden	Dampak	Frekuensi	Penyelesaian
2012 2013	Serangan virus komputer	Kinerja komputer melambat, penyebaran virus ke instansi lainnya	Frekuensi penyebarannya cukup tinggi	Meng*install* anti virus
2014 2015 2016	Akun admin server Perpustakaan bertambah dengan sendirinya.	Belum terjadi hal yang merugikan namun sangat berisiko.	Selang beberapa bulan sekali setelah *maintenance.*	Pada penyelesaian awal hanya dilakukan penghapusan akun admin, karena terjadi berulang dilakukan penggantian sistem operasi dari Windows Server menjadi Ubuntu.

Sumber: (Soleh, 2017)

Padahal banyak hal yang dapat dilakukan oleh peretas apabila mereka berhasil meretas suatu sistem misalnya menduplikasi, memanipulasi, ataupun menghapus *file-file* penting. Seperti halnya kasus yang terjadi di Perpustakaan

Universitas Gajah Mada (UGM). Dari insiden tersebut peretas hanya meninggalkan pesan peringatan pada *administrator Web portal* tersebut untuk meningkatkan keamanannya. (Chandratuna, 2010, *Perpustakaan Online UGM Dibobol Hacker*, http://teknologi.news.viva.co.id/news/read/166308-perpustakaan-online-ugm-dibobol-peretas, diakses pada tanggal 20 Februari 2017) dan kasus peretasan lainnya terjadi di Universitas Sumatera Utara, dalam kasus peretasan, terlihat ada dua foto remaja laki-laki di halaman utama situs tersebut. Satu remaja mengenakan topi dan memegang semacam laptop sembari mengacungkan jari tengah. Satu remaja lainnya hanya tampak wajahnya mengenakan kaos merah. (Muamar, 2016, *Portal USU Diretas, Muncul Foto Tak Senonoh di Halaman Muka*, http://medan.tribunnews.com/2016/07/30/portal-usu-diretas-muncul-foto-tak-senonoh-di-halaman-muka, diakses 20 Februari 2017). Peristiwa-peristiwa tersebut memperkuat argumen penulis untuk meneliti keamanan sistem informasi perpustakaan, mulai dari pengujian keamanan dan mengetahui sejauh mana ketangguhan sistem, menganalisis kerentanan, sebagai upaya terhindar dari serangan *cyber*.

Identifikasi Masalah

Berdasarkan latar belakang yang telah dijelaskan sebelumnya, maka identifikasi masalah adalah sebagai berikut :

1. Belum pernah dilakukannya pengujian kerentanan pada *website* tulis.uinjkt.ac.id.
2. Pernah terjadi peretasan pada *website* tulis.uinjkt.ac.id.
3. Melakukan *maintenance* hanya saat terjadi kerentanan.
4. Belum adanya rencana untuk melakukan pengujian kerentanan sistem meliputi *penetration testing* terhadap aplikasi TULIS, dan pendokumentasian laporan hasil *penetration testing*.

Rumusan Masalah

Berdasarkan identifikasi masalah yang ada, maka bisa dirumuskan permasalahannya yaitu:

1. Bagaimana kondisi kerentanan yang ada pada *website* TULIS setelah dilakukan pemindaian kerentanan?
2. Bagaimana hasil eksploitasi pengujian kerentanan TULIS yang didapat dari hasil pemindaian kerentanan?
3. Apa saja kerentanan yang perlu diperbaiki dengan segera?

Batasan Masalah

Berdasarkan perumusan masalah yang telah dijelaskan sebelumnya, maka batasan masalah dibatasi pada :

1. Penelitian ini hanya berfokus pada *website* tulis.uinjkt.ac.id
2. Pengujian kemanan hanya pada *web application*.
3. Penelitian ini menggunakan dua Sistem Operasi, yaitu Linux dan Windows. Untuk Linux menggunakan distro Kali 2016.2 yang memiliki nama lain Kali Rolling dengan *penetration testing tools* adalah : NMAP v7.25, Uniscan v6.2, w3af v1.6.5.4, OWASP ZAP v2.5.0, Nessus 6.10.7 dan untuk Windows dengan sistem operasi Windows 10 Single Language menggunakan *tool* Accunetix v11.
4. Penelitian ini melakukan pengujian berdasarkan kerangka kerja *Vulnerability Assesment and Penetration Testing*.
5. Penerapan dari rekomendasi yang diberikan akan diserahkan sepenuhnya pada kewenangan instasi terkait, yaitu Pusat Perpustakaan.

Tujuan Penelitian

Berdasarkan latar belakang yang dipaparkan sebelumnya, adapun tujuan dari penelitian ini adalah sebagai berikut :

1. Melakukan pengujian kerentanan pada *website* tulis.uinjkt.ac.id dengan menggunakan *penetration testing tools*.

2. Melakukan analisis terhadap kerentanan yang ada dalam *website* tulis.uinjkt.ac.id
3. Memberikan rekomendasi untuk memperbaiki keamanan yang ada dalam *website* tulis.uinjkt.ac.id berdasarkan hasil laporan pengujian.

Kajian Teori

Menurut O'Brien dan Marakas (2010) Sistem didefinisikan sebagai seperangkat komponen yang saling terkait, dengan batas yang jelas, bekerja sama untuk mencapai seperangkat tujuan dengan menerima *input* dan menghasilkan *output* dalam proses transformasi yang terorganisir.

Menurut Sutabri (2012) suatu sistem memiliki beberapa karakteristik atau ciri-ciri tertentu, yaitu :

a. Komponen Sistem *(Component)*
   Suatu sistem terdiri dari sejumlah komponen yang sering disebut dengan subsistem yang saling berinteraksi, yang artinya saling bekerjasama membentuk satu kesatuan. Komponen-komponen sistem dapat berupa subsistem atau bagian-bagian dari sistem. Contoh dalam Pusat Perpustakaan yaitu terdapat subdivisi seperti sirkulasi, pengadaan, pencatatan pengunjung dan lainnya.
b. Batas Sistem *(Boundary)*
   Batas sistem merupakan daerah yang membatasi antara suatu sistem dengan sistem yang lainnya atau dengan lingkungan luarnya. Batas sistem memungkinkan suatu sistem dipandang sebagai satu kesatuan. Batas suatu sistem menunjukkan ruang lingkup *(scope)* sistem itu sendiri. Contoh dalam Pusat Perpustakaan misalnya, Pusat Perpustakaan hanya memberikan pelayanan hanya pada seputar kepustakaan dan tidak melayani akademik.
c. Lingkungan Luar Sistem *(Environments)*
   Lingkungan luar dari suatu sistem adalah apapun di luar batas dari sistem yang mempengaruhi operasi sistem. Lingkungan luar sistem dapat bersifat menguntungkan dan dapat juga bersifat merugikan bagi sistem tersebut. Contoh yang menguntungkan dan pada Pusat Perpustakaan adalah ketika pengunjung dari luar meminjam buku, Pusat Perpustakaann dapat mendapat data seperti karangan siapa yang sering dipinjam dan menjadi refrensi untuk pengadaan buku selanjutnya. Contoh yang merugikan pada Pusat Perpustakaan seperti pengunjung melakukan peminjaman buku lalu buku yang dipinjam hilang.
d. Antar Muka Sistem *(Interface)*
   Antar muka yang dimaksud adalah media yang dapat menghubungkan antara subsistem dengan subsistem lainnya. Melalui penghubung ini memungkinkan sumber-sumber daya mengalir dari satu sistem ke subsistem yang lain. Contoh pada Pusat Perpustakaan yaitu TULIS menjadi antarmuka sistem bagi divisi pencatatan pengunjung, sirkulasi dan Pengadaan.
e. Masukan Sistem *(Input)*
   Masukan yaitu energi yang dimasukkan ke dalam sistem, dimana dapat berupa masukan perawatan dan masukan sinyal. Masukkan perawatan adalah energi yang di-*input*-kan supaya sistem tersebut dapat beroperasi, sedang masukan sinyal adalah energi yang diproses untuk mendapatkan keluaran. Contoh masukan di sini bisa berupa data harian peminjaman buku pada Perpustakaan Pusat.
f. Pengolah Sistem *(Processing System)*
   Hasil energi yang diolah dan diklasifikasikan menjadi keluaran yang berguna. Keluaran ini menjadi masukan untuk subsistem lain. Contoh pengolah sistem di sini bisa berupa data transaksi peminjaman dan pengembalian harian perpustakaan diolah menjadi laporan yang dibutuhkan manajemen.
g. Keluaran Sistem *(Output)*
   Keluaran yaitu hasil dari energi yang diolah dan diklasifikasikan menjadi keluaran yang berguna dan sisa pembuangan. Contoh keluaran sistem di sini bisa berupa sebuah informasi frekuensi peminjaman buku terbanyak berguna untuk mengambil keputusan pada divisi pengadaan untuk menjadi masukan pembelian buku selanjutnya.
h. Sasaran Sistem *(Objective)*
   Suatu sistem pasti mempunyai tujuan *(goal)*

atau sasaran *(objective)*. Jika suatu sistem tidak memiliki sasaran maka operasi sistem tidak ada gunanya.

Menurut Mulyanto (2009) Informasi merupakan data yang telah diolah menjadi sebuah bentuk yang berarti bagi penerimanya dan bermanfaat dalam pengambilan keputusan saat ini atau saat mendatang.

Menurut Gollman (1999) Keamanan komputer yaitu berhubungan dengan pencegahan diri/proteksi dan deteksi terhadap tindakan pengganggu yang tidak dikenali dalam sistem komputer.

Konsep keamanan sistem informasi menurut Cole *et al.* (2005) dijelaskan bahwa keamanan berputar di sekitar tiga kunci utama yaitu dari *Confidentiality* (Kerahasiaan), *Integrity* (Keutuhan), dan *Availability* (Ketersediaan) yang dikenal sebagai (C-I-A) yaitu :

1. Kerahasiaan *(Confidentiality)*

   Istilah *Confidentiality* secara umum berartikan tentang kerahasiaan. Menurut Cole *et al*. (2005) dijelaskan bahwa *Confidentiality* berkaitan dengan pencegahan agar hanya yang memiliki otorisasi yang dapat mengakses informasi. Misalnya suatu halaman *web*, hanya dapat diakses oleh *member*, namun bisa diakses meskipun dia bukan *member*. Jadi *Confidentiality* memastikan suatu informasi tidak bocor karena hanya dapat diakses oleh pemilik hak otorisasi.
2. Keutuhan *(Integrity)*

   Istilah *Integrity* secara umum dapat diartikan sebagai keutuhan. Menurut Cole *et al.* (2005) dijelaskan bahwa *Integrity* memiliki 3 sasaran yaitu :
   1. Pencegahan terjadinya modifikasi informasi oleh yang yang bukan pemilik otorisasi.
   2. Pencegahan agar yang bukan pemilik otorisasi atau ketidak sengajaan modifikasi oleh pemilik otorisasi.
   3. Pemeliharaan ketetapan internal dan eksternal.
3. Ketersediaan *(Avaibility)*

   Istilah *Avaibility* dapat diartikan sebagai ketersediaan. Menurut Cole *et al*. (2005) *Avaibility* meyakinkan otorisasi pengguna sistemnya dapat tepat waktu dan akses tidak terinterupsi menuju informasi dari sistem dalam suatu jaringan. Misalkan ketika kita ingin mengakses suatu *web, web* tersebut menjadi tidak bisa diakses karena adanya interupsi. Jadi yang dimaksud *Avaibility* di sini merupakan suatu kondisi di mana informasi dapat tersedia, tepat waktu dan tidak adanya interupsi dari pihak lain dalam suatu jaringan.

Menurut Yunita (2016) Perpustakaan adalah tempat penyimpanan dan pengelolaan bahan pustaka baik yang tertulis maupun yang terekam yang disusun berdasarkan aturan tertentu secara sistematis sehingga mudah ditemukan oleh pembacanya.

TULIS atau yang biasa disebut dengan *Technology UIN Library Information System* merupakan sebuah aplikasi berbasis *web* yang digunakan oleh Pusat Perpustakaan untuk memberikan akses OPAC *(Online Public Access Catalogue)* yang dapat diakses melalui http://tulis.uinjkt.ac.id .

Menurut Yunita (2016) OPAC adalah katalog yang dapat digunakan oleh penggunanya secara *online* untuk mencari informasi sebuah buku, baik di perpustakaan, toko buku, maupun unit informasi lainnya.

Secara umum, diketahui bahwa jaringan komputer bisa berarti penghubung antara satu komputer dengan komputer lainnya. Jaringan komputer merupakan model lama satu komputer yang melayani semua kebutuhan komputasi organisasi telah digantikan oleh satu komputer yang terpisah namun saling berhubungan melakukan pekerjaan itu (Tanenbaum dan Wetherall, 2011).

Komputer-komputer yang terhubung dalam jaringan dapat diklasifikasikan lagi menurut skala jangkauannya menurut Tanenbaum dan Wetherall (2011) sebagai berikut :

1. PAN *(Personal Area Networks)*

   PAN *(Personal Area Networks)* membiarkan perangkat berkomunikasi melalui jangkauan seseorang.
2. LAN *(Local Area Network)*

   LAN *(Local Area Network)* dalah jaringan

milik pribadi yang beroperasi di dalam dan di dekat suatu gedung seperti rumah, kantor atau pabrik.

3. MAN *(Metropolitan Area Network)*
   MAN *(Metropolitan Area Network)* mencakup sebuah kota. Contoh MAN yang paling terkenal adalah jaringan televisi kabel yang tersedia di banyak kota.
4. WAN *(Wide Area Network)*
   WAN *(Wide Area Network)* mencakup wilayah geografis yang luas, seringkali merupakan negara atau benua.
5. *Internetworks*
   Banyak jaringan ada di dunia, seringkali dengan perangkat keras dan perangkat lunak yang berbeda. Orang yang terhubung ke satu jaringan sering ingin berkomunikasi dengan orang-orang yang terhubung dengan orang lain.

Internet

Internet merupakan sekumpulan jaringan yang terhubung satu dengan yang lainnya, di mana jaringan menyediakan sambungan menuju global informasi (Oetomo *et al*., 2011). Komputer yang tersambung ke internet merupakan bagian dari jaringan. Komputer dapat tersambung dengan *Internet Service Provider* (ISP), lalu ISP tersambung dengan jaringan yang lebih besar.

Tiga peran teknis dalam dimiliki oleh internet Strauss dan Frost (2012) dalam Putri (2015) sebagai berikut :

1. Penyedia konten yang menciptakan informasi, hiburan dan sebgainya yang berada di komputer dengan akses jaringan.
2. Pengguna (juga dikenal sebagai komputer klien) yang mengaksses konten dan mengirim email dan data lainnya melalui jaringan.
3. Infrastruktur teknologi untuk memindahkan, menciptakan, dan melihat atau mendengar konten (perangkat lunak dan perangkat keras).

Konsep *Web*

World Wide Web (WWW), lebih dikenal dengan *web* yang merupakan salah satu layanan yang didapat oleh pemakai komputer yang terhubung ke internet dengan fasilitas *hypertext* untuk menampilkan data berupa teks, gambar, suara, animasi dan data multimedia lainnya (Kustiyahningsih, 2011).

Web dapat dikategorikan menjadi dua yaitu "*web* statis" dan "*web* dinamis". *Web* statis adalah *web* yang menampilkan informasi-informasi yang sifatnya statis. Disebut statis karena pengguna tidak bisa berinteraksi dengan *web* tersebut. Selain *web* statis ada juga yang disebut *web* dinamis. *Web* dinamis adalah *web* yang menampilkan informasi serta dapat berinteraksi dengan pengguna. *Web* yang dinamis memungkinkan pengguna untuk berinteraksi menggunakan form sehingga dapat mengolah informasi yang ditampilkan. *Web* dinamis bersifat interaktif, tidak kaku dan terlihat lebih indah.

Teknik Pengujian *Software*

Umumnya terdapat dua macam pendekatan yang digunakan dalam pengujian sistem, yaitu *black-box testing* dan *white-box testing*. Kedua pendekatan tersebut pengetesan dilakukan sesuai dengan kebutuhan.

1. *Black-box testing*
   Dijelaskan dalam Cole *et al.* (2005) *Black-box testing* merupakan suatu rangkaian pengujian yang dilakukan pada antarmuka *software* dan dilakukan pengujian beberapa aspek fundamental dari sebuah sistem dengan sedikit hal untuk struktur logika internal dari suatu *software*. Contohnya ketika pengujian aplikasi baru apakah sudah berjalan sesuai fungsinya. Jadi dalam *Black-box testing* merupakan pendekatan yang dilakukan untuk menguji suatu sistem secara parsial dan mengutamakan antarmuka dan fungsi dan penulis menjadikan ini sebagai pendekatan dalam pengujian sistem. Dalam penelitian ini digunakan *Black-box testing* dikarenakan peneliti tidak menguji *source* kode secara langsung tetapi peneliti memberikan *input* yang sifatnya spesial ke dalam aplikasi.
2. *White-box testing*
   Dijelaskan oleh Cole *et al.* (2005) *White-box testing* merupakan suatu rangkaian pengujian yang sifatnya mendasarkan da-

ri pengujian secara ketat dari tahapan-tahapan yang mendetil. Pada pendekatan ini dilakukan pengujian jalan logika melalui *software* dan kolaborasi diantara komponen-komponen diuji oleh kasus menyediakan tes yang menguji secara spesifik kumpulan-kumpulan *conditions* dan *loops*. Contohnya ketika memiliki *software* baru dilihat secara mendetil hingga *codes*. Jadi dalam *white-box testing* dilakukan pengujian secara mendalam dan menyeluruh sehingga dapat menyajikan sistem dapat berjalan dengan sempurna.

3. *Grey-box testing*
   Dijelaskan oleh *Grey-box testing* merupakan penguji mempunyai sebagian pengetahuan tentang pengujian jaringan. Penguji tidak memiliki pengatahuan lengkap mengenai arsitektur jaringan, tapi memiliki pengetahuan tentang informasi dasar dari arsitektur jaringan dan konfigurasi sistem. *Grey-box testing* juga merupakan kombinasi dari *white-box testing* dan *black-box testing* (Goel dan Mehtre, 2005).
4. *Basis Path Testing*
   Metode Basis Path memungkinkan penguji mengukur kompleksitas logika dari desain procedural dan menggunakan ukuran ini sebagai panduan untuk menggambarkan dasar eksekusi alur aplikasi (Pressman, 2005).

Vulnerability Assesment (Penilaian Celah Kerentanan)

Menurut Engebretson (2013) *Vulnerability Assesment* atau Penilaian Celah Kerentanan merupakan suatu rangkaian proses yang dilakukan untuk meninjau *services* dan *system* yang memiliki potensi celah kerentanan. Sedangkan menurut Baloch (2015) *Vulnerability Assesment* yaitu mencari tahu semua kerentanan dalam aset dan dokumentasikan sesuai dengan itu.

Pemindai Celah Kerentanan *(Vulnerability Scanner)*

Dalam melakukan *Vulnerability Assesment* dapat dipermudah salah satunya dengan menggunakan *tools* yang tersedia untuk melakukan pengujian kerentananan. Menurut Baloch (2015) Pemindai kerentanan memindai komputer, jaringan, atau aplikasi yang mencari potensi kelemahan yang bisa digunakan oleh penyerang untuk kompromi target.

Penetration Testing (Uji Penetrasi)

Menurut Engebretson (2013) *Penetration Testing* atau Uji Penetrasi merupakan suatu upaya yang dilakukan untuk mengeksploitasi kelemahan sistem komputer dengan tujuan membuat sistem komputer lebih aman dengan secara legal dan berwenang. Menurut Weidman (2014) *Penetration Testing* meliputi simulasi serangan nyata untuk menilai risiko yang terkait dengan penerobosan keamanan yang sifatnya potensial.

Vulnerability Assesment (Mencari Celah Kerentanan v.s *Pentration Testing* (Uji Penetrasi)

Seringkali sebagian orang menyalah artikan istilah *vulnerability assessment* dan *penetration testing* sebagai suatu arti yang sama dalam pengujian keamanan. Jika dilihat dari definisi-definisi yang dijelaskan sebelumnya, dapat ditelaah bahwa pada *vulnerability assessment* berfokus pada pencarian celah kerentanan saja, sementara itu *penetration testing* penguji tidak hanya menemukan kerentanan itu bisa digunakan oleh penyerang tapi juga memanfaatkan kerentanan, jika mungkin, untuk menilai apa penyerang mungkin mendapatkan setelah sukses melakukan eksploitasi.

Pengujian dan Analisis *Zero Entry Hacking* (ZEH)

Metodologi yang digunakan dalam pengujian dan analisis pada penelitian ini ialah *Zero Entry Hacking* (ZEH). ZEH merupakan salah satu metodologi yang digunakan untuk melakukan *Penetration Testing*. ZEH merupakan salah satu metodologi yang cocok digunakan untuk pemula dalam melakukan *Penetration Testing* karena menggunakan 4 tahapan sederhana saja (Engebretson, 2013).

Tahapan ZEH

Terdapat 4 tahapan dalam ZEH yang digunakan dalam pengujian sistem. Adapun em-

pat tahapannya menurut Engebretson (2013) yaitu Pengintaian Sistem *(Reconnaisance)*, Pemindaian *(Scanning)*, Eksploitasi Celah Keamanan *(Exploitation),* dan Pasca Eksploitasi *(Post Exploitation)*. Berikut ini adalah gambar dari tahapan-tahapan ZEH

METODE

Metode Pengumpulan Data

Penelitian ini menggunakan data dan informasi yang diperoleh dari berbagai sumber. Oleh karena itu dibutuhkan beberapa metode untuk mendapatkan hasil yang sesuai. Adapun metode yang digunakan sebagai berikut :

Observasi

Observasi dilakukan dengan mengamati langsung keamanan pada sistem informasi perpustakaan yaitu TULIS *(Technology of UIN Library and Information System)* yang merupakan aplikasi berbasis web pada Pusat Perpustakaan UIN Syarif Hidayatullah Jakarta. Adapun keamanan terkait dengan ada tidaknya celah kerentanan yang berpotensi merugikan berbagai pihak khususnya Pusat Perpustakaan UIN Syarif Hidayatullah. Adapun secara spesifik kegiatan observasi ini dijelaskan sebagai berikut:

Bertempat pada Pusat perpustakaan UIN Syarif Hidayatullah yang beralamat di Jl. Ir. H. Juanda No. 95, Ciputat Tangerang Selatan Banten *website*: http://tulis.uinjkt.ac.id

Wawancara

Untuk memperjelas proses observasi, peneliti juga melakukan wawancara dengan salah satu staf Pusat Perpustakaan UIN Syarif Hidayatullah Jakarta bagian TI dan Otomasi. Pertanyaan yang diajukan pada wawancara ini merupakan pertanyaan yang bersifat teknis khususnya membahas mengenai keamanan pada TULIS. Wawancara dilakukan di ruang TI dan Otomasi Pusat Perpustakaan UIN Syarif Hidayatullah, wawancara dilakukan pada tanggal 14 Maret 2017.

Melalui wawancara ini diperoleh informasi berupa opini tentang masalah yang terjadi pada proses keamanan TULIS, diantaranya seperti belum pernah dan belum ada rencana untuk melakukan penelitian kerentanan pada *website* tulis.uinjkt.ac.id, pernah terjadi peretasan pada *website* tulis.uinjkt.ac.id serta melakukan *maintenance* hanya saat terjadi kerentanan.

Studi Literatur

Data-data dan informasi yang digunakan sebagai studi literatur yang dilakukan dengan mempelajari dan mengumpulkan materi-materi yang berkaitan dengan perpustakaan dan keamanan sistem informasi pada Pusat Perpustakaan UIN Syarif Hidayatullah Jakarta. Peneliti melakukan pengumpulan data dan membandingkan dengan studi literatur sejenis yang sudah ada sebagai referensi.

Penelitian dan Analisis

Zero Entry Hacking (ZEH)

Metodologi yang digunakan dalam penelitian dan analisis pada penelitian ini ialah *Zero Entry Hacking* (ZEH).

Pengintaian Sistem *(Reconnaisance)*

Tahapan ini merupakan tahapan pertama dalam penelitian. Tahapan ini bertujuan untuk mengumpulkan informasi sebanyak-banyaknya mengenai aplikasi TULIS.

Pemindaian *(Scanning)*

Dalam tahapan setelah pengintaian, dilanjutkan dengan pemindaian. Dalam tahapan ini, dibagi lagi menjadi empat tahapan

1. Menentukan apakah TULIS dapat di *ping*. Maksudnya di sini apakah target terhubung jaringan atau tidak, apakah hanya dapat diakses dari jaringan lokal saja atau bisa diakses dari luar, bagus atau tidaknya kualitas koneksi target, berapa durasi yang dibutuhkan target untuk membalas *ping, bytes* yang dikirimkan ada hilang atau dapat diterima dengan baik, dan apakah target dapat melakukan ping pada dirinya sendiri menggunakan *Terminal* pada Kali Linux.
2. *Port scanning* sistem menggunakan NMAP terhadap TULIS. Maksud *port scanning* dengan NMAP di sini ialah penggunaan

aplikasi NMAP untuk memonitoring dan sebagai *penetration testing tool* pada *website* TULIS.

3. Memanfaatkan NMAP *Scripting Engine* (NSE) untuk menginterogasi TULIS lebih dalam. NSE di sini untuk memeriksa *services* apa saja yang berjalan, mengetahui sistem operasi target.
4. Pemindaian TULIS menggunakan *vulnerability scanner*. Pemindaian sistem di maksudnya adalah mengecek *vulnerability* yang ada pada TULIS dengan bantuan aplikasi. Adapun *vulnerability scanner* yang digunakan adalah W3AF v.1.0, OWASP ZAP v.2.5.0, Uniscan v.6.3, Nessus v.6.10.7, Acunetix v.11

HASIL dan PEMBAHASAN

Pengintaian *(Reconnaissance)*

Dalam tahapan peningintaian ini, Penulis berusaha menggali informasi sebanyak mungkin mengenai TULIS yang tersedia dalam internet.

Dengan melalui *Who is* dapat diketahui mengenai pendaftaran *domain* http://uinjkt.ac.id yaitu sebagai berikut :

1. *Domain* http://uinjkt.ac.id dibuat pada tanggal 19 Februari 2002 dan akan habis masa berlakunya pada tanggal 01 Oktober 2017, sebagaimana jika admin lupa untuk memperpanjang maka *domain* http://uinjkt.ac.id dan sub *domain*nya terancam *avaibility*-nya atau ketersediannya.
2. *Domain* http://uinjkt.ac.id dikelola oleh dua admin, dalam gambar yang 4.1 dan 4.2 dijelaskan mengenai alamat rumah, alamat kantor, alamat e-mail, organisasi tempat bekerja dan sebagainya yang tentunya dapat menjadikan kedua admin tersebut sebagai target untuk penyerangan terhadap *domain* http://uinjkt.ac.id beserta subdomainnya.
3. Nama *Hosting* yang digunakan yaitu INDOREG dijelaskan juga negara asal, kota berada, kode pos, dan no telpon kantor INDOREG yang tentunya apabila ingin menyerang melalui serangan fisik terhadap *server* yang digunakan oleh http://uinjkt.ac.id penyerang bisa melakukannya berdasarkan informasi yang ada pada
4. Jumlah *server* yang digunakan untuk *domain* http://uinjkt.ac.id yakni sebanyak 3 *server* sehingga jika ingin melakukan serangan perlu melakukan penyerang terhadap 3 *server* tersebut.

Guess Stritch

Dari *Guess Stritch* dapat diketahui bahwa aplikasi TULIS menggunakan *webserver* Apache 2.4.7 sebanyak 50%, *Framework* yang digunakan dalam pembuatan TULIS mungkin menggunakan Java, dan bahasa pemrograman yang digunakan yaitu Java sebanyak 70% dari informasi tersebut dapat Penulis gunakan selanjutnya untuk *dorking* kerentanan Java di mesin pencarian Google.

Pemindaian *(Scanning)*

Dalam melakukan pemindaian, Penulis membagi tahapan pemindaian ke dalam beberapa aktivitas. Adapun aktivitas-aktivitas tersebut antara lain :

Ping TULIS

Dalam melakukan pemindaian, perlu dilakukan pengujian apakah TULIS dapat diakses atau tidak, Penulis melakukan ping dengan mengetik perintah *ping* tulis.uinjkt.ac.id melalui *terminal* yang ada dalam kali linux

Port scanning TULIS

Dalam melakukan *Port Scanning*, penulis menggunakan ZENMAP v7.25 pemindaian, menggunakan objek http://tulis.uinjkt.ac.id, dengan perintah-perintah sebagai berikut :

1. -sS dengan fungsi TCP Syn Scan
2. -sU dengan fungsi UDP Scan
3. -T4 dengan fungsi Speed up NMAP
4. -A dengan fungsi Operating System dan Version Detection
5. -v dengan fungsi Verbosity

Pemindaian tingkat lanjut dengan *NMAP Scripting Engine* (NSE)

Berdasarkan pemindaian tingkat lanjut, didapatkan informasi-informasi yang telah diringkas sebagai berikut :

1. IP Address Server

Adapun alamat IP yang digunakan oleh server TULIS yaitu 172.27.15.147.

2. Sistem Operasi yang digunakan
   Adapun sistem operasi yang digunakan yaitu Linux dengan distro Ubuntu.
3. Services yang berjalan
   22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.3 (Ubuntu Linux; protocol 2.0)
   | ssh-hostkey:| 1024 93:2c:4e:c4:17:32:93:d9:54:06:7b:8a:61:a1:4a:c0 (DSA)
   | 2048 41:7a:5e:b2:32:09:96:f4:87:ee:4f:00:e1:cf:e4:84 (RSA)
   | _256 6a:b4:cf:d2:ef:73:d8:cc:48:9b:dc:89:19:25:c7:0c (ECDSA)
   80/tcp open http Apache httpd 2.4.7 ((Ubuntu))
   | _http-favicon: Unknown favicon MD5: 3A7BEB367DCD6544664E799A-B1A0FE97
   | http-methods:
   | _ Supported Methods: GET HEAD POST OPTIONS
   | http-robots.txt: 3 disallowed entries
   | _/ /bo /uibo
   | _http-server-header: Apache/2.4.7 (Ubuntu)
   | _http-title: OPAC - Pusat Perpustakaan UIN Syarif Hidayatullah Jakarta
   2000/tcp open tcpwrapped
   5060/tcp open tcpwrapped
   8000/tcp open http Apache httpd 2.4.7 ((Ubuntu))
   | _http-favicon: Unknown favicon MD5: D037EF2F629A22DDADCF438E-6BE7A325
   | http-methods:
   | _ Supported Methods: GET HEAD POST OPTIONS
   | http-open-proxy: Potentially OPEN proxy.
   | _Methods supported:CONNECTION
   | _http-server-header: Apache/2.4.7 (Ubuntu)
   | _http-title: phpMyAdmin
   8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
   | _ajp-methods: Failed to get a valid response for the OPTION request
   8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1
   | _http-favicon: Unknown favicon MD5: E3D3E9360C-F65A1167B20B3936BC0616
   | http-methods:
   | _ Supported Methods: GET HEAD POST OPTIONS
   | http-robots.txt: 3 disallowed entries
   | _/ /bo /uibo
   | _http-server-header: Apache-Coyote/1.1
   | _http-title: OPAC - Pusat Perpustakaan UIN Syarif Hidayatullah Jakarta
   5353/udp open mdns DNS-based service discovery
   | dns-service-discovery:
   | 9/tcp workstation
   | _Address=172.27.15.147 fe80:0:0:0:9a90:96ff:fed0:b838

Pemindaian TULIS
Menggunakan *Vulnerability Scanner*

Dalam tahapan ini, dilakukan kegiatan pemindaian celah keamanan *(vulnerability scanning)* menggunakan pemindai celah keamanan *(vulnerability scanner)* yang melakukan pemindaian aplikasi secara otomatis mencari celah keamanan yang mungkin bisa dimanfaatkan untuk kepentingan yang tidak baik.

Dalam kesempatan ini, dilakukan pemindaian celah kemanan tidak langsung kepada TULIS yang memiliki alamat http://tulis.uinjkt.ac.id melainkan menggunaan server cadangan

Eksploitasi Celah Kerentanan *(Exploitation)*

[1] Eksploitasi *Social Engineering*
Pada aktivitas ini, akan dilakukan bersamaan dengan pengujian kerentanan A8 – CSRF bagian *HTML wihout CSRF Protection.*

[2] Eksploitasi Berbasis *Web*
Setelah mendapatkan celah kerentanan yang ada pada TULIS melalui *vulnerability scanner*, dalam tahapan selanjutnya ialah mengeksploitasi kerentanan yang ada, untuk menguji apakah kerentanan tersebut benar-benar ada atau hanyalah *false alarm*. Adapun

kerentanan-kerentanan yang diuji sebagai berikut :

1. A1 – *Injection*

a. *SQL Injection*

SQL Injection memungkinkan kendali atas *database* oleh penyerang. Adapun keterangan mengenai ekpsloitasinya sebagai berikut :

a. *Tools*

a. Google Chrome Version 59.0.3071.115

b. Hasil

Adapun hasil setelah diberikan perintah dalam seperti yang diberikan OWASP ZAP

c. *Cookie Injection*

Adapun keterangan mengenai ekpsloitasinya sebagai berikut :

a. *Tools*

Adapun *Tools* yang digunakan untuk mengujinya adalah sebagai berikut:

1. Google Chrome Version 59.0.3071.115 sebagai korban.
2. Akses ke dalam TULIS.
3. Firefox ESR versi 45.3.0 sebagai penyerang.
4. Cookie Manager +v14.3 terinstall dalam Firefox.

b. Eksploitasi

1. Penulis menggunakan Chrome sebagai korban dan melakukan *log in* ke dalam sistem TULIS sebagai mahasiswa. Akses didapat melalui aktivasi member dalam Pusat Perpustakaan dan menampilkan *cookie* yang ada.
2. Penulis menggunakan Firefox sebagai penyerang memiliki *cookie* yang berbeda sehingga belum bisa masuk ke dalam sistem.
3. Penulis mencocokkan *cookie value* yang ada dalam korban dengan *cookie value* penyerang.
4. Penulis melakukan *refresh browser* penyerang setelah melakukan edit *value* dan berhasil masuk dalam sistem tanpa melakukan *log in*.
5. Penulis melakukan *session hijack* dengan melakukan *log out* pada akun penyerang dan yang akun korban ikut *log out* dari sistem.

d. Generic Script Injection

Kerentanan ini mengakibatkan skrip dapat dieksesusi. Untuk kerentanan ini.

1. *Tools*
   a. Google Chrome 59.0.3071.115
   b. Firefox ESR 45.3.0
2. Eksploitasi

Ketika Penulis mengeksekusi skrip <script>alert("a")</script> ke dua *browser* hasil yang diapatkan ialah

a. Chrome

Menggunakan Chrome tidak berhasil

b. Firefox

Skrip alert berjalan

2. A3 – XSS *Reflected*

XSS menyebabkan perintah yang berasal dari sumber tidak terpercaya dapat tereksekusi. Adapun keterangan mengenai ekpsloitasinya sebagai berikut :

a. *Tools*

i. Firefox ESR 45.3.0

b. Eksploitasi

Penulis menggunakan <marquee>test</marquee> kedalam kolom pencarian

1. A5 – *Security Missconfiguration*

a. *Buffer Overflow*

Kerentanan ini merupakan ketidakmampuan *server* dalam menangani perintah yang banyak sehingga penyerang dapat melakukan *overwrite* data. Adapun mengenai *Tools*, eksploitasi dan rekomendasi sebagai berikut:

1. *Tools*
   a. Google Chrome Version 59.0.3071.115
2. Eksploitasi

Menurut pemindai kerentanan OWASP ZAP, dengan memberikan masukan

yang banyak dapat mengakibatkan *Buffer Overflow*, namun Penulis tidak berhasil karena hanya mendapatkan *error* dan masukan yang diberikan terfilter dengan baik.

b. *Web Browser XSS Protection Not Enabled*
Kerentanan ini menyebabkan skrip bisa dieksekusi melalui *browser* karena anti XSS tidak digunakan. Adapun eksploitasinya telah dilakukan bersamaan dengan A3 – XSS bagian XSS *Reflected*.

c. *Apache JServ protocol service*
Kerentanan ini mengakibatkan halaman konfigurasi Tomcat dapat diakses oleh siapa saja. Adapun mengenai *Tools*, eksploitasi dan rekomendasi sebagai berikut:
   1. *Tools*
      a. Google Chrome Version 59.0.3071.115
   2. Eksploitasi
      Dengan terbukanya port 8009 dalam *reconnaissance* memungkinkan akses AJP melalui http://tulis.uinjkt.ac.id/manager

d. *Cookie(s) without HttpOnly flag set*
Kerentanan ini merupakan kondisi di mana penyerang dapat mengambil *cookie* melalui CSRF ataupun penyadapan yang kemudian bisa dimanfaatkan untuk *Cookie Injection* karena tidak ada nya HTTPOnly pada *header*. Untuk keterangan mengenai *Tools*, ekploitasi dan rekomendasi akan dibahas pada A8 – CSRF.

e. *Login page password-guessing attack*
Kerentanan ini menyebabkan penyerang dapat mencoba kombinasi *username* dan *password* berkali-kali tanpa pencegatan atau biasa dikenal dengan *brute force attack*.
   1. *Tools*
      a. Google Chrome Version 59.0.3071.115
   2. Eksploitasi
      a. Penulis mencoba memasukan *username* dan *password* dengan admin : admin melalui halaman admin yang didapatkan saat *reconnaissance* dengan robots.txt.
      b. Penulis tidak berhasil masuk dan kembali diarahkan menuju halaman admin tanpa ada pencegatan.
      c. Ketika diisi kembali dengan acak berkali-kali dengan berbagai kombinasi, TULIS tidak melakukan pencegatan sehingga rawan untuk diserang menggunakan metode *brute force attack*.

f. *Broken links*
Tidak dilakukan pengujian untuk kerentanan ini, karena menurut Acunetix sebagai *vulnerability scanner*, kerentanan ini tidak memiliki resiko.

g. *Allowed Method*
Kerentanan ini akan menjadi riskan apabila memiliki *methods* diluar RFC 216 seperti HEAD, GET, POST, PUT, DELETE, TRACE, OPTIONS dan CONNECT. (OWASP, 2015, Test HTTP Methods (OTG-CONFIG-006), https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006), diakses pada tanggal 1 Agustus 2017). Dalam tahapan *reconnaissance* bagian NMAP, TULIS didapati hanya menggunakan *GET HEAD POST OPTIONS* sehingga dinyatakan tidak memiliki resiko atas kerentanan.

h. DAV
Kerentanan DAV memungkinkan penyerang untuk melakukan *deface* dengan menaruh *file* langsung ke dalam direktori. Adapun mengenai *Tools*, eksploitasi dan rekomendasi sebagai berikut :
   1. *Tool*
      a. Davtest
   2) Eksploitasi :
      Dengan menginput davtest -url http://tulis.uinjkt.ac.id *-sendbd auto* ternyata tidak berhasil.

i. *Web Application Cookies Not Marked Secure*
Kerentanan ini merupakan kondisi di mana penyerang dapat mengambil *cookie* melalui CSRF ataupun penyadapan yang kemudian bisa dimanfaatkan untuk *Cookie Injection* karena *secure* belum diimplementasikan pada *header*. Untuk keterangan mengenai *Tools*, ekploitasi dan rekomendasi akan di-

bahas pada A8 – CSRF.

3. **A6 – *Sensitive Data Exposure***
   a. Apache Tomcat *Examples Directory Vulnerability*
      Kerentanan ini menyebabkan penyerang dapat mengakses *folder/examples* yang di mana *folder* tersebut berisikan *file* Tomcat secara *default*.
      1. *Tools*
         a. Google Chrome Version 59.0.3071.115
      2. Eksploitasi
         a. Membuka halaman http://tulis.uinjkt.ac.id/examples
         b. *Application Error Message*
            Untuk kerentanan ini mengakibatkan terekspos nya informasi yang tidak seharusnya terlihat. Penulis telah membahasnya bersamaan dengan A1 – *Injection* bagian SQL *Injection*.
         c. *Snoop Servlet information disclosure*
            Kerentanan ini ada ketika menggunakan IBM *Websphere* di bawah versi 7.0.0.23, namun untuk mengakses halaman IBM *Websphere* sendiri tidak berhasil dengan http://tulis.uinjkt.ac.id:9060/ibm/console sehingga tidak diuji lebih lanjut. Jika Acunetix menginformasikan IBM *Websphere* versi tersebut rentan maka perlu diperbarui.
         d. *Password type input with auto-complete enabled*
            Kerentanan ini menyebabkan *username* dan *password* menjadi tersimpan dalam *browser* klien sehingga sangat rentan apabila komputer tertinggal atau disalah pergunakan orang yang tidak bertanggung jawab. Adapun eksploitasinya :
            [1] *Tools*
               a. Web browser seperti Google Chrome Version 59.0.3071.115
            [2] Eksploitasi
               Penulis hanya memberikan masukan *username* dan *password* lalu *web browser* langsung menawarkan penyimpanan *username password*.
         e. *Possible username or password disclosure*
            Untuk kerentanan ini, tidak ditemukan informasi berharga mengenai *username* maupun *password* melalui *browsing*.
         f. *Web Application Sitemap*
            Kerentanan ini berpotensi bocornya seluruh direktori yang ada pada TULIS. Dengan mengakses http://tulis.uinjkt.ac.id/sitemaps.xml pada umumnya akan mengeluarkan *sitemaps*, namun TULIS tidak memilikinya.
         g. *Web Server Transmits Cleartext Credentials*
            Kerentanan ini mengakibatkan terekspos nya *username* dan *password* saat *sniffing*. Adapun pengujiannya sebagai berikut :
            1) *Tool*
               a. Cain and Abel v4.956
            2) Eksploitasi
               Server TULIS telah dilengkapi dengan Anti ARP sehingga baik *username* dan *password* tidak terekspos saat *sniffing*. sehingga Penulis mendapatkan *username* dan *password repository* namun TULIS tidak.
         h. *Web Server Uses Basic Authentication Without HTTPS*
            Untuk kerentanan ini tidak dilakukan pengujian karena TULIS belum menggunakan HTTPS.
         i. *Web Server robots.txt Information Disclosure*
            Kerentanan ini telah diuji dalam tahapan *Reconaissannce* dengan mengakses http://tulis.uinjkt.ac.id/robots.txt. Adapun rekomendasi untuk menutup kerentanan ini

ialah dengan menghapus *file* robots. txt dan menggantinya dengan konfigurasi pada *htaccess*.

j. *Nessus TCP scanner*
Kerentanan ini tidak diuji karena TCP *Scan* telah dilakukan pada tahapan *reconnaissance* bagian NMAP.

k. *Web Mirroring*
Web Mirorring memungkinkan terjadinya perubahan terhadap salah satu *web* yang mengakibatkan perubahan pada seluruh *web* yang ada. Saat *reconnaissance*, NMAP mendapatkan hasil mirror http://tulis.uinjkt.ac.id dengan http://172.27.15.147:8080 yang memang diperlukan oleh Pusat Perpustakaan untuk mengurangi *traffic*.

l. *Web Server Directory Enumeration*
Kerentanan mengakibatkan direktori menjadi bocor.
   1. *Tool*
      a. URL Fuzzer
   2. Eksploitasi

m. *Web Server Office File*
Kerentanan ini tidak diuji karena TULIS memang menyimpan *file* PDF dalam *repository* sebagai *file digital*.

n. *CGI Generic Tests Timeout*
Kerentanan ini tidak diuji karena menurut Nessus, karena kerentanan ini berupa *time out* saat Nessus melakukan pemindaian. Nessus pun memberikan pernyataan dalam laporan pemindaian bahwa kerentanan ini tidak memiliki resiko.

o. *Protected Web Page Detection*
Kerentanan ini tidak diuji karena, TULIS memiliki halaman untuk manajemen aplikasi yang menjadi halaman admin yang memerlukan autentikasi yang ditemukan saat reconnaissance dengan robots.txt.

p. *External URL(s)*
Dalam halaman utama TULIS, TULIS meletakan gambar Lontar di bagian bawah halaman dengan referensi ke halaman http://dl2.cs.ui.ac.id/ yang merupakan *developer* TULIS.

q. *Web Server Harvested Email Addresses*
Kerentanan ini tidak diuji karena baik dosen maupun staff UIN Jakarta memiliki domain email yang sama yaitu @uinjkt.ac.id sehingga jika ditemukan belum tentu berhasil.

r. *Private IP Disclosure*
Kerentanan ini mengakibatkan IP yang dimiliki server terkespos sehingga memudahkan penyerang untuk menyerang. Namun kerentanan yang didapatkan ini merupakan suatu *false positive*, karena saat pengujian sistem, menggunakan IP http://172.27.15.156 yang merupakan IP untuk melakukan scan.

4. A7 – *Missing Function Level Access Control*

a. *Clickjacking: X-Frame-Options header missing*
Kerentanan ini dapat membuat TULIS bisa ditampilkan dalam frame sehingga dapat mengecoh pengguna. Adapun eksploitasi mengenai kerentanan ini :
   1. *Tools*
      a. Google Chrome Version 59.0.3071.115
      b. Perintah <frame></frame>
   b. Eksploitasi
      Jika dieksekusi dengan perintah *frame*, maka TULIS dapat ditampilkan dalam web lain padahal web tersebut mungkin telah dimodifikasi sehingga rawan terjadi hal merugikan yang dapat mengecoh pengguna awam.

b. *Missing or Permissive Content-Security-Policy HTTP Response Header*

Kerentanan ini mengakibatkan TULIS tidak terproteksi dari serangan XSS karena *Content-type-header* tidak diatur dengan benar. Adapun exploitnya sebagai berikut :

1. *Tools*
   Telah dibahas dalam pengujian XSS.
2. Eksploitasi
   Telah dibahas dalam pengujian XSS.

5. A8 – *Cross Site Request Forgery*

a. *HTML form without CSRF protection*
CSRF mengakibatkan penyerang mendapatkan akses melalui ketidak pahaman ataupun kecerobohan *user* yang telah terautentikasi dengan mengklik sesuatu seperti gambar ataupun *link* sehingga penyerang mendapatkan akses.

1. *Tools*
   Adapun Tools yang digunakan untuk mengujinya adalah sebagai berikut :
   a. Firefox ESR versi 45.3.0 (browser tanpa xss filter).
   b. Akun *hosting* yang mendukung bahasa pemrograman php.
   c. Skrip PHP untuk mencuri *cookie*.
   d. Wadah berupa *file* txt untuk menyimpan *cookie* yang tercuri.
2. Eksploitasi
   a. Penulis masuk ke dalam sistem sebagai mahasiswa.
      Penulis membuat *review* buku dan menyelipkan skrip file *source cookiestealer.php* supaya jalan saat diklik dan meletakkan *cookielog.txt* pada *hosting*.
   2. Penulis melakukan interaksi dengan staf untuk mengecek *review* yang telah Penulis buat.
   3. Informasi pun tersimpan, namun cookie kosong, sehingga Penulis menyimpulkan bahwa TULIS telah menetapkan HTTP *Only* dan HTTP *Secure* karena *cookie* nya.

6. A9 – *Using Components With Known Vulnerabilities*

a. *Vulnerable Javascript library*
Tidak dilakukan pengujian karena tidak diberitahukan mendetail dari Acunetix.

b. HTTP *Server* Type and Version
Kerentanan ini ditemukan bersamaan dengan tahapan *reconnaissance* yang dimana mendapatkan informasi mengenai versi apache yang digunakan, yaitu 2.4.7. Adapun keterangan mengenai eksploitnya sebagai berikut :
   1. *Tools*
      a. NMAP v7.25
   2. Eksploitasi
   Kerentanan ini ditemukan saat tahapan reconnaissance dengan NMAP.

c. *HyperText Transfer Protocol (HTTP) Information*
Kerentanan ini ditemukan di tahapan *reconnaissance* pada bagian NMAP. Untuk keterangan mengenai *Tools*, eksploitasi dan rekomendasi kerentanan ini telah dipaparkan di A9 – *Using Components With Known Vulnerabilities* HTTP *Server* Type and Version.

7. A10 – Unvalidated Redirect and Forwards

a. Global Redirect
Kerentanan ini diuji bersamaan dengan A8 – CSRF dan dapat diketahui bahwa TULIS tidak memiliki halaman konfirmasi ketika ke halaman luar. Untuk keterangan mengenai *Tools*, eksploitasi dan rekomendasi kerentanan ini telah dipaparkan di A8–CSRF.

Setelah Eksploitasi dan Mempertahankan Akses *(Post Exploitation dan Maintaining Access)*

Mempertahankan Akses

a. Penulis telah menanamkan *backdoor* yang berupa *skrip* dalam *review* buku yang berfungsi untuk mencuri *cookie*, namun TULIS telah menerapkan *HTTPOnly* yang mengakibatkan Penulis tidak dapat melakukan serangan *Cookie Injection*.
b. Penulis juga menanamkan *payload* berupa *javascript* yang memungkinkan penulis dapat

merekan jejak aktivitas *keyboard* atau biasa disebut *keylogger. Skrip* kemudian diinjeksian kedalam TULIS ke dalam kolom *review* buku dan berjalan dengan baik.

SIMPULAN

Kesimpulan

Setelah melakukan pengujian kerentanan atas aplikasi TULIS yang merupakan Sistem Informasi Perpustakaan pada Pusat Perpustakaan, dapat disimpulkan bahwa :

1. Berdasarkan hasil pemindaian kerentanan, TULIS memiliki kerentanan mulai dari level sedang (XSS *Reflected, Security, Apache Jserv protocol service, Login page password guessing attack,* dan HTML *form without CSRF protection*) sampai dengan berat *(Sensitive Data Exposure bagian web server robots.txt information disclosure).*
2. Setelah dilakukan eksploitasi kerentanan yang mengacu pada hasil pemindaian sebelumnya, ada kerentanan level berat yang tidak benar-benar ada atau salah pendeteksian *(false positive)* yaitu *buffer overflow* dan SQL *injection*.

Saran

Adapun saran yang penulis dapat berikan kepada tim pengembang aplikasi TULIS :

1. Memperbaiki celah kerentanan yang telah ditemukan berdasarkan hasil pengujian dan analisis yang telah dijelaskan sebelumnya.
2. Melakukan pengujian sistem sebelum diserahkan ke *customer* sehingga aplikasi yang diserahkan bebas dari kerentanan.

Sedangkan saran yang dapat diberikan untuk Pusat Perpustakaan :

1. Membuat *Standard Operating Procedure* (SOP) sebagai pencegahan jika terjadi serangan *cyber*.
2. Memperkuat pertahanan terutama dari sisi jaringan komputer.

DAFTAR PUSTAKA

Baloch, Rafay. (2015). *Ethical Hacking and Penetration Testing Guide.*

Boca Raton: *Taylor and Francis Group.* Cole, Eric et al. (2005). Network Security Bible. Indiana :Wiley Publishing.

Dharma Oetomo, Budi Sutedjo et. al. (2007). *Pengantar. Teknologi Informasi Internet, Konsep dan Aplikasi*. Yogyakarta: CV Andi Offset

Engebretson, Patrick. (2013). *The Basic of Hacking and Penetration Testing*. Waltham: Elsevier Hadnagy,

Christopher. (2011). *Social Engineering: The Art of Human Hacking.* Indiana:JohnWiley & Sons.

Jogiyanto. (2008). *Dalam Metodologi Penelitian Sistem Informasi: Pedoman dan Contoh Melakukan Penelitian di bidang Sistem Informasi Teknologi.* Yogyakarta: Penerbit ANDI Yogyakata.

Kozierok, M. Charles. (2005). *TCP/IP Guide*. San Fransisco: No Starch Press,Inc.

Mulyanto, Agus. (2009). *Sistem Informasi Konsep dan Aplikasi.* Yogyakarta: Pustaka Belajar.

Nazir, Moh. (2009). *Metode Penelitian.* Jakarta: Ghalia Indonesia

O'Brien dan Marakas, 2010. *Management System Information*. McGraw Hill,.

New York Pressman, R. S. (2010). *Software Engineering A Practitioner's Approach 7th*. New York : McGraw-Hill. Stallings,

William. (2007). *Komunikasi & Jaringan Nirkabel, Jilid 1, Edisi kedua*. Jakarta: Erlangga

Simarmata, Janner. (2006). *Pengenalan Teknologi Komputer dan Informasi.* Yogyakarta : Andi Offset.

Sofana, Iwan. (2008). *Membangun Jaringan Komputer. Bandung :Informatika. Sutabri, Tata.* (2012). Analisis Sistem Informasi. Andi. Yogyakarta

Sutarman. (2009). *Pengantar Teknologi Informasi*. Yogyakarta : Bumi Aksara Tanenbaum, AS &

Wetherall, DJ. (2011) *Computer Networks, 5th Edition*, Prentice Hall.

Warsita, Bambang. (2008) *Teknologi Pembelajaran: Landasan &Aplikasinya,* Jakarta:

Rineka. Weidman, Georgia. (2014). *Penetration Testing: A Hands-on Introduction to Hacking.* San Fransisco: No Starch Press, Inc.