BAB IV

METODE PENELITIAN

4.1. Lokasi dan Waktu Penelitian

4.1.1. Lokasi

Riset ini dilaksanakan di Universitas Muhammadiyah Palembang yang beralamat di Jalan, Jendral, Ahmad Yani, 13 Ulu, Seberang Ulu II, Kota Palembang.

4.1.2. Waktu Penelitian

Waktu penelitian ini dilakukan dari tanggal 01 November 2017 sampai tanggal 30 Desember 2017.

4.2. Jenis Data

4.2.1. Data Primer

Menurut Sutabri (2012:3), Data Primer adalah sumber data dalam bentuk ucapan lisan atau tulisan dari pemiliknya sendiri, yaitu orang yang melakukan observasi sendiri. Data yang dikumpulkan dan diolah sendiri atau seorang atau organisasi langsung dari obyeknya. Dalam hal ini data primer diperoleh langsung dari Universitas Muhammadiyah Palembang berupa Password Jaringan Nirkabel UMP dan jumlah website yang dikelola oleh UMP melalui wawancara.

4.2.2. Data Sekunder

Menurut Sutabri (2012:3), Data Sekunder adalah sumber data yang diperoleh bukan dari orang lain yang melakukan observasi melainkan

melalui seseorang atau sejumlah orang lain. Data yang diperoleh dalam bentuk sudah jadi, sudah dikumpulkan dan diolah pihak lain (biasanya sudah dipublikasikan). Data tersebut diperoleh dari Website Universitas Muhammadiyah Palembang (http://www.um-palembang.ac.id) berupa Sejarah singkat, visi dan misi, struktur organisasi serta Pembagian tugas dan wewenang.

4.3. Teknik Pengumpulan Data

Dalam penyusunan penelitian ini penulis mengumpulkan data yang dibutuhkan menggunakan metode pengumpulan data sebaagai berikut :

1. Wawancara (*Interview*)

   Menurut Narbuko (2012:83), Wawancara adalah proses tanya-jawab dalam penelitian yang berlangsung secara lisan dimana dua orang atau lebih bertatap muka mendengarkan secara langsung informasi-informasi atau keterangan-keterangan. Untuk mendapatkan informasi mengenai *website* Universitas Muhammadiyah Palembang, peneliti melakukan wawancara langsung dengan Staff IT di Universitas Muhammadiyah Palembang yang bernama Bapak Taufik.

2. Pengamatan (*Observation*)

   Menurut Narbuko (2012:70), Observasi adalah alat pengumpulan data yang dilakukan cara mengamati dan mencatat secara sistematik gejala-gejala yang diselidiki.

   Data dikumpulkan dengan melihat secara langsung dari objek yang diteliti untuk mengetahui informasi dan kerentanan pada situs Universitas

Muhammadiyah Palembang, objek yang diteliti tentang *website* dan keamanan yang ada pada *website* tersebut.

3. Studi kepustakaan (*Literature*)

   Menurut Afrizal (2015:122), Studi pustaka adalah penyajian hasil bacaan literatur yang telah dilakukan oleh peneliti. Literatur meliputi buku, artikel di jurnal dan makalah seminar. Studi pustaka yang dilakukan penulis adalah pengumpulan data dari bahan-bahan referensi, arsip, jurnal, buku dan dokumen yang berhubungan dengan permasalahan dalam penelitian.

   Data diperoleh melalui studi kepustakaan *(leterature)* yaitu dengan mencari bahan dari *internet*, jurnal dan perpustakaan serta buku yang sesuai dengan obyek yang akan diteliti.

4.4. Metode Penelitian OWASP *Testing* v 4

Pengujian keamanan tidak akan pernah menjadi ilmu pasti dimana daftar lengkap dari semua kemungkinan masalah yang harus diuji dapat didefinisikan. Sebuah pengujian keamanan dapat dikatakan sebagai pengujian yang tepat apabila digunakan dalam situasi dan kondisi tertentu. Tujuan dari proyek ini adalah mengumpulkan semua kemungkinan teknik pengujian, menjelaskan teknik pengujiannya, dan terus memperbarui panduan ini.

Metode OWASP Testing didasarkan pada pendekatan *black box*. Penguji tidak mengetahu apapun atau hanya memiliki sedikit informasi tentang aplikasi yang akan diuji.

Model pengujian terdiri dari:

1. Tester: Siapa yang melakukan aktivitas pengujian
2. Alat dan metodologi: OWASP *Testing* v.4.
3. Aplikasi: Aplikasi yang akan diuji.

Tes dibagi menjadi 2 fase:

1. Passive Mode

Dalam *passive mode,* penguji mencoba memahami logika yang digunakan dalam aplikasi dan bermain dengan aplikasi. Beberapa *Tools* dapat digunakan untuk *Information Gathering*. Sebagai contoh, sebuah HTTP *proxy* dapat digunakan untuk mengamati semua HTTP *Request* dan HTTP *Response.* Di akhir fase ini, penguji harus memahami semua jalur akses (gerbang) ke aplikasi (misalnya, HTTP *header*, *parameter*, dan *cookies*). Pada bagian *Information Gathering* inilah dijelaskan bagaimana melakukan *passive mode testing*.

Sebagai contoh penguji dapat menemukan :

https://www.*target*.com/*login*/*Authentic_Form*.html

Ini mungkin mengindikasikan sebuah *form* otentikasi dimana aplikasi tersebut meminta sebuah *username* dan *password* .

Parameter berikut mewakili dua jalur akses (gerbang) ke arah aplikasi:

https://www.*target*.com/Appx.jsp?a=1&b=1

Dalam kasus ini, aplikasi menunjukkan dua gerbang (parameter a dan b). Semua gerbang yang ditemukan pada fase ini merupakan titik pengujian. Semua jalur akses yang ditemukan akan berguna di fase kedua.

2. Active Mode

Pada tahap ini penguji akan mulai menguji dengan menggunakan metodologi yang dijelaskan sebagai berikut. Pada fase *active mode* terdiri dari 63 control yang masuk kedalam 8 sub kategori standard dan dapat dilihat pada tabel 5.5.

Tabel 5.5: Standar Kontrol Audit OWASP Testing v.4

No	ID Kontrol	Standar Kontrol
1.	***Information Gathering***	
1	OTG-INFO-001	*Conduct Search Engine Discovery & Reconnaissance for Information*
2	OTG-INFO-002	*Fingerprint Web Server*
3	OTG-INFO-003	*Review Webserver Metafiles for Information Leakage*
4	OTG-INFO-004	*Enumerate Applications on Webserver*
5	OTG-INFO-005	*Review Webpage Comments and Metadata for Information Leakage*
6	OTG-INFO-006	*Identify application entry points*
7	OTG-INFO-007	*Map execution paths through application*
8	OTG-INFO-008	*Fingerprint Web Application Framework*
9	OTG-INFO-009	*Fingerprint Web Application*
10	OTG-INFO-010	*Map Application Architecture*
2	***Configuration and Deploy Management Testing***	
1	OTG-CONFIG-001	*Test Application Platform Configuration*

No	ID Kontrol	Standar Kontrol
2	OTG-CONFIG-002	*Test File Extensions Handling for Sensitive Information*
3	OTG-CONFIG-003	*Backup and Unreferenced Files for Sensitive Information*
4	OTG-CONFIG-004	*Enumerate Infrastructure and Application Admin Interfaces*
5	OTG-CONFIG-005	*Test HTTP Methods*
6	OTG-CONFIG-006	*Test HTTP Strict Transport Security*
7	OTG-CONFIG-007	*Test RIA cross domain policy*
8	OTG-CONFIG-008	*Test Network/Infrastructure Configuration*
3	***Identity Management Testing***	
1	OTG-IDENT-001	*Test Role Definitions*
2	OTG-IDENT-002	*Test User Registration Process*
3	OTG-IDENT-003	*Test Account Provisioning Process*
4	OTG-IDENT-004	*Testing Account Enumeration & Guessable User*
5	OTG-IDENT-005	*Testing for Weak or unenforced username policy*
6	OTG-IDENT-006	*Test Permissions of Guest/Training Accounts*
7	OTG-IDENT-007	*Test Account Suspension/Resumption Process*
4	***Authentication Testing***	
1	OTG-AUTHN-001	*Testing for Credentials Transported over an Encrypted*
2	OTG-AUTHN-002	*Testing for default credentials*

No	ID Kontrol	Standar Kontrol
3	OTG-AUTHN-003	*Testing for Weak lock out mechanism*
4	OTG-AUTHN-004	*Testing for bypassing authentication schema*
5	OTG-AUTHN-005	*Test remember password functionality*
6	OTG-AUTHN-006	*Testing for Browser cache weakness*
7	OTG-AUTHN-007	*Testing for Weak password policy*
8	OTG-AUTHN-008	*Testing for Weak security question/answer*
9	OTG-AUTHN-009	*Testing for weak password change or reset functionalities*
10	OTG-AUTHN-010	*Testing for Weaker authentication in alternative channel*
5	***Authorization Testing***	
1	OTG-AUTHZ-001	*Testing Directory traversal/file include*
2	OTG-AUTHZ-002	*Testing for bypassing authorization schema*
3	OTG-AUTHZ-003	*Testing for Privilege Escalation*
4	OTG-AUTHZ-004	*Testing for Insecure Direct Object References*
6	***Session Management Testing***	
1	OTG-SESS-001	*Testing for Bypassing Session Management Schema*
2	OTG-SESS-002	*Testing for Cookies attributes*
3	OTG-SESS-003	*Testing for Session Fixation*
4	OTG-SESS-004	*Testing for Exposed Session Variables*
5	OTG-SESS-005	*Testing for Cross Site Request Forgery*

No	ID Kontrol	Standar Kontrol
6	OTG-SESS-006	*Testing for logout functionality*
7	OTG-SESS-007	*Test Session Timeout*
8	OTG-SESS-008	*Testing for Session puzzling*
7	***Input Validation Testing***	
1	OTG-INPVAL-001	*Testing for Reflected Cross Site Scripting*
2	OTG-INPVAL-002	*Testing for Stored Cross Site Scripting*
3	OTG-INPVAL-003	*Testing for HTTP Verb Tampering*
4	OTG-INPVAL-004	*Testing for HTTP Parameter pollution*
5	OTG-INPVAL-006	*Testing for SQL Injection* *Oracle Testing* *SQL Server Testing* *Testing PostgreSQL* *MS Access Testing* *Testing for NoSQL injection*
6	OTG-INPVAL-007	*Testing for LDAP Injection*
7	OTG-INPVAL-008	*Testing for ORM Injection*
8	OTG-INPVAL-009	*Testing for XML Injection*
9	OTG-INPVAL-010	*Testing for SSI Injection*
10	OTG-INPVAL-011	*Testing for XPath Injection*
11	OTG-INPVAL-012	*IMAP/SMTP Injection*
12	OTG-INPVAL-013	*Testing for Code Injection*

No	ID Kontrol	Standar Kontrol
		Testing for Local File Inclusion
		Testing for Remote File Inclusion
13	OTG-INPVAL-014	*Testing for Command Injection*
14	OTG-INPVAL-015	*Testing for Buffer overflow*
		Testing for Heap overflow
		Testing for Stack overflow
		Testing for Format string
15	OTG-INPVAL-016	*Testing for incubated vulnerabilities*
16	OTG-INPVAL-017	*Testing for HTTP Splitting/Smuggling*
8	***Error Handling Testing***	
1	OTG-ERR-001	*Analysis of Error Codes*
2	OTG-ERR-002	*Analysis of Stack Traces*

Sumber: OWASP Testing Guide v.4 hal.211.

4.5 Metode Pengujian *Penetration Testing*

Uji penetrasi telah menjadi teknik umum yang digunakan untuk menguji keamanan jaringan selama bertahun-tahun. Hal ini juga biasa dikenal dengan pengujian *black box* atau *ethnical hacking*. *Penetration Testing* pada dasarnya "seni" untuk menguji aplikasi yang sedang berjalan dari jarak jauh untuk ditemukan kerentanan keamanannya, tanpa mengetahui cara kerja dalam aplikasi itu sendiri. Biasanya, tim uji penetrasi akan melakukannya memiliki akses ke aplikasi seolah-olah mereka pengguna. Penguji itu bertindak seperti

penyerang dan mencoba menemukan dan mengeksploitasi kerentanan. Banyak kasus penguji akan diberi akun yang valid pada sistem.

Sementara *Penetration Testing* terbukti efektif di jaringan keamanan, teknik ini tidak secara alami menerjemahkan ke aplikasi. Saat pengujian penetrasi dilakukan pada jaringan dan sistem operasi, sebagian besar berusaha terlibat dalam pencarian dan kemudian memanfaatkan kerentanan yang diketahui dalam teknologi tertentu. Seperti aplikasi web yang hampir secara eksklusif dipesan lebih dahulu, *Penetration Testing* di arena aplikasi web lebih mirip dengan penelitian murni. *Penetration Testing Tools* telah dikembangkan dengan proses otomatis , namun dengan sifat efektivitasnya yang biasanya buruk. Banyak orang saat ini menggunakan *Web Application Penetration Testing* sebagai teknik pengujian keamanan utama mereka.