e-ISBN 978-623-93343-0-7
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 28 Januari 2020

VULNERABILITY ASSESMENT DAN KAJIAN ASPEK APPLICATION SECURITY PADA APLIKASI SKRIPSI ONLINE (SIPSO) FTI PERBANAS

Fahmi Hardiansyah [1], IGN. Mantra, M. Kom [2]

Program Studi

Teknik Informatika

Jl. Perbanas, Karet Kuningan, Setiabudi, Jakarta, 12940
fahmihardiansyah8@gmail.com1, ign.mantra@perbanas.id2

Abstrak. Dunia maya sudah bukan hal yang baru pada zaman sekarang ini. Banyak kegiatan dari individu sampai ke organisasi yang menggunakan dunia maya sebagai media informasi. Akan tetapi, sama halnya seperti dunia nyata yang memiliki sisi negatif. Dunia maya juga memiliki sisi negatif yaitu kejahatan dunia maya (cyber crime). Dan yang paling sering menjadi target serangan cyber crime adalah Web Server. Demi menjaga informasi digital yang ada pada Web server. Maka setiap individu atau organisasi diharuskan memiliki sistem keamanan yang bisa meminimalisir cyber crime. Karena satu hal yang pasti adalah tidak ada satupun yang aman di dunia maya. Dari pada orang lain yang tidak bertanggung jawab menemukan celah keamanan web web skripsi onlie FTI Pebanas Institute (SIPSO) lebih baik saya dahulu yang menemukannya dan melaporkan ke administrator. Maka dari itu peneliti akan melakukan analisa keamanan terhadap SIPSO. Tujuan dari penelitian ini salah satunya adalah untuk mencari celah keamanan terhadap serangan dari luar maupun dalam oleh orang yang tidak bertanggung jawab dan juga membantu administrator dalam melakukan pengujian pada web.

Kata Kunci: Security, Cyber Crime, Web Server, Perbanas Instituite.

1 Pendahuluan

Seiring dengan perkembangan yang ada keamanan informasi dalam sebuah website menjadi sangat penting. Dikhawatirkan ada pihak yang tidak bertanggung jawab dapat mengambil data-data penting dalam website ataupun dapat merusak website tersebut. Banyak celah keamanan yang dapat dimanfaatkan oleh penyerang untuk mendapatkan informasi penting tanpa sepengetahuan dari pengelola website. Bahkan anak SMA kelas 1 bisa melakukan defacing ke target meraka (Cobantoro, 2016). Celah keamanan yang kerap ditemukan p ada website yang dirilis oleh Open Web Application Security Project (OWASP) Top 10: Injection, Broken Authentication and Session Management, Cross Site Scripting (XSS), Insecure Direct Object Reference, Security Misconfiguration, Sensitive Data Exposure, Missing Function Level Access Control, Cross Site Request Forgery (CSRF), Using Components with Known Vulnerabilities, dan Unvalidated Redirects and Forwards (OWASP, 2010)
Fakultas Teknik Informatika Perbanas Institute merupakan salah satu Perguruan Tinggi Swasta yang menyediakan skripsi online berupa website, didalamnya tedapat informasi seputar pengumuman, alur sipso, daftar mahasiswa, jadwal sidang skripsi, serta proposal outline mahasiswa. Berbagai macam sistem informasi tersebut disediakan secara online dalam bentuk website. Hal tersebut memiliki resiko yang besar ketika sistem yang dibangun kurang memperhatikan sisi keamanan dari sistem tersebut. Akhir-akhir ini website SIPSO kerap mengalami trouble (masalah) seperti lumpuhnya website dan tidak bisa diakses data. Berdasarkan hal tersebut peneliti melakukan analis dan pengujian terhadap keamanan website Sipso dengan menggunakan metode pengujian secara umum maupun dengan pengujian secara empiris, hal tersebut dilakukan untuk mendapatkan data-data yang valid mengenai celah keamanan pada sistem tersebut, sehingga dari data-data tersebut dapat ditarik sebuah kesimpulan untuk kemudian dipelajari dan digunakan untuk meningkatkan keamanan pada sistem yang dimiliki oleh Sipso FTI.
Penelitian sebelumnya pernah dilakukan oleh (Iqbaludin, 2018) terkait dengan mengumpulkan informasi mengenai aplikasi web, melakukan analisis celah keamanan pada aplikasi web dan melakukan pengujian berdasarkan celah keamanan yang memiliki tingkat risiko sedang (medium) dan berdasarkan salah satu ancaman yang paling sering terjadi yang dimuat dalam OWASP Top 10 – 2017.

e-ISBN 978-623-93343-0-7
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 28 Januari 2020

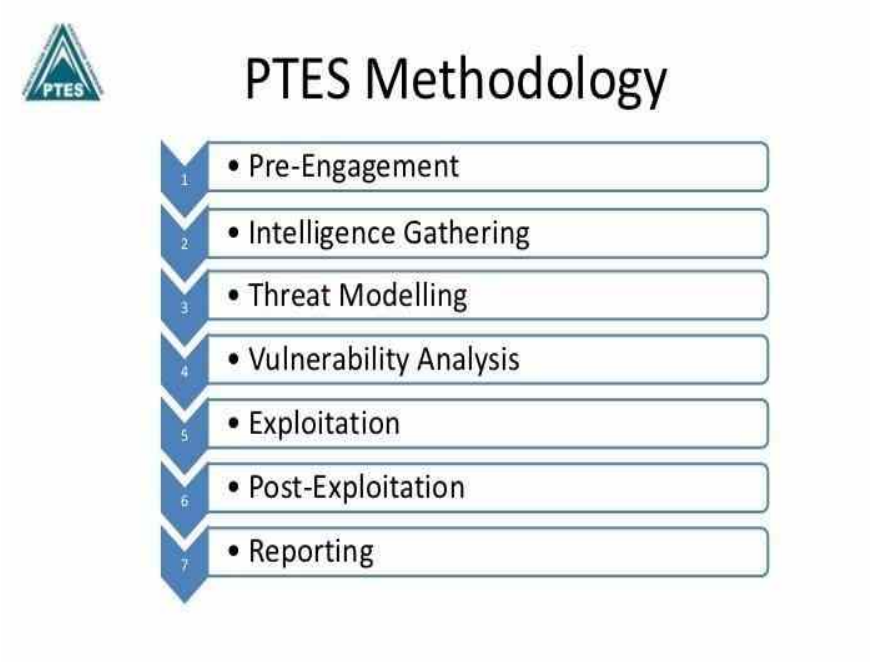
1.2 Tujuan Penelitian

Tujuan dari penelitian ini adalah menjawab berbagai masalah yang telah penulis uraikan pada perumusan masalah, yaitu :

1. Melakukan pengujian atau penetration testing pada website skripsi online dengan berdasarkan celah keamanan yang diperoleh dan dengan berdasarkan OWASP Top 10 – 2017.
2. Mengembangkan aplikasi guna mempermudah melakukan pengujian celah keamanan terhadap serangan dari luar oleh orang yang tidak bertanggung jawab.
3. Memberikan rincian mengenai cara pengamanan sistem secara detail dari hasil pentest
4. Membuat output berupa sebuah hasil pentest ke dalam sebuah laporan yang dapat dimengerti semua orang.

2 Metodologi Penelitian

Metodologi penelitian berasal dari kata “Metode” yang artinya cara yang tepat untuk melakukan sesuatu dan “Logos” yang artinya ilmu atau pengetahuan. Sehingga metodologi dapat diartikan sebagai cara melakukan sesuatu dengan menggunakan pikiran secara seksama untuk mencapai suatu tujuan. Sedangkan “Penelitian” adalah suatu kegiatan untuk mencari, mencatat, merumuskan dan menganalisis hingga menyusun laporan (Priyono, 2016). Dalam melakukan penelitian vulnerability asessment terhadap web aplikasi SIPSO PERBANAS ini metode penelitian yang digunakan dalam penelitian ini adalah metode Penetration Testing, metode ini terdapat 7 tahapan. Gambaran mengenai tahapan dari metode Penetration Testing



2.1 Vulnerability Assesment

Karena penelitian ini terfokus pada tahap vulnerability Assesment maka tahap dibagi menjadi 4 tahapan dengan tujuan mendapatkan hasil yang maksimal untuk melakukan vulnerability assessment berikut tahapannya yaitu :

1. Pre-Engangement
2. Intelligence Gathering
3. Vulnerabilty Alanysis
4. Reporting

e-ISBN 978-623-93343-0-7
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 28 Januari 2020

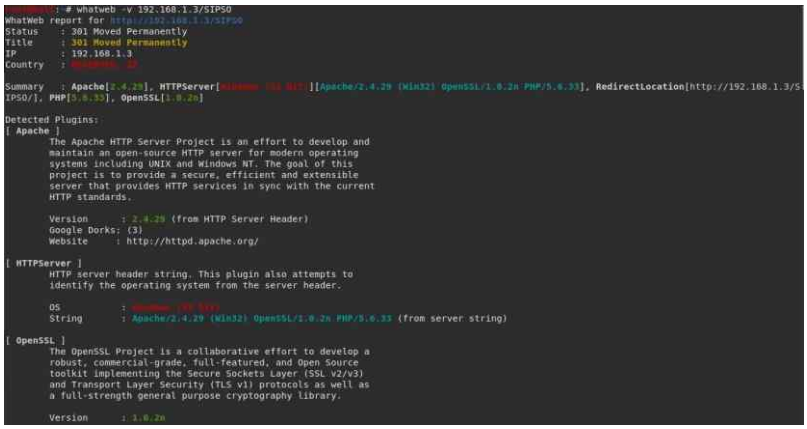
Gambar 3.2 Work Flow Vulnerability Assesment

3 Hasil Dan Pembahasan

3.1 Intelligence Gathering

Pada proses pengumpulan informasi, peneliti melakukan dengan beberapa tools yang digunakan pada sistem operasi linux untuk mengumpulkan semua informasi mengenai sistem target. Beberapa tools yang digunakan sebagai berikut:

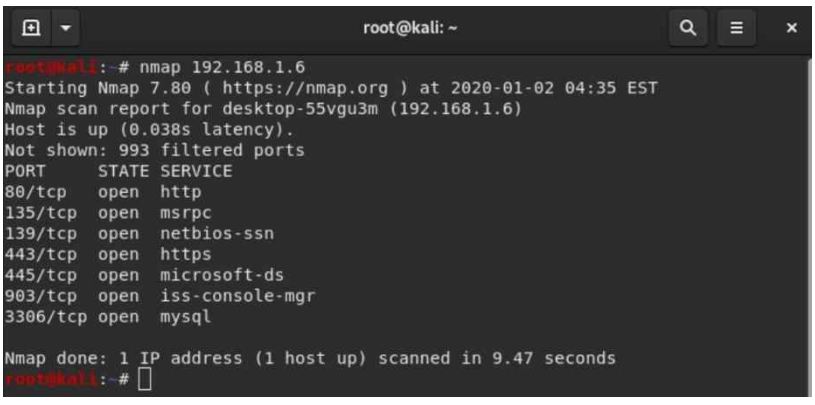
1.1.1 WhatWeb



Gambar 4.8 WhatWeb

Dari hasi scanning didapatkan beberapa informasi pada web SIPSO yang dijalankan seperti IP yang digunakan 192.168.1.3, OS server yang digunakan windows 32bit kemudian web servernya adalah Apache versi 2.4.29, OpenSSL versi 1.0.2n, PHP versi 5.6.33, menggunakan CodeIgniter-PHP-Framework (CI), HTML 5, dan Jquery nya memakai versi 1.12.3, dari whatweb peneliti bisa mendapatkan banyak informasi.

1.1.2 NMAP



e-ISBN 978-623-93343-0-7
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 28 Januari 2020

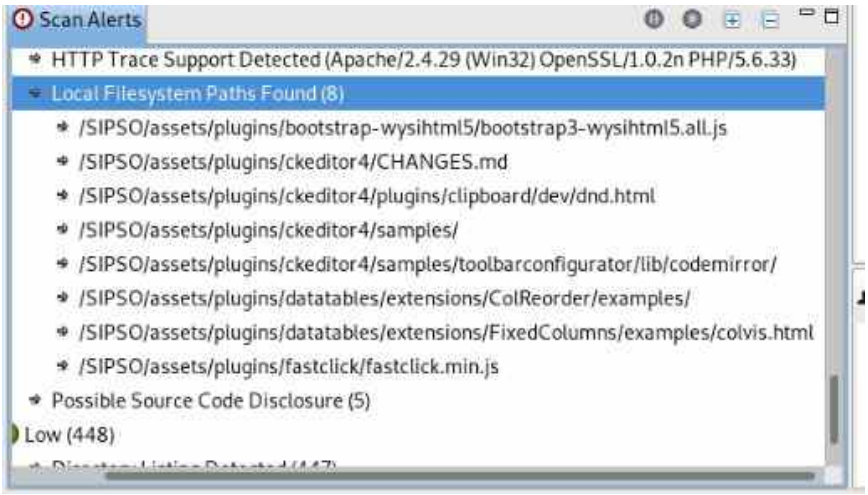
Gambar 4.9 NMAP SIPSO

Ada banyak Port terbuka pada hasil scaning yang didapatkan terlihat pada gambar 4.6 Nmap. Port 445 berstatus open, port 445 sangat rentan terhadap serangan worm dan tindakan eksploitasi apabila dibiarkan terbuka. Serangan Worm sangat mirip dengan virus komputer secara fungsi dan desainnya. Bisa dianggap worm adalah sub-kelas dari virus. Worm juga menyebar dari komputer ke komputer yang lain, tetapi tidak seperti virus, untuk kebanyakan kasus sistem yang terinfeksi worm akan banyak mengkonsumsi terlalu banyak sistem memori atau bandwidth jaringan, menyebabkan web server crash, server jaringan juga dapat terganggu, dan bisa saja masing-masing sistem komputer dapat berhenti merespons.

3.3 Vulnerabilty Analysis

Mengidentifikasi kelemahan keamanan pada Skripsi Online Perbanas. Peneliti menggunakan beberapa tools yang digunakan sebagai berikut :

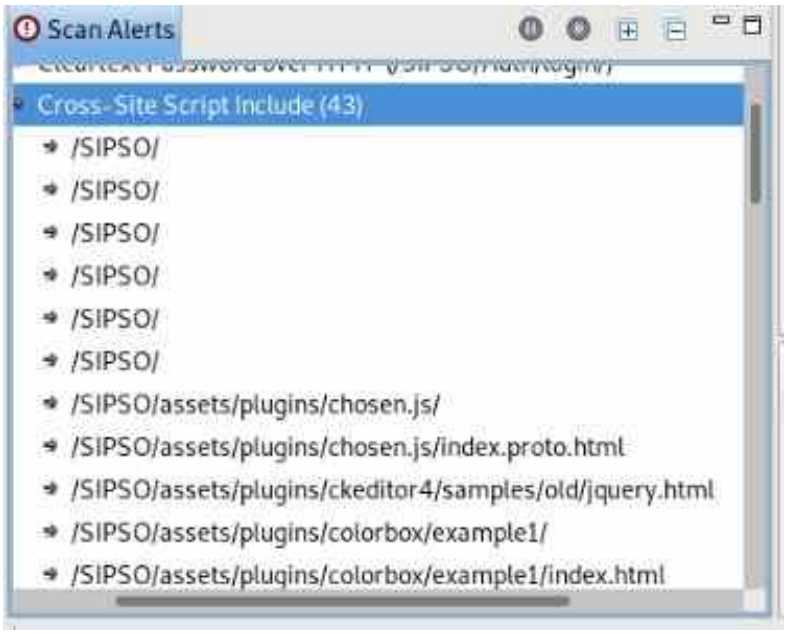
1.1.1 VEGA



Gambar 4.11 Kelemahan LFI

Terlihat pada Gambar 5.0 Kelemahan LFI sangat banyak ditemukan. Metode yang memanfaatkan kelemahan script PHP include(), include_once(), require(), require_once() yang variabel nya tidak dideklarasikan dengan sempurna.

e-ISBN 978-623-93343-0-7
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 28 Januari 2020



Gambar 4.12 Kelemahan XSS

Pada hasil scaning yang paling rentan dan banyak didapatatkan dengan menggunakan VEGA kelemahan XSS terletak pada direktori SIPSO/assests/plugins dan juga pada kelemahan Local File Inclusion (LFI) terdapat pada direktori yang sama.

1.1.2 Nikto

```
root@kali:~# nikto -C all --host http://192.168.1.5/SIPSO/
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.1.5
+ Target Hostname:    192.168.1.5
+ Target Port:        80
+ Start Time:         2020-01-04 09:32:06 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.29 (Win32) OpenSSL/1.0.2n PHP/5.6.33
+ Retrieved x-powered-by header: PHP/5.6.33
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against so
me forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of t
he site in a different fashion to the MIME type
+ Apache/2.4.29 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for t
he 2.x branch.
+ PHP/5.6.33 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may al
so current release for each branch.
+ OpenSSL/1.0.2n appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also c
urrent.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01
xdh%28VS.80%29.aspx for details.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3268: /SIPSO/db/: Directory indexing found.
+ OSVDB-3092: /SIPSO/db/: This might be interesting...
+ OSVDB-3092: /SIPSO/system/: This might be interesting...
+ OSVDB-3092: /SIPSO/LICENSE.txt: License file found may identify site software.
+ OSVDB-3092: /SIPSO/license.txt: License file found may identify site software.
+ OSVDB-3092: /SIPSO/LICENSE.TXT: License file found may identify site software.
+ /SIPSO/composer.json: PHP Composer configuration file reveals configuration information - https://getcom
poser.org/
+ 26522 requests: 0 error(s) and 17 item(s) reported on remote host
+ End Time:           2020-01-04 09:40:45 (GMT-5) (519 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Gambar 4.13 Nikto

Kerentanan aplikasi web celah yang didapatkan oleh tools ini pun beragam seperti yang didapatkan oleh penetili, mendapatkan kelemahan yang menarik yaitu pada OSVDB – 3092 direktorinya /SIPSO/db/ apabila di telurusi lebih dalam. Direktori ini adalah direktori yang mengarah ke database pada mysql yang tentunya berisi data -data penting seperti username dan password hal ini sangat membahayakan apabila direktori tersebut terpublikasikan yang mana nanti bisa saja hacker menggunakan ini untuk merusak system dari sipso tersebut.

1.1.3 Uniscan

e-ISBN 978-623-93343-0-7
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 28 Januari 2020

Gambar 4.14 Uniscan

Ada beberapa metode yang terdapat dalam uniscan yang pertama crawling, pada metode ini peneliti mendapatkan informasi dan juga kerentanan pada Directory check, terlihat ada informasi konfigurasi PHP yaitu CODE: 200 URL: http://192.168.1.3/SIPSO/phpmyadmin direktori ini sangat berbahaya apabila tidak diberi akses khusus yang mana nantinya attacker bisa saja melihat dan mengambil data-data yang ada pada file konfigurasi ini. Selanjutnya ada file check, check robots.txt, check sitemap.xml,crawling finished, dan ada file upload yang tertangkap pada uniscan berupa direktori http://192.168.1.3/SIPSO/upload. Kemudian e-mail, external hosts, dan ignored files.

e-ISBN 978-623-93343-0-7
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 28 Januari 2020

Selanjutnya ada tahapan dynamic test pada tahap ini seperti FCKedetior, Timthumb, Backup files, Blind SQL Injection, Local File Include (LFI), PHP CGI Argument Injection, Remote Command Execution, Remote File Include, dan SQL Injection tidak ditemukan kelemahan.

1.1.4 Nessus

Sev	Name	Family	Count
HIGH	Apache 2.4.x < 2.4.39 Multi...	Web Servers	2
MEDIUM	Apache 2.4.x < 2.4.33 Multi...	Web Servers	2
MEDIUM	Apache 2.4.x < 2.4.34 Multi...	Web Servers	2
MEDIUM	Apache 2.4.x < 2.4.35 DoS	Web Servers	2
MEDIUM	Apache 2.4.x < 2.4.38 Multi...	Web Servers	2
MEDIUM	Apache mod_info /server-inf...	Web Servers	2
MEDIUM	Apache mod_status /server-...	Web Servers	2
INFO	Apache HTTP Server Version	Web Servers	2

Gambar 4.18 Kelemahan Apache

Selanjutnya kelamahan yang ditemukan ialah pada Apache kerentanan bypass kontrol akses ada di mod_auth_digest karena kondisi jaringan saat berjalan di server berulir. Penyerang dengan kredensial yang valid dapat mengautentikasi menggunakan nama pengguna lain. (CVE-2019-0217). Dengan mengirimkan frame PENGATURAN dengan ukuran maksimum, koneksi HTTP / 2 yang sedang berlangsung dapat tetap sibuk dan tidak akan pernah habis. Ini dapat disalahgunakan untuk DoS di server. Ini hanya memengaruhi server yang telah mengaktifkan protokol h2. Penyerang jarak jauh yang tidak diautentikasi dapat memperoleh gambaran umum konfigurasi server web Apache jarak jauh dengan meminta URL '/ server-info'. Tinjauan umum ini mencakup informasi seperti modul yang dipasang, konfigurasinya, dan berbagai macam pengaturan waktu berjalan.

Sev	Name	Family	Count
MEDIUM	OpenSSL 1.0.x < 1.0.2o Mul...	Web Servers	2
MEDIUM	OpenSSL 1.0.x < 1.0.2p Mul...	Web Servers	2
MEDIUM	OpenSSL 1.0.x < 1.0.2q Mul...	Web Servers	2
MEDIUM	OpenSSL 1.0.x < 1.0.2r Info...	Web Servers	2
LOW	OpenSSL 1.0.2 < 1.0.2t Mult...	Web Servers	2
INFO	OpenSSL Version Detection	Web Servers	2

Gambar 4.19 Kelemahan SSL

Pada versi OpenSSL yang berjalan pada host jarak jauh adalah 1.0.x sebelum 1.0.2r. Oleh karena itu, ini dipengaruhi oleh kerentanan pengungkapan informasi karena cara yang dapat diuraikan aplikasi menanggapi catatan 0 byte. Penyerang jarak jauh yang tidak diautentikasi dapat mengeksploitasi kerentanan ini, melalui

e-ISBN 978-623-93343-0-7
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 28 Januari 2020

serangan padding oracle, untuk berpotensi mengungkapkan informasi sensitif. Kemudian Sertifikat SSL yang digunakan yaitu sertifikat X.509 tidak dapat dipercaya

1.1.5 Reporting (Laporan)

No	Jenis Serangan	Tools	Keterangan	Status	Koneksi
1	Injection	-	Melakukan injeksi ke halaman korban dengan metode POST dan GET	Tidak Berhasil	-
2	Broken Authentification and Session Management	-	Melakukan login berulang kali dan tidak terblokir	Berhasil	Tidak Login
3	Cross-Site Scripting (XSS)	Vega	Mendapatkan URL yang rentan terhadap serangan XSS	Berhasil	-
4	Insecure Direct Object References	Uniscan	Mendapatkan alamat / URL yang memungkinkan attacker mendapatkan informasi yang tidak seharusnya di akses	Berhasil	Mendapatkan Direktori Database
5	Security Misconfiguration	-	Memanfaatkan aplikasi,web server yang tidak terkonfigurasi	Tidak Berhasil	-
6	Sensitive Data Exposure	-	Memanfaatkan data atau informasi yang tidak di proteksi dengan ekstra	Tidak Berhasil	-
7	Missing Function Level Acces Control	Nessus	Memanfaatkan kelemahan fungsi aplikasi yang tidak di *coding* dengan benar	Berhasil	-
8	Cross-Site Request Forgery (CSRF)		Memaksa masuk menggunakan HTTP palsu	Tidak Berhasil	-
9	Using Known Vulnerable Components	Nikto	Memanfaatkan URL yang rentan untuk mendapatkan hak penuh	Berhasil	Mendapatkan Database
10	Unvalidated Redirects and Forwards	-	Mengarahkan client ke halaman web phising	-	-

Tabel 4.2 Aspek Aplication Security SIPSO Offline

Kajian Aspek Aplication Security ini merupakan hasil dari analisa dan pembahasan peneliti. Solusi dari beberapa kelemahan yang peneliti dapatkan pada penelitian diatas yaitu:

1. Cross-Site Scripting (XSS)
   Solusi dari serangan ini diantaranya melakukan Filtering Menapis masukan dari klien browser dengan mewaspadai karakter-karakter khusus. Karakter-karakter khusus yang harus diwaspadai. Selain menggunakan filtering, melakukan pengkodean karakter yang dinilai membahayakan menjadi karakter yang bisa diabaikan merupakan tujuan dari encoding. Dibandingkan dengan filtering, encoding juga memiliki keuntungan, yaitu tidak mengakibatkan hilangnya data. Kemudian validasi teknik ini dilakukan untuk menjamin hanya input yang tepat yang akan dipilih.
2. Insecure Direct Object References

e-ISBN 978-623-93343-0-7
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 28 Januari 2020

Untuk mengatasinya sebaiknya direct object reference dihilangkan. Bisa diganti dengan temporary mapping value, atau random mapping. Selain itu penting dilakukan validasi terhadap direct object reference dan penerapan Access Control List (ACL).

3. Missing Function Level Acces Control (MFLAC)
   Cara Memproteksi Aplikasi Web dari Kelemahan MFLAC sebaiknya designer/developer aplikasi menerapkan 'best practice' berikut:
   a. Kontrol akses tidak di-hardcode, melainkan di-konfigurasi sehingga dapat di-audit dan didiubah sesuai akses kontrol.
   b. Semua mekanisme harus diset by default adalah false.
   c. Jika suatu fungsi digunakan dalam suatu alur kerja, maka pastikan persyaratannya untuk mengakses fungsi ini ditulis dengan jelas.
4. Unvalidated Redirects and Forwards
   Solusinya yaitu dengan terus melakukan update versi terbaru komponen tersebut dari sisi klien, server dan dependensinya, harus mengetahui vulnerability nya, setelah itu melakukan security assessment test, lalu analisis komponen/library tersebut benar-benar pada saat runtime tidak ada perubahan atau sesuatu hal yang aneh, setelah itu mengidentifikasi semua library dan versi yang digunakan pada aplikasi web tidak hanya database dan versi framework saja, lalu jauhkan semua komponen seperti database publik, mailing list dan lain-lain.

4 Kesimpulan

4.1 Kesimpulan

1. Tidak ditemukannya kelemahannya Injection, Security Misconfiguration, Missing Function Level Acces Control, dan Cross-Site Request Forgery (CSRF).
2. SIPSO masih rentan terhadap serangan Broken Authentification and Session Management, Cross-Site Scripting (XSS), Insecure Direct Object References, Missing Function Level Acces Control, dan Using Known Vulnerable Components

Referensi

[1] Cobantoro, A. F. (2016). UNTUK UJI KERENTANAN WEB SERVER (STUDI KASUS EJURNAL SERVER KAMPUS X MADIUN), (Selisik), 74–79
[2] Iqbaludin. (2018). PENGUJIAN CELAH KEAMANAN PADA WEBSITE CAPTIVE PORTAL DENGAN MENERAPKAN PENETRATION TESTING (Studi Kasus: Teknik Informatika Universitas Pasundan).
[3] Mail, J. (2013). Project WebGoat, Webscarab dan OWASP top10, 2014.
[4] Nurya, D. (2015). Analisis Kemanan Menggunakan Metode Pentest.
[5] Owasp. (2010). OWASP Top 10 - 2010. Open Web Application Security Project (OWASP）.
[6] Siagian, H. P., Akbar, M., & Andri. (2011). VULNERABILITY ASSESSMENT PADA WEB SERVER, (12). [7] Angir, Devi Christiani et al. 2013. "Vulnerability Mapping Pada Jaringan Komputer Di Universitas X."
[8] Deny. 1970. "SEJARAH LINUX."
[9] Dewanto, Adetya Putra. 2018. "PENETRATION TESTING PADA DOMAIN UII.AC.ID MENGGUNAKAN OWASP 10.