PENETRATION TESTING MENGGUNAKAN OWASP TOP 10 PADA DOMAIN XYZ.AC.ID

PENETRATION TESTING USING OWASP TOP 10 ON DOMAIN XYZ.AC.ID

Alexander Dharmawan[1], Yani Prihati[2], Harto Listijo[3]

[1]Universitas AKI
[2]Universitas AKI
[3]Universitas AKI
[1]alexander.dharmawan@unaki.ac.id, [2]yani.prihati@unaki.ac.id, [3]harto.listijo@unaki.ac.id

Abstrak

Dengan semakin bertambahnya pengguna layanan internet maka semakin banyak informasi yang dapat diperoleh dari internet. Informasi sendiri menjadi hal penting di era digital ini baik untuk organisasi, bisnis maupun individu. Semakin banyak individu memberikan informasi tentang mereka di internet membuat semakin menipisnya privasi yang dimiliki belakangan ini banyak individu yang mulai sadar dengan bagaimana informasi yang mereka berikan dimanfaatkan dan semakin banyak pula organisasi yang mulai memperhatikan resiko keamanan informasi yang dapat memberikan dampak buruk dan kerugian materil terhadap proses bisnis, citra terhadap organisasi, kepercayaan pelanggan serta mempengaruhi hubungan dengan pelanggan atau mitra bisnis mereka
Dalam mengupayakan untuk menjaga keamanan data dan informasi, terdapat sebuah metode yang disebut *penetration tesing. Penetration testing* merupakan serangkaian cara yang dilakukan untuk menguji keamanan pada sebuah sistem. Proses *penetration testing* dengan melibatkan proses analisis kepada sebuah sistem untuk mencari potensi celah keamanan seperti kesalahan konfigurasi sistem, cacat dalam pengembangan *software* maupun *hardware* dan kelemahan dalam logika dari sebuah proses.

Kata kunci : keamanan informasi, *penetration testing*, OWASP TOP 10

Abstract

With the increasing number of internet service users, more and more information can be obtained from the internet. Information itself is important in this digital era for organizations, businesses and individuals. More and more individuals provide information about them on the internet, making their privacy less and more recently, many individuals are starting to become aware of how the information they provide is used and more and more organizations are starting to pay attention to information security risks that can have a negative impact and material loss on the process. business, image of the organization, customer trust and affect relationships with customers or their business partners. In an effort to maintain data and information security, there is a method called penetration testing. Penetration testing is a series of methods used to test the security of a system. The penetration testing process involves an analysis of a system to look for potential security vulnerabilities such as system configuration errors, defects in software and hardware development and weaknesses in the logic of a process.

Keywords: information security, penetration testing, OWASP TOP 10

1. PENDAHULUAN

Penggunaan web terus meningkat, khususnya di Indonesia. Hal ini bisa dilihat dari pengguna internet yang selalu bertambah setiap tahunnya. Menurut Asosiasi Penyelenggara Jasa Internet Indoensia (APJII) ada 210,03 juta pengguna internet dalam negeri pada periode 2021-2022, yang menunjukkan ada peningkatan sebesar 3,32% dari tahun sebelumnya [1].

Dengan bertambahnya pengguna internet, semakin banyak informasi yang bisa didapat dari internet. Informasi menjadi hal yang penting di era digital ini baik untuk keperluan pribadi, organisasi maupun bisnis. Tetapi sayangnya ada oknum-oknum tertentu yang mendapat informasi dengan cara yang tidak sewajarnya. Salah satunya adalah serangan web. Serangan semacam itu dapat terjadi secara dua arah, dari pengguna terhadap situs web, atau sebaliknya. Meskipun lebih umum bagi mereka untuk diterapkan terhadap server web (karena server biasanya memiliki data berharga pada banyak orang, tidak seperti satu pengguna). Insiden ini mencoba mengelabui sistem manajemen basis data untuk mengungkapkan informasi yang dikendalikan [2].

Dalam menjaga keamanan data dan informasi, terdapat sebuah metode yang disebut penetration testing. *Penetration testing* merupakan serangkaian cara yang dilakukan untuk menguji keamanan pada sebuah sistem. Proses *penetration testing* dengan melibatkan proses analisis kepada sebuah sistem untuk mencari potensi celah keamanan seperti kesalahan konfigurasi sistem, cacat dalam pengembangan *software* maupun *hardware* dan kelemahan dalam logika dari sebuah proses[3].

Pada penerapan *penetration testing* pada sebuah *website* , terdapat sebuah standar yang digunakan sebagai panduan dalam melakukan proses analisa keamanan pada sebuah *website* , panduan tersebut adalah OWASP (*Open Web Application Security Project*) TOP 10. OWASP merupakan sebuah organisasi nirlaba yang mempunyai visi untuk menjaga keamanan website dengan banyak menyediakan resource atau sumber daya [4].

Pada penelitian ini, pengujian atau *penetration testing* terhadap website XYZ.AC.ID akan dilakukan berdasarkan metode OWASP TOP 10 tahun 2017. Penerapan *penetration testing* ini bertujuan utnuk menemukan celah keamanan yang ada pada website. Hasil dari *penetration testing* dapat digunakan oleh pengelola website untuk memperbaiki celah-celah keamanan yang ada dari pihak yang tidak bertanggung jawab.

2. DASAR TEORI /MATERIAL DAN METODOLOGI/PERANCANGAN

2.1 Tinjauan Pustaka

Menurut penelitian yang berjudul *Pentesting* Dan Analisis Keamanan *Web* PAUD DIKMAS [5], untuk melakukan pengamanan sebuah *website* perlu diadakan analisa serta pengujian penetrasi untuk menemukan celah pada sebuah *website*. Uji penetrasi dilakukan dengan metode-metode yang dikembangkan oleh para *pentester*. Laporan dari hasil pengujian keamanan *website* diharapkan dapat digunakan bagi para *developer* untuk menutup celah keamanan pada *website* dan mempersempit ruang bagi para pihak yang tidak bertanggung jawab untuk membobol keamanan *website*. Pengujian keamanan ini sebaiknya dilakukan secara periodik dan memberikan laporan yang komprehensif.

Dalam peneliitian yang berjudul *Penetration Testing Server* Sistem Informasi manajemen dan *Website* Universitas Kristen Petra [6], disebutkan bahwa dalam melindungi *website* dan *server* dari serangan dari pihak yang tidak bertanggung jawab, maka harus dilakukan sebuah evaluasi terhadap keamanan *website* dan *server* tersebut. Dalam melakukan evaluasi terhadap keamanan *website* dan *server*, maka digunakan sebuah metode *penetration testing* yang akan digunakan untuk menganalisa objek yang dimana berupa *website* dan *server*.

Pada penelitan yang berjudul *Web Application Safety by Penetration Testing* [7], dalam menghadapi banyaknya jenis serangan terhadap sebuah *website* seperti: *SQL Injection, cross site scripting, remote file incluision* dan *local incluision* maka perlu adanya pendekatan dalam mengamankan *website* dari serangan-serangan tersebut. Meskipun pengamanan sebuah *website* dapat dilakukan dengan berbagai cara, namun perlu sebuah metode yang dapat digunakan menjadi landasan dalam melakukan *penetration testing.* Dalam penelitian ini peneliti menjelaskan metode-metode yang digunakan oleh pihak yang tidak bertanggung jawab untuk menjebol keamanan *website*, seperti *SQL Injection, cross site scripting* dan remote *file incluision.*

2.2 Definisi Penetration Testing

Penetration Testing adalah sebuah metode pengujian terhadap sebuah sistem atau jaringan komputer yang bertujuan untuk mengevaluasi keamanan sistem atau jaringan komputer tersebut. Evaluasi dilakukan dengan cara melakukan sebuah simulasi serangan (*attack*) terhadap suatu sistem atau jaringan guna menemukan celah keamanan yang disebabkan oleh kelemahan dari suatu sistem, konfigurasi yang tidak benar atau kelemahan operasional dalam proses teknis. Laporan hasil dari sebuah *penetration testing* akan memberikan masukan terhadap pemelik sistem tentang celah keamanan terhadap sistem mereka yang dapat digunakan sebagai bahan evaluasi dari sistem keamanan komputer yang sedang berjalan guna melakukan penambalan kebocoran celah yang terdapat dalam sistem mereka sehingga dapat segera dilakukan tindakan pencegahaan lebih dini [3].

2.3 OWASP

OWASP (*Open Web Application Security Project*) adalah komunitas terbuka yang mendedikasikan untuk membuat sebuah organisasi yang bertujuan untuk mengembangkan, membeli, dan memelihara aplikasi yang terpercaya. Di OWASP pengunjung akan menemukan semua gratis dan terbuka. Seluruh tools, dokumen, forum, dan cabang OWASP bebas dan terbuka bagi semua orang yang tertarik memperbaiki aplikasi keamanan. OWASP mendukung pendekatan keamanan aplikasi sebagai masalah perseorangan, proses, dan masalah teknologi karena pendekatan paling efektif terhadap keamanan aplikasi membutuhkan perbaikan diseluruh area. OWASP adalah jenis organisasi baru yang bebas dari tekanan komersial sehingga memungkinkan untuk memberikan informasi terkait keamanan aplikasi yang tidak bias, praktis, dan efektif biaya. OWASP tidak terafiliasi dengan perusahaan teknologi manapun, meskipun OWASP mendukung penggunaan teknologi keamanan komersial. Serupa dengan banyak proyek *software open-source*, OWASP menghasilkan beragam jenis materi dengan cara kolaborasi dan terbuka. Yayasan OWASP merupakan lembaga non-profit yang memastikan kesuksesan jangka panjang proyek. Hampir semua yang terasosiasi dengan OWASP adalah sukarelawan[8].

2.4 OWASP Top 10

OWASP Top 10 atau yang biasa disebut OWASP10 adalah sebuah daftar yang dirilis oleh komunitas OWASP yang berisikan 10 daftar teratas celah keamanan yang dapat mengancam keamanan suatu website daftar ini terus berkembang dan berubah-ubah mengikuti perkembangan teknologi website yang terus berkembang. OWASP Top 10 pertama kali dirilis tahun 2003 lalu *update minor* pada tahun 2004 , 2007, 2010 dan 2017 (OWASP, 2018). OWASP Top 10 sendiri dibuat dengan tujuan untuk meningkatkan kesadaran tentang keamanan aplikasi dengan mengidentifikasi beberapa risiko celah keamanan yang sering dihadapi atau ditemui dalam banyak kasus.

Dalam versi yang terbaru, OWASP Top 10 2017[4] memberikan beberapa perubahan dalam struktur pengujian keamanan yang disarankan, beberapa saran pengujian tersebut adalah :

A. Injection

Injection yang dimaksud pada poin ini adalah celah keamanan seperti SQL , NoSQL, OS dan LDAP Injection. Hal ini terjadi ketika data yang tidak bisa diverifikasi asalnya dikirim menuju sebuah intepreter menjadi dalam bentuk perintah atau *query*. Data yang dikirim oleh penyerang dapat menipu intepreter untuk menjalankan perintah-perintah yang tidak diinginkan atau digunakan untuk mengakses data-data yang ada tanpa menggunakan otentikasi yang benar.

B. Broken Authentication

Fungsi yang terdapat di dalam aplikasi yang berhubungan dengan otentikasi dan manajemen sesi, sering tidak diimplementasikan dengan benar. Hal ini memungkinkan para penyerang untuk melakukan eksploitasi pada *password, keys* atau *session token* yang digunakan untuk masuk kedalam sistem dengan identitas dari *user* yang ada baik secara sementara ataupun secara permanen.

C. Sensitive Data Exposure

Sensitive data exposure yang dimaksud disini adalah data-data sensitif milik para pengguna website, seperti data keuangan, data kesehatan maupun identitas pribadi. Para pihak yang tidak bertanggung jawab dapat menggunakan data ini untuk berbagai macam penipuan.

D. XML External Entities

Beberapa website yang masih menggunakan XML untuk menangani dokumen dapat digunakan oleh para penyerang untuk mendapatkan informasi dari *website* seperti *port* yang ada pada *server website, file internal,* mengeksekusi perintah pada server dan *denial of service*.

E. Broken Access Control

Batasan dalam suatu pengguna dalam mengakses sebuah menu atau informasi kadang tidak diatur dengan baik. Para penyerang dapat mengubah hak akses mereka sehingga para penyerang dapat mengakses informasi yang memerlukan hak akses tinggi, seperti menambah pengguna dan melihat informasi sensitif.

F. Secority Misconfiguration

Kesalahan dalam konfigurasi sistem dapat berupa pesan error dari aplikasi, HTTP header yang tidak terenkripsi ataupun pengaturan default yang tidak aman dari sebuah sistem.

G. Cross-Site Scripting (XSS)

Cross-Site Scripting dapat terjadi ketika sebuah aplikasi tidak memiliki filter terhadap kiriman yang dilakukan oleh pengguna. *XSS* memungkinkan penyerang untuk menjalankan perintah dalam skrip *javascript* untuk melakukan *deface* pada sebuah *website* atau mengalihkan pengguna lainnya menuju *website* yang berbahaya.

H. Insecure Deserialization

Insecure Deserialization dapat terjadi ketika aplikasi membaca sebuah *string* dan tidak melakukan filter terhadapnya sehingga aplikasi mengeksekusi *string* tersebut sebagai perintah. *Insecure Deserialization* dapat berujung kepada serangan *privilidge escalation* maupun i*njection*.

I. Using Components with Known Vulnerabilities

Komponen yang digunakan dalam membangun sebuah aplikasi seperti *framework, library* dan modul lainnya berjalan pada level hak akses yang sama dengan aplikasi yang dibangun. Jika terdapat sebuah komponen dari aplikasi tersebut yang diketahui memiliki celah keamanan , maka penyerang dapat memanfaatkan celah tersebut untuk menyerang sistem.

J. Insufficient Logging and Monitoring

Catatan dari berjalannya sistem sangat diperlukan untuk analisa bila terjadi adanya serangan pada aplikasi. Terkadang catatan *log* dari sebuah aplikasi tidak diatur dengan baik sehingga tidak mencatat apapun saat terjadi serangan.

2.5 Metodologi

Berikut ini adalah tahapan penelitian yang dilakukan dengan judul "Penetration Testing menggunakan OWASP TOP 10 pada Domain xyz.ac.id" :

Gambar 1. Alur Penelitian

Pada tahapan ini, *penetration testing* dengan metode OWASP TOP 10 dilakukan dengan beberapa tahapan, yaitu :

1. *Footprinting*
   Tahap awal yang dilakukan adalah mengumpulkan segala informasi mengenai *website* yang memiliki domain xyz.ac.id yang akan dilakukan *penetration testing*.
2. *Scanning*
   Setelah mendapatkan segala informasi mengenai *website* target, proses selanjutnya adalah melakukan proses *scanning*. Proses *scanning* ini dilakukan untuk mencari *port* atau celah keamanan yang ada pada *website* yang dapat disusupi.
3. Uji keamanan *website*
   Melakukan pengujian pada website yang memiliki domain xyz.ac.id menggunakan metode OWASP TOP 10.
4. Pembuatan laporan hasil pengujian
   Laporan berisi penjabaran dan penjelasan dari hasil pengujian yang telah dilakukan menggunakan metode OWASP TOP 10 disertai solusi untuk celah keamanan yang ditemukan.

3. PEMBAHASAN

Dari proses scanning yang dilakukan kepada domain XYZ.AC.ID didapat informasi sebagai berikut :

3.1. *Footprinting*

Proses *footprinting* dilakukan untuk melakukan identifikasi terhadap arsitektur yang ada pada sebuah sistem. Hasil dari proses *footprinting* ini digunakan untuk menemukan celah keamanan yang sudah diketahui pada arsitektur sistem tersebut.

Tool yang digunakan untuk melakukan *footrprinting* adalah subdomain finder, nmap dan WhatCMS. Hasil dari proses *footprinting* dapat dilihat pada bagian dibawah ini.

Tabel 1. *Footprinting* Server

IP Address Server	Service	Version / Service Name	Port
182.253.60.106			
	FTP	Pure-FTPd	21
	DNS	-	53
	Web server	Microsoft ISA Server http	80

		proxy	
	Web server	Microsoft Terminal Services	3389
	SSH	OpenSSH 5.3	7777
	Web Server	Apache httpd 2.2.15	8080
216.58.215.51			
	DNS	Generic DNS	53
	Web server	Google HTTPd	80
	Web server	-	443

Tabel 2. *Footprinting* Subdomain

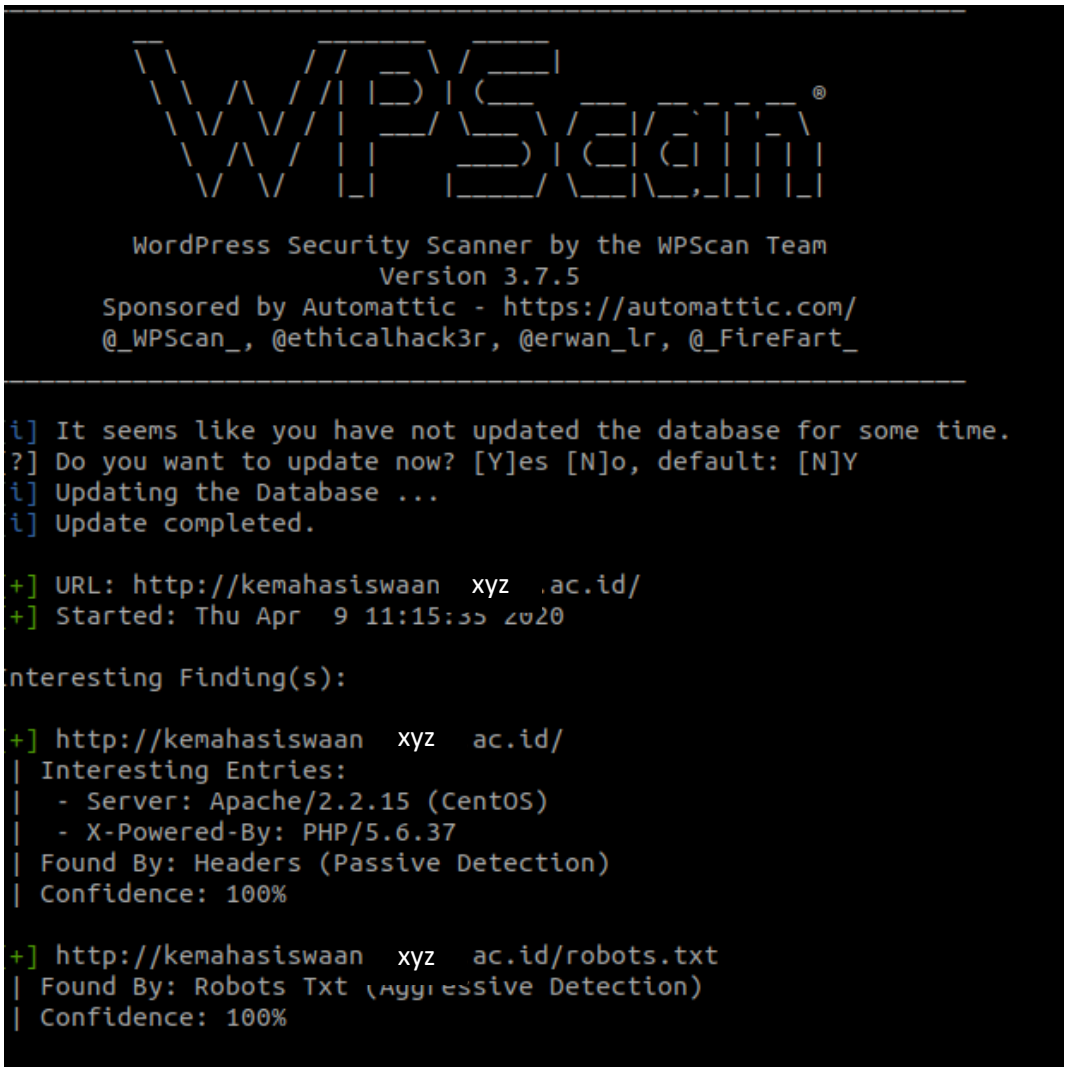
Alamat Subdomain	**IP Address**
alumni.xyz.ac.id	182.253.60.106
fbb.xyz.ac.id	182.253.60.106
iasol.xyz.id	182.253.60.106
kemahasiswaan.xyz.ac.id	182.253.60.106
mail.xyz.id	216.58.215.51
maingtw.xyz.ac.id	182.253.60.106
perpustakaan.xyz.ac.id	182.253.60.106
www.xyz.ac.id	182.253.60.106
student.xyz.ac.id	182.253.60.106

Tabel 3. *Footprinting* CMS Detection

Alamat Subdomain	**Programming Language**	**Versi CMS**
alumni.xyz.ac.id	PHP	Wordpress 4.4.19
fbb.xyz.ac.id	PHP	-
iasol.xyz.id	PHP	Wordpress 4.4.19
kemahasiswaan.xyz.ac.id	PHP	Wordpress 5.0.8
mail.xyz.id	Java	-
maingtw.xyz.ac.id	PHP	Wordpress 4.4.19
perpustakaan.xyz.ac.id	PHP	-
www.xyz.ac.id	PHP	Joomla
student.xyz.ac.id	PHP	Wordpress 4.4.19

3.2. *Vulnerability Scanning*

Proses *vulnerability scanning* dilakukan untuk melakukan deteksi terhadap celah keamanan yang ada berdasarkan hasil *footprinting* yang telah dilakukan pada tahap *footprinting*. Berdasarkan hasil dari tahap *footprinting*, terdapat 3 versi Content Management System yang digunakan pada website XYZ, yaitu Wordpress, Joomla dan CMS yang tidak dapat terdeteksi. Untuk melakukan proses *vulnerability scanning* pada CMS yang berbasis Wordpress, maka digunakan tool yang bernama WPScan, sedangkan untuk CMS Joomla dan CMS yang tidak terdeteksi, akan digunakan tool OWASP ZAP.



Gambar 2. Proses Vulnerability Scanning dengan WPScan

3.3 *Penetration Testing*

Pada tahapan ini dilakukan pengujian terhadap kemungkinan celah keamanan yang ada

a. SQL Injection

Pada proses *vulnerability scanning* ditemukan beberapa celah SQL injection, untuk daftar subdomain yang memiliki celah sql injection dapat dilihat pada tabel di bawah ini.

Tabel 4. Celah *SQL Injection*

Subdomain
perpustakaan.xyz.ac.id
student.xyz.ac.id
maingtw.xyz.ac.id

Proses pengujian SQL injection pada CMS Wordpress tidak bisa dilakukan karena celah keamanan menggunakan plugin yang tidak bisa didapatkan. Sedangkan pada situs yang menggunakan framework PHP, menunjukkan hasil false positive, dimana pada hasil scan

menunjukkan bahwa terdapat celah keamanan, tetapi saat dilakukan penetration test, celah keamanan tersebut tidak terbukti.

b. Cross Site Scripting

Pada proses *vulnerability scanning* ditemukan beberapa celah *Cross Site Scripting*, untuk daftar subdomain yang memiliki celah sql injection dapat dilihat pada tabel di bawah ini.

Tabel 5. Celah keamanan *Cross Site Scripting*

Subdomain
perpustakaan.xyz.ac.id
student.xyz.ac.id
maingtw.xyz.ac.id

Untuk melakukan pengujian celah keamanan *cross site scripting*, menggunakan simulasi wordpress dengan versi yang sama dikarenakan untuk melakukan pengujian, harus masuk kedalam sistem tersebut.

Pengujian yang dilakukan berdasarkan *vulnerability* yang ditemukan adalah, menambah sebuah post baru dan menambahkan payload cross site scripting vector pada shortcode yang ada pada wordpress, payload yang digunakan adalah "'"><img src=1 onerror=prompt(1)>". Ketika ada pengunjung atau korban yang mengakses ke halaman tersebut maka *payload* akan tereksekusi.

c. Sensitive Data Exposure

Pada proses *vulnerability scanning* ditemukan beberapa celah *sensitive data exposure*, untuk daftar subdomain yang memiliki celah *sensitive data exposure* dapat dilihat pada tabel di bawah ini.

Tabel 6. Celah Keamanan *Sensitive Data Exposure*

Subdomain	Username
student.xyz.ac.id	alumniadmin
kemahasiswaan.xyz.ac.id	mahasiswa
maingtw.xyz.ac.id	alumniadmin

3.4. Pembahasan

Dapat dilihat pada tabel diatas, penelitian yang telah dilakukan pada website XYZ memiliki perbedaan hasil dengan beberapa penelitian yang telah ada. Perbedaan hasil terjadi dikarenakan terdapat perbedaan pada framework yang digunakan pada sebuah website, teknik pemrogramman dan bahasa pemrograman yang digunakan.

Dari hasil scanning yang telah dilakukan pada proses sebelumnya ditemukan bahwa 3 website target terdapat beberapa celah keamanan yang dapat membahayakan keamanan web yang dikelola oleh XYZ sehingga perlu segera dilakukan tindakan pencegahaan lebih dini dan rata-rata kemungkinan celah keamanan yang ditemukanpada hasil scanning menggunakan aplikasi WPScan dan OWASP Zap terdeteksi pada *plugin* yang terdapat dalam web. Kebanyakan *plugin* belum dilakukan pembaruan oleh pengelola sehingga terdapat *query* tertentu yang terindikasi sebagai celah keamanan oleh aplikasi scanning . Dari hasil scanning menggunakan WPScan dan OWASPZap juga terdapat *false positive* dimana peringatan keamanan yang ditemukan tidak terbukti atau palsu hal ini terjadi karena aplikasi mendeteksi *query* yang

mungkin menjadi ciri-ciri dari sebuah celah keamanan sehingga aplikasi memberikan peringatan. Selain itu juga perlu dilakukan konfigurasi kembali terhadap pengaturan server yang dimiliki 3 web target penelitian karena terdapat celah keamanan yang cukup sensitif. Dari semua proses yang telah dilakukan pada tahap sebelumnya, maka perlu direkomendasikan antara lain:

1. Melakukan update pada framework atau CMS yang ada , beberapa *website* masih menggunakan versi PHP , apache dan CMS Wordpress yang sudah *out of date*, dan memiliki banyak celah keamanan.
2. Menyembunyikan username pada CMS yang berbasis wordpress.
3. Selalu melakukan *vulnerability scanning* secara rutin untuk menjaga keamanan *website* dari segala celah keamanan yang ada.

4. KESIMPULAN

Dalam melakukan uji penetration testing menggunakan metode OWASP10 tahun 2017 yang bertujuan untuk menguji tingkat keamanan pada sistem 3 web yang berdomain xyz.ac.id, berdasarkan dari seluruh kegiatan yang dilakukan maka dapat diambil beberapa kesimpulan yang antara lain sebagai berikut:

a. Metode OWASP10 tahun 2017 masih sangat cocok dijadikan sebagai dasar dalam melakukan uji penetration testing pada 3 web yang berdomain xyz.ac.id. Karena masih ditemukan beberapa celah keamanan yang sesuai dengan daftar OWASP10 tahun 2017
b. Beberapa website pada subdomain xyz.ac.id masih memiliki celah keamanan.

DAFTAR PUSTAKA

[1] APJII, “Profil Internet Indonesia 2022,” 2022.
[2] A. Wibowo, *Keamanan Sistem Jaringan Komputer*. Semarang: Yayasan Prima Agus Teknik, 2021.
[3] A. G. Bacudio, “An Overview Of Penetration Testing,” *Int. J. Netw. Secur. Its Appl.*, vol. 3, 2011.
[4] T. O. Foundation, *OWASP Top 10 - 2017*. .
[5] I. Syarifudin, “Pentesting Dan Analisis Keamanan Web PAUD DIKMAS,” no. Politeknik Negeri Jakarta, 2018.
[6] R. Pangalila, “Penetration Testing Server Sistem Informasi Manajemen dan Website Universits Kristen Petra,” *INFRA*, vol. 3, no. 2, 2015.
[7] A. Hasan, “Web Application Safety by Penetration Testing,” 2018.
[8] M. Meucci, *Release Testing Guide OWASP*.