PENERAPAN INFORMATION GATHERING BERDASARKAN OWASP TESTING GUIDE 2014 V4.0 STUDI KASUS WEBSITE SCRIPTI

Skripsi

oleh
TOAR LUKKI ROGI
22084503

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2015

PENERAPAN INFORMATION GATHERING BERDASARKAN OWASP TESTING GUIDE 2014 V4.0 STUDI KASUS WEBSITE SCRIPTI

Skripsi

Diajukan kepada Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana
Sebagai Salah Satu Syarat dalam Memperoleh Gelar
Sarjana Komputer

Disusun oleh

TOAR LUKKI ROGI
22084503

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2015

PERNYATAAN KEASLIAN SKRIPSI

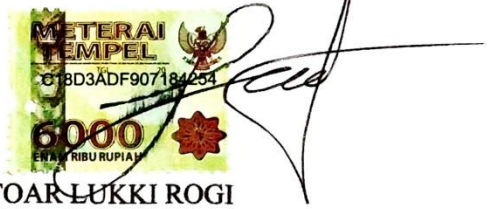
Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

PENERAPAN INFORMATION GATHERING BERDASARKAN OWASP TESTING GUIDE 2014 V4.0 STUDI KASUS WEBSITE SCRIPTI

yang saya kerjakan untuk melengkapi sebagian persyaratan menjadi Sarjana Komputer pada pendidikan Sarjana Program Studi Teknik Informatika Fakultas Teknologi Informasi Universitas Kristen Duta Wacana, bukan merupakan tiruan atau duplikasi dari skripsi kesarjanaan di lingkungan Universitas Kristen Duta Wacana maupun di Perguruan Tinggi atau instansi manapun, kecuali bagian yang sumber informasinya dicantumkan sebagaimana mestinya.

Jika dikemudian hari didapati bahwa hasil skripsi ini adalah hasil plagiasi atau tiruan dari skripsi lain, saya bersedia dikenai sanksi yakni pencabutan gelar kesarjanaan saya.

Yogyakarta, 28 Januari 2016



TOAR LUKKI ROGI
22084503

HALAMAN PERSETUJUAN

Judul Skripsi	:	PENERAPAN INFORMATION GATHERING BERDASARKAN OWASP TESTING GUIDE 2014 V4.0 STUDI KASUS WEBSITE SCRIPTI
Nama Mahasiswa	:	TOAR LUKKI ROGI
N I M	:	22084503
Matakuliah	:	Skripsi (Tugas Akhir)
Kode	:	TIW276
Semester	:	Gasal
Tahun Akademik	:	2015/2016

Telah diperiksa dan disetujui di
Yogyakarta,
Pada tanggal 28 Januari 2016

Dosen Pembimbing I	Dosen Pembimbing II
Willy Sudiarto Raharjo, S.Kom.,M.Cs.	Budi Susanto, SKom.,M.T.

HALAMAN PENGESAHAN

PENERAPAN INFORMATION GATHERING BERDASARKAN OWASP TESTING GUIDE 2014 V4.0 STUDI KASUS WEBSITE SCRIPTI

Oleh: TOAR LUKKI ROGI / 22084503

Dipertahankan di depan Dewan Penguji Skripsi
Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana - Yogyakarta
Dan dinyatakan diterima untuk memenuhi salah satu syarat memperoleh gelar
Sarjana Komputer
pada tanggal 7 Januari 2016

Yogyakarta, 28 Januari 2016
Mengesahkan,

Dewan Penguji:

1. Willy Sudiarto Raharjo, S.Kom.,M.Cs.
2. Budi Susanto, SKom.,M.T.
3. Lukas Chrisantyo, S.Kom., M.Eng.
4. Gani Indriyanta, Ir. M.T.

Dekan	Ketua Program Studi
(Budi Susanto, S.Kom., M.T.)	(Gloria Virginia, Ph.D.)

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Tuhan Yesus Kristus atas anugerah, berkat, rahmat, dan karunianya sehingga penulis dapat menyelesaikan Tugas Akhir dengan judul "Penerapan Information Gathering Berdasarkan OWASP Testing guide 2014 V4.0 Studi Kasus Website Scripti" dengan baik.

Penulisan laporan ini merupakan kelengkapan dan pemenuhan dari salah satu syarat dalam memperoleh gelar Sarjana Komputer. Selain itu, penulisan laporan Tugas Akhir ini juga bertujuan untuk melatih mahasiswa agar dapat menghasilkan suatu karya yang dapat dipertanggungjawabkan secara ilmiah, sehingga dapat bermanfaat bagi penggunanya.

Dalam menyelesaikan penelitian dan laporan Tugas Akhir ini, penulis telah banyak menerima bimbingan, saran, dan masukkan dari berbagai pihak, baik secara langsung maupun secara tidak langsung. Untuk itu dengan segala kerendahan hati, pada kesempatan ini penulis menyampaikan ucapan terima kasih kepada :

1. Tuhan Yesus Kristus yang telah menyertai penulis untuk menyelesaikan penelitian dan penyusunan Laporan Tugas Akhir.
2. Bapak Willy Sudiarto Raharjo, S.Kom.,M.Cs. selaku dosen pembimbing I yang telah sabar dalam membimbing penulis dalam mengerjakan penelitian dan penyusunan laporan Tugas Akhir.
3. Bapak Budi Susanto, SKom.,M.T. selaku dosen pembimbing II yang selalu sabar dan baik membimbing penulis dalam mengerjakan penelitian dan penyusunan laporan Tugas Akhir.
4. Keluarga dan saudara yang selalu memberikan doa dan semangat kepada penulis dalam menyelesaikan Tugas Akhir.
5. Yonathan Bambang dan Tisa Indah Nugraheni selaku bapak gembala dan ibu gembala yang senantiasa memberikan dukungan kepada penulis dalam menyelesaikan Tugas Akhir.
6. Rekan-rekan sepelayanan Gereja Behany Magelang yang dengan tulus memberikan dukungan, saran, dan, sharing dalam pengerjaan Tugas Akhir maupun penulisan laporan Tugas Akhir.

7. Rekan-rekan penulis yang dengan senang hati memberikan arahan, saran, dan, sharing dalam pengerjaan Tugas Akhir maupun penulisan laporan Tugas Akhir.
8. Pihak lain yang tidak dapat penulis sebutkan satu per satu, sehingga Tugas Akhir ini dapat terselesaikan dengan baik.

Penulis menyadari bahwa penelitian dan laporan Tugas Akhir ini masih jauh dari sempurna. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun dari pembaca sekalian.

Akhir kata penulis meminta maaf bila ada kesalahan dalam penyusunan laporan maupun sewaktu penulis melakukan penelitian Tugas Akhir. Semoga penelitian dan laporan Tugas Akhir ini dapat berguna bagi kita semua.

Yogyakarta, 28 Januari 2016

Penulis

INTISARI

Information Gathering merupakan tahapan bagi seorang *penetration testing* dalam melakukan pengujian terhadap sistem atau aplikasi. Information Gathering berperan sebagai pijakan awal sebelum penguji melanjutkan ke tahapan ekspoitasi atau penyerangan terhadap sistem atau aplikasi yang menjadi target. Information Gathering pada penelitian ini menggunakan panduan OWASP Testing Guide V4.0 yang memberikan beberapa kontrol yang secara umum dilakukan untuk mendapatkan sebanyak mungkin informasi penting yang berguna bagi penguji untuk melakukan eksploitasi pada sistem atau aplikasi target.

Penelitian ini bertujuan untuk menggali informasi sebanyak mungkin terkait dengan semua hal dapat diperoleh dari *website* scripti.ukdw.ac.id.melalui beberapa metode yang telah dipaparkan melalui OWASP Testing Guide V4.0 dengan melibutkan cara secara langsung dan menggunakan beberapa *tool* yang memiliki fungsi untuk *scanning* dan *fingerprinting* akan teknologi yang ada pada *website* scripti.ukdw.ac.id.

Hasil dari analisa dengan menggunakan metode tersebut memberikan informasi penting mengenai beberapa kelemahan yang memiliki potensi sebagai celah keamanan aplikasi *website* tersebut salah satunya ialah versi aplikasi yang digunakan teridentifikasi memiliki fitur yang yang berpotensi sebagai celah kelemahan, selain itu penelitian ini memberikan rekomendasi atau saran dalam pengelolaan selanjutnya demi kelangsungan layanan aplikasi *website* scripti.ukdw.ac.id. Penelitian ini memberikan manfaat bagi pengelola dalam memberikan gambaran terkini mengenai keamanan *website* scripti.ukdw.ac.id, celah maupun kelemahan yang berpotensi di kemudian hari dapat diantisipasi dengan hasil analisa yang telah dilakukan pada penelitian ini.

Kata Kunci : *Information Gahtering, OWASP, Penetration Testing,* Security

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Information Gathering merupakan tahapan bagi seorang *penetration testing* dalam melakukan pengujian terhadap sistem atau aplikasi. Information Gathering berperan sebagai pijakan awal sebelum penguji melanjutkan ke tahapan ekspoitasi atau penyerangan terhadap sistem atau aplikasi yang menjadi target. Information Gathering pada penelitian ini menggunakan panduan OWASP Testing Guide V4.0 yang memberikan beberapa kontrol yang secara umum dilakukan untuk mendapatkan sebanyak mungkin informasi penting yang berguna bagi penguji untuk melakukan eksploitasi pada sistem atau aplikasi target.

Penelitian ini bertujuan untuk menggali informasi sebanyak mungkin terkait dengan semua hal dapat diperoleh dari *website* scripti.ukdw.ac.id.melalui beberapa metode yang telah dipaparkan melalui OWASP Testing Guide V4.0 dengan melibutkan cara secara langsung dan menggunakan beberapa *tool* yang memiliki fungsi untuk *scanning* dan *fingerprinting* akan teknologi yang ada pada *website* scripti.ukdw.ac.id.

Hasil dari analisa dengan menggunakan metode tersebut memberikan informasi penting mengenai beberapa kelemahan yang memiliki potensi sebagai celah keamanan aplikasi *website* tersebut salah satunya ialah versi aplikasi yang digunakan teridentifikasi memiliki fitur yang yang berpotensi sebagai celah kelemahan, selain itu penelitian ini memberikan rekomendasi atau saran dalam pengelolaan selanjutnya demi kelangsungan layanan aplikasi *website* scripti.ukdw.ac.id. Penelitian ini memberikan manfaat bagi pengelola dalam memberikan gambaran terkini mengenai keamanan *website* scripti.ukdw.ac.id, celah maupun kelemahan yang berpotensi di kemudian hari dapat diantisipasi dengan hasil analisa yang telah dilakukan pada penelitian ini.

Kata Kunci : *Information Gahtering, OWASP, Penetration Testing,* Security

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Keamanan sebuah sistem atau aplikasi merupakan salah satu faktor terpenting yang perlu dirancang sedemikian rupa demi melindungi informasi penting yang menjadi tujuan dilancarkannya serangan oleh pihak tertentu guna memperoleh suatu informasi dalam sistem atau aplikasi tersebut atau bahkan memiliki motivasi yang bersifat merugikan yakni untuk melumpuhkan sistem atau aplikasi agar tidak dapat beroperasi. Bagi seorang penyerang untuk bisa melakukan sebuah serangan yang ditujukan kepada sebuah sistem tentunya perlu mengetahui terlebih dahulu informasi apakah yang dimiliki oleh sistem yang menjadi target. Dari proses pengumpulan informasi inilah penyerang menganalisa dan memperoleh kesimpulan mengenai celah atau kelemahan sistem tersebut yang selanjutnya berlanjut pada teknik *Penetration Testing*.

Proses pengumpulan informasi tersebut dapat dilakukan dengan berbagai cara yakni dengan menggunakan *tools* yang umum seperti *search engine*, *scanner*, dengan mengirimkan *request* HTTP sederhana, atau *request* khusus yang memungkinan aplikasi tersebut membocorkan informasi. Misalnya dengan memberikan umpan balik berupa pesan kesalahan atau memaparkan versi dan teknologi yang digunakan pada aplikasi tersebut. Sedangkan *penetration testing* lebih fokus pada sejauh apakah seorang penyerang dapat menyerang dan masuk ke suatu sistem dengan memanfaatkan beragam kelemahan atau celah yang ditemukan, salah satunya dengan menggali lebih dalam beragam informasi yang telah diperoleh dari target yang telah berhasil di eksploitasi.

Dalam kasus ini penulis akan melakukan proses pengumpulan informasi (*Information Gathering*) dari *website* scripti.ukdw.ac.id yang menjadi studi kasus untuk melancarkan *Information Gathering* berdasarkan pada *The Open Web Application Securty Project (OWASP) Testing Guide 2014 V4.0*.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan di atas, maka penulis akan melakukan penelitian terkait dengan:

1. Informasi penting terkait dengan kelemahan *website* scripti.ukdw.ac.id yang dapat digali dengan penggunaan metode Information Gathering berdasarkan OWASP 2014 V.4.

1.3 Batasan Sistem

Penulis membatasi masalah yakni langkah apa saja yang diperlukan dalam proses penelitian ini. Penulis diasumsikan sebagai penguji (*tester)* dari pihak luar, bukan pihak dalam yang memiliki akun yang teregistrasi pada *website* scripti. Waktu pengujian yang dilakukan oleh penulis dimulai pada 12 Oktober 2015 dan berakhir pada 17 Desember 2015.

1.4 Tujuan Penelitian

Penulisan tugas akhir ini bertujuan untuk :

1. Mengetahui proses pengumpulan informasi (*Information Gathering*) berdasar OWASP Testing Guide V4.0.
2. Menilai tingkat kerentanan (*vulnerability*) pada sebuah aplikasi website setelah dilakukan metode OWASP Tesing Guide V4.0 yaitu pada *website* scripti.ukdw.ac.id.
3. Memberikan rekomendasi kepada pengelola layanan scripti menghadapi kelemahan yang dimiliki website scripti.ukdw.ac.id tersebut.

Dengan mengacu pada penelitian ini diharapkan dapat memberikan kontribusi bagi pihak pengelola *website* scripti.ukdw.ac.id dan juga gambaran akan hal-hal yang perlu diperhatikan dalam membangun sebuah aplikasi *website* yang handal dalam mengantisipasi ketika terdapat serangan berdasar OWASP Testing Guide V4.0.

1.5 Metodologi Penelitian

Metode penelitian yang akan digunakan dalam penelitian ini adalah:

1. Metode yang digunakan untuk mengumpulkan data dan informasi dalam tugas akhir ini dengan studi kasus *website* scripti.ukdw.ac.id ialah dengan mempelajari metode Information Gathering bedasarkan *OWASP Testing Guide 2014 V4.0,* selanjutya penulis melakukan proses pengumpulan informasi secara langsung terhadap *website* yang sudah ditentukan.
2. Konsultasi dengan dosen pembimbing dari awal proses dilakukannya penelitian sampai selesainya laporan yang dikerjakan.

1.6 Sistematika penulisan

Sistematika laporan tugas akhir ini secara garis besar dapat dituliskan sebagai berikut:

BAB 1 : Pendahuluan

Berisi latar belakang beserta batasan masalah, tujuan tugas akhir dan sistematika penulisan.

BAB 2 : Landasan Teori

Berisi teori-teori yang mendasari topik yang telah ditentukan beserta ilmu-ilmu lain yang mendukung.

BAB 3 : Perancangan Sistem

Berisi tentang langkah yang akan dilakjkan dalam proses Information Gathering secara umum mulai dari tahap analisa kontrol awal sampai pada tahap peniliaian dari hasil analisa penerapan proses Information Gathering terhadap *website* scripti.ukdw.ac.id.

BAB 4 : Analisis

Berisi tentang proses Information Gathering secara umum mulai dari tahap kontrol awal analisa sampai pada tahap kontrol akhir proses Information Gathering terhadap *website* scripti.ukdw.ac.id.

BAB 5: Kesimpulan dan Saran

Berisi kesimpulan dari hasil analisa menggunakan metode penerapan Information Gathering berdasarkan OWASP 2014 V.4.0.

BAB V

KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan analisa yang telah dilakukan terhadap *website* scripti.ukdw.ac.id dengan metode *Information Gathering* sesuai dengan OWASP Testing Guide V4.0, maka diambil kesimpulan sebagai berikut :

1. Secara umum *website* scripti.ukdw.ac.id pada saat diakses tanpa melakukan *login* sistem tidak ditemukan masalah atau kelemahan terkait keamanannya, karena informasi penting yang lebih detil dan fitur-fitur mengenai sistem hanya dapat diakses lebih lanjut ketika penguji sudah melakukan *login* ke dalam sistem tersebut.
2. Informasi mengenai versi PHP 5.4.45 yang digunakan *website* scripti.ukdw.ac.id terdapat *bug* yang telah teridentifikasi dan telah diumukan melalui situs resminya. Informasi tersebut menjadi sangat penting karena dapat menjadi celah keamanan bagi aplikasi *website.*

5.2. Saran

Berdasarkan hasil penelitian *Information Gathering* yang diperoleh, adapun saran bagi pengelolaan *website* scripti.ukdw.ac.id :

1. Melakukan *upgrade* versi PHP 5.4.45 yang saat ini masih digunakan untuk mengantisipasi terjadi kerusakan di kemudian hari.
2. Mengikuti *update* yang telah dilakukan oleh tim OWASP untuk selanjutnya hasil penelitian tersebut dapat digunakan untuk menguji keamanan sistem atau aplikasi yang dimiliki oleh universitas .
3. Melakukan pengujian berkala terhadap sistem atau aplikasi yang digunakan oleh pihak universitas, karena hanya dibutuhkan satu celah untuk dapat merusak suatu sistem atau aplikasi. Keamanan sistem atau aplikasi merupakan proses yang harus terus dilakukan.

DAFTAR PUSTAKA

Huang, Y.-W., Huang, S.-K.,Lin, T.-P., Tsai, Ch.-H. (2003) *Web application security assessment by fault injection and behavior monitoring*. In: Proceedings of the 12th international conference on World Wide Web, May 20-24 (2003).

Hutahaean, I.H. (2004). *Program Bantu Pencarian Kerentanan Web Server Dengan Memanfaatkan Aplikasi Cgi.* (Undergraduate thesis, Duta Wacana Christian University, 2004). Retrieved from http://sinta.ukdw.ac.id

Mullins, M. (2005). *Choose the Best Penetration Testing Method for your Company*. Diakses pada tanggal 24 September 2014, diambil dari alamat situs http://www.techrepublic.com/article/choose-the-best-penetration-testing-method-for-yourcompany/5755555

Nilasari, E.S. (2014). *Studi Standar Keamanan Sistem Informasi Berdasarkan Iso 1799.* (Undergraduate thesis, Duta Wacana Christian University, 2014). Retrieved from http://sinta.ukdw.ac.id

Novianto, W.P. (2011). *Owasp Testing Guide Berbasis Web.* (Undergraduate thesis, Duta Wacana Christian University, 2011). Retrieved from http://sinta.ukdw.ac.id

OWASP. (2014. *OWASP Testing Guide 2014 V.4).* [Versi Elektronik]. Diakses pada 30 Oktober 2014 dari World Wide Web: https://www.owasp.org.

Shewmaker, J. (2008). *Introduction to Penetration Testing* [Versi Elektronik]. Diakses pada 24 September 2014 dari World Wide Web: http://www.dts.ca.gov/pdf/news_events/SANS_Institute-Introduction_to_Network_Penetration_Testing.pdf, accessed on Nov. 23, 2011

Su, Zh., Wassermann, G. (2006). *The essence of command injection attacks in web applications*. In: ACM SIGPLAN Notices, vol. 41, no.1, pp. 372-382.

Syafrizal, M. (2005). *Pengantar Jaringan Komputer*. ANDI offset, Yogyakarta.

Wiegenstein, A., Weidemann, F., Schumacher, M., Schinzel, S. (2006). *Web Application Vulnerability Scanners - a Benchmark*. Virtual Forge GmbH.