EVALUASI KEAMANAN WEBSITE PT. XYZ DENGAN MENGGUNAKAN SOFTWARE VEGA DAN NMAP

Kundang K. Juman
Fakultas Ilmu Komputer, Universitas Esa Unggul
Jalan Arjuna Utara No. 9 Kebon Jeruk Jakarta
kundang.karsono@esaunggul.ac.id

Abstrak

Evaluasi dan pengujian sistem keamana pada web site PT.XYZ, ditujuan untuk mencegah, mengatasi, melindungi sistem informasi dari risiko tindakan ilegal seperti penggunaan yang tidak sah, intrusi, dan penghancuran berbagai informasi yang dimiliki. Sistem atau sistem informasi dapat dimanfaatkan oleh penyusup yang memanfaatkan celah keamanan di berbagai sistem, aplikasi dan database. Penggunaan metode pengujian penetrasi untuk mengidentifikasi kerentanan keamanan di aplikasi untuk mengevaluasi sistem atau jaringan dalam berbagai teknik yang berbahaya. Tujuan dari tes dan evaluasi ini adalah untuk mengamankan data penting dari luar seperti penyusup yang mungkin memiliki akses tidak sah ke sistem. Memiliki kerentanan diidentifikasi digunakan untuk mengeksploitasi sistem dalam rangka untuk mendapatkan akses ke informasi sensitif. Sehubungan dengan pentingnya web site PT.XYZ,

Kata kunci: *Teknik pengujian, Evalusi keamanan web site, data, informasi, aplikasi, database, website, penyusupan, kerentanan.*

Pendahuluan

Pemanfaatan Teknologi Informasi sangat pesat dampak penggunaan Teknologi Informasi selain menguntungkan dan mempermudah dalam kehidupan sehari-hari juga ada celah yang dapat digunakan kegiatan kriminal yaitu permasalahan keamanan jaringan komputer , perlu kita sadari bahwa untuk mencapai suatu keamanan itu adalah suatu hal yang sangat mustahil, seperti yang ada dalam dunia nyata sekarang ini. Tidak ada satu daerah pun yang betul-betul aman kondisinya, walau penjaga keamanan telah ditempatkan di daerah tersebut, begitu juga dengan keamanan sistem komputer. Namun yang bisa kita lakukan adalah untuk mengurangi gangguan keamanan tersebut. Pada dasar website memiliki empat elemen dasar [1], yaitu: 1) browser, 2) server, 3) uniform resource locator (URL), dan 4) pages. Web server merupakan sebuah perangkat lunak server yang berfungsi menerima permintaan yyper text transfer protocol (HTTP) atau hyper text transfer protocol secure (HTTPS) dari klien yang dikenal dengan web browser dan mengirimkan kembali hasilnya dalam bentuk website (halaman web) yang pada umumnya berbentuk dokumen *hyper text markup language* (HTML),

Tujuan

Tujuan pengujian/evaluasi keamanan untuk menyelidiki kerentanan lingkungan sisi klien, komunikasi jariangan yang terjadi saat data dilewatkan dari klien ke server dan kembali lagi dan lingkungan sisi server ing kembali lagi dan lingkungan sisi server. – Pada sisi klien kerentanan dilacak pada bug yang telah ada sebelumnya pada browser, email program ,PL komunikasi, akses tidak sah ke cookie yang ditempatkan pada browser k Testipada browser. – Pada sisi server kerentanan meliputi serangan DOS (Denial of service) dan skrip jahat yang diteruskan ke sisi klien atau diguankan untuk mematahkan operasi server Tekni – Perlindungan keamanan :

1. Firewall – mekanisme penyaringan yang merupakan kombinasi dari perangkat keras dan perangkat lunak yang memeriksa setiap paket informasi yang datang untuk memastikan bahwa informasi tersebut berasal berasal dari sumber yang sah, memblokir memblokir data yang dicurigai dicurigai.
2. Otentifikasi – mekanisme verifikasi identtias yang menvalidasi semua klien dan server, yang memungkinkan komunikasi

terjadi hanya bila kedu abelah pihak telah diverifikasi.

3. Enkripsi – mekanisme penyandian yang melindungi data sensitif dengancara memodifikasi data dengan teknik-tenik tertentu

Metode Pengumpulan Data Dalam menyusun penelitian ini, kegiatan pengumpulan data dilakukan dengan beberapa cara antara, antara lain: 1. Library Research Pengumpulan data dilakukan dengan mempelajari bahan-bahan tertulis berupa buku, browsing melalui internet terhadap masalah yang berkaitan. 2. Interview dan Observasi Pada teknik ini penulis memperoleh data-data yang memiliki relevansi dengan penelitian dengan langsung melakukan observasi virtual dan nonvirtual. Virtual dengan mengunjungi website umk.ac.id, sedangkan 8 nonvirtual dengan langsung mengunjungi Unit Pelaksana Teknis Sistem keamanan web untuk pengamanan dalam melindungi para penggunanya.

Identifikasi Permasalahan

Identifikasi Permasalahan terkait dengan evaluasi dan pengujian sistem keamanan web pada PT. XYZ adalah:

1. Keamanan web adalah hal yang sangat penting dalam proses pengamanan data dalam suatu intitusi/perusahaan
2. Banyaknya perusahaan yang belum meng-optimalkan sistem keamanan web site
3. Masih lemahnya Administrator jaringan komputer pada banyak perusahaan
4. Perlunya penerapan keamanan web site untuk melindungi kemanan dan privasi para klien

Metode Penelitian

Research and information collecting; Dalam tahap ini dilakukan studi literatur dan studi aplikasi yang berkaitan dengan penulisan dan pengembangan aplikasi cross-platform lalu persiapan untuk merumuskan rencana penelitian; erencanaan dan persiapan dimulai dengan mendefinisikan tujuan dan sasaran dari pengujian penetrasi.Klien dan tester bersama-sama menentukan tujuan sehingga kedua pihak memiliki tujuan dan pemahaman yang sama. Tujuan umum dari pengujian penetrasi adalah -

- Untuk mengidentifikasi kerentanan dan meningkatkan keamanan sistem teknis.
- Memiliki keamanan IT dikonfirmasi oleh pihak ketiga eksternal.
- Meningkatkan keamanan infrastruktur organisasi / personil.

Teknik Pengujian Penetrasi yang Diterapkan pada *Website* PT. XYZ

Pengujian Penetrasi adalah proses untuk mengidentifikasi kerentanan keamanan dalam aplikasi dengan mengevaluasi sistem atau jaringan dengan berbagai teknik. Tujuan dari tes ini adalah untuk mengamankan data penting dari pihak luar seperti penyusup yang dapat memiliki akses tidak sah ke sistem. Setelah kerentanan diidentifikasi digunakan untuk mengeksploitasi sistem dalam rangka untuk mendapatkan akses ke informasi sensitif. Penyebab kerentanan antara lain:

1. Kesalahan pada desain dan pengembangan system
2. Konfigurasi sistem yang buruk
3. Kesalahan manusia

Melakukan pengujian penetrasi dengan tujuan:

1. Untuk mengamankan data pengguna
2. Untuk menemukan kerentanan keamanan dalam aplikasi

Ini sangat penting bagi setiap organisasi untuk mengidentifikasi masalah keamanan hadir dalam jaringan internal dan komputer. Menggunakan informasi organisasi ini dapat merencanakan pertahanan terhadap semua jenis upaya penyusupan. Privasi pengguna dan keamanan data adalah kekhawatiran terbesar saat ini.

Jenis pengujian penetrasi:

1. Rekayasa Sosial: kesalahan manusia adalah penyebab utama dari kerentanan keamanan. Standar dan kebijakan keamanan harus diikuti oleh semua anggota staf untuk menghindari rekayasa sosial penetrasi upaya. Contoh standar ini mencakup tidak menyebutkan informasi sensitif di email atau telepon komunikasi. Audit keamanan dapat dilakukan untuk mengidentifikasi dan kelemahan proses yang benar.

2. Pengujian keamanan aplikasi: Menggunakan metode perangkat lunak yang dapat memverifikasi jika sistem terkena kerentanan keamanan. Teknik pengujian aplikasi dilakukan menggunakan otomatisasi alat uji penetrasi.

Tahap Pengujian Sistem Pengujian Penetrasi

Pendekatan yang digunakan pada situs web ini menggunakan metodologi pengujian penetrasi, dan menerapkan CVSS (*Common Vulnerability Scoring System*) metode untuk menilai dan mengevaluasi risiko kerentanan.

CVSS digunakan untuk penilaian risiko kerentanan teknis dan kemampuannya untuk memberikan metrik komposit berdasarkan beberapa elemen. Penilaian CVSS dapat dianggap sebagai teknis objektif, *up-to-date*, dan kontekstual dan karena itu akan memprioritaskan upaya-upaya

Aspek Teknologi

Dalam melakukan pengujian penetrasi, pada umumnya para pengguna mengandalkan alat *open source*, pada pengembangan terbaru dari teknologi yang terkait. Penulis juga menggunakan berbagai selektif komersial / *lisensi* perangkat lunak berkualitas untuk membantu dalam menutupi skenario pengujian yang spesifik dan persyaratan. Pada *Vulnerability Scanning* dilakukan dengan alat otomatisasi yaitu Vega dan pada *Port Scanning* dilakungan dengan alat otomatisasi yaitu NMAP

Pengkajian Keamanan Jaringan pada *Website* PT.XYZ

Port Scanning

Hal ini mirip dengan pencuri yang akan melewati lingkungan Anda dan memeriksa setiap pintu dan jendela di setiap rumah untuk melihat mana yang terbuka dan mana yang terkunci. TCP (*Transmission Control Protocol*) dan UDP (*User Datagram Protocol*) adalah dua protokol yang membentuk *TCP / IP protocol suite* yang digunakan secara universal untuk berkomunikasi di Internet. Masing-masing memiliki *port* 0 sampai 65535 tersedia sehingga pada dasarnya ada lebih dari 65.000 pintu untuk mengunci. Beberapa alamat juga memiliki layanan umum terkait, namun sebagian besar port ini tidak terkait dengan layanan apapun dan tersedia untuk suatu program atau aplikasi yang akan digunakan untuk berkomunikasi. *Port software scanning*, dalam keadaan yang paling dasar, hanya mengirimkan permintaan untuk menghubungkan ke komputer target pada setiap *port* secara berurutan dan membuat catatan dari respon port atau yang tampaknya terbuka untuk diselidiki lebih mendalam.Jika *port scan* yang dilakukan dengan maksud jahat, penyusup biasanya lebih memilih untuk tidak terdeteksi. Aplikasi keamanan jaringan dapat dikonfigurasi untuk mengingatkan administrator jika penyusup mendeteksi permintaan sambungan di berbagai *port* dari sebuah *host*. Untuk menyiasati hal ini penyusup dapat melakukan *port scan*. Dalam membatasi *port* untuk target yang lebih kecil diatur daripada lapisan *scanning* pada semua *port* sebanyak 65536. *Scanning Stealth* menggunakan teknik seperti memperlambat *scan*. Dengan memindai port selama periode lebih lama dari waktu yang semestinya mengurangi kemungkinan bahwa target akan memicu peringatan.

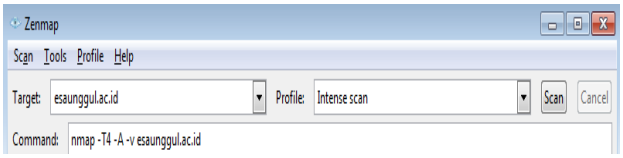
Dengan menetapkan bendera TCP yang berbeda atau mengirim berbagai jenis TCP paket-paket *port scan* dapat menghasilkan hasil yang berbeda atau mencari *port* yang terbuka dengan cara berbeda. *Scan SYN* akan memberitahu *port scanner port* yang mendengarkan dan yang tidak, tergantung pada jenis respon yang dihasilkan. *Scan* FIN menghasilkan respon dari *port*- tertutup, tapi *port* yang terbuka dan mendengarkan tidak mengirim jawaban, sehingga port scanner dapat menentukan port terbuka dan yang tidak.

Hasil dari Penelusuran Port Scanning

Setelah dilakukan penulesuran *port* pada IP address 202.152.198.227 secara otomatis. Berikut adalah beberapa tahapan scanning menggunakan aplikasi Nmap, didapatkan hasil atau output sebagai berikut:

Membuka aplikasi Nmap

Masukan alamat website dalam kolom target, kemudian tekan tombol scan.



Gambar 1
Scan Target - Nmap

Pengkajian Keamanan Aplikasi pada *Website* PT.XYZ *Vulnerability Scanning*

Proses otomatis secara proaktif mengidentifikasi kerentanan keamanan sistem komputasi dalam jaringan untuk menentukan apakah dan di mana sistem dapat dimanfaatkan dan / atau terancam. Kerentanan pemindaian biasanya mengacu pada pemindaian sistem yang terhubung ke Internet, tetapi juga dapat merujuk kepada audit sistem pada jaringan internal yang tidak terhubung ke Internet untuk menilai suatu ancaman pada sistem. Sementara server publik yang penting untuk komunikasi dan transfer data melalui Internet, penyusup membuka pintu untuk melakukan pelanggaran keamanan potensial oleh pelaku ancaman, seperti penyusup jahat.

Vulnerability Scanning menggunakan perangkat lunak yang berusaha keluar dari kelemahan keamanan berdasarkan kerentanan *database*, pengujian sistem untuk terjadinya kekurangan dan menghasilkan laporan dari temuan bahwa seorang individu atau perusahaan dapat menggunakan untuk memperketat keamanan jaringan.

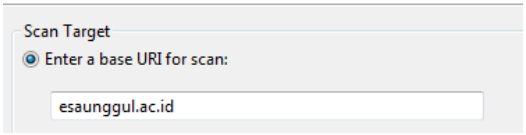
Sebuah cacat yang tidak diinginkan dalam kode perangkat lunak atau sistem yang terbuka untuk potensi eksploitasi dalam bentuk akses yang tidak sah atau perilaku berbahaya seperti *virus, worm, trojan* horse dan bentuk lain dari *malware*. Disebut juga sebagai eksploitasi keamanan, kerentanan keamanan dapat hasil dari *bug software*, *password* yang lemah atau perangkat lunak yang sudah terinfeksi oleh virus komputer atau kode *script injeksi*, dan kerentanan keamanan ini membutuhkan *patch*, atau perbaikan, untuk mencegah potensi untuk dikompromikan integritas oleh penyusup atau *malware*.

Hasil dari Penelusuran PT.XYZ

Vulnerability assesment yang dilakukan pada *website* Esa Unggul dilakukan secara otomatis. Berikut adalah beberapa tahapan *vulnerability scanning* muenggunakan aplikasi Vega, penelusuran kerentanan pada *website* Universitas Esa Unggul:

Membuka aplikasi Vega

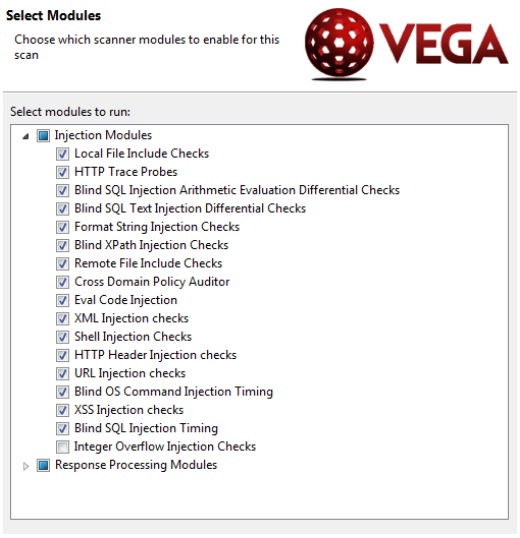
Masukan alamat website dalam kolom target, kemudian tekan tombol scan.



Gambar 2

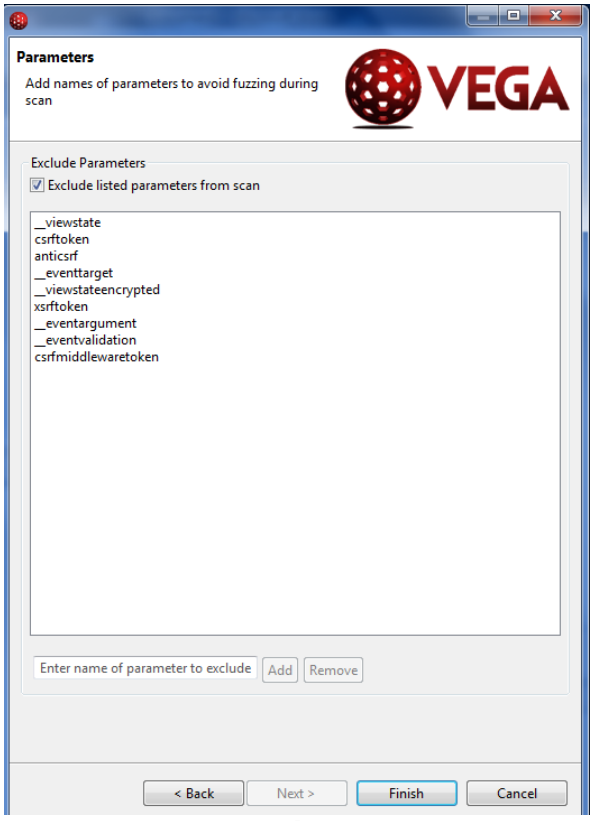
Scan Target Vega – Enter URL for scan

Checklist semua yang ada dimenu *Injection Modules* kecuali *Integer Overflow Injection checks*



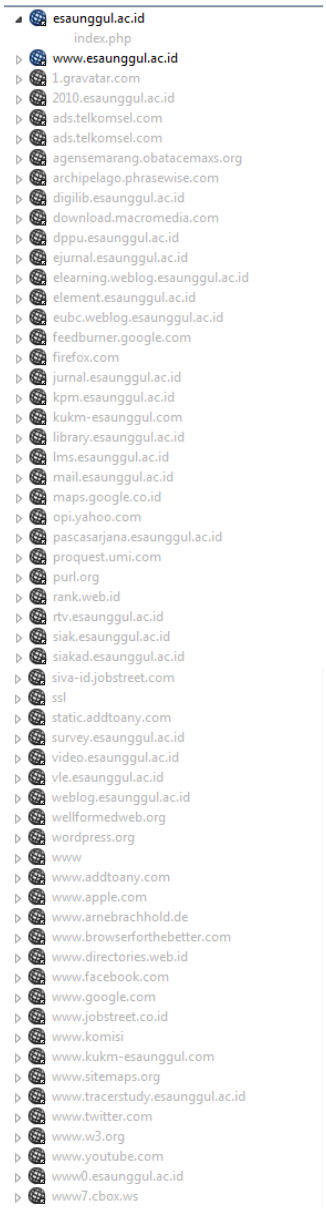
Gambar 3

Select Module – Injection Modules



Gambar 4

Select Parameters

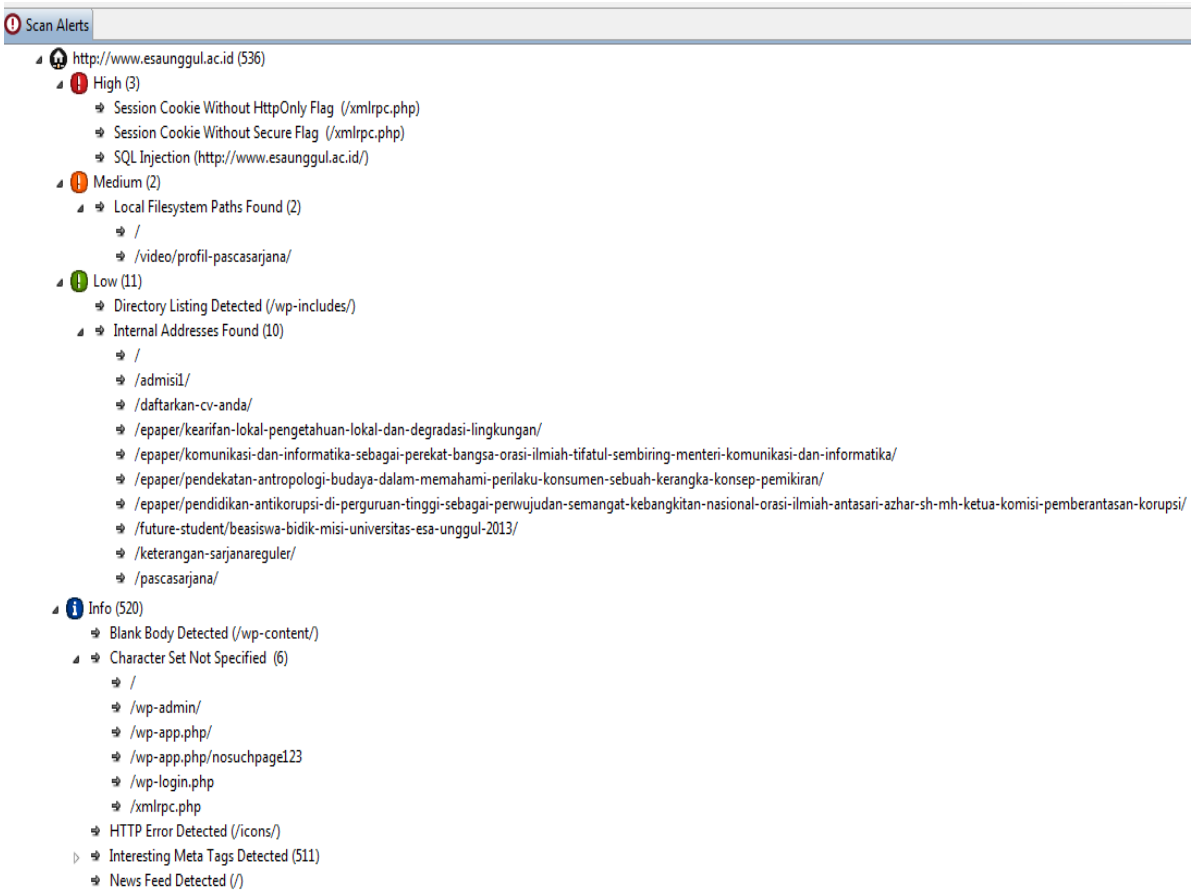


Gambar 5
Website View

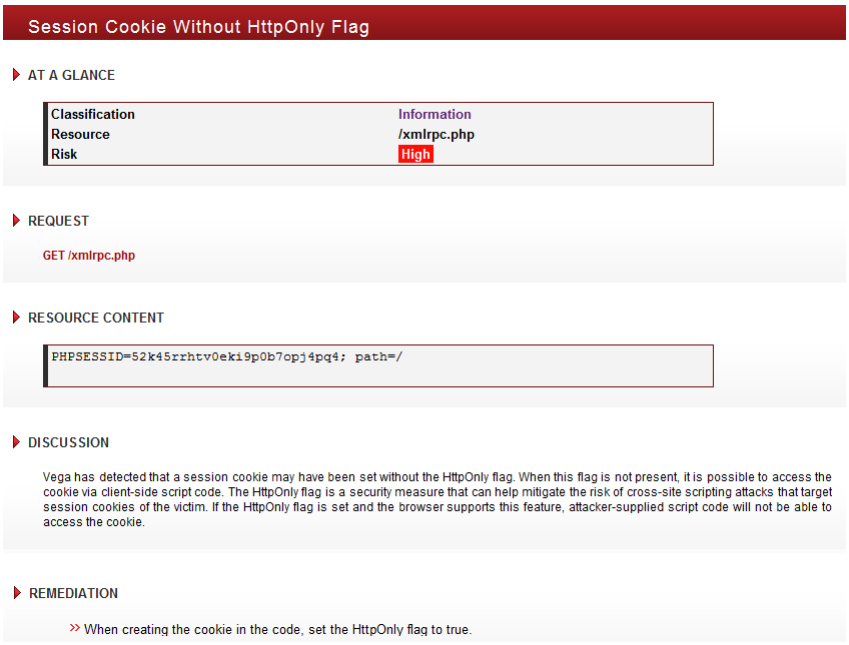
Scan Alert Summary

High		(3 found)
Session Cookie Without Secure Flag	1	
Session Cookie Without HttpOnly Flag	1	
SQL Injection	1	
Medium		(2 found)
Local Filesystem Paths Found	2	
Low		(11 found)
Internal Addresses Found	10	
Directory Listing Detected	1	
Info		(520 found)
Interesting Meta Tags Detected	511	
News Feed Detected	1	
Character Set Not Specified	6	
Blank Body Detected	1	
HTTP Error Detected	1	

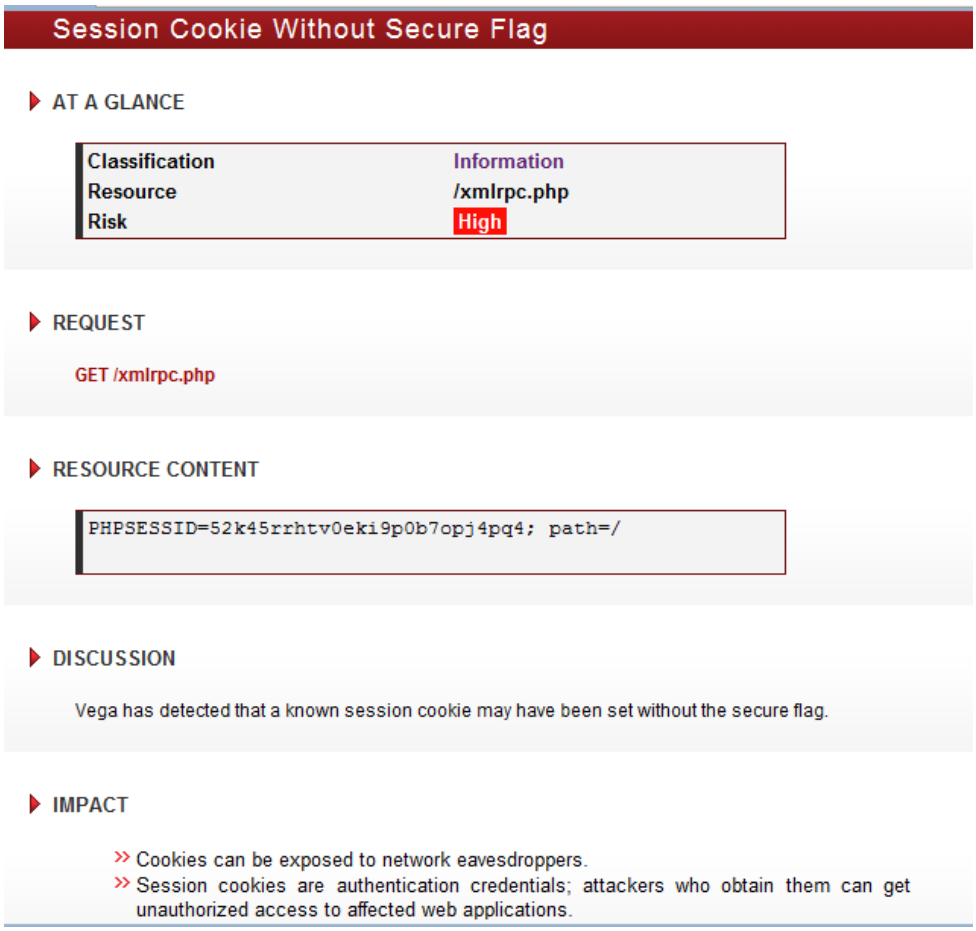
Gambar 6
Scan Alart Summary



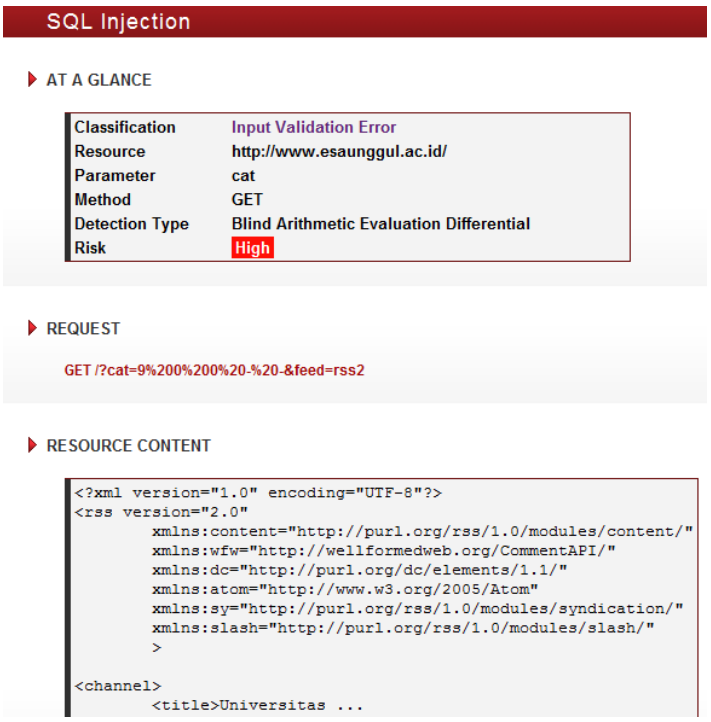
Gambar 7
Scan Alart



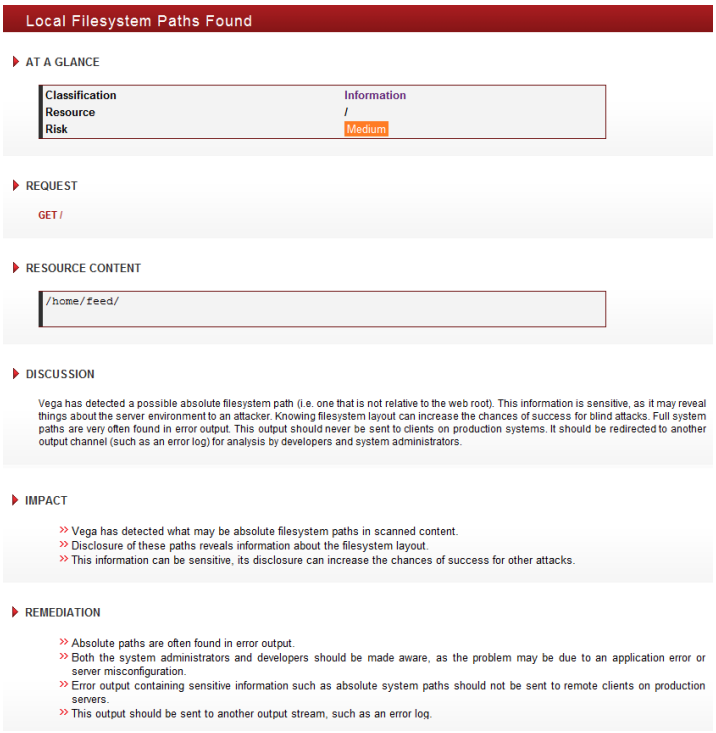
Gambar 8
Session Cookie Without Http Only Flag Detail



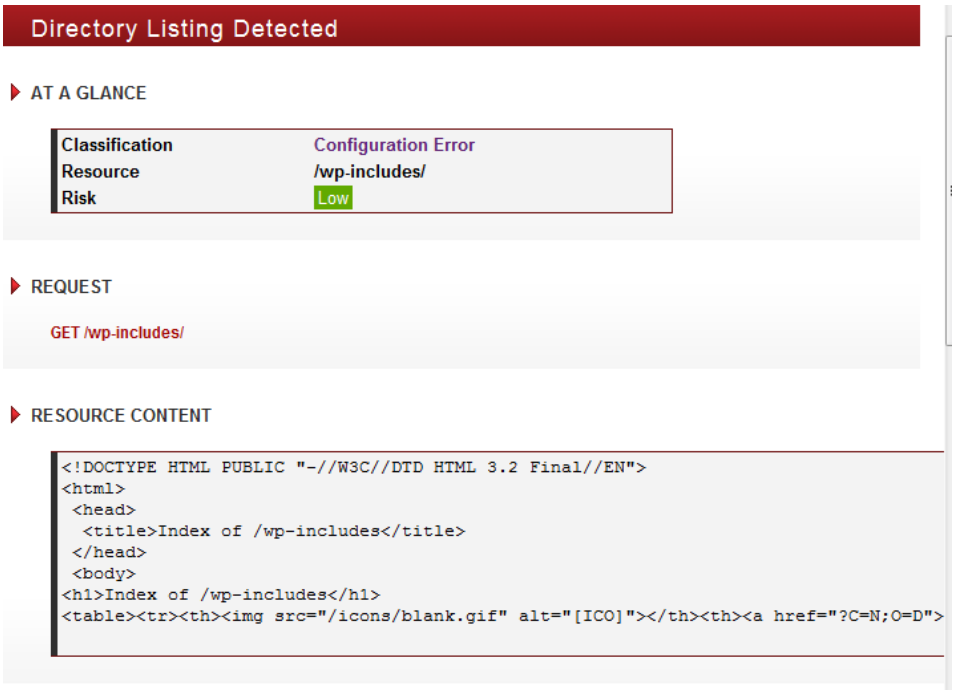
Gambar 9
Session Cookie Without Secure Flag Detail



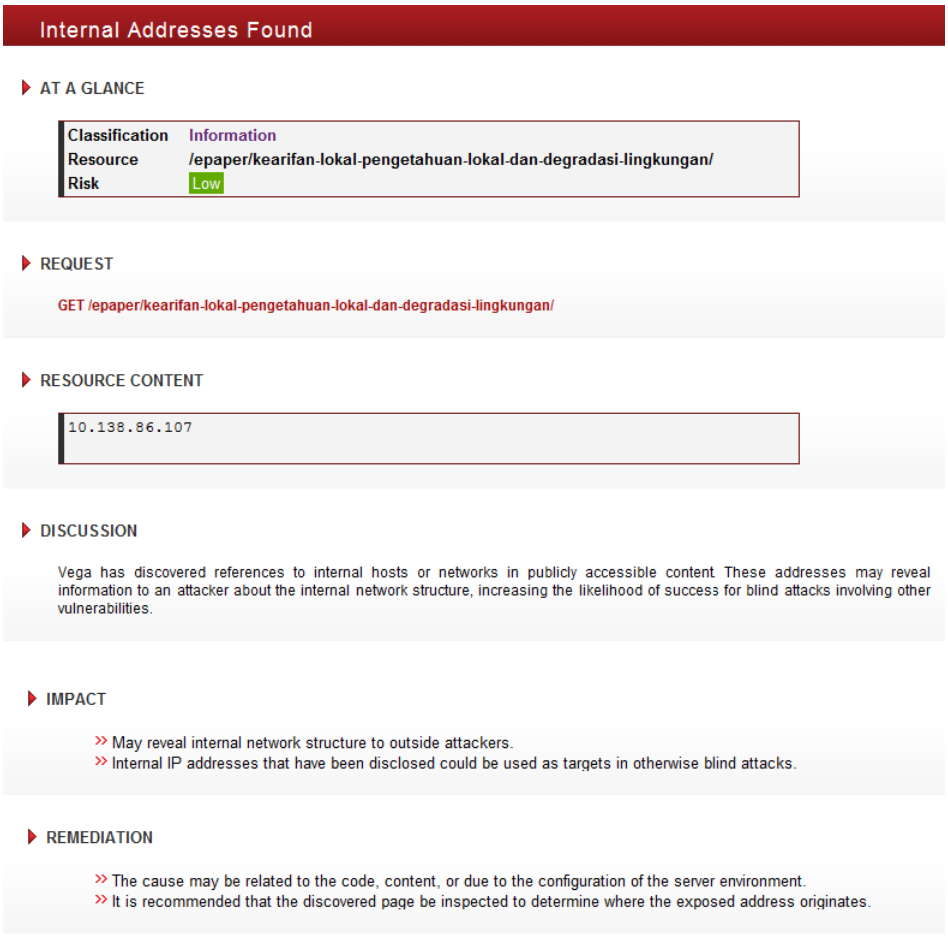
Gambar 10
SQL Injection Detail



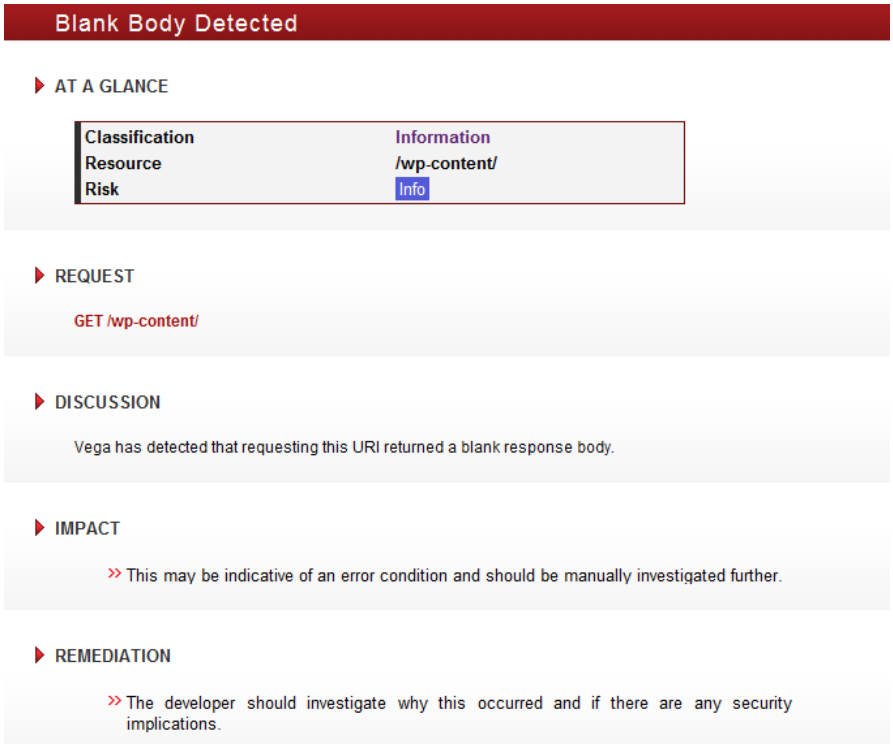
Gambar 10
Local System Path Found Detail



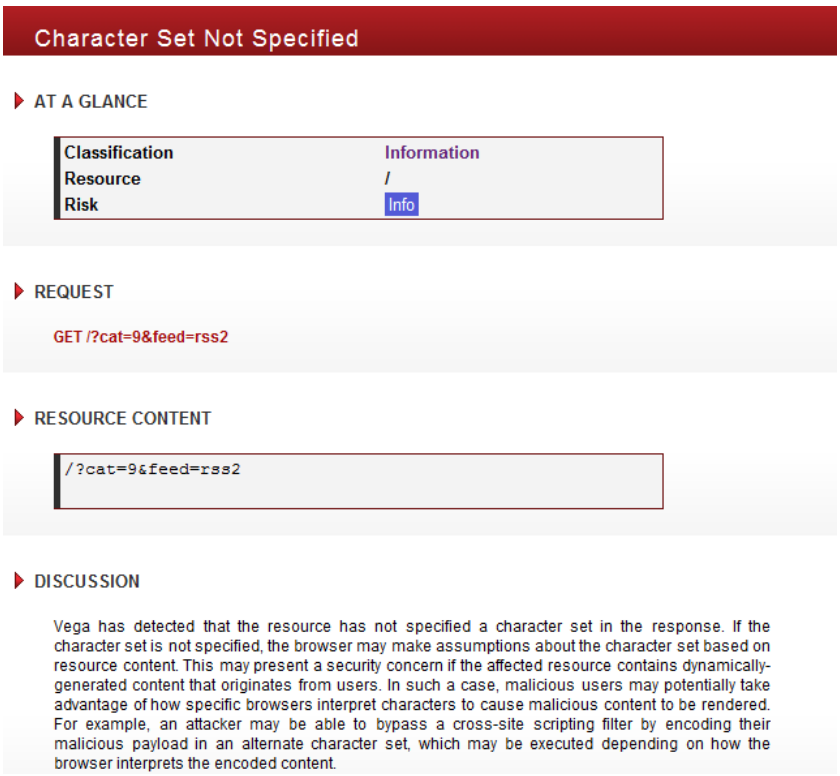
Gambar 11
Dictionary Listing Detected Detail



Gambar 12
Internal Address Found Detail



Gambar 13
Blank Body Detected Detail



Gambar 14
Character Set Not Specified

Setelah dilakukan penelusuran secara otomatis melalui URL *website* PT.XYZ didapati beberapa kesimpulan dari peringatan atas beberapa resiko atau kerentanan pada *website* yaitu:

1. *High*:
- *Session Cookie without Secure Flag*

Session cookie yang digunakan tanpa menggunakan HttpOnly. Ketika flag ini tidak ditemukan, cara pengaksesan *cookie* melalui *script* dari sisi klien. Flag HttpOnly dalam ukuran keamanan dapat membantu mengurangi risiko *cross-site scripting* serangan yang menargetkan session cookies korban. Jika flag HttpOnly diatur dan browser mendukung fitur ini, kode script penyerang yang disediakan tidak akan dapat mengakses cookie.

- *Session Cookie without HTTP Only Flag*

Sesi cookie mungkin telah ditetapkan tanpa flag keamanan.

SQL Injection

Kemungkinan kerentanan injeksi SQL. Kerentanan ini hadir ketika masukan eksternal yang dipasok digunakan untuk membangun sebuah query SQL. Jika tindakan pencegahan tidak dilakukan, input eksternal yang dipasok (biasanya parameter GET atau POST) dapat memodifikasi string query sedemikian rupa sehingga melakukan tindakan. Tindakan ini termasuk mendapatkan sah membaca atau menulis akses ke data yang tersimpan dalam database, serta memodifikasi logika aplikasi.

2. *Medium*:

Local File System Path Found

Informasi ini sensitif, karena dapat mengungkapkan hal-hal tentang lingkungan server untuk penyerang. Mengetahui layout file system dapat meningkatkan peluang keberhasilan serangan buta. Sistem jalur penuh

sangat sering ditemukan dalam *output* kesalahan.

3. *Low*:

- *Internal Addresses Found*

Daftar isi direktori ketika tidak ada file indeks hadir dalam kesalahan konfigurasi yang umum. Isi direktori dapat memberikan informasi yang berguna untuk seorang penyerang, terutama jika ada file yang tidak dimaksudkan untuk menjadi diakses, seperti kode sumber atau backup. Daftar direktori juga dapat memberikan informasi yang berguna tentang kebiasaan administrasi server dan / atau pengembang web, seperti penamaan file konvensi, yang dapat digunakan untuk meningkatkan keberhasilan kemungkinan *brute-force* atau serangan lainnya.

- *Directory Listing Detected*

Referensi untuk host internal atau jaringan dalam konten yang dapat diakses publik. Alamat ini dapat mengungkapkan informasi kepada penyerang tentang struktur jaringan internal, meningkatkan kemungkinan keberhasilan untuk serangan buta yang melibatkan kerentanan lainnya.

4. *Info*:

- *Interesting Meta Tags Detected*

Meta tag yang dapat mengungkapkan informasi sensitif atau menjamin pemeriksaan lebih dekat.

Feed Detected

SS (*Really Simple Syndication*) dan format terkait metode untuk mempublikasikan konten web secara teratur diperbarui. RSS *feed* adalah dokumen XML yang dibuat tersedia untuk download klien dan sering disertakan dengan sistem managament konten, seperti blog.

Character Set Not Specified

Sumber daya karakter belum ditentukan untuk di respon. Jika karakter tidak ditentukan, browser dapat membuat asumsi tentang karakter berdasarkan konten sumber daya. Ini dapat menimbulkan masalah keamanan jika sumber daya yang terkena berisi konten yang dihasilkan secara dinamis yang berasal dari pengguna. Dalam kasus seperti itu, pengguna yang jahat bisa berpotensi memanfaatkan bagaimana spesifik browser menginterpretasikan karakter menyebabkan konten berbahaya yang akan diberikan.

Blank Body Detected

Permintaan URL kembali sebagai respon kosong.

HTTP Error Detected

Menghasilkan respon HTTP dengan kode status kesalahan. Ini harus diselidiki dengan memeriksa baik request dan respon.

Pembuatan laporan hasil pengkajian keamanan sistem

Laporan Pengujian Penetrasi

Menulis laporan pengujian penetrasi adalah suatu seni yang harus dipelajari untuk memastikan bahwa laporan tersebut telah tersampaikan dengan tepat dan kepada orang yang tepat. Laporan ini akan dikirim ke tim senior management dan tim teknikal dengan baik. Untuk alasan ini, sebagai penguji penetrasi, perlu memberikan pelaporan yang baik dan tetap mengamankan informasi.

Banyak tersedia saat ini sumber daya pengujian penetrasi namun terdapat kekurangan dalam penulisan laporan metodologi dan pendekatan yang mengarah pada kesenjangan yang sangat besar dalam siklus pengujian penetrasi. Laporan adalah pernyataan dari hasil investigasi atau dari setiap masalah yang memerlukan sebuah informasi. Sebuah pengujian penetrasi tidak berguna tanpa sesuatu yang nyata untuk diberikan kepada klien atau pejabat eksekutif. Laporan harus merinci atas hasil pengujian. Penulisan Laporan adalah bagian penting untuk setiap penyedia layanan terutama dalam pelayanan IT. Dalam pengujian penetrasi, hasil akhir adalah laporan yang menunjukkan kesediaan layanan, metodologi yang dianut, serta hasil pengujian dan rekomendasi.

Laporan pengujian penetrasi disajikan dengan mengikuti pendekatan, hasil penilaian kerentanan dan uji penetrasi sistem target dengan rekomendasi rinci tentang bagaimana cara untuk mengurangi risiko. Target untuk laporan pengujian penetrasi akan bervariasi, ringkasan eksekutif akan dibaca oleh manajemen senior dan rincian teknis akan

dibaca oleh IT dan / atau orang-orang keamanan yang bertanggung jawab. Hal ini dimulai dengan pendekatan konvensional untuk mengembangkan laporan pengujian penetrasi mulai dari mengumpulkan informasi, menyusun laporan pertama dan berakhir dengan laporan profesional. Seperti ditunjukkan dalam gambar, tahap penulisan laporan pengujian penetrasi adalah: Laporkan perencanaan, pengumpulan informasi, menulis draft pertama dan meninjau dan finalisasi. Metode pembuatan laporan keamanan sistem adalah:

Laporan Perencanaan (*Report Planning*)

Hal ini dapat ditemukan dalam permintaan yang dijelaskan dalam proposal, bagian dari analisis risiko, bagian dari pernyataan yang menjelaskan lingkup sasaran pengujian. Beberapa perencanaan yang diperluakan antara lain:

Waktu

- Penguji menyebutkan waktu pengujian karena berbagai alasan:
- Perubahan harus membekukan lingkup pengujian penetrasi selama tes untuk memastikan bahwa pengujian tersebut medapatkan nilai yang persis dan tidak ada perubahan lagi dalam proses pengembangan.
- Meskipun tidak ada keamanan 100%, laporan ini akan menunjukkan risiko dalam lingkup pengujian penetrasi selama periode waktu ini risiko setelah waktu ini mungkin timbul karena beberapa perubahan dalam infrastruktur TI perubahan dalam konfigurasi.

Di sisi lain, selama waktu perencanaan proyek pengiriman laporan harus hati-hati dan perlu dipertimbangkan. Pembagian tulisan dalam laporan menjadi tugas-tugas untuk disederhanakan. Perencanaan laporan akan membantu dalam memberikan laporan yang efektif. Biasanya, 60% dari waktu yang harus dihabiskan dalam menulis draft.

Pertimbangan target pembaca laporan

Penguji penetrasi perlu mempertimbangkan proses penerimaan klien serta fakta bahwa mungkin memakan waktu lebih lama dari yang diharapkan. Pertimbangkan sasaran laporan pengujian penetrasi biasanya memiliki sejumlah target / kelompok untuk dicapai, sehingga laporan akan sering memiliki struktur hirarkis untuk mendukung berbagai tingkat rincian. Dalam merancang bentuk laporan, berikut karakteristik target audiens yang harus dipertimbangkan:
Laporan audience termasuk Informasi Security Manager, Chief Information Security Officer, Manajer Teknologi Informasi dan tim teknis. Informasi lebih lanjut tentang khalayak lingkup dan sasaran dapat ditemukan juga dalam lingkup kerja penugasan.

Laporan klasifikasi

Sejak laporan pengujian penetrasi memiliki informasi sensitif seperti, alamat server IP dan informasinya, beberapa informasi aplikasi, kerentanan, ancaman, eksploitasi dan lebih, harus dianggap dalam setiap peringkat tinggi kerahasiaan misalnya TOP SECRET dan laporan akan ditangani sesuai.

Distribusi laporan

Softcopy perlu hati-hati dikendalikan dalam server yang aman yang dimiliki oleh departemen yang telah meminta layanan pengujian penetrasi. Mendistribusikan softcopy laporan biasanya akan dikendalikan oleh pemilik dokumen (pemilik laporan) dan akan berada di bawah tanggung jawabnya. Akhirnya setelah mengirimkan laporan tersebut, penguji penetrasi harus menghapus informasi yang ada bahwa ia memiliki dan menginformasikan klien bahwa semua informasi terkait telah telah terhapus (Langkah ini harus disebutkan secara jelas dan disepakati dalam dokumen.

Pengumpulan Informasi (Information Collection)

Karena sifat pengujian penetrasi dapat memanfaatkan lebih dari satu cara, alat, komputer, dll, penguji penetrasi perlu memastikan bahwa ia mengumpulkan semua informasi dalam semua tahapan, sistem yang digunakan dan alat-alat yang digunakan. Hal ini akan memudahkan penulisan laporan dan membuat semua informasi yang ia butuhkan tersedia baik dalam setiap tahap, pindah ke tahap berikutnya, dengan menggunakan

informasi dan menganalisisnya baik dalam kegiatan pengujian penetrasi atau selama penulisan laporan.

Menggunakan catatan yang relevan (*Writing the first draft*)

Pada tahap ini, sangat dianjurkan untuk tidak khawatir tentang koreksi cetakan percobaan dan editing. Dalam perbaikan laporan dapat menggunakan simbol seperti "#" atau menambahkan highlights untuk menandai tempat di mana penguji perlu kembali lagi nanti untuk mengedit paragraf.

Review dan Finalisasi

Draft perlu dikaji untuk peningkatan kualitas laporan. Pengkajian kembali laporan adalah sangat dianjurkan untuk memiliki pendapat kedua. Dalam hal pengujian penetrasi telah dilakukan oleh tim, semua anggota tim perlu meninjau dan / atau mengeditnya. pengkajian kembali laporan tergantung pada jenis pengujian penetrasi dilakukan, jika itu adalah pengujian penetrasi black box , salah satu tim pengujian penetrasi perlu meninjau laporan. Jika tes ini pengujian penetrasi white box, seseorang dengan pengetahuan tentang sistem target akan meninjau laporan bersama-sama. Hal ini akan menyebabkan hasil yang lebih baik.

Laporan Pengkajian Keamanan Jaringan

Dari hasil penelusuran, telah didapatkan analisis kerentanan pada jaringan. Tahap selanjutnya adalah pembuatan laporan sebagai bukti adanya proses analisis dan kemudian di berikan kepada pihak selanjutnya untuk segera diperbaiki pada sisi jaringan. Misalnya kepada tim *security networ*k dan tim *developer*. Format laporan dibuat berdasarkan kebutuhan, seperti berikut:

Perancangan laporan terhadap hasil penelusuran keamanan jaringan adalah dengan format yang berdasarkan kebutuhan. Penjelasan project atau sistem yang sedang dilakukan penelusuran. Environment adalah lingkungan atau alat URL pada *website* Universitas Esa Unggul. Date of Scan menjelaskan tanggal dilakukan penelusuran secara otomatis. Selain header dari format laporan, beberapa format pada kolom utama yang menjelaskan tentang hasil dari penelusuran jaringan yaitu kunci di antara informasi itu adalah pada "tabel port ". Tabel yang berisi daftar port number, protocol, service name, dan state. Statusnya adalah *open*, *filtered*, *closed*, atau *unfiltered*. Terbuka berarti bahwa aplikasi pada mesin target sedang mendengarkan untuk koneksi / paket pada port tersebut. Disaring berarti bahwa firewall, filter, atau penghalang jaringan lainnya memblokir port sehingga tidak bisa dikatakan apakah itu terbuka atau tertutup. Port tertutup memiliki aplikasi yang sedang mendengarkan, meskipun penyusup bisa membuka setiap saat. Ports diklasifikasikan sebagai unfiltered ketika penyusup menanggapi beberapa kemungkinan, namun Nmap atau Zenmap tidak dapat menentukan apakah penyusup terbuka atau tertutup. Nmap atau Zenmap melaporkan kombinasi status *open* | *filtered* dan ditutup | disaring ketika tidak dapat menentukan mana dari dua menggambarkan sebuah port. Tabel port mungkin juga menyertakan detil versi *software* ketika deteksi versi telah diminta. Ketika sebuah pemeriksaan protokol IP diminta (-sO), dengan memberikan informasi tentang protokol IP yang mendukung daripada mendengarkan port.

Laporan Pengkajian Keamanan Aplikasi

Dari hasil penelusuran, telah didapatkan analisis kerentanan pada aplikasi yaitu melalu *velnerability assesment*. Tahap selanjutnya adalah pembuatan laporan sebagai bukti adanya proses analisis dan kemudian di berikan kepada pihak selanjutnya untuk segera diperbaiki pada sisi aplikasi, yaitu kepada tim *developer*. Format laporan dibuat berdasarkan kebutuhan, seperti berikut:

Format laporan terdiri dari:

1. *Risk*:Menjelaskan tentang tingkat resiko dari keamanan aplikasi. Tingkatan resiko tersebut adalah *High, Medium, Low, Information, False Positive.*

Comment: Pemberian keterangan atau penjelasan lainnya dapat ditambahkan pada kolom *comment*.

Perancangan Aplikasi *Security System Control*

Tujuan dari tahap mencari kebutuhan adalah memahami dengan sesungguhnya

kebutuhan dari sistem yang baru dan mengembangankan sebuah sistem yang memadai kebutuhan tersebut atau memutuskan bahwa pengembangan sistem yang baru tidak dibutuhkan. Pada tahap ini merupakan tahap yang sangat penting dalam tahap SDLC. Untuk mempermudah menganalisis sebuah sistem dibutuhkan dua jenis kebutuhan.

Tujuan utama dari *System Analysis* adalah mengumpulkan informasi mengenai sistem yang telah ada, untuk menentukan mana diantar tiga solusi di atas yang akan dilakukan dan menentukan kebutuhan akan sistem yang baru. Tahapan *system Analysis* menghasilkan informasi-informasi sebagai berikut : Kelebihan (*strengths*) dan kelemahan (*weaknesses*) sistem yang telah ada. Fungsi-fungsi yang harus dimiliki oleh sistem yang baru untuk memecahkan permasalahan yang ada.

Programming

Banyak organisasi memutuskan untuk membeli perangkat lunak (*software*), namun banyak juga organisasi yang memutuskan untuk membuat perangkat lunak (*software*) yang dibutuhkan sendiri. Programming merupakan proses menterjemahkan (*translation*) spesifikasi rancangan/design menjadi kode-kode komputer. Proses ini dapat berlangsung lama karena membuat kode-kode komputer merupakan seni dari *science*.

Pengujian Aplikasi

Tahapan testing atau uji coba bertujuan untuk memeriksa apakan kode komputer akan menghasilkan hasil yang diinginkan dan diharapkan untuk suatu kondisi tertentu. Testing dirancang untuk menemukan kesalahan-kesalahan (*error*) pada kode komputer. Terdapat dua jenis *error*, yaitu *syntax error* dan *logic error*. *Syntax error* adalah kesalahan pada penulisan kode komputer, sehingga lebih mudah ditemukan, sementara *logic error* masih memungkinkan program untuk berjalan, namun menghasilkan output yang tidak benar untuk suatu input tertentu. Kesalahan untuk *logic error* tidak nyata terlihat, sehingga susah ditemukan.

Implementasi dan Pemeliharaan

Implementasi adalah proses pengubahan atau konversi dari sistem yang lama menjadi sistem yang baru. Suatu organisasi menggunakan 2 strategi konversi, yaitu:

1. *Pilot Conversion*

Proses memperkenalkan sistem yang baru pada suatu bagian organsasi dalam suatu jangka waktu tertentu, untuk kemudian dilakukan pengukuran. Ketika sistem telah berjalan dengan benar, barulah diperkenalkan pada seluruh bagian organisasi.

2. *Phased Conversion*

Proses memperkenalkan komponen-komponen dari sistem yang baru, kemudian setiap modul dilakukan pengukuran. Ketika modul telah berjalan dengan benar, modul lain diperkenalkan hingga keseluruhan komponen sistem.

Pemeliharaan

Setelah melakukan konversi, sistem yang baru akan dioperasikan untuk suatu jangka waktu tertentu. Ketika operasi sistem telah stabil, dilakukan audit pada saat proses operasi untuk mengukur kemampuan sistem dan menentukan apakah system digunakan dengan benar. Sistem memerlukan beberapa jenis maintenance, yaitu :

Kesimpulan

Setelah dilakukan dan Evaluasi keamanan web PT. XYZ dapat disimpulkan sebagai berikut :

Analisis pada kerentanan sistem dapat dilakukan dengan melakukan *port scanning* dan *vulnerability scanning*. *Port scaninng* dapat mendeteksi status *port*, *address*, sistem operasi dan detail lainnya seputar informasi tentang server yang digunakan pada lingkup atau environment *website.* Vulnerability scanning dilakukan untuk menemukan kerentanan sistem dari sisi aplikasi dan dapat membantu penguji dalam menemukan dan memvalidasi SQL Injection, Cross-Site Scripting, dan inforamasi kerentanan lainnya.

Daftar Pustaka

Elleithy, Khaled. 2010. *Advanced Techniques in Computing Sciences and Software Engineering* : Springer, USA

Engebretson, Patrick. 2013. *The Basics of Hacking and Penetration Testing* : SYNGRESS, USA

Hambling, Brian. 2007. *Software Testing: An ISEB Intermediate Certificate* : BCS Learning & Development Limited, British

Hardcastel, Elizabeth. 2008. *Business information systems.* BookBoon, British

Hidayat, Rahmat. 2010. *Cara Mudah Membangun Website Interaktif menggunakan Content Management System Joomla* : PT Elex Media Komputindo, Jakarta

Komputer, Wahana. 2010. *Cara Mudah Membangun Jaringan Komputer & Internet* : PT. TransMedia, Ciganjur

Mujilan, Agustinus. 2012. *Sistem Informasi Akuntansi - Teori dan Wawasan di Dunia Elektronis* : WIMA Pers, Madiun

Nixon, Robin. 2012. *Learning PHP, MYSQL,JavaScript & CSS* : O'Reilly Media, USA

OWASP Foundation. 2013. *OWASP Testing Guide*, USA