ANALISA CELAH KEAMANAN DALAM PENGEMBANGAN WEBSITE E-COMMERCE (STUDI KASUS: MATAHARIMU.COM)

Muhammad Fierza Eries Erlangga[1)]

[1)] *Program Studi Informatika, Fakultas Teknik, Universitas Muhammadiyah Surabaya*
Jl Sutorejo No. 59, Surabaya
Email : m.fierza.eries.erlangga-2020@ft.um-surabaya.ac.id[1)]

Abstrak

Di tengah gempuran pandemi COVID-19, bisnis e-commerce di Indonesia masih berkembang dengan pesat. Namun perkembangan itu diimbangi dengan munculnya resiko keamanan IT. Mataharimu.com adalah situs E-Commerce buatan civitas akademika Universitas Muhammadiyah. Sebagai salah satu situs E-Commerce, perlu dilakukan tindakan pengamanan untuk menanggulangi resiko keamanan IT. Pencegahan lebih baik daripada pengobatan, sehingga dilakukan Penetration Testing dalam langkah menganalisa celah keamanan untuk mencegah serangan cyber. Dalam penelitian ini, ditemukan setidaknya ada 3 celah keamanan. Rekomendasi yang diberikan adalah perbaikan baris kode dan pengaturan ulang beberapa fungsi web.

Kata kunci: *Celah Keamanan, Situs E-Commerce, Penetration Testing..*

Abstract

In the midst of the onslaught of the COVID-19 pandemic, the e-commerce business in Indonesia is still growing rapidly. However, this development is offset by the emergence of IT security risks. Mataharimu.com is an E-Commerce website created by the Muhammadiyah University academic community. As one of the E-Commerce sites, it is necessary to take security measures to overcome IT security risks. Prevention is better than treatment, so Penetration Testing is carried out in the step of analyzing security holes to prevent cyber attacks. In this study, it was found that there were at least 3 security holes. The recommendations given are code improvements and reorganization of some web functions.

Keywords : *Vulnerabilities, E-Commerce Website , Penetration Testing.*

1. Pendahuluan

Di tengah gempuran pandemi, bisnis e-commerce di Indonesia diprediksi tumbuh 33,2 persen dari 2020 yang mencapai Rp253 triliun menjadi Rp337 triliun pada tahun 2021 [1]. Namun, dengan meningkatnya keuntungan, maka resiko keamanan akan semakin meningkat. Hal ini dibuktikan dengan masuknya Indonesia ke dalam peringkat 21 kategori keamanan siber terburuk di dunia [2]. Umumnya serangan siber ditujukan kepada website ataupun perusahaan besar. Namun bukan berarti website kecil akan aman dari serangan hacker. Berdasarkan laporan salah satu penyedia asuransi siber, terjadi peningkatan cyber-attack sebesar 57% untuk organisasi level kecil yang memiliki karyawan di bawah 250 orang [3].

Sekecil apa pun skala cyber-attack pasti akan tetap merugikan pihak yang terkena serangan tersebut. Jika tidak berhati-hati, maka perusahaan tempat kita bekerja bisa mengalami kerugian finansial, seperti Facebook yang diretas 3 tahun lalu dan menyebabkan anjloknya nilai valuasi pasar terhadap Facebook sebesar 119 Milyar Dolar Amerika Serikat [4]. Oleh karena itu, perlu dilakukan tindakan khusus untuk menangani masalah ini dan tentunya langkah pencegahan lebih murah dibandingkan langkah pengamanan. Hal ini sesuai dengan budaya IT di Indonesia yang sering kali suka menggunakan anggaran seminimal mungkin untuk pengamanan. Untuk mencegah terjadinya serangan hacker bisa dilakukan beberapa cara, yaitu: penetration testing, bug bounty, dan lain sebagainya. Penetration Testing adalah tindakan pencegahan yang memiliki tingkat efektivitas paling tinggi dibanding teknik lainnya. Sehingga dengan dilakukan penetration testing, akan terlihat lubang-lubang keamanan yang perlu ditindak lanjuti untuk mengurangi resiko cyber-attack.

Mataharimu.com merupakan e-commerce karya anak bangsa lingkungan Universitas Muhammadiyah Surabaya yang diprakarsai P2EK2 dan Tim Teknik Komputer Lutfi Maulana, dkk. sebagai ajang bisnis online untuk mengoptimalkan potensi entrepreneurship yang dimiliki mahasiswa dan civitas akademika [5][6]. Sebagaimana situs E-Commerce lainnya, Mataharimu.com mewadahi kegiatan transaksi yang dilakukan penjual dan pembeli secara digital sehingga mau tidak mau pasti berhubungan dengan uang. Dalam E-Commerce, serangan cyber-attack bisa menyebabkan pencurian data pelanggan, serangan malware, penipuan kartu kredit, botnet, serangan phising, dan e-skimming [7]. Macam-macam serangan tersebut tentunya akan menyebabkan situs E-Commerce kehilangan kepercayaan pengguna yang berakibat merugikan perusahaan. Oleh karena itu dalam penelitian ini, kami melakukan Penetration Testing terhadap situs Mataharimu.com sebagai langkah awal dari pencegahan cyber-attack, yaitu identifikasi celah keamanan.

2. Dasar teori

Berikut ini beberapa landasan teori yang digunakan dalam penelitian ini

2.1 Kemanan Sistem Informasi

Teknologi informasi yang semakin maju dan berkembang memiliki banyak keuntungan dalam kehidupan manusia. Namun aspek negatifnya juga banyak terjadi seperti: kejahatan komputer (meliputi pencurian, penipuan, pemerasan, dan banyak lainnya). Jatuhnya informasi ke tangan pihak lain (misalnya pihak lawan bisnis) dapat menimbulkan kerugian bagi pemilik informasi. Sebagai contoh, banyak informasi dalam sebuah perusahaan yang hanya diperbolehkan diketahui oleh orang-orang tertentu di dalam perusahaan tersebut.

Cara mengamankan, menjaga, menjamin sistem agar informasi dapat tersedia saat dibutuhkan adalah definisi dari Keamanan Sistem Informasi. Dalam dunia IT, risiko keamanan setidaknya ada 3 macam, yaitu: Assets, Threats, dan Vulnerabilities [8].

Assets (aset) adalah data, perangkat, ataupun komponen apapun dari sebuah organisasi yang bersifat *valuable*, seringkali karena aset tersebut memiliki data yang sensitif atau bisa mengakses data *confidential*. Contoh dari aset adalah: hardware, software, dokumentasi, data, komunikasi, lingkungan, dan manusia. Dalam sebuah organisasi, aset yang paling umum adalah aset informasi, yang seringkali berbentuk database ataupun dokumen fisik. Pengamanan minimal yang biasanya dilakukan untuk aset informasi adalah menyimpannya dalam sebuah *information asset container*. *Information asset container* ini bisa berbentuk brankas penyimpanan untuk dokumen fisik, ataupun aplikasi yang digunakan untuk mengembangkan database.

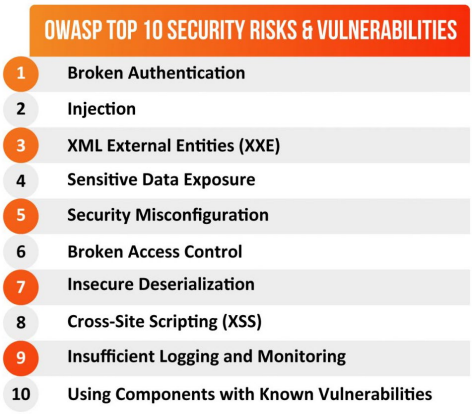
Threats (ancaman) adalah kejadian/insiden apapun yang bisa berdampak negatif terhadap aset perusahaan, misalnya: kehilangan aset, aset diakses oleh orang yang tidak berkepentingan, ataupun aset menjadi tidak bisa diakses oleh perusahaan. Dalam sebuah organisasi, threats bisa muncul dari internal maupun eksternal. Berikut ini adalah beberapa titik kritis munculnya threats: pemakai (users), teroris, kecelakaan, crackers, penjahat kriminal, bencana alam, intel, dsb.

Vulnerabilities (kelemahan) adalah titik lemah dari sebuah organisasi yang bisa dieksploitasi oleh Threats dengan tujuan untuk merusak, menghancurkan, ataupun menyandera sebuah aset perusahaan. Vulnerabilities ini bisa muncul pada beberapa hal, misalnya: software/hardware bugs, unathorized users, print out, keteledoran, dsb.

2.2 Celah Keamanan (Vulnerability)

Dalam dunia keamanan sistem informasi, tidak adap sistem yang sempurna. Cepat atau lambat, hacker pasti akan menemukan cacat/celah untuk masuk ke dalam sistem tanpa izin. Cacat/celah keamanan ini sering kali disebut dengan Vulnerability. Vulnerability adalah suatu cacat pada system/infrastruktur

yang memungkinkan terjadinya akses tanpa izin dengan meng-exploitasi kecacatan sistem. Cacat ini terjadi akibat kesalahan dalam merancang, membuat atau mengimplementasikan sebuah sistem. Vulnerability digunakan sebagai dasar pembuatan exploit oleh hacker sebagai jalan untuk masuk kedalam sistem secara ilegal. Hacker biasanya akan membuat Exploit yang disesuaikan dengan vulnerability yang telah ditemukannya [9]. Celah keamanan ini bervariasi, namun ada 10 celah keamanan yang paling sering dimanfaatkan oleh hacker, sebagaimana yang bisa dilihat pada Gambar 1 [10].



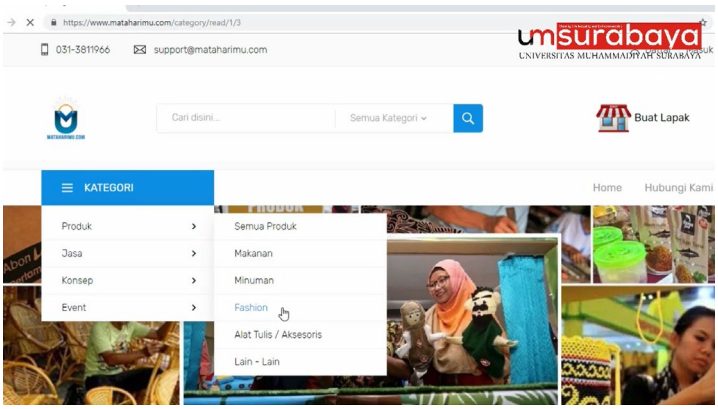
Gambar 1. *10 Celah Keamanan Versi OWASP(Open Web Application Security Project)*

2.3 Penetration Testing

Penetration Testing (pen test) adalah serangan simulasi resmi yang dilakukan pada sistem komputer untuk mengevaluasi keamanannya. Pelaku pen test menggunakan alat, teknik, dan proses yang sama dengan hacker untuk menemukan dan menunjukkan dampak bisnis dari kelemahan dalam suatu sistem. Pen test biasanya mensimulasikan berbagai serangan yang dapat mengancam bisnis [11]. Mereka dapat memeriksa apakah suatu sistem cukup kuat untuk menahan serangan dari posisi yang diautentikasi dan tidak diautentikasi, serta berbagai peran sistem. Dengan cakupan yang tepat, pen test dapat menyelami aspek sistem apa pun.

2.4 Mataharimu.com

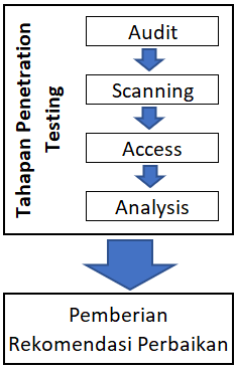
Mataharimu.com adalah situs E-Commerce yang dikembangkan oleh Lutfi Maulana beserta Tim Teknik Komputer dan P2EK2. Situs ini ditujukan untuk menampung produk-produk buatan civitas akademika Universitas Muhammadiyah Surabaya beserta masyarakat sekitar. Saat ini, Mataharimu.com menawarkan sebuah platform untuk menjual produk makanan, minuman, fashion, alat tulis, aksesoris, dan barang-barang lainnya. Tidak hanya itu, pengguna juga bisa menawarkan jasa yang bisa mereka sediakan melalui Mataharimu.com. Mataharimu.com juga tersedia dalam platform Android sehingga bisa diakses dimanapun dan kapan pun [12].



Gambar 2. *Tampilan situs Mataharimu.com*

3. Metodologi Penelitian

Secara garis besar, metode Penetration Testing yang digunakan dalam penelitian ini adalah metode External Testing, dengan cara menarget aset yang bisa diakses melalui internet. Metode ini dipilih dengan pertimbangan hacker akan berusaha menarget titik eksternal seperti: situs perusahaan, akun e-mail, dan nama domain untuk melakukan ekstraksi data. Tahapan yang dilakukan dalam penetration testing ini selanjutnya dibagi menjadi 4 tahap, yaitu: Audit, Scanning, Access, dan Analysis [7], [13]. Setelah penetration testing, diberikan rekomendasi perbaikan yang bisa dilakukan, sebagaimana yang bisa dilihat pada Gambar 3.



Gambar 3. *Tahapan Penelitian*

3.1 Audit

Tahapan ini dilakukan dengan cara melakukan audit dengan menggunakan sudut pandang keamanan. Tahapan ini membantu menunjukkan permasalahan keamanan bahkan sebelum pengujian keamanan dilakukan. Tahapan ini juga membentuk cakupan dari proses pengujian.

3.2 Scanning

Tahapan ini dilakukan untuk memahami bagaimana situs E-commerce merespon proses Penetration Testing. Proses Scanning website memungkinkan kita untuk mendapatkan informasi rinci terkait kinerja situs.

3.3 Access

Pada tahapan ini, serangkaian cyber-attack direncanakan dengan sengaja untuk mengambil alih akses dari situs. Dilakukan percobaan *exploit* terhadap celah keamanan yang ada di dalam logika aplikasi, logika bisnis, database, dan module penting lainnya dalam situs E-Commerce.

Simulasi serangan hacker dilakukan dengan cara meningkatkan level priviliges dari pengguna biasa dan pencurian informasi. Password yang lemah, informasi pelanggan yang tidak dienkripsi, informasi kartu kredit, dan sebagainya merupakan area yang umum ditarget dalam serangan. Tahapan ini merupakan tahapan yang instrumental dalam mencegah pelanggaran data/data breaches yang bersifat serius dan bisa mengancam *brand* dari organisasi pemilik E-commerce.

3.4 Analisis

Celah keamanan yang ditemukan pada tahapan sebelumnya dilakukan analisa lebih mendalam, untuk mengetahui aspek keamanan dari situs E-Commerce. Analisa juga bisa dilakukan untuk mengidentifikasi celah keamanan lebih lanjut, karena bisa jadi sebuah cyber-attack tertahan di satu module namun serangan serupa bisa dilakukan di module lain. Hasil analisis selanjutnya menjadi dasar pemberian rekomendasi untuk perbaikan celah keamanan.

3.5 Pemberian Rekomendasi

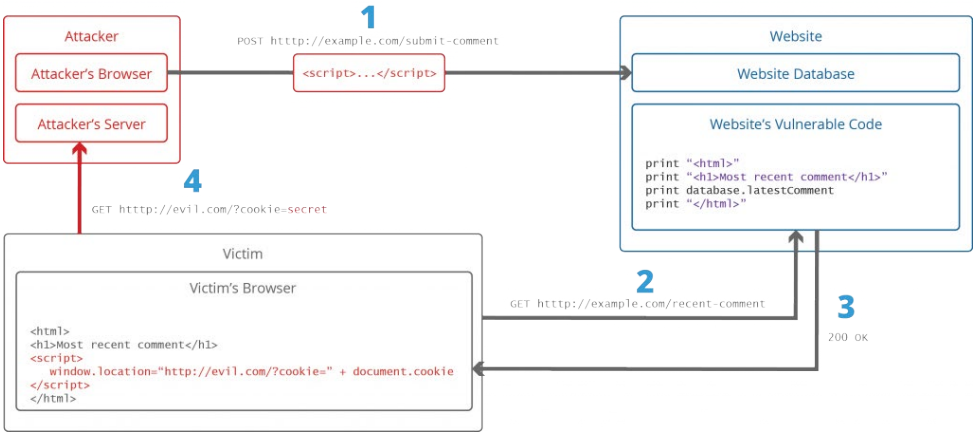
Berdasarkan tahapan penetration testing yang telah dilakukan, akan diberikan rekomendasi perbaikan yang perlu dilakukan oleh webmaster/pemilik situs. Rekomendasi perbaikan bisa berupa saran penambahan/pengubahan kode program, pengubahan setting di dashboard hosting/domain, ataupun hal-hal lainnya yang bisa mendukung proses penambalan celah keamanan.

4. Pengujian dan Pembahasan

Berdasarkan proses Penetration Testing yang telah dilakukan, ditemukan beberapa bug berikut

4.1 XSS

XSS merupakan kependekan yang digunakan untuk istilah cross site scripting. XSS merupakan salah satu jenis serangan injeksi code. XSS dilakukan oleh penyerang dengan cara memasukkan kode HTML atau client script code lainnya ke suatu situs. Serangan ini akan seolah-olah datang dari situs tersebut. XSS merupakan salah satu bentuk gangguan berupa Code Injection Attack atau serangan injeksi kode. Penyerang yang merupakan orang luar menyisipkan code – code berbahaya yang biasanya berbentuk Javascript, VBScript atau bahkan client script code. Alur XSS bisa dilihat pada Gambar 4 berikut.



Gambar 4. *Alur penyerangan XSS sederhana*

Pada situs Matahariku.com bisa dilakukan XSS dengan memasukkan Payload/Exploit berikut ke ke dalam salah satu form HTML yang ada:

```
<script>
   Alert('injected By Mr.MF33')
</script>
```

Penyebab dari celah keamanan ini adalah terjadi karena programmer (pengembang aplikasi) tidak mengimplementasikan filter terhadap metakarakter (&, ;, `, ‘, \, “, |, *, ?, ~, <, >, ^, (,), [,], {, }, $, \n, dan \r). Solusi untuk menutup celah keamanan ini adalah menggunakan fungsi htmlspecialchar() untuk setiap form pada setiap halaman. contoh:

```
<?php
   $url = htmlspecialchars($_GET["kata"]);
?>
```

4.2 HTML Injection

HTML injection adalah istilah yang lebih spesifik kepada cara 'menyisipkan' kode HTML kedalam sebuah situs. Sebagai programmer web, penanganan untuk Cross-site Scripting maupun HTML injection merupakan hal yang sangat penting, terutama dalam pembuatan kode form dengan PHP.

Pada situs Matahariku.com bisa dilakukan HTML Injection dengan memasukkan Payload/Exploit berikut ke ke dalam salah satu form HTML yang ada:

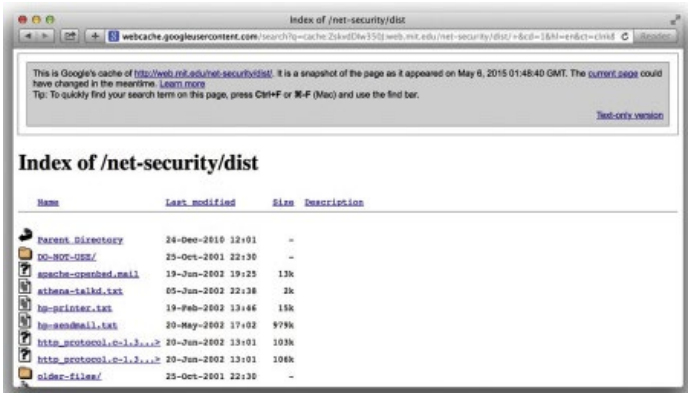
```
<center>
   <h1>Injected By Mr.MF33</h1>
</center>
```

Sebagaimana XSS, penyebab dari celah keamanan HTML Injection adalah kurangnya pemfilteran terhadap metakarakter seperti <,>,',--,+,dll. Solusi untuk menutup celah keamanan ini adalah menggunakan fungsi htmlspecialchar() untuk setiap form pada setiap halaman. contoh:

```
<?php
   $url = htmlspecialchars($_GET["kata"]);
?>
```

4.3 Directory Listing

Directory listing adalah jenis halaman Web yang mencantumkan file dan direktori yang ada di server Web. Dirancang untuk di-navigasi dengan mengklik tautan direktori, daftar direktori biasanya memiliki judul yang menggambarkan direktori saat ini, daftar file dan direktori yang dapat diklik, dan sering kali footer yang menandai bagian bawah daftar direktori. Masing-masing elemen ini ditunjukkan dalam contoh daftar direktori pada Gambar 4 berikut.



Gambar 5. *Tampilan Directory Listing*

Pada E-Commerce mataharimu.com, dilakukan brute-force menggunakan list buatan Dave Yesland serta dikombinasikan dengan pemanfaatan Google Dorks [14]. Sehingga ditemukan adanya Payload/Exploit berikut: https://mataharimu.com/assets/ . Hal ini kemungkinan besar dikarenakan tidak dilakukan setting mana halaman web yang bisa diakses oleh user dan mana halaman yang tidak boleh diakses oleh user.

Berdasarkan hasil analisa, sebaiknya dilakukan setting file .htaccess untuk setiap sub-directory yang ditemukan dengan isian sebagai berikut:

```
<IfModule mod_rewrite.c>
    <IfModule mod_negotiation.c>
        Options -MultiViews -Indexes <---- This Works for Me :)
    </IfModule>


   ....etc stuff

</IfModule>
```

Catatan: untuk … etc stuff bisa ditambahkan dengan baris kode lainnya jika dibutuhkan

5. Kesimpulan

Setelah dilakukan proses identifikasi celah keamanan serta serangkaian tahap penelitian lainnya, dapat disimpulkan sebagai berikut:

1. Situs E-Commerce yang dibuat tanpa menggunakan bantuan CMS atau Framework tertentu, rawan memiliki celah keamanan XSS dan HTML Injection.
2. Situs E-Commerce perlu mempekerjakan webmaster atau network analyst khusus agar permasalahan celah keamanan di sisi hosting/domain, seperti Directory Listing, bisa diperbaiki dengan lebih mudah.
3. Input Sanitization merupakan fungsi yang penting ditulis dalam pengembangan situs apapun, karena tanpa adanya pemfilteran, setidaknya ada 2 celah keamanan yang melakukan exploit berdasarkan input, yaitu XSS dan HTML Injection

Berdasarkan proses penelitian yang telah dilakukan, ada beberapa saran pengembangan yang bisa dilakukan agar hasil penelitian lanjutan bisa lebih baik.

1. Sampel situs E-commerce yang digunakan bisa lebih banyak agar hasil penelitian lebih representatif dalam menggambarkan
2. Proses Penetration Testing, khususnya pada tahapan Audit dan Scanning, sebaiknya dilakukan menggunakan tools terlebih dahulu agar hasil yang didapat lebih menyeluruh, juga bisa dikombinasikan berdasarkan *vulnerability list* yang diterbitkan oleh OWASP agar lebih mudah melakukan pencarian celah keamanan.
3. Saran perbaikan ke depannya sebaiknya dikombinasikan dengan manajemen resiko IT agar bisa mempertimbangkan impact, probability, serta besaran sumber daya yang dibutuhkan untuk melakukan tindakan pengamanan.

Daftar Pustaka

[1] F. Hidranto, "Bisnis E-Commerce Semakin Gurih," 2021. https://indonesia.go.id/kategori/indonesia-dalam-angka/2534/bisnis-e-commerce-semakin-gurih (accessed Oct. 21, 2021).

[2] M. Ikhsan, "BSSN Sebut Keamanan Siber RI 2020 Naik, Serangan Meningkat," *CNN Indonesia*, 2020. https://www.cnnindonesia.com/teknologi/20200925104631-185-550825/bssn-sebut-keamanan-siber-ri-2020-naik-serangan-meningkat (accessed Oct. 18, 2021).

[3] R. Roohparvar, "The Correlation Between Cyber Insurance and Increasing Cyber Risk," *Infoguard Cyber Security*, 2021. https://www.infoguardsecurity.com/the-correlation-between-cyber-insurance-and-increasing-cyber-risk/ (accessed Oct. 21, 2021).

[4] Kompas.com, "50 Juta Data Penguna Facebook Bocor, Zuckerberg Rugi Rp 67,5 Triliun," 2018. https://ekonomi.kompas.com/read/2018/03/20/211714226/50-juta-data-penguna-facebook-bocor-zuckerberg-rugi-rp-675-triliun (accessed Sep. 18, 2021).

[5] Fakultas Teknik, "Wisuda ke 44 dan Launching Mataharimu.com," *Universitas Muhammadiyah Surabaya*, 2019. https://ft.um-surabaya.ac.id/homepage/news_article?slug=wisuda-ke-44-dan-launching-mataharimucom (accessed Sep. 15, 2021).

[6] Biro Administrasi Kemahasiswaan Alumni dan Inovasi, "Selebrasi Pembukaan MOX UMS Cetak Rekor Muri Baru," *Universitas Muhammadiyah Surabaya*, 2019. https://bakai.um-surabaya.ac.id/homepage/news_article?slug=selebrasi-pembukaan-mox-ums-cetak-rekor-muri-baru (accessed Sep. 15, 2021).

[7] M. Thakkar, "HOW TO PERFORM PENETRATION TESTING FOR E-COMMERCE APPLICATIONS?," *KiwiQA*, 2021. https://www.kiwiqa.com.au/blogpost/how-to-perform-penetration-testing-for-e-commerce-applications/#:~:text=Penetration Testing (or Pen Testing,extremely difficult to be breached. (accessed Sep. 18, 2021).

[8] L. Irwin, "Risk terminology: Understanding assets, threats and vulnerabilities," *Vigilant Software*, 2020. https://www.vigilantsoftware.co.uk/blog/risk-terminology-understanding-assets-threats-and-vulnerabilities (accessed Sep. 19, 2021).

[9] Arianto, "Pengertian Vulnerability Dan Cara Mengatasi Nya," *Tembolok.id*, 2021. https://www.tembolok.id/pengertian-vulnerability-contoh-dan-pencegahan/ (accessed Sep. 18, 2021).

[10] Testbytes, "What is OWASP? Top 10 OWASP Vulnerabilities," 2020. https://www.testbytes.net/blog/what-is-owasp-top-10-vulnerabilities/ (accessed Sep. 18, 2021).

[11] Synopsis Inc., "What is Penetration Testing and How Does It Work?" https://www.synopsys.com/glossary/what-is-penetration-testing.html (accessed Sep. 19, 2021).
[12] L. Maulana, "Mataharimu.com," 2019. https://play.google.com/store/apps/details?id=com.mataharimu.app&hl=en_IN&gl=US (accessed Sep. 15, 2021).
[13] J. Billingsley, "DOES MY ECOMMERCE WEBSITE NEED PENETRATION TESTING?," *Bing Digital*, 2021. https://www.bingdigital.com/does-my-ecommerce-website-need-penetration-testing (accessed Sep. 18, 2021).
[14] D. Yesland, "List for directory brute forcing," 2019. https://gist.github.com/DaveYesland/e1d42489334049daf59d1c26543faa8b (accessed Sep. 18, 2021).