ANALISIS KEAMANAN PADA WEBSITE PT. ANEKA TIRTA TALENTA MENGGUNAKAN METODE PENETRATION TESTING

LAPORAN SKRIPSI

AZZAH HANIA DALILA 1807422013

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2022

ANALISIS KEAMANAN PADA WEBSITE PT. ANEKA TIRTA TALENTA MENGGUNAKAN METODE PENETRATION TESTING

LAPORAN SKRIPSI

Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan untuk Memperoleh Diploma Empat Politeknik

AZZAH HANIA DALILA

1807422013

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2022

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama	**: Azzah Hania Dalila**
NIM	**: 1807422013**
Tanggal	**: 27 Juni 2022**
Tanda Tangan	**:**

LEMBAR PENGESAHAN

Skripsi diajukan oleh:

Nama	:	Azzah Hania Dalila
NIM	:	1807422013
Program Studi	:	Teknik Multimedia dan Jaringan
Judul Skripsi	:	Analisis Keamanan Pada Website PT. Aneka Tirta Talenta Menggunakan Metode Penetration Testing

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Kamis, Tanggal 7, Bulan 07 Tahun 2022 Dan dinyatakan **LULUS**

Disahkan oleh

Pembimbing I : Defiana Arnaldy, S.TP, M.Si.

Penguji I : Dr. Prihatin Oktivasari, S.Si., M.Si.

Penguji II : Asep Kurniawan, S.Pd., M.Kom.

Penguji III : Ariawan Andi Suhandana, S.Kom., M.TI.

Mengetahui:

Jurusan Teknik Informatika dan Komputer

Ketua

Mauldy Laya, S.Kom., M.Kom.

NIP. 197802112009121003

SURAT PERYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan dibawah ini :

Nama : Azzah Hania Dalila

NIM : 1807422013

Jurusan/Program Studi : T.Informatika dan Komputer / Teknik Multimedia dan Jaringan

Judul Skripsi : Analisis Keamanan Pada Website PT. Aneka Tirta Talenta Menggunakan Metode Penetration Testing

Menyatakan dengan sebenarnya bahwa skripsi ini benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain dirujuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Jakarta, 24 Juni 2022

Yang membuat pernyataan

(Azzah Hania Dalila)
NIM. 1807422013

Kata Pengantar

Assalamu'alaikum Wr. Wb.

Puji syukur penulis panjatkan atas kehadirat Allah SWT karena berkat rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan perkuliahan dan skripsi ini dengan baik. Selama menjalani masa perkuliahan dan pelaksanaan penelitian skripsi, tentu banyak dukungan, bimbingan, dan saran dari berbagai pihak. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Bapak Defiana Arnaldy, S.TP, M.Si. selaku pembimbing skripsi yang telah membimbing penulis dan memberi masukan yang sangat membantu penulis dalam menyelesaikan skripsi ini.
2. PT. Aneka Tirta Talenta selaku perusahaan pemilik *Website* yang dijadikan target penelitian.
3. Ayah Ir. H. Harmen Navaro, M.Ec.Dev , Bunda Marian Anantasari Amka S.E dan Adik Ervin Zhafransyah Navaro yang telah menyayangi dan memberikan dukungan, bantuan yang tek terhingga bagi penulis dari kecil sampai sekarang.
4. Alief Dhiwangga, terimakasih telah ada setiap hari untuk mendukung, menyemangati, mendengarkan segala keluh kesah penulis dan menemani penulis mengerjakan skripsi.
5. Alief Aditya Rachman, terimakasih atas waktunya dan banyak memberikan bantuan dan masukan positif kepada penulis untuk dapat menyelesaikan skripsi ini.
6. Anggia Febrianty Harahap, Valda Zulmadaniyah, Ramandha Nurlaiz Aghniya, Ananda Nurzanah, Firdina Elivia Zahro, Ninda Ainin Alifio terimakasih atas kesediaan waktunya untuk menemani dan mengajak penulis untuk sejenak menghilangkan penat dan menghibur penulis dimasa sulit pengerjaan skripsi.

7. Laily Rachmi Tsani, Dessy Putri Alivini, Nur Suci Avina terimakasih teman seperjuangan CCIT dan selaku senior di PNJ atas dukungan dan banyak nya masukan positif kepada penulis untuk menyelesaikan skripsi ini.
8. Auryn Hanna Amelia, Gilbert Immanuel Fery, Muhammad Nazel Djibran, Muhammad Fabian Anshor, Muhammad Noviandri, Rahmat Esa M.A terimakasih teman seperjuangan skripsi dan terimakasih sudah menghibur dengan bersama – sama *refreshing* untuk melepaskan penat mengerjakan skripsi ini.
9. Alifia Afina Zalia, Aisyah Nurrul Izzan, Reyhan Immanullah, Thalita Nafalipna Immanullah terimakasih adik dan kakak sepupu yang selalu mendukung dan memberikan semangat.
10. Caki, Miko dan Chepy yang selalu setia dan menemani serta menghibur penulis dengan tingkah laku yang lucu setiap hari.

Akhir kata, semoga Allah Yang Maha Esa membalas segala kebaikan dari pihak-pihak yang telah membantu penulis. Penulis memohon maaf jika terdapat kekurangan atau kesalahn dalam laporan skripsi ini. Semoga skripsi ini dapat bermanfaat bagi pembaca dan dapat mendorong pengembangan ilmu pengetahuan. Sekian dan terima kasih.

Jakarta, 24 Juni 2022

Penulis

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya yang bertanda tangan dibawah ini :

Nama	: Azzah Hania Dalila
NIM	: 1807422013
Program Studi	: Teknik Multimedia dan Jaringan
Jurusan	: Teknik Informatika dan Komputer
Jenis Karya	: Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul :

Analisis Keamanan Pada *Website* PT. Aneka Tirta Talenta Menggunakan Metode *Penetration Testing*

Dengan Hak Bebas Royalti Noneksklusif ini Politeknik Negeri Jakarta berhak menyimpan, mengalih media/format-kan, mengelola dalam bentuk pangkalan data (*database)*, merawat, dan mempublikasikan skripsi saya selama tetap mencamtumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta Pada tanggal : 27 Juni 2022

Jakarta, 24 Juni 2022

Yang Menyatakan

Azzah Hania Dalila

NIM. 2807422013

Analisis Keamanan Pada Website PT. Aneka Tirta Talenta Menggunakan Metode Penetration Testing

ABSTRAK

Perkembangan internet dan teknologi membawa dampak besar dalam berbagai kebutuhan manusia. Menurut data dari Internet Live Stat terdapat lebih dari 5 milliar pengguna internet pada saat ini. Dengan banyaknya jumlah pengguna internet dan website maka akan semakin banyak pula kemungkinan ada nya beberapa pihak yang menyalahgunakan internet dan website tersebut untuk berbuat kejahatan. Sebuah website memerlukan tingkat keamanan yang tinggi untuk mencegah terjadinya fraud dan manipulation yang diakibatkan oleh pihak yang tidak bertanggung jawab. Dalam melindungi informasi yang terdapat pada website, maka kerentanan website menjadi perhatian penting agar tidak mudah untuk dieksploitasi. Tahapan yang dapat dilakukan yaitu dapat dimulai dengan menerapkan metode penetration testing dengan tujuan untuk mengetahui kerentanan pada website yang dijadikan sebagai object penelitian oleh penulis, sehingga hasil dari proses pengujian dapat menjadi gambaran mengenai kondisi dan kerentanan apa saja yang ada pada website target. Pada penelitian ini website yang dijadikan target adalah anekatirta-security.my.id milik PT. Aneka Tirta Talenta yang digunakan untuk operasional perusahaan dengan menggunakan beberapa tools testing yaitu Acunetix, OWASP ZAP, Vega, Burp Suite, SQL MAP dan JSQL dalam meneliti dan menguji keamanan website. Pada website ini belum pernah dilakukan pengujian celah keamanan sebelumnya. Ditemukan pada penelitian ini terdapat beberapa kerentanan pada tingkat high, medium dan low pada website target, sehingga dilakukan pengujian dan perbaikan pada website tersebut sehingga dapat meningkatkan keamanan layanan website yang akan digunakan untuk operasional perusahaan.

Kata Kunci: *Website*, Kerentanan, *Penetration Testing*, *Vulnerability Scanner*, Acunetix, OWASP ZAP, Vega, Burp Suite, SQL Map, JSQL.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan internet dan layanan *online* merupakan suatu kebutuhan yang melekat pada kehidupan sehari-hari yang dilakukan oleh manusia saat ini. Menurut data dari *internet live stat*, pada saat ini pengguna internet telah mencapai lebih 5 milliar pengguna (Internet Live Stats, 2022). Dengan banyaknya pengguna internet dan layanan *online*, hal tersebut dapat mendorong terbukanya tindak kriminal *siber* sebagai media serangan. Sehingga, aspek keamanan menjadi komponen penting dalam pengembangan *web* aplikasi untuk meminimalisir tingkat risiko yang dapat terjadi pada suatu *web* aplikasi seperti pencurian, manipulasi atau hilangnya data (Arnaldy dan Perdana, 2019; Tetskyi et al., 2018).

Pada salah satu sumber yang ditulis oleh peneliti lain telah dikatakan bahwa tidak ada aplikasi *website* tanpa adanya risiko kerentanan terhadap serangan siber (Moniruzzaman et al., 2019). Seiring perkembangannya zaman, bahwa saat ini *website* menjadi media informasi dan komunikasi yang digunakan oleh banyak perusahaan dalam mendukung operasional bisnis (Daud et al., 2014). Oleh karena itu, informasi yang tersedia didalam *website* perlu dilakukan pengamanan secara komprehensif agar tidak dapat mengakibatkan pelanggaran integritas atau pencurian data. Dalam mengetahui celah kerentanan keamanan tersebut dapat dilakukan dengan memanfaatkan metode *penetration testing* yang merupakan bagian dari proses pengujian sistem dengan harapan dapat mengetahui celah keamanan yang tersedia (Devi, 2020; Goutam dan Tiwari, 2019; Nagpure dan Kurkure, 2018; Patel, 2019).

Salah satu metode bagian dari *penetration testing* yaitu *information gathering*, dimana *information gathering* adalah langkah awal yang dilakukan pada tahapan *penetration testing* guna untuk mengetahui informasi mengenai *website* target yang diuji (Pfleeger et al., 1989). Sedangkan, langkah selanjutnya yaitu v*ulnerability assessment* yang merupakan metode untuk memindai celah pada situs *web*, untuk mengetahui kerentanan yang ada pada *website* tersebut dengan melakukan

vulnerability scanning yang dapat digunakan untuk mendeteksi kerentanan seperti *SQL injection, cross-site scripting*, dan kerentanan lainnya (Huang et al., 2017). Dalam implementasi *vulnerability scanning*, telah tersedia beberapa *tools* yang dapat dioptimalkan dalam kegiatan *vulnerability scanning* seperti *Acunetix, OWASP ZAP, Vega*, dan lainnya (Zap dan Attack, 2011) (Tsani, 2021). Selanjutnya, tahapan yang dapat dilakukan yaitu pengujian kerentanan terhadap celah yang ditemukan pada proses *scanning*, melalui eksploitasi untuk membuktikan suatu pengujian (*penetration testing).*

Pada penelitian ini, penulis akan melakukan pengujian keamananan terhadap *website* yang dimiliki oleh PT. Aneka Tirta Talenta dengan melakukan analisa terhadap fitur dan struktur data yang tersedia di aplikasi tersebut. Data yang tersedia seperti transaksi barang dan data keuangan dalam mendukung proses operasional di perusahaan tersebut. Kategori dari beberapa data tersebut bersifat rahasia, dan tidak boleh disebarluaskan. Sehingga, *website* perlu dilakukan pengujian terhadap kerentanan untuk menghindari manipulasi atau pencurian data dari pihak yang tidak memiliki hak dan tanggung jawab dalam *website* tersebut. Pada *website* ini belum pernah dilakukan pengujian celah keamanan. Oleh karena itu, penulis melakukan penelitian pada *website* tersebut yang bertujuan untuk mengetahui kelemahan dan celah keamanan *website* dari serangan yang mungkin terjadi agar kelemahan yang ditemukan dapat diperbaiki sehingga layanan *website* semakin baik dan sebagai bentuk tindakan preventif terhadap pencurian data.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan, maka rumusan masalah pada penelitian ini sebagai berikut:

a. Bagaimana menemukan celah keamanan pada *website* anekatirta-security.my.id milik PT. Aneka Tirta Talenta?
b. Bagaimana melakukan pengujian kerentanan yang ditemukan pada *website* anekatirta-security.my.id milik PT. Aneka Tirta Talenta?
c. Bagaimana proses melakukan perbaikan dari kerentanan yang ditemukan?
d. Bagaimana hasil pengujian kerentanan setelah dilakukan perbaikan?

1.3 Batasan Masalah

Agar penelitian tetap terarah dan tidak menyimpang dibutuhkan adanya batasan masalah, yaitu sebagai berikut:

a. Batasan masalah dalam penelitian ini adalah *website* yang di analisa adalah *website* anekatirta-security.my.id milik PT. Aneka Tirta Talenta
b. Pengujian yang dilakukan pada penelitian ini dengan *penetration testing*.
c. Proses pengujian kerentanan dilakukan pada situs laman untuk *testing.*
d. Penelitian ini untuk mengetahui celah keamanan pada *website* anekatirta-security.my.id dengan menggunakan *tools Acunetix, OWASP ZAP* dan *Vega*
e. Pengujian kerentanan yang dilakukan hanya mencakup pada *SQL Injection* dan/atau *Cross-site Scripting* yang ditemukan pada saat *scanning*
f. Pada penelitian ini dilakukan perbaikan kerentanan pada tingkat risiko *High* yang ditemukan.
g. Dilakukan *vulnerability scanning* ulang untuk mengetahui perbandingan celah kerentanan sebelum dan sesudah dilakukan perbaikan.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

a. Menemukan kerentanan *(vulmerability)* yang ada pada *website* anekatirta-security.my.id milik PT. Aneka Tirta Talenta dengan menggunakan metode *penetration testing.*
b. Mengetahui hasil pengujian kerentanan pada kerentanan *SQL Injection.*
c. Menangani dan memperbaiki kerentanan pada tingkat kerentana paling tinggi (*high)* yang ditemukan pada hasil deteksi pemindaian *(scanning).*
d. Merekomendasikan cara penanganan kerentanan lainnya yang belum diperbaiki.

1.4.2 Manfaat

Pengujian kerentanan pada *website* anekatirta-security.my.id milik PT. Aneka Tirta Talenta dengan menggunakan metode *penetration testing* berguna untuk mengetahui langkah atau tindakan yang akan dilakukan untuk melakukan tahap perbaikan celah keamanan yang ditemukan, maka dengan ini dapat membantu

meningkatkan keamanan layanan *website* anekatirta-security.my.id untuk operasional perusahaan.

1.5 Sistematika Penulisan

Sistematika penulisan dalam proposal ini, disusun sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi pembahasan mengenai latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat serta sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi uraian pembahasan mengenai materi atau teori yang mendukung, serta referensi dalam penelitian. Seperti keamanan jaringan, *information gathering*, *vulnerability assessment*, *vulnerability scanning* dan *penetration testing*.

BAB III PERENCANAAN DAN REALISASI

Bab ini berisi beberapa pembahasan seperti metode penelitian, rancangan penelitian, tahapan penelitian, objek penelitian, model/*framework* yang digunakan, teknik pengumpulan dan analisis data, jadwal pelaksanaan dan rincian biaya.

BAB IV PEMBAHASAN

Bab ini berisi mengenai pengujian dan hasil analisis pengujian keamanan *website* seperti deksripsi pengujian, prosedur pengujian, data hasil pengujian dan analisis data/evaluasi.

BAB V KESIMPULAN DAN SARAN

Bab ini peneliti menuliskan kesimpulan dan saran dari keseluruhan penelitan.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian yang berjudul Analisis Keamanan Pada *Website* PT. Aneka Tirta Talenta Menggunakan Metode Penetration Testing, maka dapat ditarik kesimpulan sebagai berikut :

a. Untuk menemukan celah keamanan pada *website* anekatirta-security.my.id dengan menggunakan metode *penetration testing* dan memiliki beberapa tahapan yaitu pengintaian *(reconnaissance)*, pemindaian *(scanning)*, uji kerentanan, perbaikan kerentanan, dan pemindaian ulang. Ditemukan beberapa kerentanan dengan 5 kerentanan pada tingkat *High*, 34 kerentanan pada tingkat *Medium* dan 3 kerentanan pada tingkat *Low* yang terdeteksi pada ketiga *tools vulnerability scanner* yang digunakan yaitu Acunetix, OWASP ZAP dan Vega.
b. Pengujian dilakukan pada kerentanan *SQL Injection* dan diuji dengan ketiga *tools exploit* yaitu Burp Suite, SQL Map dan JSQL membuktikan bahwa tidak terdapat kerentanan *SQL Injection* pada *website* anekatirta-security.my.id .
c. Perbaikan kerentanan pada tingkat *High* berhasil dilakukan dengan melakukan *debugging* dan perbaikan pada *source code*. Dibuktikan dengan melakukan *scanning* ulang pada *tools* Vega yang mendeteksi kerentanan tingkat *High* sudah tidak ada atau sudah tidak terdeteksi lagi.
d. Terdapat beberapa solusi penanganan kerentanan lainnya pada tingkat *Medium* dan *Low* agar nantinya dapat diperbaiki oleh pengelola *website.*

5.2 Saran

Berdasarkan penelitian yang telah dilakukan terdapat beberapa saran yang dapat diterapkan dan dikembangkan pada penelitian berikutnya. Selain itu, juga untuk *website* anekatirta-security.my.id sebagai objek penelitian, antara lan:

a. Analisis dan pengujian keamanan pada *website* anekatirta-security.my.id dapat dilakukan dengan menggunakan metode lain agar mendapatkan hasil yang berbeda.

Pengintaian, pemindaian dapat dilakukan dengan lebih banyak *tools* agar dapat mendeteksi kerentanan lain yang belum terdeteksi oleh *tools* yang digunakan pada penelitian ini.

Untuk dapat mengembangkan penelitian, uji kerentanan tidak hanya dilakukan pada kerentanan *SQL Injection* namun juga pada kerentanan lainnya.

Perbaikan celah keamanan yang belum dilakukan pada tingkat *Medium* dan *Low* yang terdeteksi perlu dilakukan untuk dapat meningkatkan keamanan layanan *website* anekatirta-security.my.id yang nanti nya digunakan oleh operasional perusahaan.

DAFTAR PUSTAKA

AcuentixReport. (2022). *Acunetix Website Audit Developer Report*. https://anekatirtatalenta.my.id:443/login

Acunetix. (2022). *Cookies without HttpOnly flag set - Vulnerabilities - Acunetix*. Invicti. https://www.acunetix.com/vulnerabilities/web/cookies-without-httponly-flag-set/

Ahmad. (2022, January 27). *√ Apa itu Whois? Inilah Pengertian Whois dan Manfaatnya*. https://www.yuksinau.id/pengertian-whois/

Arnaldy, D., & Perdana, A. R. (2019). Implementation and Analysis of Penetration Techniques Using the Man-In-The-Middle Attack. *Proceedings - 2019 2nd International Conference of Computer and Informatics Engineering: Artificial Intelligence Roles in Industrial Revolution 4.0, IC2IE 2019*, 188–192. https://doi.org/10.1109/IC2IE47452.2019.8940872

Banach, Z. (2019, May 10). *What is the local file inclusion (LFI) vulnerability? | Netsparker*. Invicti. https://www.invicti.com/blog/web-security/local-file-inclusion-vulnerability/

Chowles, D. (2020, August 18). *How to Protect Your Laravel Web Application Against the OWASP Top 10 Security Risks*. Free Code Camp. https://www.freecodecamp.org/news/protect-your-laravel-app-against-the-owasp-top-10-security-risks/

Cindy, A. (2021, August 23). *Mengapa Web Security Itu Penting?* https://www.exabytes.co.id/blog/mengapa-web-security-penting/

CMS. (2018). *Amankan Website dengan Acunetix Web Vulnerability Scanner*. https://www.centerklik.com/amankan-website-dengan-acunetix-web-vulnerability-scanner/#Mengapa_Anda_harus_memilih_Acunetix

Daud, N. I., Bakar, K. A. A., & Hasan, M. S. M. (2014). A case study on web application vulnerability scanning tools. *Proceedings of 2014 Science and Information Conference, SAI 2014*, 595–600. https://doi.org/10.1109/SAI.2014.6918247

Devi, R. S. (2020). using Ethical Hacking. *ICOEI, Icoei*, 354–361.

Fazriani, N. I. S., & Sanusi, B. C. (2019). Uji Keamanan Website Terhadap Serangan Path Traversal Pada Website Pendataan Warga. *Jurnal Riset Dan Inovasi Pendidikan*, *1*(1), 15–20.

Firch, J. (2022). *What Are The Different Types Of Penetration Testing? | Purplesec*. PURPLESEC. https://purplesec.us/types-penetration-testing/

Goutam, A., & Tiwari, V. (2019). Vulnerability Assessment and Penetration Testing to Enhance the Security of Web Application. *2019 4th International Conference on Information Systems and Computer Networks, ISCON 2019*, 601–605. https://doi.org/10.1109/ISCON47742.2019.9036175

Guder, C. B. (2009, June 7). *Plain text password over HTTPS - Stack Overflow*. Stack Over Flow. https://stackoverflow.com/questions/962187/plain-text-password-over-https

Guntoro, G., Costaner, L., & Musfawati, M. (2020). Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning). *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *5*(1), 45. https://doi.org/10.29100/jipi.v5i1.1565

Han, Z., Li, X., Xing, Z., Liu, H., & Feng, Z. (2017). Learning to predict severity of software vulnerability using only vulnerability description. *Proceedings - 2017 IEEE International Conference on Software Maintenance and Evolution, ICSME 2017*, 125–136. https://doi.org/10.1109/ICSME.2017.52

Huang, H., Laboratories, C. T., Zhang, Z., Cheng, H., & Shieh, S. W. (2017). *Web Application Security: Threats, Countermeasures, and Pitfalls*. *June*, 81–85.

Ibeankanma, C. (2022, March 29). *The 8 Most Vulnerable Ports to Check When Pentesting*. MakeUseOf. https://www.makeuseof.com/vulnerable-ports-check-when-pentesting/

IBM Security X-Force. (2022). *IBM X-Force Threat Intelligence Index 2022 Full Report*.

Internet Live Stats. (2022). *Number of Internet Users (2016) - Internet Live Stats*. https://www.internetlivestats.com/internet-users/

Invicti. (2022). *What is SQL Injection & How to Prevent it | Netsparker*. Invicti. https://www.invicti.com/blog/web-security/sql-injection-vulnerability/#PreventingSQL

Lika, S., Halim, R. D. P., & Verdian, I. (2018). Analisa Serangan Sql Injeksi Menggunakan Sqlmap. *POSITIF : Jurnal Sistem Dan Teknologi Informasi*, *4*(2), 88.

Lukan, D. (2022). *Network Topology - Infosec Resources*. INFOSEC. https://resources.infosecinstitute.com/topic/network-topology/

Moniruzzaman, M., Chowdhury, F., & Ferdous, M. S. (2019). Measuring Vulnerabilities of Bangladeshi Websites. *2nd International Conference on Electrical, Computer and Communication Engineering, ECCE 2019*, 1–7. https://doi.org/10.1109/ECACE.2019.8679426

Muniz, J., & Lakhani, A. (2013). *Web Penetration Testing with Kali Linux - PDF Drive*. https://www.pdfdrive.com/web-penetration-testing-with-kali-linux-e183573426.html

Nagpure, S., & Kurkure, S. (2018). Vulnerability Assessment and Penetration Testing of Web Application. *2017 International Conference on Computing, Communication, Control and Automation, ICCUBEA 2017*, 1–6. https://doi.org/10.1109/ICCUBEA.2017.8463920

Nisa, A. C. (2020, August 19). *Apa Itu Imunify360 dan Bagaimana Cara Kerjanya?* Exabytes. https://www.exabytes.co.id/blog/imunify360/

NKD, F. (2020, September 23). *Apa Itu Debugging ? Mengapa Programmer Perlu Melakukannya ?* Logique. https://www.logique.co.id/blog/2020/09/23/apa-itu-debugging/

NVD. (2022). *NVD - CVSS v2 Calculator*. https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator

Odogwu, C. (2021, November 13). *What Is Vulnerability Scanning and How Does It Work?* MakeUseOf. https://www.makeuseof.com/what-is-vulnerability-scanning/

Panczel, Z. (2015). *Global Information Assurance Certification Paper Burp Suite(up) with fancy scanning mechanisms GIAC (GWAPT) Gold Certification*. http://www.giac.org/registration/gwapt

Panuntun, & Bagus, A. A. (2016). *Analisis Penggunaan Openvas Untuk Vulnerability Assessment*.

Paratan, M. (2020). Analisis Sistem Keamanan Jaringan Hot-Spot. *Mersi Paratan*.

Patel, K. (2019). A Survey on Vulnerability Assessment & Penetration Testing for Secure. *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Icoei*, 320–325.

Patria, R. (2021, March 30). *Apa Itu WHOIS? Penjelasan Lengkap, Pengertian, dan Fungsinya - DomaiNesia*. https://www.domainesia.com/berita/apa-itu-whois/

Pfleeger, C. P., Pfleeger, S. L., & Theofanos, M. F. (1989). A methodology for penetration testing. *Computers and Security*, *8*(7), 613–620. https://doi.org/10.1016/0167-4048(89)90054-0

Pradana, T. P. (2020, February 28). *Mengamankan Website dari Clickjacking Dengan X-Frame-Options*. IDwebhost. https://idwebhost.com/blog/x-frame-options/#Mengamankan_Website_dari_Clickjacking_dengan_X-Frame-Options

Pratiwi, A. (2018). *Laporan Penetration Testing Pada Website Pemerintah & Pemberitaan Tingkat Kampus*.

Repeat, S. (2020). *CSP Scanner: Wildcard Directive | ScanRepeat*. Scan Repeat. https://scanrepeat.com/web-security-knowledge-base/csp-scanner-wildcard-directive

Safira, A. P. (2021, April 13). *Network Security: Pengertian, Konsep, & Jenis-Jenisnya*. https://www.goldenfast.net/blog/network-security/

Sanjaya, I. G. A. S., Sasmita, G. M. A., & Arsa, D. M. S. (2020). Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF. *Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi)*, *8*(2), 113. https://doi.org/10.24843/jim.2020.v08.i02.p05

SiteLock. (2017, April 26). *What Is A Website Vulnerability? | SiteLock*. https://www.sitelock.com/blog/what-is-a-website-vulnerability/

Smurf, I. (2018). *Apa Itu Acunetix Vulnerability Scanner Dan Bagaimana Menggunakannya ?* https://www.itsmurf.id/2018/04/apa-itu-acunetix.html

Subgraph. (2014). *Vega Vulnerability Scanner*. https://subgraph.com/vega/

Susanto, E. (2022). *OWASP (Open Web Application Security Project) Zap. – E S | Blog*. https://edysusanto.com/owasp-open-web-application-security-project-zap/

Sutiono S.Kom., M. Kom. , M. T. I. (2022). *Pengertian NMAP, Fungsi dan Cara Kerjanya - DosenIT.com*. https://dosenit.com/software/network-mapper

Swigger, P. (2022a). *Cleartext submission of password - PortSwigger*. Portswigger. https://portswigger.net/kb/issues/00300100_cleartext-submission-of-password

Swigger, P. (2022b). *CORS and the Access-Control-Allow-Origin response header | Web Security Academy*. PortSwigger. https://portswigger.net/web-security/cors/access-control-allow-origin

Swigger, P. (2022c). *Password field with autocomplete enabled - PortSwigger*. Portswigger. https://portswigger.net/kb/issues/00500800_password-field-with-autocomplete-enabled

Swigger, P. (2022d). *Source code disclosure - PortSwigger*. Portswigger. https://portswigger.net/kb/issues/006000b0_source-code-disclosure

Swigger, P. (2022e). *What is CORS (cross-origin resource sharing)? Tutorial & Examples | Web Security Academy*. Portswigger. https://portswigger.net/web-security/cors

Tashia. (2017, June 29). *Keamanan Jaringan Internet dan Firewall – Ditjen Aptika*. https://aptika.kominfo.go.id/2017/06/keamanan-jaringan-internet-dan-firewall/

Tetskyi, A., Kharchenko, V., & Uzun, D. (2018). Neural networks based choice of tools for penetration testing of web applications. *Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, DESSERT 2018*, 402–405. https://doi.org/10.1109/DESSERT.2018.8409167

Ula, M. (2019). Evaluasi Kinerja Software Web Penetration Testing. *TECHSI - Jurnal Teknik Informatika*, *11*(3), 336. https://doi.org/10.29103/techsi.v11i3.1996

Vogt, P., Nentwich, F., Jovanovic, N., Kirda, E., Kruegel, C., & Vigna, G. (2017). Cross-Site Scripting Prevention with Dynamic Data Tainting and Static Analysis. *Work*, *42*(13), 4188–4190. https://doi.org/10.1021/cm801305f

Yulianingsih, Y. (2016). Menangkal Serangan SQL Injection Dengan Parameterized Query. *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)*, *2*(1), 46–49. https://doi.org/10.26418/jp.v2i1.15507

Yunus, M. (2019). Analisis Kerentanan Aplikasi Berbasis Web Menggunakan Kombinasi Security Tools Project Berdasarkan Framework Owasp Versi 4. *Jurnal Ilmiah Informatika Komputer*, *24*(1), 37–48. https://doi.org/10.35760/ik.2019.v24i1.1988

Zakaria, M. (2020, September 1). *Pengertian NMAP Adalah : Fungsi, Cara Kerja & Penggunaannya*. https://www.nesabamedia.com/pengertian-nmap/

Zap, O., & Attack, Z. (2011). *toolsmith OWASP ZAP – Zed Attack Proxy*. 39–42.

ZAPReport. (2022). *ZAP Scanning Report*.

Zhang, E. (2020, April 16). *What is a Website Vulnerability Scanner, and Why Should You Use One? | Zeguro Blog*. https://www.zeguro.com/blog/what-is-a-website-vulnerability-scanner-and-why-should-you-use-one

LAMPIRAN
DAFTAR RIWAYAT HIDUP PENULIS

Azzah Hania Dalila

Lahir di Jakarta, 14 Juni 1999. Lulus dari SDN 10 Pagi Kebon Jeruk tahun 2011, SMPN 189 Jakarta tahun 2014, SMKN 13 Jakarta pada tahun 2017 dan Diploma II program studi *Network Administrator professional* di CCIT-FTUI pada tahun 2019. Saat ini sedang menempuh pendidikan Diploma IV Program Studi Teknik Multimedia dan Jaringan Jurusan Teknik Informatika dan Komputer di Politeknik Negeri Jakarta.

Lampiran 2 - Surat Pernyataan Izin Penelitian

YUTAKA
Solahart
TOCLAS

PT. ANEKA TIRTA TALENTA
Komp. Pertokoan Duta Merlin, Blok C No. 48
Jl. Gajah Mada RT.2 / RW.8, Petojo Utara,
Kecamatan Gambir, Kota Jakarta Pusat, DKI Jakarta 10130
Telp. : (021) 22066643, 22064280
Website :www.anekatirtagroup.com
E-mail : pt.anekatirtatalenta@gmail.com

SURAT PERNYATAAN

Nomor : -
Perihal : **Balasan Permohonan Izin Observasi**

Jakarta, 11 Maret 2022

Kepata Yth.
Bapak. Mauldy Laya, S.Kom., M.Kom
Ketua Jurusan Teknik Informatika dan Komputer
Politeknik Negeri Jakarta

Dengan hormat,

Sehubungan dengan surat yang diajukan pada 17 Februari 2022 perihal perizinan diadakan kegiatan observasi mahasiswa Jurusan Teknik Informatika dan Komputer Program Studi Teknik Multimedia dan Jaringan Politeknik Negeri Jakarta, maka dengan ini mahasiswa atas nama:

No.	Nama	NIM	Program Studi	No Hp & Email
1	Azzah Hania Dalila	1807422013	TMJ	082112600891 azzah.haniadalila.tik18@mhsw.pnj.ac.id

Telah kami setujui untuk melaksanakan observasi penelitian pada perusahaan kami sebagai syarat penyusunan Skripsi.

Demikian surat ini kami buat, atas kerjasamanya kami ucapkan terima kasih.

Direktur,
PT. Aneka Tirta Talenta

ANEKA TIRTA TALENTA YUTAKA JAKARTA

Novita Fadliah

Lampiran 3 - MOU Halaman Pertama

MEMORANDUM OF UNDERSTANDING

Saya yang bertandatangan dibawah ini :

Nama	:	Azzah Hania Dalila
Alamat Domisili	:	Jl. P1 No. 46 Rt 01 Rw 01 Kebon Jeruk, Jakarta Barat, DKI Jakarta 11530
No. Identitas Diri	:	3173055406991002 (1807422013)

Yang mana selanjutnya akan disebut sebagai Pihak Pertama

Nama	:	Alief Aditya Rachman
Alamat Domisili	:	Jln. H. Domang No.23/35 Rt.009/Rw.02, Kelapa Dua, Kebon Jeruk, Jakarta Barat, DKI Jakarta, 11550
No. Identitas Diri	:	1205-9903-002720

Yang mana selanjutnya akan disebut sebagai Pihak Kedua.

Nama	:	PT Aneka Tirta Talenta
Alamat	:	Komp. Pertokoan Duta Merlin, Blok C No.48, Jln. Gadjah Mada, RT.002/RW.08, Petojo Utara, Kec. Gambir, Jakarta Pusat, DKI Jakarta, 10130
No. Identitas Diri	:	3275096411750011

Yang mana selanjutnya akan disebut sebagai Pihak Ketiga.

Ketiga belah pihak sepakat untuk mengadakan kerjasama dalam pengembangan sistem website dengan mempertajam pada kegiatan **Observasi Keamanan Aplikasi *Website* PT Aneka Tirta Talenta** yang diatur sebagai berikut:

PASAL 1

Dalam kegiatan ini, **Observasi Keamanan Aplikasi Web PT Aneka Tirta Talenta** dilakukan oleh Pihak Pertama dan disupervisi oleh Pihak Kedua. Pihak Pertama membutuhkan Pihak Kedua dan Pihak Ketiga dalam mendukung kegiatan tersebut, terhitung dari **14 Maret 2022** sampai dengan **30 Juni 2022**.

PASAL 2

Pihak pertama akan melakukan kegiatan observasi dan analisis pada sisi *security application* untuk mendorong *service* yang aman kepada *user* dengan tujuan sebagai berikut:

1. Pihak Pertama memiliki tujuan sebagai bentuk pemenuhan kebutuhan dalam syarat kelulusan di Politeknik Negeri Jakarta dengan Program Studi Teknik Multimedia dan Jaringan Jurusan Teknik Informatika dan Komputer.
2. Pihak Pertama akan membantu Pihak Kedua untuk memenuhi persyaratan keamanan pada aplikasi yang akan digunakan oleh Pihak Ketiga.

PASAL 3

Pihak pertama akan melakukan kegiatan observasi dan analisis pada sisi *security application* dengan memerhatikan batasan penelitian ini. Adapun batasan dalam kegiatan yang dilakukan oleh Pihak Pertama yaitu:

1. Pihak Pertama akan melakukan kegiatan tersebut hanya pada Infrastuktur pengujian *(testing)*, dan tidak diperbolehkan dalam Infrastuktur *production* yang sedang digunakan di operasional.
2. Kegiatan yang dilakukan oleh pihak pertama mencakup berupa pengumpulan informasi, penilaian kerentanan, dan pengujian penetrasi.
3. Pihak Kedua akan melakukan pengawasan terhadap kegiatan tersebut secara resmi dan melakukan update laporan setiap **1 bulan sekali yang dimulai pada per-tanggal 14 April 2022** terkait kegiatan tersebut kepada Pihak Ketiga.
4. Pihak Pertama akan melakukan koordinasi dengan Pihak Kedua secara berkala pada waktu tertentu setiap sebagai bagian dari kegiatan tersebut.
5. Pihak Pertama diperbolehkan oleh Pihak Kedua dalam melakukan kegiatan pengujian penetrasi hanya mencakup pada injeksi *structure query language* (SQL) / *query* untuk manipulasi ke basisdata *(database)* dan *cross site scripting* (*XSS*) / skrip lintas situs.
6. Pihak Pertama perlu mendapatkan persetujuan dari Pihak Kedua dan Pihak Ketiga dalam melampirkan laporan dari hasil analisis dan observasi yang telah dilakukan oleh Pihak Pertama.

PASAL 4

Pihak Pertama menyepakati bahwa kegiatan observasi dan analisis keamanan pada sistem yang dimiliki oleh Pihak Ketiga dan dikembangkan oleh Pihak Kedua tidak diluar beberapa poin dibawah ini sebagai berikut:

1. Pencantuman nama perusahaan pada judul skripsi dalam kebutuhan laporan akhir pada skripsi.
2. Pencantuman informasi mengenai website seperti nama pemilik website, nama website, tanggal pembuatan dan *expire date*, *ip address*, name server, port yang terbuka, sistem operasi yang digunakan.
3. Temuan yang ditemukan akan dicantumkan sebagai bentuk informasi mengenai kerentanan website dari aspek *source code* dan terbatas pada aspek *source code*.
4. Pencantuman informasi mengenai hasil pengujian kerentanan website yang dimiliki oleh Pihak Ketiga.
5. Pencantuman nilai kerentanan website, sebelum dan sesudah dilakukan perbaikan.
6. Pihak Pertama bersedia memberikan salinan dari laporan skripsi yang bersifat *final*.

Pada beberapa poin di pasal 4 bersifat **mengikat** pada pasal 3 poin 4 dan pasal 3 poin 5 untuk setiap kegiatan yang dilakukan oleh Pihak Pertama.

Lampiran 5 - MOU Halaman Ketiga

PASAL 5

Apabila terjadi persilisihan antara ketiga belah pihak akan diutamakan dan diselesaikan secara kekeluargaan. Namun, apabila tidak ditemui jalan keluar maka akan diselesaikan secara hukum sesuai dengan perundang-undangan yang berlaku.

Demikian surat perjanjian yang tertuang dalam *memorandum of understanding* (MoU) ini kami buat sebenar-benarnya dalam rangkap tiga yang mana masing-masing rangkap mempunyai kekuatan hukum yang sama. Dalam pembuatan perjanjian kerjasama ini tidak ada paksaan dari pihak manapun.

Jakarta, 10 Maret 2022

Pihak Pertama	Pihak Kedua	Pihak Ketiga
Mahasiswi, Politeknik Negeri Jakarta (Azzah Hania Dalila)	*Project Manager System*, (Alief Aditya Rachman)	Direktur, PT Aneka Tirta Talenta (Novita Fadliah)

Lampiran 6 - Lembar Pengesahan Persetujuan Laporan Skripsi

LEMBAR PENGESAHAN

Skripsi diajukan oleh:

Nama	:	Azzah Hania Dalila
NIM	:	1807422013
Program Studi	:	Teknik Multimedia dan Jaringan
Judul Skripsi	:	Analisis Keamanan Pada Website PT. Aneka Tirta Talenta Menggunakan Metode Penetration Testing

Seluruh kegiatan observasi yang tertuang dalam laporan skripsi atas nama penulis Azzah Hania Dalila telah dilakukan pemeriksaan dan disetujui oleh PT. Aneka Tirta Talenta

Disahkan oleh

Pihak I : Azzah Hania Dalila

Pihak II : Alief Aditya Rachman

Pihak III : Novita Fadliah

Jakarta, 16 Juni 2022

Pihak I	Pihak II	Pihak III
Mahasiswi, Politeknik Negeri Jakarta (Azzah Hania Dalila)	Project Manager System, (Alief Aditya Rachman)	Direktur, PT Aneka Tirta Talenta (Novita Fadhliah)