Audit keamanan webserver pada website "www.palcomtech.com"

Alfred Tenggono[1)], Tegar Purnama[2)], Andi Setia Budi[3)]
STMIK PalComTech
Jl. Basuki Rahmat No.5 Palembang
e-mail: alfred.tenggono@gmail.com

Abstrak

Teknologi informasi memiliki peran penting untuk mendukung kinerja dan aktivitas sebuah institusi. Direktorat Keamanan Informasi Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika pada tahun 2011 telah mengeluarkan panduan tentang kemanan web server yang bertujuan merekomendasikan aspek keamanan untuk perancangan, implementasi, dan pengoperasian Web server yang dapat diakses secara public. STMIK PalComTech mempunyai Web Server yang berisi web pages, yang didalamnya berisi informasi dan dokumen yang dipublikasikan atau diperlukan oleh pengguna. Oleh sebab itu, perlu dilakukan pengujian pada web server STMIK PalComTech. www.palcomtech.com merupakan website terbuka yang dapat diakses oleh siapa saja. Pengujina dilakukan melalui 3 tahap yaitu, diagnosa, action planning, dan action taking. Berdasarkan pengujian yang telah dilakukan di dapatkan celah keamanan yang dapat menggangu penyediaan informasi oleh web www.palcomtech.com. Berdasarkan hasil pengujian yan dilakukan peneliti telah menghasilkan beberapa rekomendasi yang dapat digunakan untuk memberbaiki keamanan webserver pada STMIK PalComTech.

Kata kunci: *audit keamanan, website, penetration test*

1. Pendahuluan

Seiring semakin berkembangnya teknologi informasi, dapat memudahkan masyarakat untuk mengakses dan mencari informasi. Teknologi informasi memiliki peran penting untuk mendukung kinerja dan aktivitas sebuah institusi untuk dapat bertahan dan meraih keunggulan kompetitif. Namun dalam pengelolaannya, IT selalu memiliki resiko kerentanan.

Direktorat Keamanan Informasi Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika pada tahun 2011 telah mengeluarkan panduan tentang kemanan web server yang bertujuan merekomendasikan aspek keamanan untuk perancangan, implementasi, dan pengoperasian Web server yang dapat diakses secara publik. Aspek yang direkomendasikan dalam pedoman ini dirancang untuk membantu mengurangi resiko yang berkaitan dengan Web server dan mengetengahkan prinsip umum yang berlaku untuk semua sistem. Pedoman ini direkomendasikan bagi departemen dan lembaga pemerintah, namun dapat juga digunakan di sektor swasta dan organisasi yang tertarik dalam meningkatkan keamanan sistem Web server dan guna mengurangi jumlah dan frekuensi insiden keamanan yang terkait dengan Web.

STMIK PalComTech mempunyai *Web Server* yang berisi *web pages*, yang didalamnya berisi informasi dan dokumen yang dipublikasikan atau diperlukan oleh pengguna. *Web Server* seringkali menjadi target dari berbagai macam jenis serangan baik yang bersifat minor dan major sehingga berakibat fatal. Pengujian sangatlah penting untuk mengetahui apakah *web server* sudah aman atau belum dari tindak kejahatan yang dilakukan oleh seorang *hacker*. Oleh sebab itu, perlu dilakukan pengujian pada *web server* STMIK PalComTech. www.palcomtech.com merupakan *website* terbuka yang dapat diakses oleh siapa saja. Tetapi untuk fasilitas seperti melihat jadwal perkuliahan, transkip nilai, input krs dan ujian online hanya bisa diakses oleh dosen dan mahasiswa STMIK PalComTech.

Menurut Ilham Daniel dalam penelitiannya yang berjudul Evaluasi Celah Keamanan Web Server pada LPSE Kota Palembang disimpulkan bahwa setelah dilakukan pengujian terhadap webserver LPSE kota Palembang terdapat celah keamanan yang harus di perbaiki dan harus dilakukan secara berkala [1] menurut Moh Dahlan dalam penelitiannya yang berjudul Analisa Keamanan Web Server Terhadap Serangan Possibility SQL Injection Studi Kasus: Web Server UMK disimpulkan bahwa Pada Web Server Universitas Muria Kudus (UMK) terdapat beberapa aktifitas yang berusaha masuk ke sistem jaringan melalui notifikasi alert IDS Snort (ping), meskipun aktifitas tersebut hanya sekedar melihat-lihat web

yang aktif, namun kegiatan ini perlu di waspadai. Dengan adanya IDS Snort, seluruh aktifitas jaringan yang berjalan di web server UMK dapat dipantau setiap saat. [2]. Menurut Nazwita dalam penelitiannya yang berjudul Analisis Sistem Keamanan Web Server dan Database Server Menggunakan Suricata disimpulkan bahwa perlu adanya analisis keamanan terhadap webserver yang berjalan, sehingga apabila terjadi serangan langsung dapat terdeteksi [3]. Menurut Ari Muzakir dalam penelitiannya yang berjudul Sistem Keamanan Data pada *Web Service* Menggunakan Xml *Encryption* disimpulkan bahwa Desain dan implementasi modul yang telah dilakukan dengan menggunakan *library* keamanan serta dukungan *library* XMLSEC sebagai *library* pendukung dan *library* class_wss. Hal ini mampu mengatasi masalah keamanan pada proses pengiriman yaitu keamanan otentikasi, dan konfidensialitas pesan SOAP *request* yang dihasilkan. Hasil dari implementasi mengindikasikan bahwa konfidensialitas dapat terpecahkan dengan menerapkan konsep keamanan berbasis *library* keamanan yaitu XML *encryption*. Pesan SOAP *request* pada proses pengiriman dapat memenuhi standar keamanan *web service*, dimana data ketika dikirimkan dalam keadaan terenkripsi dengan menggunakan *library* class_wss yang telah dibangun. [4] dari penelitian yang telah dilakukan sebelumnya peneliti menyimpulak perlu adanya pengujian yang dilakukan terhadap web server STMIK PalComTech.

2. Metode Penelitian

2.1. Action Research

Menurut Chandra *Action research* pada hakikatnya merupakan rangkaian yang dilakukan secara sistematik, dalam rangka memecahkan masalah, sampai masalah itu terpecahkan. *Action research* termasuk penelitian kualitatif walaupun data yang dikumpulkan bias saja bersifat kuantitatif. *Action research* berbeda dengan penelitian formal, yang bertujuan untuk menguji hipotesis dan membangun teori yang bersifat umum *(general*). Action research lebih bertujuan untuk memperbaiki kinerja, sifatnya kontekstual dan hasilnya tidak untuk digeneralisasi. Namun demikian hasil *action research* dapat saja diterapkan oleh orang lain yang mempunyai latar yang mirip dengan yang dimiliki peneliti. [5]

2.1.1 Melakukan Diagnosa *(Diagnosing)*

Melakukan diagnosa (*diagnosing*), yaitu mengidentifikasi masalah-masalah pokok yang ada guna menjadi dasar bagi organisasi untuk melakukan perubahan ke arah yang lebih baik. Peneiti akan mencari pokok permasalahan dan apa saja yang dibutuhkan dalam penelitian ini.

2.1.2 Membuat Rencana Tindakan *(Action Planning)*

Membuat rencana tindakan (*action planning*), Peneliti dan partisipan bersama-sama memahami pokok masalah yang ada kemudian dilanjutkan dengan menyusun rencana tindakan yang tepat untuk menyelesaikan masalah yang ada. Pada tahap ini peneliti akan melakukan atau menyusun rencana tindakan yang akan dilakukan pada tahap selanjutnya *(action taking)*, seperti menjadwalkan proses:

1. Menentukan ruang lingkup penelitian
2. Menentukan *stakeholder*
3. Menentukan jadwal penelitian

2.1.3 Membuat Tindakan *(Action Taking)*

Melakukan tindakan (*action taking*), Peneliti mengimplementasikan rencana tindakan dengan harapan dapat menyelesaikan masalah. Pada tahap ini peneliti melakukan tindakan dengan memulai analisa kinerja jaringan yang ada pada STMIK PalComTech Palembang.

3. Hasil dan Pembahasan

3.1. Diagnosa

Anher (2016), WPScan merupakan tool vulnerability scanner untuk CMS Wordpress yang ditulis dengan menggunakan bahasa pemograman ruby, WPScan mampu mendeteksi kerentanan umum serta daftar semua plugin dan themes yang digunakan oleh sebuah website yang menggunakan CMS Wordpress.
Mengapa peneliti menggunakan WPScan, karena pada www.palcomtech.com menggunakan cms wordpress, dan dilihat dari hasil report dari wpscan palcomtech.com menggunakan wordpress versi 4.1.1 dan terdapat 23 vulnerability dari hasil scan tersebut.

1. *Title: WordPress 4.1.1 - Unauthenticated Stored Cross-Site Scripting (XSS)*
   Stored XSS lebih jarang ditemui dan dampak serangannya lebih besar. Sebuah serangan *stored XSS* dapat berakibat pada seluruh pengguna. *Stored XSS* terjadi saat pengguna diizinkan untuk memasukkan data yang akan ditampilkan kembali. Contohnya adalah pada *message board*, buku tamu, dll. Penyerang memasukkan kode HTML atau *client script code* lainnya pada posting mereka.
2. *Title: WordPress 3.9-4.1.1 - Same-Origin Method Execution*

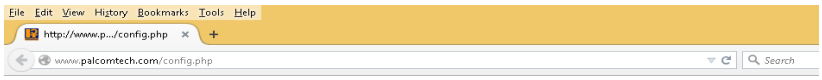
SOME adalah suatu celah yang memungkinkan dalam penguploadan suatu file dengan memanipulasi parameter *GET* pada skrip untuk mengeksekusi fungsi *javascript*.

3. *Title: WordPress 4.1-4.2.1 - Genericons Cross-Site Scripting (XSS)*
   Dokumen *Object* Model atau DOM berbasis *Cross-Site Scripting* (XSS) ditemukan kerentanan plugin atau tema yang menggunakan *Genericons* rentan karena file tidak aman termasuk dalam paket. *Genericons ships* dengan file bernama example.html yang rentan terhadap serangan dari DOM adalah serangan XSS dimana serangan payload dijalankan sebagai akibat dari memodifikasi '*environment*' DOM di *browser* korban yang digunakan oleh *original client side script*, sehingga kode sisi klien berjalan secara 'tak terduga'. Artinya, halaman itu sendiri (respon HTTP) yang tidak berubah, tapi kode sisi klien yang terdapat di halaman mengeksekusi berbeda karena modifikasi berbahaya yang telah terjadi di lingkungan DOM. Serangan XSS berbasis DOM juga agak sulit untuk dieksploitasi, karena memerlukan beberapa tingkat rekayasa sosial untuk membuat seseorang mengklik *link exploit.*
4. *Title: WordPress 4.1 - 4.1.1 - Arbitrary File Upload*
   adalah celah mengenai halaman yang mengizinkan *user* untuk mengupload sesuatu, contoh serangan dalam *vulnerability* ini adalah *attacker* mengupload file berupa gambar lalu menggunakan tamperdata untuk merubah kembali file tersebut.
5. *Title: WordPress 4.2.3 - wp_untrash_post_comments SQL Injection*
   SQL injection adalah sebuah aksi hacking yang dilakukan di aplikasi *client* dengan cara memodifikasi perintah SQL yang ada di memori aplikasi *client* dan teknik mengeksploitasi web aplikasi yang didalamnya menggunakan *database* untuk penyimpanan data.
6. *Title: WordPress <= 4.2.3 - Timing Side Channel Attack*
   Side channel attack adalah serangan yang memanfaatkan kebocoran informasi yang ditimbulkan karena aktivitas yang dilakukan mesin atau program. Seperti halnya di dunia fisik, setiap aktivitas yang dilakukan program sebenarnya menimbulkan "efek samping" atau jejak yang bisa diamati.
7. *Widgets Title Cross-Site Scripting* (XSS)
   kesalahan koding yg memungkinkan xss yang memanfaatkan *script default widget.*
8. Title: WordPress 3.7-4.4.1 - *Local URIs Server Side Request Forgery (SSRF)*
   Server Side Request Forgery adalah salah satu *vulnerability* yang mana *attacker* dapat melakukan *request* kepada *server* untuk melakukan request tersebut misal.
   http://target/proxy.php?csurl=http://localhost:631
9. *Title: WordPress 3.7-4.4.1 - Open Redirect*
   Open Redirect vulnerability adalah celah keamanan aplikasi yang tidak melakukan *verifikasi* saat proses *redirect*. Kelamahan ini dapat digunakan dalam serangan *phising* untuk mendapatkan banyak pengunjung ke situs berbahaya tanpa disadari oleh user.
   Contoh sederhana penyerangan phising dengan memanfaatkan kelemahan open redirect:
   a. http://vulnerable.com?redirect=http://situsphising.com
   b. atau disisipkan ke dalam HTML, seperti contoh dibawah ini <ahref="http://vulnerable.com/redirect?url=http://fesbook.net">Silahkan login disini
   Report hasil scan menunjukan bahwa beberapa *aplikasi* atau *plugin* dari wordpress masih *outofdate* atau belum *update* yang dimana *plugin* yang lama telah ditemukan banyak *vulnerability* yang mungkin bisa digunakan oleh *attacker.*

3.2. Pengujian dari Hasil *Report*

1. *Vulnerable Sensitive data exposure*

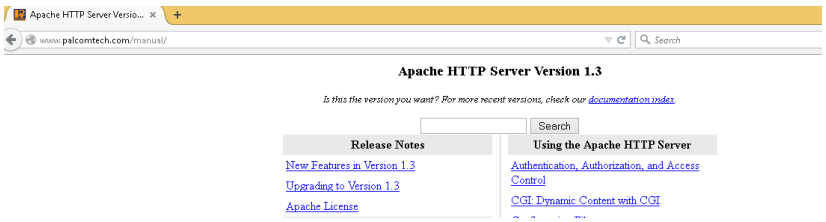
a. http://www.palcomtech.com/config.php



Gambar 1 : Hasil *Report Config.php*

Pada gambar 5.12 bisa dilihat bahwasanya file config.php dapat di akses oleh client namun tidak terlihat isi konfigurasi dari file tersebut.

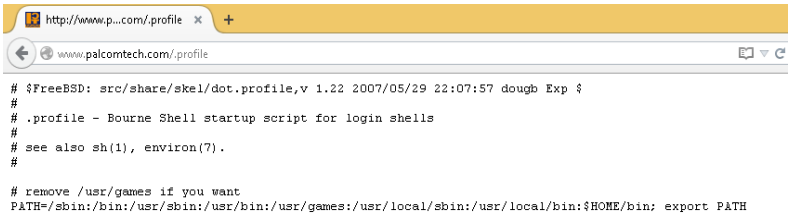
a. http://www.palcomtech.com/manual/



Gambar 2 : Hasil *Report* Manual

Pada gambar 5.13 bisa dilihat Direktori manual dapat di akses, yang memungkinkan attacker mendapatkan informasi apa saja tentang server.

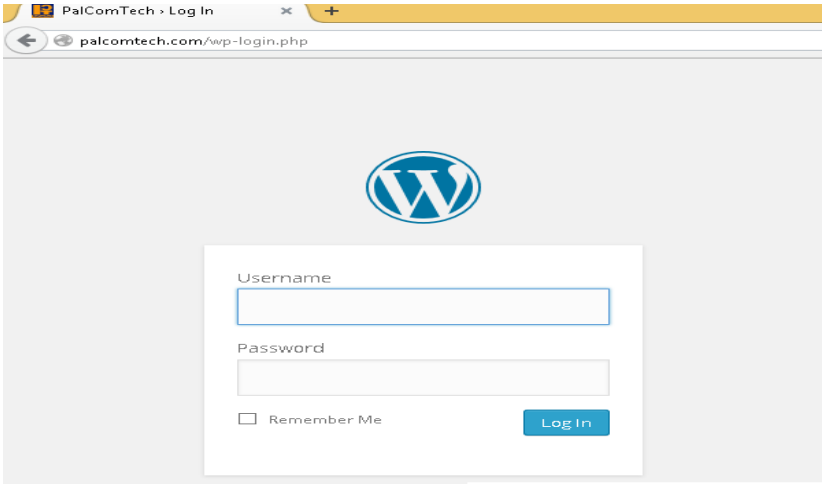
b. http://www.palcomtech.com/.profile



Gambar 3 : Hasil *Report* Profile

Pada gambar 5.14 bisa dilihat bahwasannya perintah /.profile/ dapat di akses yaitu menampilkan informasi shell pada server.

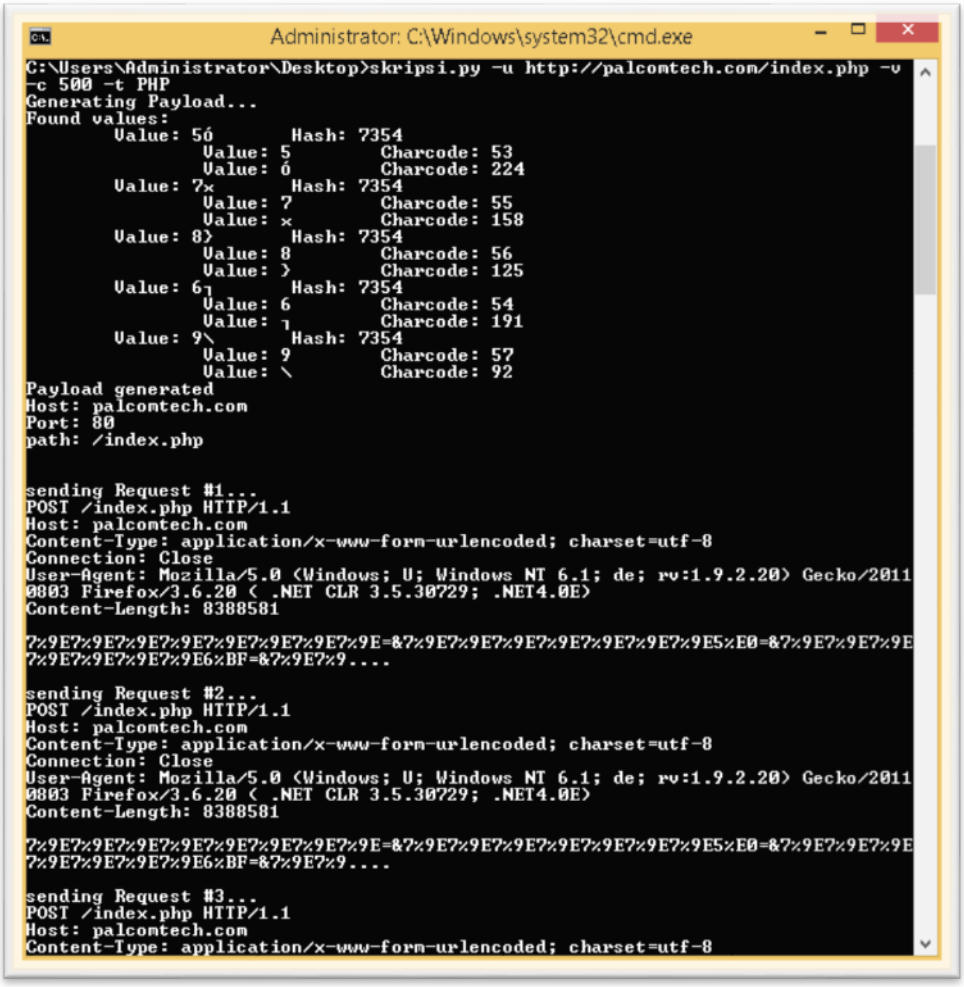
c. http://palcomtech.com/wp-login.php



Gambar 4 : Hasil *Report Login.php*

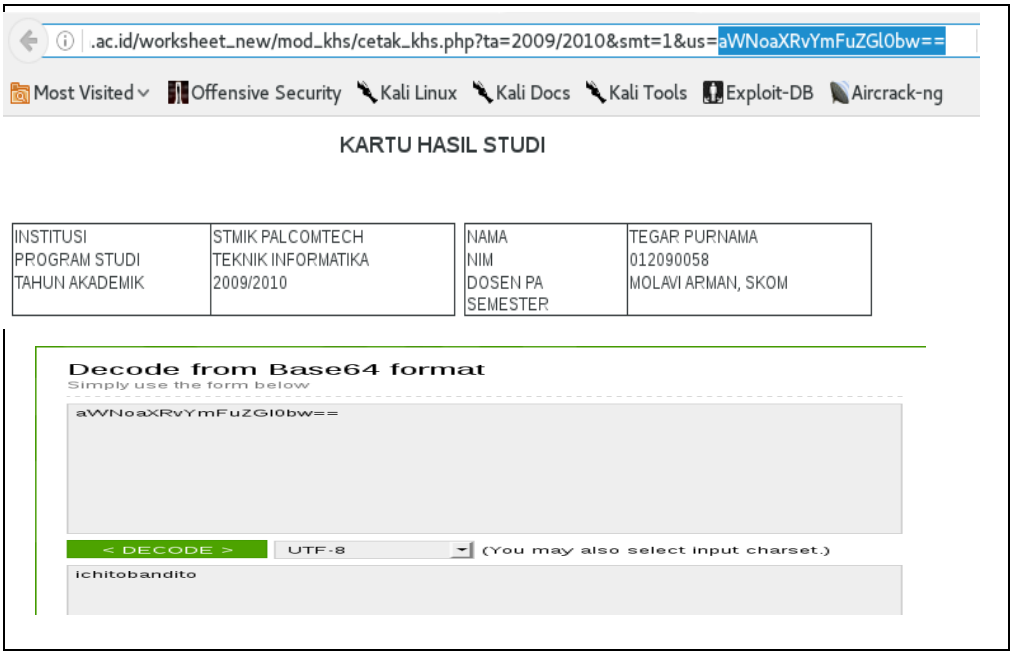
Pada gambar 5.15 bisa dilihat bahwasannya halaman login wordpres yang sangat rentan dengan serangan brute force,PHP Hash Collision denial of service vulnerability Yaitu php yang out of date/ kadaluarsa yang dapat menimbulkan serangan DDOS.

Peneliti mencoba melakukan DoS dengan target PHP dengan reques sebanyak 500x dan serangan DoS dapat dijalankan, adapun hasil pengujian dengan DoS tampak pada gambar 5.16



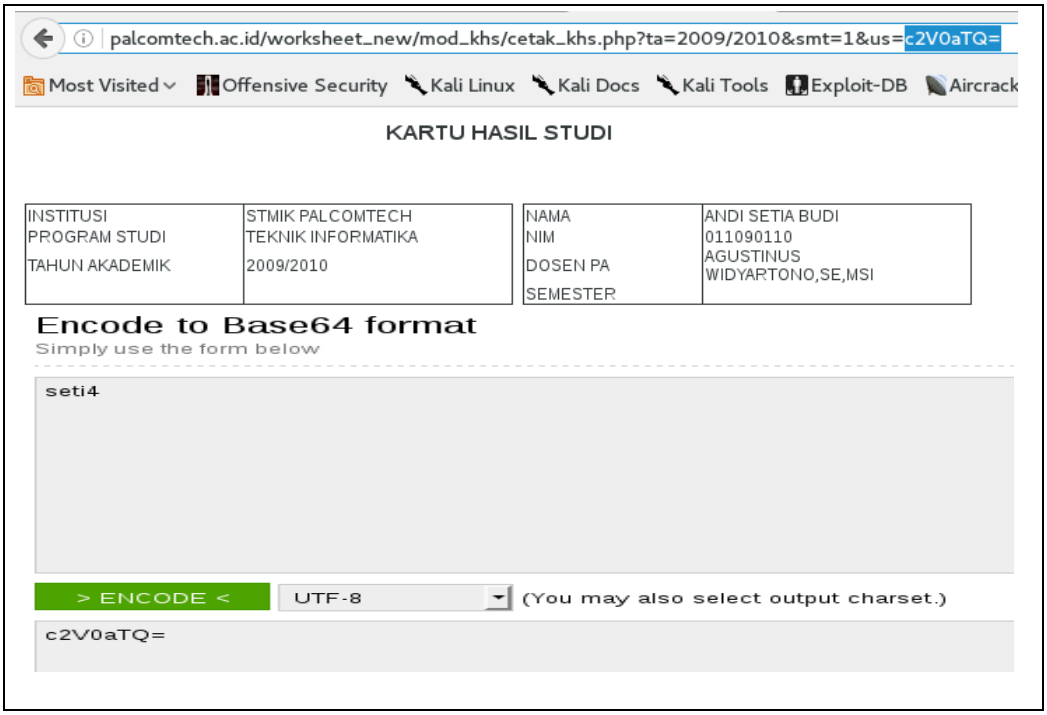
Gambar 5 : Pengujian Menggunakan DDOS

Lalu peneliti melukakan pengujian untuk mencari celah dari dalam web dengan login, dan peneliti menemukan celah atau vulnerability yang menggunakan fungsi cookies yang diakses pada halaman khs mahasiswa padaurl.http://palcomtech.ac.id/worksheet_new/mod_khs/cetak_khs.php?ta=2009/ 2010 &smt=1&us=aWNoaXRvYmFuZG10bw==, yang mana aWNoaXRvYmFuZGl0bw, adalah enkripsi base64 yang jika di dekripsi adalah ichitobandito, ichitobandito yaitu username dari peneliti, lalu peneliti melakukan ujicoba dengan username lainya. Adapun hasil pengujian yang dilakukan ini tampak pada gambar 5.17 dan 5.18.



Gambar 6 : Hasil Pengguian dengan *user* ichitobandito

Lalu peneliti melakukan pengujian dengan user lain dan peneliti menggunakan hasil dari encode tadi kedalam url menjadi http://palcomtech.ac.id/worksheet_new/mod_khs/cetak_khs.php?ta=2009/2010&smt=1&us=c2V0aTQ= dan hasilnya tanpa login user lain, peneliti dapat melihat informasi mahasiswa lain yaitu Andi Setia Budi dengan username seti4.



Gambar 7 : Hasil Pengujian dengan User seti4

3.3. Rekomendasi Perbaikan

1. Untuk solusi pencegahan serangan XST ada baiknya menambahkan fungsi html specialchars pada baris script yang perintahnya berfungsi menampilkan perintah missal yang awal nya <?php echo "$nama";?> Menjadi <?php echo htmlspecialchars($nama);?>
2. Untuk menutup celah Vulnerability Sensitive data Exposure yang terdapat pada direktori /library, /new, /manual, /.profile, /images ada baiknya admin merubah direktori atau file dengan permition 644 atau yang hanya bisa diakses oleh administrator atau root saja, karena bisa saja attacker mendapatkan informasi yang dapat membantu penyerangan seperti cms apa yang di instal, direktori apa saja yang dapat di akses, dan gambar apa saja yg dapat di akses.
3. Pada halaman login.php dan wp-login.php ada baiknya admin merubah nama (rename) login.php ini dengan nama yang tidak ada hubungan dengan login sama sekali, missal kursi.php karena ketika attacker sudah mendapatkan username dan password admin, maka attacker akan sulit mencari halaman login untuk masuk kedalam web tersebut.
4. Pada vulnerability Session fixation serangan session fixation tidak akan terjadi bila sessionid ditentukan oleh server, bukan oleh client. client tidak memberikan sessionid dalam bentuk apapun, maka serverlah yang akan memberi sessionid. web server harus menolak seluruh session id user pada saat client login dan mengubah beberapa script pada baris PHPSESSID=
5. Memasang CSRF protection bisa di download di github https://github.com/expressjs/csurf. Lalu di pasang di server (install) setelah itu tambahkan script input(type="hidden", name="_csrf", value="#{csrf}") di dalam form.
6. Memasang SSL , hampir setiap web besar dipasang SSL yang gunanya untuk enkripsi protocol yang sensitive, dalam kasus ini peneliti melihat euniversity.palcomtech.com merupakan halaman login mahasiswa maupun dosen yang tidak di enkripsi dengan SSL yang di mana dapat digunakan attacker sebagai web phising, atau fake page, atau fake login.
7. Pemasangan cloudflare atau server cloud yang gunanya untuk menangkal serangan ddos, jika bisa cloudflare yang ketika user mengakses halaman, user itu melakukan authentivikasi gambar terlebih dahulu.

4. Simpulan

1. Peneliti mendapatkan beberapa celah keamanan pada webserver STMIK PalComTech
2. Penelitian ini menghasilkan rekomendasi untuk memperbaiki celah keamamn pada webserver STMIK PalComTech

Daftar Pustaka

[1] Muhammad Ilham Daniel, Leon Andretti Abdillah, Kiky Rizky Nova Wardani. Evaluasi Celah Keamanan Web Server pada LPSE Kota Palembang. *Student Colloquium Sistem Informasi & Teknik Informatika (SC-SITI).* 2015; 19-24.

[2] Moh Dahlan, Anastasya Latubessy, Mukhamad Nurkamid. *Analisa Keamanan Web Server Terhadap Serangan Possibility SQL Injection Studi Kasus: Web Server Umk*. Prosiding SNATIF Ke-2. Kudus. 2015; 251-258; ISBN: 978-602-1180-21-1.

[3] Nazwita, Siti Ramadhani. *Analisis Sistem Keamanan Web Server Dan Database Server Menggunakan Suricata*. Seminar Nasional Teknologi Informasi, Komunikasi dan Industri (SNTIKI) 9. Riau. 2015; 308-317. ISSN (Printed) : 2579-7271 ISSN (Online) : 2579-5406.

[4] Ari Muzakir. *Sistem Keamanan Data pada Web Service Menggunakan Xml Encryption.* Seminar Nasional Teknologi Informasi dan Multimedia. Yogyakarta. 2013; 25-7 – 25-12. ISSN: 2302 -2805

[5] Huda, Nurul. *Akuntabilitas Pengelolaan Zakat Melalui Pendekatan Modifikasi Action Research. Skripsi tidak diterbitkan*. 2013. Jakarta: Universitas Yarsi Jakarta Pusat.