OPEN ACCESS
LEDGER, VOL. 2, NO. 1, FEB 2023
ISSN: 2963 – 8798 (ONLINE)

LEDGER: Journal Informatic and Information Technology

Analisis Celah Keamanan Pada Website Dengan Menggunakan Metode Penetration Testing Dan Framework Issaf Pada Website SMK Al-Kautsar

Sulis Andriyani*, M. Fajar Sidiq, Bita Parga Zen

Teknik Informatika, Institut Teknologi Telkom Purwokerto, Indonesia
*Corresponding Author: 18102106@ittelkom-pwt.ac.id

Abstract

The utilization of the website as an information system currently provides many conveniences for every community institution. One of them is that at educational institutions the website is used as a medium to convey information. Both in the form of information about school activities, registration, teacher data, and other information related to the school. As is the case with the website of SMK Al-Kutsar Purwokerto. Apart from providing convenience, websites can also have security holes that can harm users such as SQL injection, clickjacking, brute force, XSS, and others. So with that, it is necessary to know the security gaps contained in the information system website. To find out the security holes that exist, researchers use the penetration testing method with the ISSAF framework. After penetration testing, the Al-kautsar Vocational High School website has a vulnerability to DDoS attacks, this is evidenced by DDoS testing using LOIC tools, the result is that the Al-Kautsar Vocational High School website cannot be accessed during the DDoS attack process. This DDoS attack aims to make the server busy with requests from clients. However, this website is protected from XSS attacks, as well as attacks that utilize an open port, namely port 21. On testing XSS and port 21, the author failed to gain access to the website.

Keywords: security holes, penetration testing, websites

Abstrak

Pemanfaatan website sebagai system informasi saat ini memberikan banyak kemudahan bagi setiap lembaga masyarakat. Salah satunya yaitu pada lembaga pendidikan website dimanfaatkan sebagai salah satu media untuk menyampaikan informasi. Baik berupa informasi mengenai kegiatan sekolah, pendaftaran, data guru pengajar, dan informasi lain yang berkaitan dengan sekolah tersebut. Seperti halnya dengan website dari SMK Al-Kutsar Purwokerto ini. Selain memberikan kemudahan, website juga dapat memiliki sebuah celah keamanan yang dapat merugikan pengguna seperti *sql injection*, *clickjacking*, *brute force*, *XSS*, dan lainnya. Maka dengan itu perlu mengetahui celah keamanan yang terdapat dalam website system informasi. Untuk mengetahui celah keamanan yang ada peneliti menggunakan metode penetration testing dengan framework ISSAF. Setelah dilakukan penetration testing, website SMK Al- kautsar memiliki kerentanan terhadap serangan ddos, hal ini dibuktikan dengan pengujian ddos menggunakan *tools* LOIC hasilnya website SMK Al Kautsar tidak bisa diakses selama proses serangan ddos. Serangan ddos ini bertujuan untuk membuat server sibuk dengan permintaan dari *client.* Akan tetapi website ini terhindar dari serangan XSS, serta serangan yang memanfaatkan port yang terbuka yaitu port 21. Pada pengujian xss serta port 21, penulis gagal mendapatkan akses ke dalam website tersebut.

Kata Kunci: celah keamanan, penetration testing, website

I. INTRODUCTION

Dengan adanya kemajuan teknologi saat ini, menjadikan website sebagai salah satu sarana untuk menyampaikan informasi. Contohnya yaitu pada website sistem informasi dari SMK Al-Kautsar. Di dalam

ISSN: 2963 – 8798 (ONLINE)

website tersebut terdapat informasi seperti profil SMK Al-Kautsar, sejarah sekolah, fasilitas yang disediakan, fasilitas sekolah, data guru, informasi terkait pendaftaran online, ektrakulikuler, dan informasi lainnya. SMK Pesantren Al kautsar Purwokerto adalah lembaga Pendidikan yang masih termasuk dalam Yayasan Al-Hidayah Karangsuci Purwokerto, Sekolah ini terletak di dalam Pondok Pesantren Al-Hidayah Karangsuci Purwokerto, SMK Al-Kautsar memiliki dua program keahlian yaitu Perbankan Syari'ah (PBS) serta Teknik Komputer dan Jaringan (TKJ)[2].

System informasi berbasi website ini banyak memberikan manfaat serta kemudahan bagi penggunanya. Akan tetapi tidak dapat dihindari bahwa sebuah website dapat terhindar dari ancaman yang dapat menyerang system keamanan yang dapat mengakibatkan kerugian. Ada beberapa ancaman yang mungkin dapat terjadi diantaranya *clickjacking, sql injection, XEE, XSS, brute force,* dan lainnya. Dengan adanya hal itu perlu dilakukan pengujian terhadap system keamanan website. Salah satu pengujiannya yaitu dengan menggunakan metode *penetration testing*. Penetration testing merupakan sebuah simulasi serangan yang terkendali dengan tujuan untuk melakukan identifikasi kerentanan terhadap aplikasi, jaringan, dan cabang system informasi [3]. Hal ini dilakukan agar jika terdapat celah keamanan, maka akan dapat teridentifikasi serta ditangani lebih awal sebelum celah tersebut dimanfaatkan oleh orang yang tidak bertanggung jawab. Peneliti menggunakan *lawful pentest,* yang mana peneliti telah mendapatkan izin dari pihak sekolah untuk melakukan pengujian terhadap website SMK Al Kautsar Purwokerto. Untuk melakukan pengujian ini ada beberapa *framework* yang bisa digunakan, salah satunya yaitu *framework The Information System Security Assessment* (ISSAF). ISSAF merupakan kerangka terstruktur yang mengkategorikan penilaian keamanan system informasi dalam berbagai domain dan rincian kriteria [4]. Dalam menggunakan *framework* ISSAF ini memiliki tiga fase pendekatan diantaranya adalah fase *planning and preparation,* fase *assessment,* dan fase *reporting.*

II. LITERATURE REVIEW

A. Penelitian Terkait

Penelitian ini mengacu pada beberapa hasil penelitian sebelumnya diantaranya, penelitian[3] melakukan *penetration testing* pada website pendaftaran *online* dari SMKN 1 Cibatu. Penelitian ini menggunakan metode *Penetration Testing Execution Standard* (PTES). Hasil yang didapat dari penelitian ini ditemukan kerentanan seperti *Cross Site Scripting, Cross Site Request Forgery,* dan *Eavesdropping* yang dapat berakibat kebocoran data.

Penelitian[1] melakukan *penetration testing* untuk mendeteksi celah keamanan pada website system informasi kampus. Penelitian ini menggunakan beberapa domain yang berbeda dari kampus. Hasilnya terdapat dua alamat website yang celahnya memiliki tingkat sedang dan rendah. Serta ditemukan beberapa celah lain yang dapat mengakibatkan terjadinya memanipulasi file, mengganggu kinerja server, *clickjacking,* serta *cross site request forgery.*

Penelitian[5] menggunakan metode *penetration testing* untuk mengetahui celah keamanan website dapodik (data pokok pendidikan). Penetian ini menggunakan teknik serangan *sql injection.* Hasilnya aplikasi dapodik tidak dapat diserang menggunakan teknik *sql injection* serta tingkat ancaman berada pada level 0 atau aman. Serta belum ditemukannya celah yang memungkinkan terjadinya ancaman dan akses illegal yang berpotensi merusak sistem.

Penelitian[6] penelitian ini dilakukan untuk evaluasi keamanan website lembaga X yang menjadi lembaga pemilihan umum. Penelitian ini menggunakan metode *penetration testing* serta menggunakan *framework* ISSAF. Hasil dari penelitian ini yaitu ditemukan keamanan yang berbahaya seperti SQL *injection,* dan XSS pada website serta port TCP yang terbuka pada website lembaga X.

Penelitian[7] dilakukan pada webserver system informasi akademik suatu perguruan tinggi. Penelitian ini dilakukan karena seringnya terjadi permasalahn seperti *hacking system,* dirubah file index hingga meng injectkan file backdoor dalam sistem, dan serangan yang terus menerus pada website akademik. Hasil dari penelitin ini yaitu didapatkan tiga kategori level hight, medium, dan low. Bagian yang dilakukan penyeranga yaitu pada port 22 mengenai ssh. Dan terdapat bug pada sistem yang dapat dimanfaatkan penyerang sebagai celah keamanan.

B. Website

Website adalah salah satu media informasi yang ada di internet. Website sendiri mempunyai pengertian yaitu sebutan dari kumpulan halaman web yang merupakan bagian dari nama domain atau

ISSN: 2963 – 8798 (ONLINE)

subdomain di World Wide Web (WWW). Sebuah halaman web adalah sebuah dokumen yang ditulis dalam format html yang dapat diakses melalui http atau https. Halaman dari situs web dapat diakses melaui URL yang disebut beranda. Web dapat dibuka dengan browser baik pada komputer maupun smartphone. Diantaranya seperti mozilla, internet explorer, firefox, opera, google chrome, dan lain-lain. [8]

C. Web Server

Menurut Effendi Yusuf, web server adalah perangkat lunak yang menyediakan layanan data berfungsi untuk menerima permintaan Hypertext Transfer Protocol (HTTP) oleh pengguna dan mengirimkan kembali hasilnya dalam baik berupa teks, gambar, animasi, dan video [9]. Selain berfungsi untuk mengolah data, webserver juga berfungsi untuk mengirimkan data baik dalam bentuk foto, video, dan teks sesuai dengan permintaan dari client.

D. System Informasi

Menurut Jogiyanto (2009) sistem informasi adalah sistem dalam organisasi yang memproses transaksi sehari-hari, mendukung operasi, manajemen dan aktivitas strategi organisasi serta memenuhi kebutuhan penyediaan informasi spesifik, bersama dengan laporan yang diperlukan kepada pihak eksternal [10]. Sistem informasi adalah sistem yang menggabungkan aktivitas manusia dan teknologi untuk kegiatan manajemen serta operasional. Tujuan dari sistem informasi adalah untuk menciptakan produk yang berisi kumpulan informasi. Sistem informasi bisa berupa website, aplikasi, blog.

E. Keamanan Jaringan

Keamanan jaringan adalah pendekatan untuk mengendalikan sumber daya jaringan. Tujuan dari pengontrolan akses jaringan yaitu supaya jaringan tersebut hanya bisa diakses oleh pihak tertentu yang memiliki hak untuk mengaksesnya [5].

F. *Cyber Attack*

Cyber attack adalah serangan yang dapat terjadi dalam dunia maya baik yang ditunjukkan untuk melakukan serangan atau pertahanan yang mengakibatkan terjadinya kerusakan pada objek yang dituju [11]. Ada banyak cyber attck yang dapat menyerang sebuah website, diantaranya yaitu sql injection (teknik hacking dimana penyerang memasukkan perintah sql melalui url untuk dieksekusi oleh database), remote code/command execution (jenis serangan dimana penyerang melakukan eksekusi kode dari jarak jauh), cross site scripting attacks (merupakan serangan yang dilakukan dengan cara penyerang memasukkan kode pemrograman tertentu ke dalam situs tersebut), dan banyak lagi jenis cyber attack lainnya [12].

G. *Penetration Testing*

Penetration testing atau uji penetrasi adalah sebuah upaya untuk mengetahui kelemahan dari sistem informasi dengan tujuan agar sistem informasi tersebut lebih aman dengan secara legal dan berwenang [13]. Penetration testing merupakan suatu kegiatan berupa simulasi yang dilakukan oleh pihak yang sudah memiliki ijin untuk melakukan eksploitasi suatu sistem berdasarkan celah keamanan yang ada. Penetration testing berbeda dengan hacking, dimana kegiatan hacking tidak memiliki ijin untuk melakukan serangan terhadap sistem tersebut. Tujuan dari penetration testing adalah untuk mengidentifikasi kerentanan dalam sistem keamanan. Pengujian penetrasi dapat digunakan untuk pengujian kebijakan keamanan sistem yang terdapat pada perusahaan atau organisasi untuk melakukan identifikasi dan penanganan jika masalah tersebut mengancam keamanan sistem[6]. Proses penetration testing terdiri dari pengumpulan informasi, identifikasian celah-celah keamanan, dan melakukan pelaporan terhadap hasil dari pengujian yang dilakukan.

H. ISSAF (*Information Sistem Security Assessment Framework*)

ISSAF (*Information Sistem Security Assessment Framework*) adalah framework yang penggunannya terarah dan terdiri dari langkah dalam pengelompokkan informasi, penilaian dan laporan hasil pengujian sistem keamanan terhadap domain yang diuji serta melakukan Analisa terhadao hasilnya[14]. Dalam ISSAF ini memiliki tiga fase pendekatan, diantaranya adalah sebagai berikut:

1. Fase *planning and preparation*

ISSN: 2963 – 8798 (ONLINE)

Tahapan awal yang terdiri dari persiapan serta pengumpulan informasi dari web target yang akan dilakukan *penetration testing* [15].

2. Fase *Assessment*

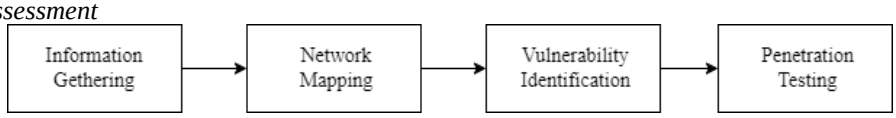

Fig.1. Fase *Assesment*

Langkah pengujian pada sistem informasi yang terdiri dari empat langkah yaitu:
Berikut adalah penjelasan dari masing-masing langkah pada gambar diatas:

a. *Information Gathering*
   Pengumpulan informasi umum terkait sistem informasi target seperti alamat ip, informasi domain, email, dan lain-lain.
b. *Network Mapping*
   Tahap ini dilakukan untuk mengetahui informasi seperti nama port, jenis, serta versi port yang terbuka.
c. *Vulnerability Identification*
   Yaitu mengidentifikasi kerentanan atau kelemahan pada sistem informasi target.
d. *Penetration Testing*
   Yaitu dengan melakukan pengujian terhadap sistem keamanan target [16].

3. Fase Reporting
   Pada fase ini yaitu membuat laporan dari hasil yang sudah didapatkan dari fase sebelumnya.

I. Kali Linux

Linux adalah sistem operasi yang bersifat terbuka atau open source, yang memiliki arti bahwa sistem operasi ini dapat dikembangkan oleh siapa saja . Sistem operasi ini diciptakan oleh Linus Benedict Torvolds, yang mana beliau ini adalah seorang hacker. Kali linux merupakan salah satu jenis linux. Kali linux banyak digunakan untuk penetration testing baik terhadap website maupun jaringan komputer. Kali linux ini dikembangkan oleh Offensive Security [12].

J. Virtual Box

Virtualbox adalah sebuah program open source yang berkaitan dengan virtualisasi. Virtualisasi sendiri merupakan sebuah teknologi yang bisa digunakan oleh pengguna untuk memiliki komputer beserta dengan sistem operasi yang seoalah-olah seperti nyata[17]. Virtualbox dikeluarkan oleh innotec GmbH yang kemudian dibeli oleh Sun Microsistems pada tahun 2008 yang sekarang dikembangkan oleh Oracle. Perangkat lunak ini diinstall dalam sistem operasi utama sebagai sebuah aplikasi. Yang mana aplikasi ini dapat memungkinkan sistem operasi utama untuk menginstall sistem operasi tambahan pada host OS, masing-masing dikenal dengan istilah Guest OS.

K. OWASP ZAP

Owasp zap merupakan sebuah tools untuk membantu mendeteksi kerentanan keamanan pada web application. Menurut website resmi Owasp zap, Owasp zap didefinisikan sebagai komunitas terbuka yang memungkinkan untuk bisa dikembangkan oleh masing-masing individua tau organisasi. Owasp zap dapat diinstall dalam berbagai jenis sistem operasi seperti windows, linux, maupun macOs.

L. Jenis-Jenis Serangan

1. Serangan DDos (Denial of Service)
   DDoS merupakan sebuah serangan yang bekerja dengan cara membajiri permintaan dari pengguna ke sumber daya server. Hal ini bertujuan agar server tidak mampu untuk menangani banyaknya permintaan pengguna. Sehingga server tidak dapat bekerja dengan benar [18].
2. Serangan Brute Force
   Serangan brute force merupakan teknik serangan pada sebuah sistem keamanan komputer yang dilakukan dengan cara melakukan percobaan terhadap semua kunci yang memunyai kemungkinan benar [19]. Brute force ini digunakan untuk melakukan pembobolan akses ke suatu host (server/network/workstation) atau terhadap data yang terenkripsi. Brute force ini banyak dipakai oleh penyerang untuk mendapatkan akun secara tidak sah. Serangan brute force ini akan memakan banyak waktu apabila suatu pengguna menggunakan kombinasi password yang sulit untuk ditebak.

ISSN: 2963 – 8798 (ONLINE)

Lama tidaknya serangan ini bergantung pada tingkat kerumitan pengguna dalam membuat password. Semakin rumit paswordnya maka akan semakin lama waktu yang dibutuhkan penyerang.

3. Serangan Clickjacking
   Adalah jenis serangan yang terjadi pada aplikasi berbasis website. Serangan ini akan membuat korbannya secara tidak sengaja mengklik sebuah elemen pada halaman web yang seharusnya tidak ingin diklik. Serangan ini biasanya dilakukan dengan memanipulasi tampilan halaman website.
4. Serangan SQL Injection
   SQL sendiri merupakan kepanjangan dari Structured Query Language. SQL adalah sebuah bahasa tingkat empat yang mempunyai fungsi untuk menampilkan hasil atau melakukan sesuatu terhadap data yang tidak diinginkan. Sedangkan SQL injection merupakan sebuah teknik hacking yang memiliki tujuan untuk menyusup ke dalam sistem agar bisa mengetahui isi dari database sebuah website. Serangan ini terjadi karena terdapat sebuah kode program lemah serta keamanan yang kurang dari pengelola website [20].

III. RESEARCH METHOD

Pada penelitian ini, peneliti menggunakan metode *penetration testing* untuk melakukan pengujian pada website SMK Al Kautsar Purwokerto. Berikut adalah Langkah-langkah yang dilakukan saat pengujian *penetration testing* pada gambar dibawah ini.

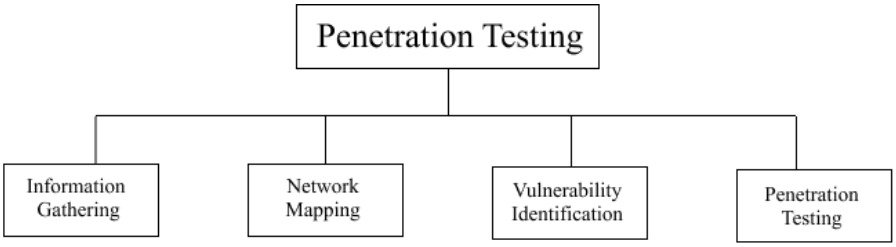

Fig.2. Tahapan *Penetration Testing*

Pada tahapan *information gathering* berguna untuk mencari informasi yang berkaitan dengan website target. Seperti informasi mengenai alamat ip yang dapat diketahui dengan menggunakan terminal pada kali linux. Informasi mengenai dns target dengan menggunakan *tools* dnscan, informasi detail mengenai website dengan *tools* whatweb, serta informasi mengenail email yang terkandung dalam website target menggunakan *tools* infoga. Tahap *network mapping* dilakukan untuk mengetahui jenis, nama, serta versi dari port yang terbuka dari website target yang memiliki kemungkinan untuk dilakukan serangan. Untuk mengetahui jenis port yang terbuka dengan menggunakan *tools* nmap. *Vulnerability testing* dilakukan untuk mengidentifikasi celah yang ada pada website target. Untuk mengetahui celahnya, penelti menggunakan *tools* owasp zap. Setelah mendapatkan informasi mengenai website target dan celah yang ada, peneliti melakukan tahap penetrasi. Tahap ini dilakukan dengan mencoba melakukan serangan pada website target. Serangan yang dilakukan yaitu berupa serangan *sql injection*, dimana untuk melakukan serangan ini penulis menggunakan *tools tools* yang bernama sqlmap. Serangan yang kedua yaitu serangan ddos dengan menggunakan *tools* LOIC. Serangan yang selanjutkan yaitu serangan dengan memanfaatkan port 21, serangan dilakukan dengan menggunakan Metasploit. Serangan yang terakhir yaitu dengan menggunakan teknik *brute force* untuk mengetahui username serta password masuk ke dalam akun webhosting website target. Serangan ini menggunakan *tools* yang bernama hydra. Setelah melakukan tahapan *penetration testing*, peneliti melakukan pengumpulan data dari hasil yang didapat saat pengujian terhadap website target. Dan dari data yang terkumpul, peneliti akan menganalisis hasil yang didapat dari pengujian.

IV. RESULTS AND DISCUSSION

Dalam hal ini peneliti melakukan pengujian pada website smk-alkautsar.sch.id menggunakan framework ISSAF dengan langkah-langkah pengujian sebagai berikut:

A. Information Gathering

1. Mendapatkan Ip Target

ISSN: 2963 – 8798 (ONLINE)

Untuk mendapatkan alamat ip pada website smk-alkautsar.sch.id ini dengan menggunakan tools terminal yang berada di Kali Linux. Dengan mengetikkan perintah ping smk-alkautsar.sch.id dan didapatkan bahwa alamat ip yang digunakan pada website ini adalah 1*1.2*1.44.2*6. Alamat ip ini dapat digunakan untuk mengakses website dari smk-alkautsar.sch.id.

2. Mendapatkan Informasi Target

Untuk mendapatkan informasi lainnya, peneliti menggunakan *tools* bernama whois. Untuk menggunakan *tools* tersebut dengan mengetikkan perintah whois 1*1.2*1.44.2*6. Berikut adalah hasil yang didapatkan pada Table 1 dibawah ini.

TABLE I
INFORMASI LAIN WEBSITE

Nama	Eko Junaedy
Nama perusahaan	PT. Jupiter Jala Arta
Alamat	Gedung Cyber One Lantai 10 Jl. Kuningan Barat No.8 Jakarta 12710
Email	ej@jalanet.co.id
No. HP	+6221xxxxxxxx

Hasil dari pengujian menggunakan *tools* whois, penulis mendapatkan informasi berupa nama, nama perusahaan penyedia layanan website, alamat, email, serta no hp.

3. SSL (*Secure Socket Layer)*

Untuk pengujian ssl ini, peneliti menggunakan *tools* sslscan dengan mengetikkan perintah sslcan smk-alkautsar.sch.id. Berikut adalah gambar dari perintah serta hasil yang didapat dari pengujian SSL ini.

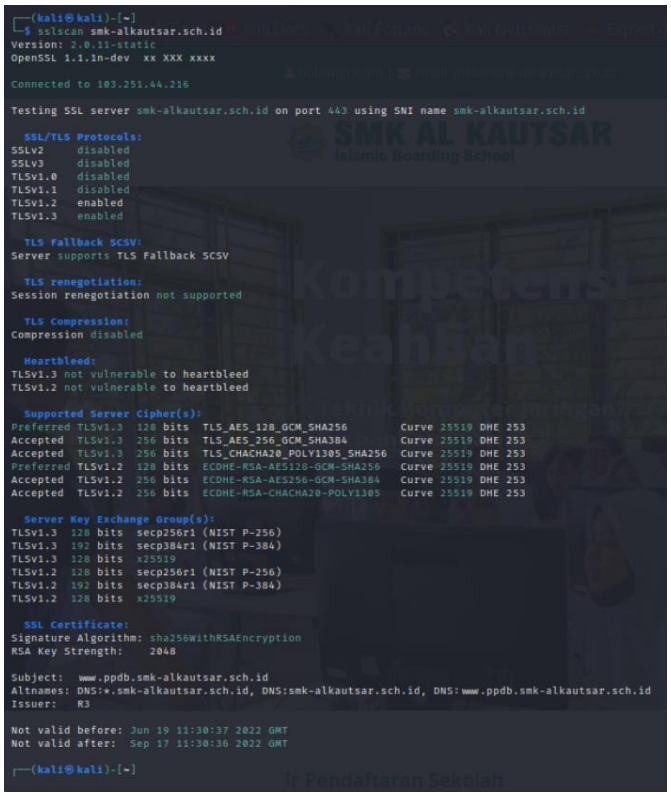

Fig.3. Perintah serta hasil dari pengujian SSL menggunakan sslscan

ISSN: 2963 – 8798 (ONLINE)

Dari pengujian ini didapatkan hasil bahwa website tersebut menggunakan TLSv1.2 serta TLSv1.3. TLSv1.2 dan TLSv1.3 merupakan sebuah protokol kriptografi yang digunakan untuk keamanan dalam berkomunikasi antara *client* dengan web server dalam jaringan internet. Perbedaan antara kedua protocol tersebut yaitu pada kecepatan dalam merespon permintaan *client* serta tingkat keamanan yang diberikan. Protocol ini bekerja ketika *client* melakukan *request* kepada web server kemudian webserver akan memastikan bahwa kunci yang diberikan oleh *client* sesuai dengan yang dimiliki oleh server. Selanjutnya server akan mengirim permintaan *client* tersebut. Serta dari pengujian tersebut, peneliti menemkan informasi bahwa website tersebut telah memiliki sertifikat ssl yang berlaku sampai dengan 17 September 2022.

4. Mendapatkan dns Target

   Untuk mengetahui domain apa saja yang terdapat dalam website smk-alkautsar.sch.id, peneliti menggunakan *tools* dnscan. Untuk menjalankan *tools* ini yaitu dengan mengetikkan perintah python dnscan -d smk-alkautsar.sch.id. Berikut hasilnya yang terdapat pada Tabel 2 sebagai berikut.

TABLE 2
SUBDOMAIN DAN ALAMAT IP SMK AL KAUTSAR

Subdomain
smk-alkautsar.sch.id
cpanel.smk-alkautsar.sch.id
ftp.smk-alkautsar.sch.id
mail.smk-alkautsar.sch.id
webdisk.smk-alkautsar.sch.id
webmail.smk-alkautsar.sch.id
whm.smk-alkautsar.sch.id
www.smk-alkautsar.sch.id

Dari hasil yang didapatkan, penulis menemukan 8 domain yang berkaitan dengan website SMK Al Kautsar Purwokerto.

5. Mendapatkan Email Info

   Langkah pengujian selanjutnya yaitu dengan mendapatkan informasi email, untuk mendapatkan informasi tersebut peneliti menggunakan tools yang bernama infoga. Untuk menjalankan tools tersebut dengan mengetikkan perintah python infoga.py –domain smk-alkautsar.sch.id. Berikut adalah gambar dari hasil pengujian yang didapatkan.

 ISSN: 2963 – 8798 (ONLINE)

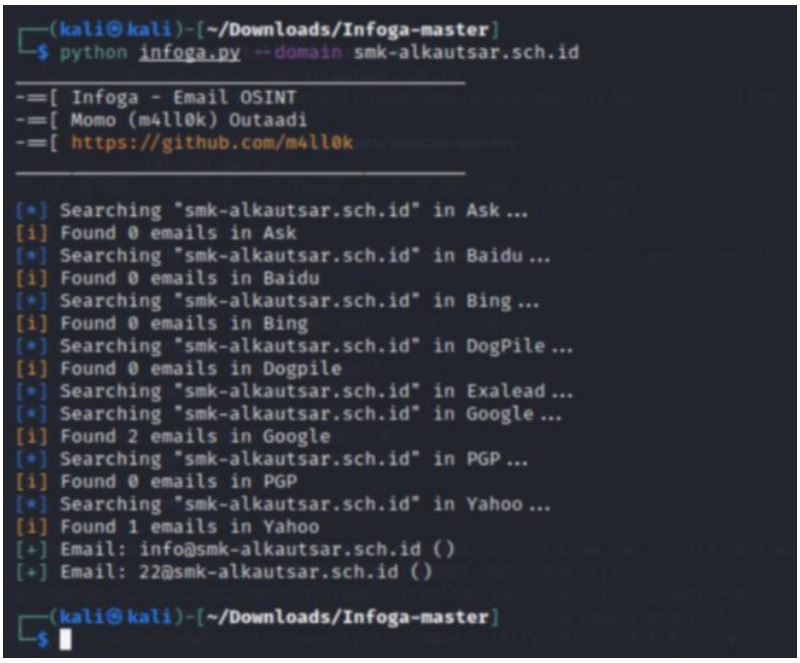

Fig.4. Perintah serta hasil pengujian mendapatkan email

Dan dari pengujian tersebut terdapat informasi mengenai email. Email yang terdapat dalam pengujian ini yaitu email info@smk-alkautsar.sch.id dan juga 22@smk-alkautsar.sch.id.

6. Identifikasi CMS

Pada tahap ini penguji menggunakan *tools* yang Bernama whatweb. Tujuan dari pengujian ini yaitu untuk mengetahui cms yang digunakan oleh website SMK Al Kautsar ini. Berikut adalah hasil pengujian yang telah dilakukan pada table dibawah ini.

TABLE 3
HASIL PENGUJIAN CMS

Kota	Indonesia
IP Address	1*3.2*1.44.2*6
HTTP Server	LiteSpeed
Framework	Bootstrap 3.3.6 dan 3.3.7
JQuery	Versi 1.12.4

B. Network Mapping

Pengujian network mapping dilakukan untuk mengetahui port yang terbuka dan juga untuk mengetahui jenis layanan yang digunakan. Pengujian ini dilakukan dengan menggunakan *tools* nmap yaitu Dengan mengetikkan perintah nmap -sV 1**.*1.***.2*6. Dan dari pengujian ini, peneliti dapat merangkumkan informasi yang didapat dari pengujian ini ke dalam Tabel 4 dibawah ini:

TABLE 4
INFORMASI PORT DAN SERVICE YANG TERBUKA

No	Port	Service
1	21/tcp	ftp
2	53/tcp	Domain

ISSN: 2963 – 8798 (ONLINE)

No	Port	Service
3	80/tcp	http
4	110/tcp	Pop3
5	143/tcp	Ssl/https
6	465/tcp	Ssl/smtp
7	587/tcp	Smtp
8	843/tcp	Unknown
9	993/tcp	Ssl/imap
10	995/tpc	Ssl/pop3

Dalam tabel tersebut terdapat port 21/tcp yang terbuka, port 21 merupakan port yang digunakan untuk melakukan koneksi dari *client* ke ftp server ketika seorang *client* akan mengakses ftp server. Port 53/tcp digunakan untuk layanan domain (dns). DNS (*Domain Name Service*) adalah sebuah sebuah sistem yang digunakan untuk mengubah alamat URL (*Uniform Resource Locators*) ke dalam alamat ip. Port 80/tcp merupakan port yang digunakan untuk layanan http (*Hypertext Transfer Protocol*). HTTP sendiri merupakan sebuah layanan yang dapat memungkinkan browser untuk terhubung ke halaman website. Pada port 110/tcp merupakan port yang digunakan sebagai layanan POP3 (*Post Office Protocol*), POP3 ini merupakan sebuah *protocol* yang digunakan untuk mengirim email ke local mail. Port 143/tcp merupakan sebuah port yang digunakan sebagai layanan IMAP (*Internet Message Access Protocol*). IMAP merupakan *protocol* yang memungkinkan *client* untuk mengakses ataupun mengambil e-mail dari server. Port 443/tcp merupakan protocol yang digunakan untuk layanan HTTPS, dalam komunikasi data antara client dengan server sudah terenkrispi dan dilindungi dengan sertifikat keamanan. Port 465/tcp digunakan untuk layanan SMTPS (*Simple Mail Transfer Protocol Secure*), protocol yang memungkinkan untuk berkirim email secara aman. Selanjutnya adalah port 587/tcp yang digunakan untuk layanan *submission*. Port 843/tcp merupakan port yang digunakan layanan *unknown* atau tidak diketahui. Port 993/tcp digunakan untuk layanan IMAPS (*Internet Message Access Protocol Secure*) sama saja dengan protocol IMAP, yang membedakan yaitu pada sisi keamanan. Dan port terakhir yang terbuka adalah port 995/tcp digunakan sebagai layanan POP3S, sama halnya dengan layanan POP3 yang membedakan hanya pada sisi keamanan.

C. Vulnerability Identification

Untuk mencari kerentanan pada website, peneliti menggunakan *tools* yang bernama OWASPZAP. Dari identifikasi kerentanan menggunakan *tools* OWASPZAP, berhasil mengidentifikasi 7 kerentanan pada website smk-alkautsar.sch.id. Berikut ini peneliti rangkumkan hasil yang didapat berserta dengan level kerentanan dalam Tabel 5 dibawah ini:

TABLE 4
JENIS DAN LEVEL KERENTANAN

Jenis Kerentanan	Level Kerentanan
Content Security Policy (CSP) Header Not Set	Medium
Missing Anti-clickjacking Header	Medium
Vulnerable JS Library	Medium
Information Disclosure – Debug Error Messages	Low
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low
X-Content-Type-Options Header Missing	Low

 ISSN: 2963 – 8798 (ONLINE)

Jenis Kerentanan	Level Kerentanan
Information Disclosure – Suspicious Comments	Informational
Re-examine Cache-control Directives	Informational

Pada hasil identifikasi celah kerentanan menggunakan *tools* OWASPZAP, terdapat celah keamanan *content security policy* (CSP) dapat menyebabkan sebuah website terserang cross site scripting (XSS) serta data injection. CSP sendiri merupakan sebuah layer keamanan yang digunakan untuk mendeksi serta mengenali beberapa serangan termasuk serangan cross site scripting dan *data injection.* Yang kedua terdapat celah pada anti *clickjacking header*, celah ini dapat menyebabkan sebuah website dapat memilii celah clickjacking. *Clickjacking* adalah sebuah serangan yang dapat memanipulasi sebuah tampilan website yang membuat seolah-olah ketika seorang pengguna melakukan klik dapat beresiko serta menyebabkan kerugian seperti dapat mengakses webcam, pencurian akses email atau data pribadi lainnya yang dilakukan dengan cara menyembunyikan *user interface sensitive* dengan membuatnya transparan sehingga berpptensi mengungkapkan informasi rahasiaatau mengendalikan komputer pada halaman web yang terlihat berbahaya. Celah ketiga yaitu *vulnerability js library*, terdapat dua celah dalam *vulnerability js library* ini yaitu *library* pada *jquery* serta *bootstrap*. Yang harus dilakukan untuk mengatasi celah tersebut yaitu diharuskan melakukan *update* versi *js library* serta versi *bootstrap* ke dalam versi yang lebih baru. Celah selanjutnya yaitu *information disclosure-debug error messages*, celah ini dapat diatasi dengan mendisable atau menonaktifkan error tersebut sebelum mengupload file ke dalam website. *Server leaks information via 'x-powered-by' HTTP Response header field(s)* yang memiliki tingkat kerentanan rendah, dapat diatasi dengan memastikan bahwa web server terkonfigurasi dengan *'x-powered-by' header*. Yang terakhir yaitu celah *X-Content-Type-Options Header Missing*, celah ini dapat diatasi dengan mengatur web server untuk menggunakan *Content-Type header.*

D. Penetration Testing

1. *XSS Injection*

Serangan XSS merupakan serangan yang dilakukan dengan cara penulis menyisipkan script ke dalam website SMK Al Kautsar Purwokerto. Serangan ini dilakukan berdasarkan hasil dari identification vulnerability menggunakan OWASPZAP. Dalam hasil tersebut terdapat celah keamanan berupa XSS. Serangan XSS ini bertujuan untuk mendapatkan informasi pengguna, cookies, session tokens, serta informasi penting lainnya. Untuk melakukan serangan ini yaitu dengan mengetikkan perintah <script>alert("serangan xss")</script> pada alamat domain SMK Al Kautsar. Berikut adalah perintah untuk melakukan serangan XSS:

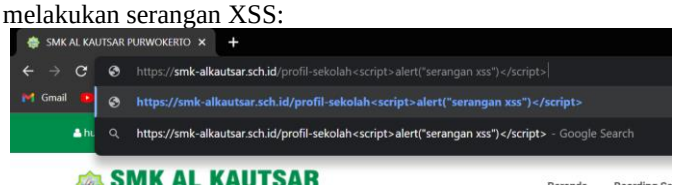

Fig.5. Pengujian *xss injection*

Hasil dari serangan XSS terhadap website tersebut yaitu gagal melakukan serangan. Serta website tersebut mengembalikan perintah serangan ke halaman beranda dari website SMK Al Kautsar.

2. Serangan DDoS

Serangan ini dilakukan untuk memenuhi lalu lintas pada server. Sehingga seolah-olah server terbanjiri dengan akses yang berlebihan dari client. Serangan ini mengakibatkan website tidak bisa diakses. Untuk melakukan pengujian serangan ddos ini, penguji menggunakan *tools* yang bernama LOIC. Untuk menggunakannya yaitu dengan mengetikkan perintah mono LOIC.exe pada terminal linux.Berikut adalah tampilan dari serangan ddos yang sudah dilakukan dengan menggunakan LOIC.

ISSN: 2963 – 8798 (ONLINE)

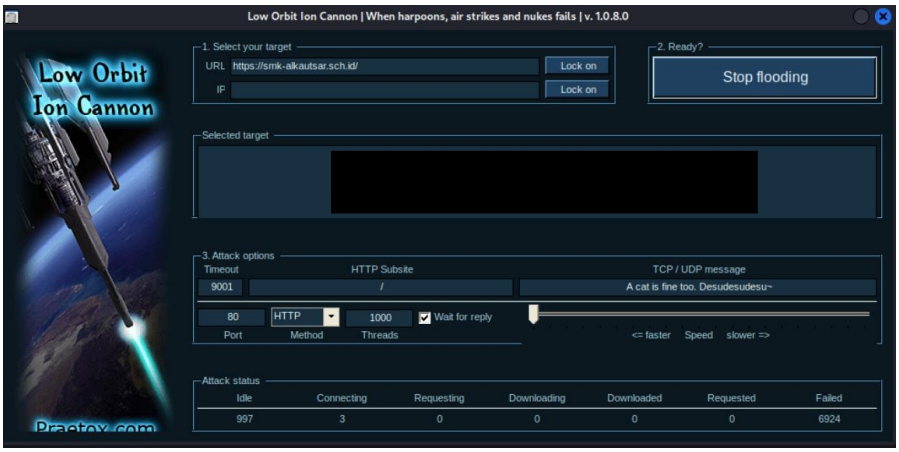

Fig.6. Tampilan LOIC untuk tahapan serangan ddos

Setelah jendela aplikasi LOIC terbuka, pada bagian url dituliskan alamat domain sekolah yang beralamatkan https://smk-alkautsar.sch.id dengan port 80, method yang digunakan http dengan thread 1000. Dan ketika dijalankan, pengujian ini berhasil. Penggunaan port 80 serta method http dikarenakan penulis ingin melakukan serangan kepda layanan http yaitu berupa akses terhadap website.Serangan ddos ini berhasil dilakukan, Website tidak dapat diakses karena terlalu banyak yang mengakses website tersebut. Serangan ddos dilakukan dengan tujuan untuk mengganggu aktivitas pengguna dalam menggunakan website SMK Al Kautsar Purwokerto. Untuk mencegah terjadinya serangan ddos yaitu dengan meningkatkan keamanan baik dari *hardware* maupun *software*, menggunakan *cloud server*.

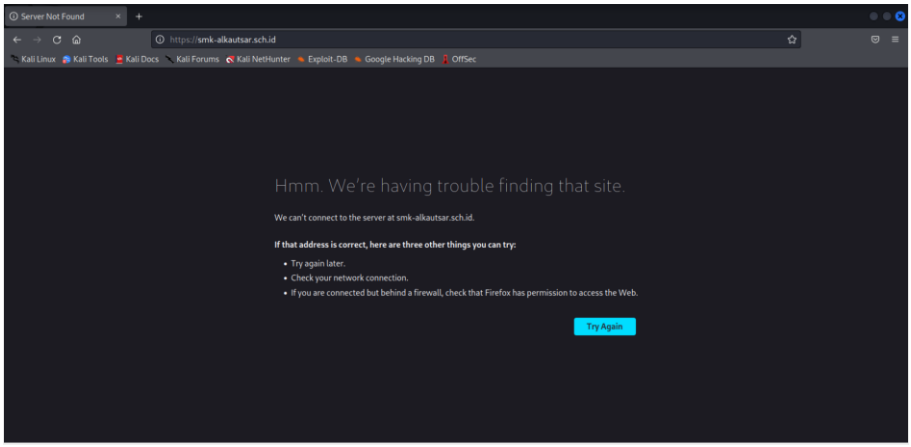

Fig.7. Hasil pengujian serangan ddos pada browser

3. Serangan Port 21 Menggunakan Metsploit

Serangan ini dilakukan untuk mengetahui keamanan pada port 21 yaitu port ftp serta untuk mendapatkan akses masuk kedalam ftp server dengan password serta username yang didapatkan. Serangan ini dilakukan atas dasar hasil scan port yang terbuka. Pengujian ini menggunakan *tols* metsploit. Hasil scan menggunakan nmap, dapat diketahui bahwa jenis ftp-server yang digunakan website smkalkautsar.sch.id adalah Pure-FTPD. Serangan yang dilakukan menggunakan metasploit bernama *exploit/multi/ftp/pureftpd_bash_env_exec 2014-09-24.* Berikut adalah perintah serta hasil yang didapat dari pengujian serangan port 21 menggunakan Metasploit.

ISSN: 2963 – 8798 (ONLINE)

Fig.8. Perintah melakukan serangan port 21 menggunakan metasploit

Dari hasil serangan yang telah dilakukan diatas, ditemukan hasil bahwa serangan tersebut tidak berhasil untuk mendapatkan akses untuk masuk ke dalam ftp server dari website smk-alkautsar.sch.id serta tidak mendapatkan *username* serta *password.*

V. Conclusion

Dalam penelitian ini yang menggunakan metode *penetration testing* menggunakan framework ISSAF untuk menganalisis celah keamanan pada website SMK Al-Kautsar Purwokerto memberikan hasil sebagai berikut webiste tersebut tidak mempunyai celah keamanan yang dapat menyebabkan serangan sql injection, hal ini terbukti dengan peneliti melakukan pengujian website menggunakan *tools* sql injection. Dan hasilnya tidak ditemukan sebuah database. Website tersebut rentan terhadap serangan ddos, hal ini dibuktikan dengaan peneliti melakukan pengujian menggunakan *tools* LOIC. Dan hasil yang didapat website tersebut tidak dapat diakses selama serangan berlangsung. Website tersebut aman dari serangan yang memanfaatkan port 21 yaitu port ftp. Peneliti berhasil mengambil akses untuk masuk ke dalam akun cpanel serta webhosting dengan menggunakan serangan *brute force*.

REFERENCES

[1] Sahren, R. Ashari Dalimuthe, and M. Amin, “Prosiding Seminar Nasional Riset Information Science (SENARIS) Penetration Testing Untuk Deteksi Vulnerability Sistem Informasi Kampus,” no. September, pp. 994–1001, 2019.
[2] S. Al-kautsar, “Sejarah SMK Al-Kautsar Purwokerto.” https://smk-alkautsar.sch.id/sejarah-sekolah (accessed Feb. 15, 2022).
[3] S. Utoro, B. A. Nugroho, M. Meinawati, and S. R. Widianto, “Analisis Keamanan Website E-Learning SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard,” *Multinetics*, vol. 6, no. 2, pp. 169–178, 2020, doi: 10.32722/multinetics.v6i2.3432.
[4] Adam Malik Sitinjak, “Penerapan Framework Issaf Dan Owasp Versi 4 Untuk Analisis Dan Pengujian Kerentanan Website ittelkom-pwt.ac.id,” *Metod. Penelit.*, pp. 32–41, 2019.
[5] A. Bastian, H. Sujadi, and L. Abror, “Analisis Keamanan Aplikasi Data Pokok Pendidikan (Dapodik) Menggunakan Penetration Testing Dan Sql Injection,” *Infotech J.*, vol. 6, no. 2, pp. 65–70, 2020.
[6] I. G. A. S. Sanjaya, G. M. A. Sasmita, and D. M. S. Arsa, “Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF,” *J. Ilm. Merpati (Menara Penelit. Akad. Teknol. Informasi)*, vol. 8, no. 2, p. 113, 2020, doi: 10.24843/jim.2020.v08.i02.p05.
[7] F. Fachri, A. Fadlil, and I. Riadi, “Analisis Keamanan Webserver menggunakan Penetration Test,” *J. Inform.*, vol. 8, no. 2, pp. 183–190, 2021, doi: 10.31294/ji.v8i2.10854.
[8] R. Harminingtyas, “Analisis Layanan Website Sebagai Media Promosi, Media Transaksi Dan Media Informasi Dan Pengaruhnya Terhadap Brand Image Perusahaan Pada Hotel Ciputra Di Kota Semarang,” *J. Site Semarang*, vol. 70, no. 4, pp. 921–946, 2014.
[9] S. R. Widianto and I. A. Azzam, “Analisis Upaya Peretasan Web Application Firewall dan Notifikasi Serangan Menggunakan Bot Telegram pada Layanan Web Server,” *J. Elektra*, vol. 3, no. 2, pp. 19–28, 2018.
[10] I. M. Syafangatun, “Analisis Manajemen Risiko Sistem Informasi Di Kopkun Purwokerto Menggunakan Metode Octave Allegro,” Universitas Amikom Purwokerto, 2020.
[11] Nagitec, “Cyber Attack Dan Upaya Mencegahnya,” *nagitec.com*, 2020. https://nagitec.com/cyber-attack-dan-upaya-mencegahnya/ (accessed Jan. 23, 2022).
[12] Andria, “Analisis Celah Keamanan Website Menggunakan Tools WEBPWN3R di Kali Linux,” *Gener. J.*, vol. 4, no. 2, pp. 69–76, 2020.
[13] M. S. S. Wardaya, “Penetration Testing Terhadap Website Asosiasi Pekerja Profesional Informasi Sekolah Indonesia (APISI),” UIN Jakarta, 2019.
[14] S. Eko Prasetyo and N. Hassanah, “Analisis Keamanan Website Universitas Internasional Batam Menggunakan Metode Issaf,” *J. Ilm. Inform.*, vol. 9, no. 02, pp. 82–86, 2021, doi: 10.33884/jif.v9i02.3758.
[15] dan S. A. M. Agus Rochman, Rizal Rohian Salam, “Analisis Keamanan Website Dengan Information System Security Assessment Framework (Issaf) Danopen Web Application Security Project (Owasp)Di Rumah Sakit XYZ,” *J. Indones. Sos. Teknol.*, vol. 2, no. 1, pp. 506–519, 2021, [Online]. Available: http://journal.unilak.ac.id/index.php/JIEB/article/view/3845%0Ahttp://dspace.uc.ac.id/handle/123456789/1288.
[16] M. S. Adam, “Penerapan Framework Issaf Dan Owasp Versi 4 Untuk Analisis Dan Pengujian Kerentanan Website ittelkom-pwt.ac.id,” Institut Teknologi Telkom Purwokerto, 2019.

ISSN: 2963 – 8798 (ONLINE)

[17] Z. Halim Alfidzar, "Implementasi HoneyPy Dengan Malicious Traffic Detection System (Maltrail) Guna," vol. 8106, pp. 32–45, 2022.
[18] M. Zidane, "Klasifikasi Serangan Distributed Denial-Of-Service (DDOS) Menggunakan Metode Data Mining Naïve Bayes memperoleh gelar Sarjana Komputer Disusun oleh :," *Univ. Brawijaya*, vol. 6, no. 1, p. 63, 2021.
[19] H. S. Pratita, "Analisa Brute Force Attack menggunakan Scanning Aplikasi pada HTTP Attack," *2016*, no. 672010194, 2016.
[20] A. M. Elu, "Rancang Bangun Aplikasi Pendeteksian Vulnerability Structured Query Language (Sql) Injection Untuk Keamanan Website," *Respati*, vol. 8, no. 22, pp. 111–124, 2017, doi: 10.35842/jtir.v8i22.53.
[21] D. Anggraeni, B. Zen, and M. Pranata, "Security Analysis On Websites Using The Information System Assessment Framework (Issaf) And Open Web Application Security Version 4 (Owaspv4) Using The Penetration Testing Method," *J. Pertahanan*, vol. 8, no. 3, pp. 497–506, 2022, [Online]. Available: http://dx.doi.org/10.33172/jp.v8%0Ai3.1777.
[22] B. P. Zen, R. A. G. Gultom, and A. H. S. Reksoprodjo, "Analisis Security Assessment Menggunakan Metode Penetration Testing dalam Menjaga Kapabilitas Keamanan Teknologi Informasi Pertahanan Negara," *J. Teknol. Penginderaan*, vol. 2, no. 1, pp. 105–122, 2020.