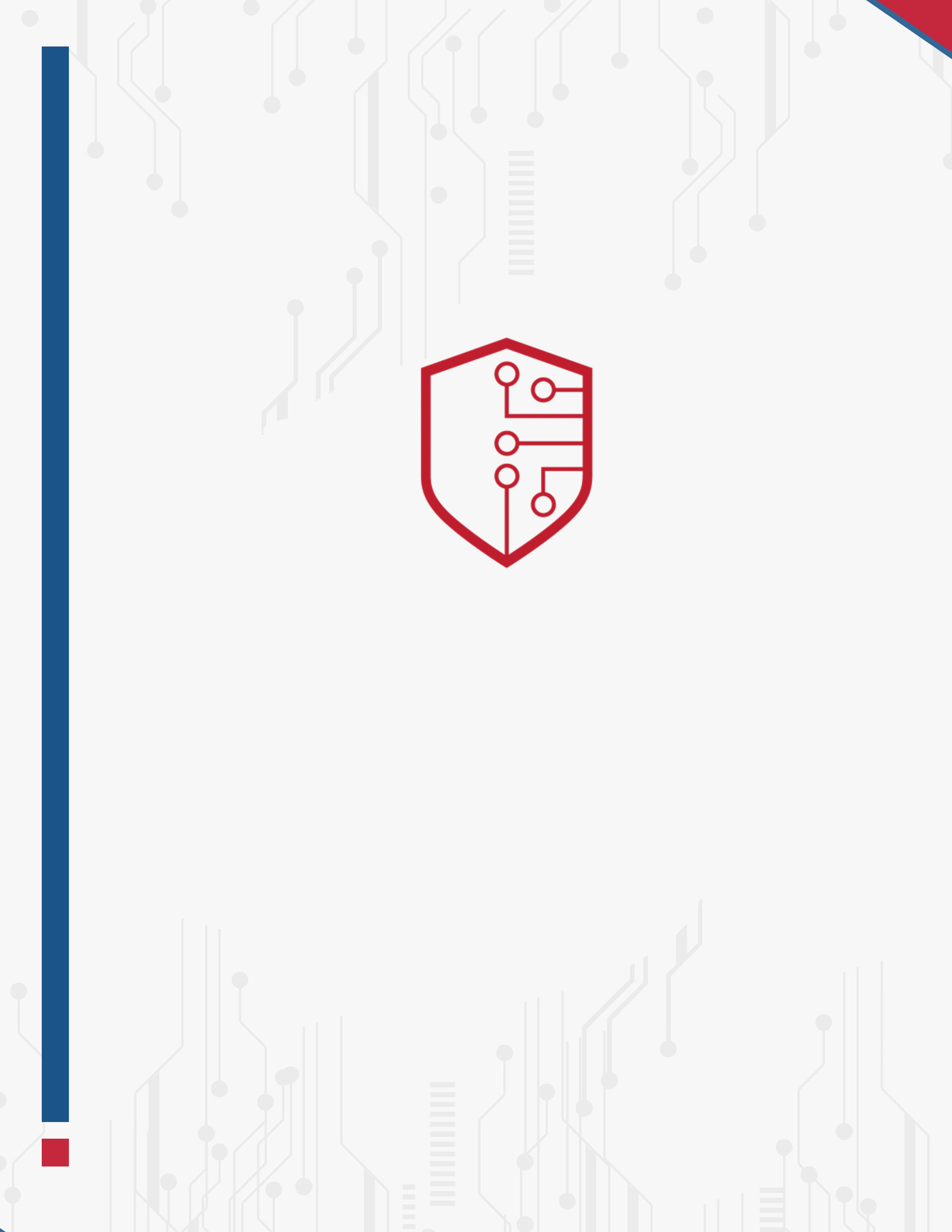
08 Januari 2024



**Penetration Testing**

**Report**

**Client**

**PT. TEST 8**

Widya Security

Jl. Anggajaya 2 No.105, Sanggrahan, Condongcatur, Kec. Depok, Kab. Sleman, Daerah Istimewa Yogyakarta 55281

# DAFTAR ISI

# DAFTAR TABEL

# DAFTAR GAMBAR

# Confidentiality Statement

Dokumen ini adalah milik eksklusif PT. TEST 8 dan PT Widya Adijaya Nusantara (Widya Security). Dokumen ini berisi informasi hak milik dan rahasia (Confidential). Penggandaan, pendistribusian ulang, atau penggunaan, seluruhnya atau sebagian, dalam bentuk apapun, memerlukan persetujuan PT. TEST 8 dan PT Widya Adijaya Nusantara (Widya Security).

Revision History

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Description** |
| 0.1 | 08 Januari 2024 | Initial Test |
| 0.2 |  | Re-Test |

Author Document

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Assignment** | **Sign** | **Date** |
| Rizky Eka Maulana | Lead Pentest |  | 17 Januari 2024 |
| Zukhrufan Ramadhan | Pentester |  | 17 Januari 2024 |

Contact Information

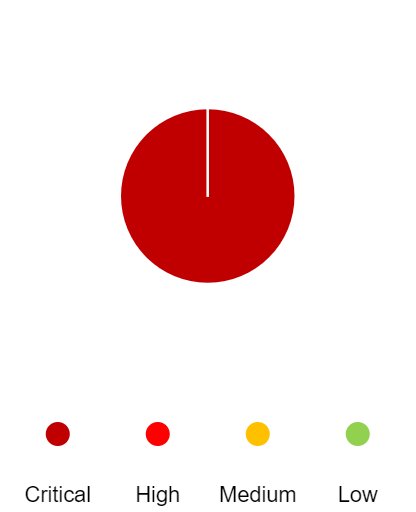
|  |  |  |
| --- | --- | --- |
| **Company** | **Name** | **Email** |
| Widya Security | Hapsari SHP | sari@gmail.com |

# Executive Summary

PT Widya Adijaya Nusantara (Widya Security) melakukan kajian celah keamanan sebagai salah satu rangkaian kegiatan untuk menentukan dan mengetahui serangan-serangan yang bisa terjadi terhadap kerentanan yang ada pada sistem dan mengetahui dampak yang diakibatkan yang dilakukan oleh penyerang.

Berdasarkan pengujian yang telah dilakukan dalam rentang waktu dan ruang lingkup yang telah ditentukan. Penguji menemukan bahwa ada 1 kerentanan keamanan di situs web yang perlu segera diperbaiki sesuai dengan peraturan dan kebijakan internal untuk mengurangi risiko eksploitasi yang dapat membahayakan kerahasiaan, integritas, dan ketersediaan. Berikut ini adalah daftar hasil yang diurutkan berdasarkan tingkat risiko kerentanan.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Critical** | **High** | **Medium** | **Low** | **Total** |
| 1 | 0 | 0 | 0 | 1 |



# Scope Application

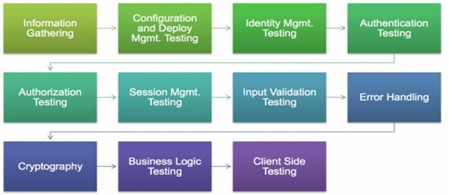
Sebelum pengujian, PT. TEST 8 memberi informasi kepada PT Widya Adijaya Nusantara (Widya Security) berupa URL aplikasi web yang digunakan untuk proses pengujian. Cakupan Penetration Testing terbatas pada URL tersebut dan layanan lain yang dijalankannya (yang berhubungan dengan layanan tersebut). Pengujian Penetration Testing dilakukan dengan menggunakan perspektif sebagai penyerang (attacker) yang tidak memiliki informasi sensitif mengenai sistem dan authentikasi pengguna (hak akses) ke sistem dari otoritas pengelola sistem (pendekatan pengujian Grey Box).

Rincian cakupan pengujian tersebut disajikan pada tabel berikut ini:

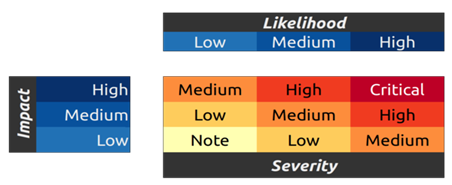
|  |  |
| --- | --- |
| ***Client*** | PT. TEST 8 |
| ***Category*** | *Mobile Apps* |
| ***Approach*** | *Penetration Testing* |
| ***URLs/App*** | <../api/1>  <../api/2> |
| ***Credentials*** | Username: abc@mail.com  Password: 12345678 |

# Methodology

Pengujian pada web aplikasi menggunakan Open Source Security Testing Methodology Manual (OSSTMM) dan Open Web Application Security Project (OWASP) sebagai acuan pengujian, tetapi tidak terbatas pada OWASP Top 10 Web Application Security & API Security. yang dijelaskan pada diagram berikut.



Kerentanan yang ditemukan dalam pengujian akan dinilai sebagai beberapa tingkat risiko. Tabel berikut menjelaskan tingkat risiko berikut sebagai acuan penilaian risiko.



Alat yang digunakan dalam pengujian ini adalah alat umum dan enterprise, seperti Burp Suite Professional, Nessus Professional, Acunetix dan alat sumber terbuka diantaranya adalah OWASP ZAP, SQLMAP, dan WFUZZ. pada tahap ini dilakukan secara eksternal melalui jaringan publik (internet) dengan menggunakan metode pengujian Grey Box Testing.

# Summary of Findings

## Vulnerability Analysis

Berdasarkan pengujian yang telah dilakukan, pada ruang lingkup yang telah ditentukan. Berikut ditampilkan daftar temuan **yang diurutkan berdasarkan tingkatan risiko kerentanan** sebagai berikut.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No. | Finding | Severity | CVSS | Status |
| 1 | *Broken Authentication (Improper Restriction of Excessive Authentication Attempts)* | 9 | Critical | Open |

Berdasarkan daftar kerentanan yang ditemukan, berikut tampilan grafik temuan kerentanan berdasarkan tingkatan risiko sebagai informasi mengenai besaran risiko setiap website atau aplikasi secara utuh.

# Finding Vulnerabilities

## ***Broken Authentication (Improper Restriction of Excessive Authentication Attempts)***

|  |  |
| --- | --- |
| **9**  ***Critical*** | **Sistem Target** |
| Vulnerability path:  Vulnerability path: |
| **Deskripsi** | |
| Kerentanan Improper Restriction of Excessive Authentication Attempts terjadi ketika suatu sistem atau aplikasi tidak menerapkan pembatasan yang memadai terhadap percobaan otentikasi yang berlebihan. Ini berarti bahwa penyerang dapat mencoba otentikasi berkali-kali tanpa batasan yang cukup, seperti batasan jumlah percobaan yang gagal, penundaan antar percobaan, atau langkah-langkah keamanan tambahan. Akibatnya, ini membuka peluang bagi serangan brute force, serangan spam, atau percobaan otentikasi yang tidak sah lainnya.  **Impact:**   1. Serangan Brute Force: Penyerang dapat mencoba kombinasi kata sandi atau metode otentikasi secara berulang-ulang tanpa risiko akun mereka diblokir atau mendapatkan peringatan. Ini dapat mengarah pada pencurian akun yang berhasil, akses ilegal, atau bahkan pengambilalihan akun. 2. Serangan Spam: Dalam konteks otentikasi, serangan spam bisa berarti penyerang mencoba masuk ke sistem dengan akun palsu atau bot secara berulang-ulang. Hal ini dapat digunakan untuk mengirimkan spam atau bahkan untuk melakukan serangan yang lebih serius seperti pencurian data. | |
| **Bukti *(Evidence)*** | |
| Image 3      Image 1    CA1 | |
| **Rekomendasi** | |
| 1. Batasan Jumlah Percobaan: Terapkan batasan yang ketat pada jumlah percobaan otentikasi yang dapat dilakukan oleh pengguna dalam jangka waktu tertentu. Setelah melewati batasan ini, pengguna harus mengikuti proses pemulihan akun yang lebih kuat atau dihentikan sementara. 2. Penundaan Setelah Gagal: Setelah beberapa percobaan otentikasi yang gagal, terapkan penundaan antara percobaan berikutnya. Ini akan mengurangi kemampuan penyerang untuk mencoba kata sandi atau otentikasi lainnya dengan cepat. 3. Penggunaan Autentikasi Multi-Faktor (MFA): Menerapkan MFA akan membuat serangan brute force lebih sulit dilakukan karena penyerang juga harus mengatasi faktor otentikasi tambahan. | |
| **Referensi** | |
| 1. <https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html> 2. [https://cheatsheetseries.owasp.org/cheatsheets/Key\_Management\_Cheat\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Key_Management_Cheat_Sheet.html ) 3. [https://owasp.org/www-community/attacks/Credential\_stuffing](https://owasp.org/www-community/attacks/Credential_stuffing ) 4. <https://cwe.mitre.org/data/definitions/307.html> | |
| **Tanggapan Manajemen & Status Remediasi** | |
|  | |

# Conclusion

Penetration Testing adalah kegiatan pengujian celah keamanan pada teknologi informasi yang bertujuan untuk mengidentifikasi dan memvalidasi kerentanan teknologi informasi, serta untuk menilai risiko dari kerentanan yang ditemukan. Laporan ini adalah hasil dokumentasi dari semua kegiatan Penetration Testing yang telah dilakukan. Laporan ini diklasifikasikan sebagai informasi rahasia. Secara keseluruhan kegiatan Penetration Testing dilakukan oleh PT Widya Adijaya Nusantara (Widya Security) untuk PT. TEST 8 dengan lingkup pembatasan masalah, sesuai dengan perjanjian yang telah dibuat. Pengujian dilakukan berdasarkan parameter celah keamanan yang berhasil ditemukan pada setiap aplikasi, sehingga perbaikan sistem harus dilakukan untuk menghindari kebocoran data sensitif.

Temuan kerentanan sistem yang disajikan pada dokumen ini berdasarkan potensi Risiko yang bisa terjadi dengan situasi dan kondisi tertentu baik dilakukan dengan metode yang terstruktur mengikuti standar tertentu, pengujian diluar standar tidak dilakukan guna penerapan keamanan sistem yang berjalan. Risiko yang telah dianalisis dan dikaji berdasarkan referensi perlu mendapatkan perhatian berupa perbaikan dan peningkatan keamanan sistem berdasarkan rekomendasi teknis yang tersaji pada dokumen, namun demikian kebijakan internal organisasi dapat menentukan tindakan apa yang dirasa perlu untuk mengurangi risiko tersebut.

|  |
| --- |
| Co-Founder & Chief Executive Officer |
| Alwy Herfian Satriatama |

# About Us

PT Widya Adijaya Nusantara (Widya Security) adalah perusahaan Cyber Security yang berfokus pada Cyber Security Analytic dan Academy. PT Widya Adijaya Nusantara (Widya Security) menawarkan penilaian keamanan sistem informasi secara komprehensif yang bertujuan mengidentifikasi kerentanan terhadap fitur aplikasi, sistem, atau jaringan dan layanan pembelajaran untuk meningkatkan teknikal & soft skill terutama di bidang Cyber Security, yang dipersembahkan untuk para akademisi, profesional, dan umum. Berikut layanan dan produk yang disediakan oleh kami.

1. Cyber Security Academy
2. Cyber Security Training
3. Vulnerability Assessment
4. Penetration Testing Services
5. Cyber Security Consulting and Advisory
6. Cyber Security Products
7. Cyber Security Analytic
8. Digital Forensics and Incident Response

PT Widya Adijaya Nusantara (Widya Security) percaya bahwa kerahasian data dan keamanan data anda adalah prioritas utama kami dengan motto “Feel SAFE with Us”.