Jurnal (Irwan Syarifudin) Pentesting dan Analisis Keamanan Web Paud Dikmas

Research · April 2018

CITATIONS
0

READS
1,363

1 author:

Irwan Syarifudin
Politeknik Negeri Jakarta
2 PUBLICATIONS **0** CITATIONS

SEE PROFILE

PENTESTING DAN ANALISIS KEAMANAN WEB PAUD DIKMAS

Irwan Syarifudin
Jurusan Teknik Informatika dan Komputer
Politeknik Negeri Jakarta
Depok, Indonesia
Irwansyarifudin16@gmail.com

Abstrak **--** Semakin berkembangnya teknologi website semakin memberikan ruang bagi pihak yang tidak berwenang dalam melakukan tingkat kejahatan didunia maya. Perlu adanya antisipasi untuk mengamankan(*security*) assest-asset penting suatu instansi khususnya di instansi pemerintahan. Banyak celah yang terjadi pada website Paud Dikmas yang merupakan website milik Direktorat Jenderal Paud dan Dikmas Kementerian Pendidikan dan Kebudayaan RI. Terdapat beberapa celah-celah kerentanan dan memiliki tingkat risiko yang berbeda-beda diantaranya *web information application disclosure*, *Anonymous* FTP, *Bypass Login*, dan *Gaining Access*. Celah-celah tersebut dapat memberikan dampak buruk pada integritas data pemerintah yang bersifat *private*. Hal itu bisa terjadi karena kurangnya sistem keamanan website dan kekeliruan pihak *programmer* dalam melakukan coding website. Perlu diadakan eksplorasi dan pengujian lebih dalam celah tersebut yaitu dengan uji penertrasi yang dapat memberikan referensi bagi pihak *programmer* untuk mengembangkan website lebih baik lagi Dengan metode-metode dan simulasi uji penetrasi yang dilakukan oleh *pentester* diharapkan dapat menjadi pertimbangan pihak developer untuk menutup celah pada website sehingga ruang bagi attacker untuk membobol website semakin kecil. Uji penetrasi pun perlu dilakukan secara periodik dan harus mampu memberikan hasil laporan uji penetrasi (*pentesting report*) yang ditulis secara komprehensif.

Kata kunci**--** **web, *security, pentesting, pentesting report, web information application disclosure, Anonymous* FTP, *Bypass Login, Gaining Access***

I. PENDAHULUAN

Indonesia sekarang masih menduduki peringkat pertama untuk kasus *cybercrime*. Dalam laporan "*State of The Internet*" yang dirilis Akamai pada kuartal II 2013, nama Indonesia berada di posisi puncak sebagai negara dengan sumber serangan kejahatan cyber (38%), melampaui China di posisi kedua dengan raihan 33% (Akamai.com, 2013). Walaupun pemerintah Indonesia sudah mengupayakan pencegahan terhadap kejahatan di dunia maya dengan membuat undang-undang tindak kejahatan dunia maya tetap saja mencari pelaku/penjahat dunia maya itu cukup sulit. Semua itu karena dunia maya tidak kenal batas wilayah maupun waktu. Yang bisa dilakukan saat ini tidak lain adalah antisipasi dengan cara mengamankan asset-asset penting perseorangan, perusahaan hingga pemerintahan yang ada di internet. Pada instansi pemerintah masalah keamanan website tidak bisa disepelekan dan perlu diberikan sistem keamanan yang optimal. Seperti halnya di Direktorat Jenderal Paud dan Dikmas yang berada dibawah naungan Kementerian Pendidikan dan Kebudayaan RI memiliki website yang mempunyai celah-celah kerentanan seperti XSS, Bypass Login, Web Disclosure dan lainnya. Diantara beberapa bug dan celah tersebut memilik dampak yang bisa merugikan sistem website Paud dan Dikmas. Padahal sebuah website pemerintahan jelas harus memberikan informasi yang valid dan mengamankan berbagai informasi-informasi yang bersifat *private* milik Kementerian, seandainya ada *attacker* yang mempunyai maksud jahat bisa mengubah informasi yang ada pada website tersebut, tentu ini akan sangat membahayakan dan merugikan berbagai pihak. Dalam praktek kerja lapangan yang telah saya lakukan, yaitu melakukan *Penetration Testing* (*Pentesting*) terhadap website Paud Dikmas yang kemudian dapat menjadi referensi bagi pihak staff IT Paud dan Dikmas dalam menerapkan sistem keamanan website yang lebih optimal. Sehingga website tersebut dapat lebih aman dan terhindar dari risiko serangan dan eksploitasi sistem yang dilakukan oleh *hacker*.

Adapun tujuan yang ingin dicapai dari penelitian ini adalah:

1. Mencari sebanyak-banyaknya celah kerentanan yang terdapat dalam website Paud Dikmas.
2. Menganalisis dan membuat laporan dari hasil *Pentesting* pada website Paud dan Dikmas.

II. TINJAUAN PUSTAKA

A. Penetration Testing Flow

Serangkaian proses berisi prosedur dan teknik mengevaluasi keamanan terhadap sistem komputer atau jaringan untuk menjalankan uji penetrasi. Alur uji penetrasi yang secara luas penulis terapkan untuk menguji web Paud Dikmas diantaranya:

1. *Planning*

   Di tahap *planning* mempersiapkan ruang lingkup uji penetrasi, jangka waktu, dokumen legal (NDA), jumlah tim, *tools* yang digunakan, dan lain-lain.

2. *Attack*

Pemindaian informasi simulasi serangan terhadap sistem dilakukan pada tahap ini dimana penulis selaku penguji penetrasi melakukan deteksi terhadap celah-celah kerentanan. Rincian tahap pemindaian (*scanning)* dan simulasi penyerangan meliputi *footprinting*, *scanning fingerprinting*, *vulnerability scan*, SQL Attack, *Enumeration*, *Gaining Access*, *Privilege Escalation*, *Covering Attacks*, *Backdooring*, dan *Report*.

3. *Discover*

Hasil temuan celah kerentan yang ditemukan dalam uji penetrasi ini seperti *web information application disclosure*, sistem berhasi ditembus dengan *gaining access*, *Anonymous FTP*, dan *ByPass Login* penulis analisis. Dalam analisis tersebut dijabarkan deskripsi, faktor penyebab celah-celah kerentanan dapat terjadi, teknik yang dilakukan serta dampak yang dihasilkan dari masing-masing celah terhadap integritas sistem website perusahaan. Setelah melakukan proses *discover* penguji penetrasi bisa saja kembali ke tahap *scanning* atau penyerangan untuk memastikan kembali kerentanan lain yang terjadi pada web kemudian dilanjutkan dengan proses dokumentasi (*reporting*).

4. *Reporting*

Keterlibatan penguji penetrasi dalam menuliskan apa saja hasil yang didapat selama uji penetrasi sangat penting. Dalam uji penetrasi ini penulis menyusun sebuah *report* secara rinci dari hasil teknis dan pengujian. Kemudian *report* tersebut diberikan kepada pihak staff IT Paud Dikmas untuk dikaji dan dievaluasi terkait segala bentuk temuan celah kerentanan yang terjadi pada web.

B. Report Planning

Dalam pengujian penetrasi, penulisan laporan adalah tugas komprehensif yang mencakup metodologi, prosedur, penjelasan yang benar tentang isi dan desain laporan, contoh terperinci laporan pengujian, dan pengalaman pribadi penguji. Setelah laporan disiapkan, ini dibagi di antara staf dan tim *developer* dari Paud Dikmas. Jika ada jenis kebutuhan semacam itu yang muncul di masa depan, laporan ini digunakan sebagai referensi.

a. *Report Planning*

Perencanaan laporan dimulai dengan tujuan, yang membantu pembaca memahami poin utama pengujian penetrasi. Bagian ini menjelaskan tujuan pengujian dilakukan, apa manfaat pengujian penetrasi, dan lain-lain. Pada tahap ini juga penulis menentukan estimasi waktu yang dibutuhkan untuk pengujian.

b. *Information Collection*

Karena proses yang rumit dan panjang, pentester diharuskan menyebutkan setiap langkah untuk memastikan bahwa pengumpulan semua informasi di semua tahap pengujian. Seiring dengan metode pengujian dilakukan, penulis menyebutkan tentang sistem dan alat, pemindaian hasil, penilaian kerentanan, dan rincian temuannya.

c. *Writing The First Draft*

Penulis menyiapkan semua alat dan informasi, setelah mendapt sebuah temuan celah dilakukan penulisan laporan pertama. Terutama, perlu menulis *draft* pertama dalam rincian menyebutkan segala sesuatu tentang semua aktivitas, proses, dan pengalaman selama melakukan uji penetrasi.

d. *Review Finalization*

Begitu dibuat, laporan terlebih dahulu oleh penguji sendiri dan kemudian oleh atasan dan staff IT. Saat melakukan peninjauan pihak perusahaan dapat memeriksa setiap detail laporan dan menemukan kekurangan yang perlu dikoreksi.

Secara keseluruhan tahap-tahap yang dilakukan untuk menguji keamanan sistem mengacu pada *penetration testing flow*. Dalam penerapannya, tahap-tahap dari *penetration testing flow* seperti *planning*, *Attack*, *discover*¸dan *report* dapat dirincikan lagi (*generate*). Bagi seorang *pentester* dapat memodifikasi dengan mengurangi atau menambahkan tahap-tahap uji penetrasi tersebut sesuai kebutuhan, sehingga tujuan dari uji penetrasi dapat tercapai. Di dunia *penetration testing* dan *hacking* istilah tersebut dinamakan *Anatomy Hacker*, dimana langkah-langkah uji penetrasi yang secara rinci berasal dari anatomi penulis sendiri dalam menguji sistem secara aktif dan mendalam mulai dari mencari informasi, mengidentifikasi kerentanan yang bersifat potensial, hingga mensimulasikan serangan yang terdeteksi memiliki risiko buruk pada website (Desai dan Joshi, 2012). Berikut langkah-langkah dari *Anatomy Hacker* yang penulis lakukan selama melakukan uji penetrasi:

1. *Footprinting*

Footprinting adalah proses menggali informasi sebanyak-banyaknya dari target (box). Selain whois penerapan *footprinting* juga menggunakan aplikasi lain yang berbasis web, yaitu yougetsignal. Aplikasi ini digunakan untuk mengetahui *Reverse IP Lookup*.

2. *Scanning Fingerprinting*

Scanning fingerprinting yaitu identifikasi *service* apa saja yang berjalan di dalam server. Pada tahap scanning fingerprinting ini meliputi analisis dan scanning terhadap *service* apa saja yang dijalankan pada sistem website Paud dan Dikmas. Selain menggunakan Nikto, penulis juga menggunaan Nmap untuk mengetahui informasi-informasi port-port yang terbuka atau tertutup dan mengetahui *service* DNS yang tersedia pada server

3. *Vulnerability Scan*

Kriteria tingkat kerentanan celah pada tabel diatas menjadi acuan bagi penulis untuk menyimpulkan tingkat kerentanan pada celah yang telah ditemukan. Tingkat kerentanan High menandakan bawah celah memiliki risiko yang fatal untuk seorang *attacker* bisa membobol sistem, Medium menandakan celah risiko cukup tinggi untuk *attacker* bisa membobol sistem pada kondisi tertentu, dan Low memiliki kerentanan rendah namun kemungkinan memiliki risiko bagi *attacker* untuk menyerang lewat cara lain.

4. SQL Attack

Bentuk injeksi SQL ini terjadi ketika masukan pengguna tidak disaring dari karakter-karakter pelolos dan kemudian diteruskan ke dalam sebuah pernyataan SQL. Hal ini menimbulkan potensi untuk memanipulasi pernyataan-pernyataan yang dilakukan pada basis data oleh pengguna akhir aplikasi.

5. *Enumeration*

Tahap enumerasi (*enumeration*) adalah mencari *poorly protected password.* Penulis mencoba menggali informasi akun berupa username dan password terlemah yang digunakan untuk akses page admin pada website. Dalam aplikasi Hydra terdapat *Wordlist. Wordlist* merupakan kumpulan-kumpulan username dan password yang terdaftar dan bersifat umum digunakan.

6. *Gaining Access*

Gaining Access merupakan langkah untuk mendapatkan data lebih banyak lagi untuk mulai mencoba mengakses sasaran. Meliputi mengintip dan merampas password, menebak password, serta melakukan *buffer overflow*. *Gaining access* adalah mencoba mendapatkan akses ke dalam suatu sistem sebagai user biasa.Tahap ini adalah kelanjutan dari kegiatan enumerasi, sehingga biasanya di sini penyerang sudah mempunyai paling tidak user akun yang absah**.**

7. *Privilege Escalation*

Pada tahap *enumeration* dan *gaining access* bagi *Attacker* yang sudah berhasil didapatkan akses masuk ke *admin page*. Pada tahap *privilege escalation* ini seorang *Attacker* akan berusaha mencari akses yang lebih dalam yaitu mendapatkan akses pada web server melalui port 80. Penulis telah mencoba untuk mendapat akses web server melalui port 80 namun belum berhasil. Dikarenakan website memberikan respon *bad request*, sehingga penulis tidak dapat mendapat koneksi dan masuk kedalam webserver.

8. *Backdooring*

Apabila seorang *Attacker* ingin memutuskan koneksi dengan server kemudian dilain waktu ingin membangun koneksi kembali dengan server tidak perlu repot-repot membuat konfigurasi *hacking* dari awal. Cukup melalui *backdoor* yang telah tertanam dalam sistem dengan mengunggah *backdoor* secara sembunyi-sembunyi di antara ribuan file website. Skrip *backdoor* sendiri biasa dilakukan melalui form upload yang ada pada halaman website. Namun, pada uji penetrasi dengan *backdoor* kali ini penulis belum berhasil menanamkan *backdoor* pada website. Dikarenakan pada website belum terdapat celah form untuk upload skrip *backdoor* dan target tidak bersifat *exploitable*.

9. *Covering Attacks*

Sebuah sistem pasti mempunyai *log*, *log* adalah sebuah file yang merekam apa saja yang dilakukan oleh sistem atau misalanya ketika terjadi error dalam sistem maka akan disimpan dalam error *log*. Pada kerja praktek yang penulis lakukan penulis tidak menghapus *log*, karena *log* ini nanti yang bisa dijadikan sebagai bukti untuk ditunjukkan pada admin server web yang bersangkutan.

10. *Pentesting Report*

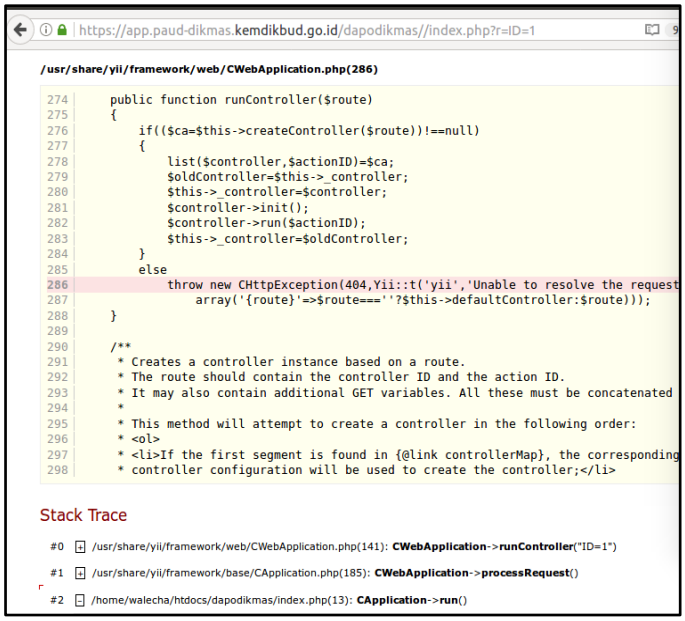
Pada tahap terakhir pengujian *Pentesting*, penulis memberikan sebuah laporan yang dapat menjadi rekomendasi bagi staff IT lainnya di Sub Bagian Data dan Informasi untuk memperbaiki *bug-bug* yang terjadi pada website Paud Dikmas. Hal ini dilakukan agar website tersebut tidak lagi meninggalkan celah dan memiliki risiko kerentanan yang tinggi terhadap serangan-serangan cyber di masa yang akan dating.

III. HASIL DAN PEMBAHASAN

Pada bab ini penulis memamparkan dan menganalisa beberapa celah yang memiliki risiko dan kerentanan dari beberapa tahap pengujian diantaranya *vulnerability scanning*, *fingerprinting*, SQL Attack, dan enumerasi. Terdapat risiko-risiko buruk yang akan terjadi apabila celah tersebut tidak segera diperhatikan, ditanggulangi, dan ditutup. Berikut hasil identifikasi dan penanganan celah kerentanan terhadap web Paud Dikmas:

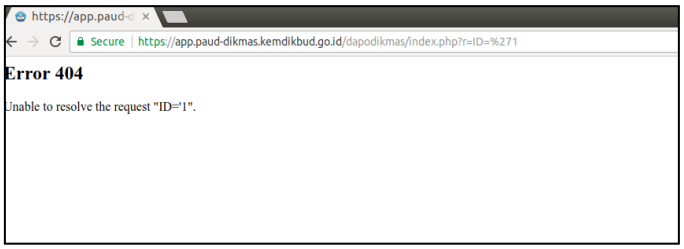
A. Web Information Application Disclosure

Penulis melakukan teknik pengujian ini untuk membuktikan kerentanan yang telah dilaporkan melalui *scanning nessus* dan uji coba menggunakan tahap SQL Attack. Dari hasil tersebut menginformasikan bahwa website paud dikmas rentan terhadap *web application information disclosure*. Percobaan SQL Attack dilakukan dengan memasukan parameter *ID* = 1 pada url https://app.paud-ikmas.kemdikbud.go.id/dapodikmas/index.php?r=ID=1, terlihat informasi yang terungkap dari skrip pemrograman php yang ditulis *programmer* pada website Paud dan Dikmas. Hal tersebut merupakan *Web Application Information Disclosure* yang cukup berbahaya dengan status tingkat kerentanan *medium* menurut hasil *scanning* dari aplikasi Nessus. Bagi *Attacker* celah tersebut dimanfaatkan untuk mengakses lebih dalam direktori utama web server.



Gambar 1 Kondisi Awal *Web Application Disclosure Information*

Solusi yang diberikan penulis agar kerentanan website tersebut tidak terlihat dan dimanfaatkan oleh *Attacker* dimasa yang akan datang pihak staff IT atau programmer harus menutup informasi tersebut dengan menambahkan *filter* pesan eror yang muncul agar output dari pesan kesalahan tidak merujuk ke direktori website. Penanganan *information disclosure* yang terjadi pada website paud dikmas telah diperbaiki secara tanggap dan cepat. Berikut hasil filter pesan eror yang diperbaiki.



Gambar 2 Kondisi Akhir *Web Application Disclosure Information*

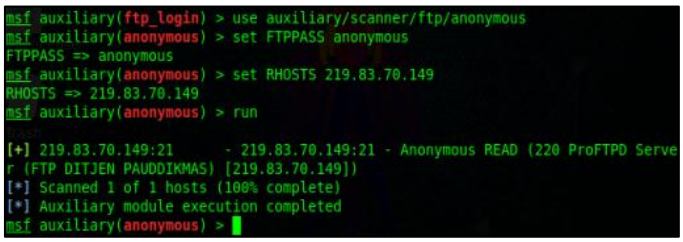
Berdasarkan gambar diatas, ketika *attacker* memasukan parameter untuk memanfaatkan celah dari *web information disclosure* website tersebut tidak memberikan *output* yang berupa informasi tentang kebocoran direktori dan skrip *back-end* dari website, melainkan dialihkan pada halaman yang bertuliskan pesan "Error 404". Pesan kesalahan tersebut menandakan adanya kesalahan pada sisi *client*. Website merespon bahwa ada sesuatu yang salah yang berkaitan dengan *request* pengunjung semisal ejaan url yang salah, atau page tidak ditemukan.

B. *Anonymous* FTP

Dari hasil percobaan pada tahap *scanning fingerprinting*, diketahui FTP yang dibuka oleh pihak Paud dan Dikmas ialah jenis publik FTP atau biasa disebut *Anonymous* FTP yang mana mengizinkan siapapun untuk memperoleh (mengunduh) file-file yang terdapat pada FTP server tersebut.:

Gambar 3 *Anonymous FTP* dari PAUD dan DIKMAS

Pemberian akses *Anonymous* FTP diperlukan agar pihak lain dapat mengakses dokumen yang berada dalam direktori FTP tersebut. Melalui uji penetrasi ini penulis juga melakukan pengecekan terkait status hak akses pada *Anonymous* FTP target menggunakan Metasploit.

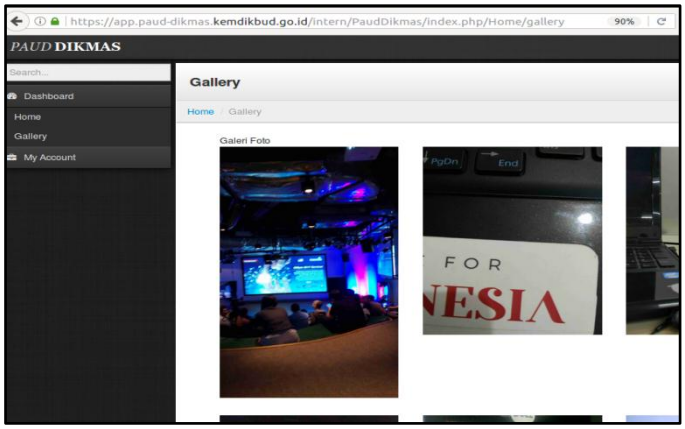


Gambar 4 Hasil Pengecekan Hak Akses Anonymous FTP

Dari gambar diatas menunjukan bahwa *Anoymous* FTP pada target memiliki hak akses "*READ*" yang berarti layanan FTP hanya bisa dilihat dan diunduh oleh pengguna *Anonymous*.

C. *Bypass Login*

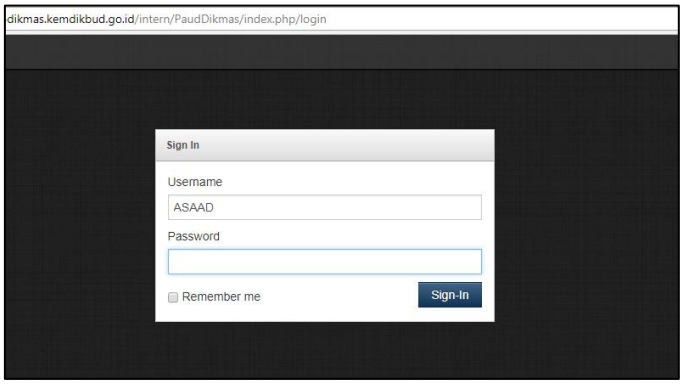
Dalam penetration testing ditemukan *bug* yang cukup fatal yaitu, terdapat halaman website yang tidak diberikan *session*, yaitu halaman ini merupakan Sistem Informasi Geografis (SIG) Paud dan Dikmas. Berikut tampilan halaman yang berhasil penulis *Bypass* dalam uji coba penetrasi.



Gambar 5 Kondisi awal Website SIG

Halaman tersebut merupakan bagian dari direktori domain web Paud dan Dikmas yang memilik alamat *app.paud-dikmas.kemdikbud.go.id/intern/PaudDikmas*. *Bug* semacam ini terjadi apabila pihak programmer tidak memberikan autentikasi user (*session*) untuk *log*in dahulu sebelum mengakses *dashboard* tersebut. Dan, risiko terbesar yang terjadi apabila programmer tidak menutup *bug* tersebut dan membuatkan *session login* maka pihak luar yang tidak memiliki wewenang dapat menngambil data-data yang bersifat penting dan rahasia milik kementerian.

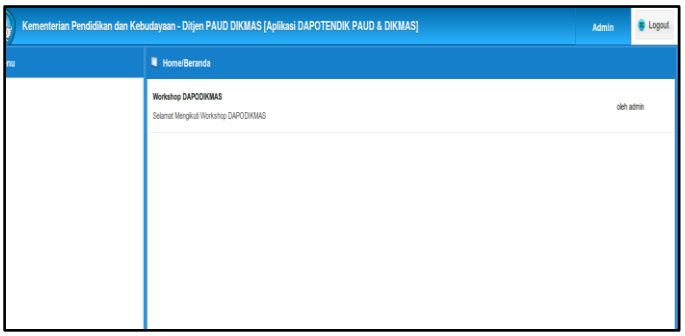
Beberapa hari setelah pelaporan kerentanan terkait *Bypass Login* diinformasikan kepada staff IT Paud dan Dikmas, *bug* tersebut diperbaiki dan sistem autentikasi *log*in untuk masuk ke direktori SIG telah dibuat. Sehingga pengguna yang tidak memiliki akun secara absah tidak dapat mengakses dan mengambil data darii direktori tersebut. Berikut gambaran kondisi website pada direktori SIG setelah diperbaiki



Gambar 6 Kondisi Akhir Website SIG

D. Gaining Access

Uji penetrasi menggunakan Hydra pada tahap enumerasi telah memberikan hasil yang cukup valid. Penulis berhasil mendapatkan kecocokan antara username dan password untuk melakukan autentikasi *log*in kedalam *dashboard* atau *page admin* dari direktori website TENDIK. Berikut merupakan tampilan dashboard admin dari direktori website TENDIK yang berhasil penulis akses dengan akun yang diperoleh dari teknik enumerasi.



Risiko terbesar dari celah ini seorang *attacker* akan leluasa melakukan perubahan pada isi website. Hal ini tentu sangat berbahaya, solusi yang diberikan kepada pihak staff IT terkait celah ini adalah melakukan penghapusan akun tersebut dari database atau menggantinya dengan kombinasi *username* dan *password* yang kuat dan sulit ditebak oleh aplikasi Hydra.

IV. KESIMPULAN DAN SARAN

A. Kesimpulan

Tidak ada sistem yang benar-benar aman dan sempurna di dunia *cyber*. Sebagai seorang *web programmer* hanya bisa mengupayakan untuk mengamankan web dengan semaksimal mungkin dan mengurangi risiko-risiko terjadinya celah kerentanan yang bisa dimasuki oleh *hacker*. Pihak staff IT Paud dan Dikmas bisa melakukan pengamanan pada *back-end* website melalui *coding*. Pada uji penetrasi (*pentesting*) yang dilakukan dapat menentukan kualitas dari keamanan website Paud dan Dikmas itu sendiri. Dari hasil *pentesting* ini juga menjadi aspek yang perlukan diperhatikan oleh pihak staff IT Paud dan Dikmas, mengingat website tersebut merupakan aset penting yang menyimpan ratusan data-data paud dan tenaga pendidik yang tersimpan didatabase website. *Pentesting* tentu tidak berhenti sampai disini karena masih banyak celah kerentanan web yang dapat terjadi selain yang sudah ditemukan seperti *web disclosure* karena *SQL attack*, lemahnya keamanaan autentikasi untuk *login* pada website, dan Anonymous FTP.

B. Saran

Semua celah itu berbahaya, baik itu celah di website yang timbul dari kesalahan coding, ataupun kesalahanan dalam konfigurasi jaringan, maupun *tools* yang mengandung bug/celah. Oleh karena itu sebagai seorang *web programmer* harus mengantisipasi hal ini. Adapun saran yang ingin penulis berikan kepada pihak perusahaan, yaitu :

a. Untuk meminimalisir kesalahan *coding* yang bisa menimbulkan bug/celah seorang *web programmer* seharusnya selalu melakukan *testing* terlebih dahulu terhadap skrip *coding* di komputer lokal, kemudian

upload ketika memang semuanya sudah benar dan bebas dari *bug*.

b. Responsif terhadap celah atau *bug* yang didapatkan dari hasil pentesting. Saat ini pihak staff IT masih menyimpan daftar kombinasi akun *username* dan *password* yang lemah dalam *database* sehingga mudah ditebak oleh aplikasi Hydra. Potensi pihak yang tidak berwenang untuk mengakses halaman admin direktori TENDIK pada web Paud dan Dikmas bisa sangat tinggi. Perlu adanya pembaharuan akun yang memiliki kombinasi *username* dan *password* yang rumit atau tidak mudah ditebak oleh Hydra dan aplikasi enumerasi lainnya.

c. Tingkat keberhasilan uji penetrasi dapat diukur dari semakin banyak celah kerentanan yang ditemukan oleh *pentester*. Hal ini juga menandakan semakin tinggi pula tingkat risiko kerusakan yang akan terjadi pada sistem yang menjadi target. Untuk itu, perlu uji penetrasi secara berkelanjutan dan terjadwal serta dilakukan menggunakan *tools* yang lebih canggih lagi, agar setiap *bug* dapat diketahui lebih dalam dan bisa memberikan evaluasi dari setiap *bug* secara lengkap dan rinci kepada pihak staff IT.

.

REFERENSI

[1] Anonim. *Whois*. https://www whois.net.[10 November 2017]

[2] Anonim. *Virtual Box*. https://www.virtualbox.org/wiki/VirtualBox.[12 November 2017]

[3] Anonim. Akamai Releases Second Quarter 2013 State of The Internet Report.

[4] https://www.akamai.com/us/en/about/news/press/2013-press/akamai-releases-second-quarter-2013-state-of-the-internet-report.jsp.[2 November 2017]

[5] Alharbi. 2010. Writing a Penetration Testing Report. https://www.sans.org/reading-room/whitepapers/bestprac/writing-penetration-testing-report-33343. [15 Januari 2018]

[6] Ariyus, Dony. 2004. Kamus Hacker. Yogyakarta: Andi.

[7] Beggs, W. Robett. 2014. Mastering Kali Linux for Advanced Penetration Testing. Birmingham: Packt Publishing.

[8] Desai M. dan Joshi D. 2012. Anonymous Attack Anatomy Hacker Intelligence *Report*. London : Hacking Tech.

[9] Engerbreston, Patrick. 2013. The Basics of Hacking and Penetration Testing, Second Edition:Ethical Hacking and Penetration Testing Made Easy. Rockland: Syngress.

[10] Gula, Ron. 2007. CVSS Version 2 Scoring with Nessus and the Passive Vulnerability Scanner. https://www.tenable.com/blog/cvss- version-2-scoring-with-nessus-and-the-passive-vulnerability-scanner. [16 November 2017]

[11] Jaswal, Nipun. 2014. *Mastering Metasploit*. Birmingham: Packt Publishing.

[12] Kennedy, D., O'Gorman J., dan Kearns, D., And Aharoni, Mati. 2011. *Metasploit* : *The Penetration Tester's Guide*. San Francisco: No Starch Press.

[13] Kurtz George, McClure Stuart, dan Scambray Joel. *Hacking Exposed: Network SecuritySolutions, Sixth Edition*. New York City: McGraw-Hill Osborne Media

[14] Mackey David. Web Security For Network And System Administrator. Stamford : Thomson Learning.

[15] Muniz, Joseph dan Lakhani, Aamir. 2013. *Web Penetration Testing With Kali Linux*.Birmingham: Packt Publishing.

[16] Najera, Gilberto. 2016. Kali Linux Web Penetration Testing Cookbook. Birmingham: Packt Publishing.

[17] Oriyano Philip dan Gregg Michael. 2010. *Hacker Techniques, Tools, and Incident Handling*.Burlington: Jones & Bartlett Publishers.

[18] Ouimet, Kirk. *You Get Signal*. https://www.yougetsignal.com/about. [10 November 2017]

[19] Rothe, Ben. 2004. *Computer Security: 20 Things Every Employee Should Know*. New York: McGraw-Hill.

[20] Weidman, Georgia. 2014. Penetration Testing: A Hands-On Introduction to *Hacking*. San Francisco: No StarCH Press.