

## DAFTAR ISI

|                                                              |             |
|--------------------------------------------------------------|-------------|
| <b>HALAMAN ORISINALITAS PENELITIAN .....</b>                 | <b>iii</b>  |
| <b>HALAMAN PERSETUJUAN .....</b>                             | <b>iv</b>   |
| <b>HALAMAN PENGESAHAN.....</b>                               | <b>v</b>    |
| <b>HALAMAN MOTTO .....</b>                                   | <b>vi</b>   |
| <b>RIWAYAT HIDUP .....</b>                                   | <b>vii</b>  |
| <b>KODE ETIK PENELITIAN.....</b>                             | <b>viii</b> |
| <b>DAFTAR ISI.....</b>                                       | <b>ix</b>   |
| <b>DAFTAR TABEL .....</b>                                    | <b>xiii</b> |
| <b>DAFTAR GAMBAR.....</b>                                    | <b>xiv</b>  |
| <b>KATA PENGANTAR.....</b>                                   | <b>xvii</b> |
| <b>ABSTRAK .....</b>                                         | <b>xx</b>   |
| <b>BAB I PENDAHULUAN.....</b>                                | <b>1</b>    |
| 1.1 Latar Belakang Masalah .....                             | 1           |
| 1.2 Rumusan Masalah.....                                     | 3           |
| 1.3 Batasan Masalah .....                                    | 4           |
| 1.4 Tujuan Penelitian.....                                   | 4           |
| 1.5 Manfaat Penelitian.....                                  | 5           |
| 1.6 Sistematika Penulisan .....                              | 5           |
| <b>BAB II LANDASAN TEORI.....</b>                            | <b>7</b>    |
| 2.1 Website Desa .....                                       | 7           |
| 2.2 Keamanan Sistem Informasi.....                           | 7           |
| 2.2.1 Pentingnya Keamanan Sistem Informasi .....             | 7           |
| 2.2.2 Konsep Keamanan dalam Sistem Informasi: CIA Triad..... | 8           |
| 2.3 Autentikasi dalam Sistem Informasi.....                  | 9           |

|                                                                        |    |
|------------------------------------------------------------------------|----|
| 2.3.1 Email Authentication Multi-Factor Authentication (MFA).....      | 9  |
| 2.3.2 Teknologi Pengenalan Wajah dalam Autentikasi .....               | 9  |
| 2.3.3 Time-Based One-Time Password (TOTP).....                         | 10 |
| 2.4 Keamanan Akun .....                                                | 10 |
| 2.4.1 Login Attempt Throttling.....                                    | 10 |
| 2.4.2 Password Recovery .....                                          | 11 |
| 2.4.3 Logging .....                                                    | 11 |
| 2.4.4 Non Repudiation .....                                            | 11 |
| 2.5 Serangan terhadap sistem informasi .....                           | 12 |
| 2.5.1 Insider Attack .....                                             | 12 |
| 2.5.2 Dictionary Attack .....                                          | 13 |
| 2.5.3 Brute Force Attack .....                                         | 13 |
| 2.5.4 Hybrid Attack.....                                               | 14 |
| 2.6 MockUp .....                                                       | 14 |
| 2.7 Alat dan Teknologi Pengembangan Sistem Keamanan WEBSITE DESA ..... | 15 |
| 2.7.1 WGET .....                                                       | 15 |
| 2.7.2 VS Code .....                                                    | 15 |
| 2.7.3 PHP .....                                                        | 15 |
| 2.7.4 XAMPP.....                                                       | 16 |
| 2.7.5 MySQL.....                                                       | 16 |
| 2.7.6 PHP Mailer.....                                                  | 16 |
| 2.7.7 Twilio .....                                                     | 17 |
| 2.8 Perlindungan Data Pribadi.....                                     | 17 |
| 2.9 Metodologi Penelitian.....                                         | 18 |
| 2.9.1 Waterfall.....                                                   | 18 |
| 2.9.2 Penetration Testing.....                                         | 20 |

|                                                               |           |
|---------------------------------------------------------------|-----------|
| 2.9.3 Alat Penetration Testing.....                           | 23        |
| 2.10 Penelitian Terkait.....                                  | 23        |
| <b>BAB III METODE PENELITIAN .....</b>                        | <b>29</b> |
| 3.1 Pendekatan Penelitian.....                                | 29        |
| 3.2 Requirements .....                                        | 29        |
| 3.2.1 Pre-Engagement Interactions .....                       | 29        |
| 3.3 Design.....                                               | 33        |
| 3.3.1 Intelligence Gathering .....                            | 34        |
| 1. Observasi Halaman Pendaftaran .....                        | 34        |
| 2. Temuan Pola Password .....                                 | 35        |
| 3. Ketiadaan Autentikasi Multi Faktor .....                   | 35        |
| 4. Ketidakfungsian Fitur Reset Password .....                 | 36        |
| 3.3.2 Threat Modeling.....                                    | 37        |
| 3.3.3 Vulnerability Analysis .....                            | 39        |
| 1. Kerentanan Akun Admin .....                                | 39        |
| 2. Kerentanan Password .....                                  | 39        |
| 3. Kebocoran Username .....                                   | 39        |
| 4. Ketiadaan Pembatasan Login .....                           | 40        |
| 5. Ketiadaan Multi-Faktor Authentication (MFA).....           | 40        |
| <b>BAB IV HASIL PENELITIAN DAN PEMBAHASAN .....</b>           | <b>41</b> |
| 4.1 Hasil Penelitian.....                                     | 41        |
| 4.2 Implementation .....                                      | 41        |
| 4.2.1 Exploitation .....                                      | 41        |
| 1. Pengujian Ketiadaan Multi-Factor Authentication (MFA)..... | 41        |
| 2. Ketiadaan Pembatasan Login .....                           | 42        |
| 3. Pengujian Hydra pada Mockup .....                          | 43        |

|                                                                                      |           |
|--------------------------------------------------------------------------------------|-----------|
| 4.2.2 Post-Exploitation.....                                                         | 49        |
| 4.2.3 Reporting.....                                                                 | 57        |
| 1. Pendahuluan .....                                                                 | 57        |
| 2. Temuan.....                                                                       | 57        |
| 3. Dampak Potensial.....                                                             | 58        |
| 4. Rekomendasi Mitigasi.....                                                         | 58        |
| 2. Percobaan Pengujian Hybrid Attack setelah penerapan Mitigasi pada<br>MockUP ..... | 84        |
| <b>BAB V KESIMPULAN DAN SARAN .....</b>                                              | <b>88</b> |
| 1.2 Kesimpulan.....                                                                  | 88        |
| 1.3 Saran .....                                                                      | 89        |
| <b>DAFTAR PUSTAKA.....</b>                                                           | <b>91</b> |
| <b>LAMPIRAN.....</b>                                                                 | <b>95</b> |

## DAFTAR TABEL

|                                                                 |    |
|-----------------------------------------------------------------|----|
| Tabel 2.10.1 Penelitian Terkait .....                           | 23 |
| Tabel 3.2.1 Wawancara dengan Operator Desa .....                | 30 |
| Tabel 3.2.2 Wawancara dengan Mantan DevOps Website .....        | 32 |
| Tabel 3.3.1 Observasi Sampel Format Username dan Password ..... | 35 |
| Tabel 3.3.2 Threat Modeling .....                               | 37 |
| Tabel 4.2.1 Tabel Percobaan Login .....                         | 43 |
| Tabel 4.2.2 Percobaan Pengujian Hydra .....                     | 48 |
| Tabel 4.2.3 Hasil Mitigasi .....                                | 85 |

## DAFTAR GAMBAR

|                                                                             |    |
|-----------------------------------------------------------------------------|----|
| Gambar 2.2.1 CIA Triad Keamanan Informasi dan Data.....                     | 8  |
| Gambar 2.9.1 Metode <i>Waterfall</i> .....                                  | 19 |
| Gambar 2.9.2 Methodology Penetration Testing Execution Standard (PTES)..... | 22 |
| Gambar 3.3.1 Kerentanan pada halaman Pendaftaran .....                      | 34 |
| Gambar 3.3.2 Halaman Login Akun Admin Website Desa .....                    | 36 |
| Gambar 4.2.1 Proses Login Pada Website Desa .....                           | 42 |
| Gambar 4.2.2 Dashboard Admin Setelah Berhasil Login.....                    | 42 |
| Gambar 4.2.3 wordlist username.txt .....                                    | 44 |
| Gambar 4.2.4 wordlist dictionary.txt .....                                  | 44 |
| Gambar 4.2.5 wordlist hybrid.txt.....                                       | 45 |
| Gambar 4.2.6 Perintah Hydra (Dictionary Attack) .....                       | 45 |
| Gambar 4.2.7 Perintah Hydra (Hybrid Attack).....                            | 45 |
| Gambar 4.2.8 Hasil Hydra (Dictionary Attack).....                           | 46 |
| Gambar 4.2.9 Hasil Hydra (Hybrid Attack).....                               | 47 |
| Gambar 4.3.1 Halaman Data Kartu Keluarga Masyarakat .....                   | 50 |
| Gambar 4.3.2 Halaman Detail Data Penduduk 1 .....                           | 50 |
| Gambar 4.3.3 Halaman Detail Data Penduduk 2 .....                           | 51 |
| Gambar 4.3.4 Halaman Identitas Desa 1 .....                                 | 52 |
| Gambar 4.3.5 Halaman Identitas Desa 2 .....                                 | 52 |
| Gambar 4.3.6 Halaman Pengelolaan Data Akun Admin.....                       | 53 |
| Gambar 4.3.7 Halaman Pengelolaan Password Akun Admin.....                   | 53 |
| Gambar 4.3.8 Halaman Pengelolaan Akun Aparat Desa .....                     | 54 |
| Gambar 4.3.9 Tampilan Proses Penghapusan Akun Aparat Desa.....              | 55 |
| Gambar 4.3.10 Tampilan Proses Edit Akun Aparat Desa .....                   | 55 |
| Gambar 4.3.11 Halaman Pendaftaran Akun Admin Desa.....                      | 56 |
| Gambar 4.4.1 Perintah WGET untuk memperoleh file FrontEnd .....             | 59 |
| Gambar 4.4.2 File Hasil dari perintah WGET .....                            | 59 |
| Gambar 4.4.3 Flowchart fitur Reset Password .....                           | 60 |
| Gambar 4.4.4 Proses Reset Password 1 (Tombol Reset Password) .....          | 61 |

|                                                                                  |    |
|----------------------------------------------------------------------------------|----|
| Gambar 4.4.5 Proses Reset Password 2 (Masukkan Email Valid).....                 | 62 |
| Gambar 4.4.6 Proses Reset Password 3 (Email Valid) .....                         | 63 |
| Gambar 4.4.7 Proses Reset Password 4 (Email Tidak Valid) .....                   | 63 |
| Gambar 4.4.8 Proses Reset Password 5 (Email terkirim).....                       | 64 |
| Gambar 4.4.9 Proses Reset Password 6 (Masukkan Password Baru).....               | 64 |
| Gambar 4.4.10 Proses Reset Password 7 (Password diperbarui).....                 | 65 |
| Gambar 4.4.11 Proses Reset Password 8 (Gagal) .....                              | 65 |
| Gambar 4.4.12 Flowchart Login Attempt Throttling .....                           | 66 |
| Gambar 4.4.13 Proses Login Attempt Throttling 1 (Input Username & Password)..... | 67 |
| Gambar 4.4.14 Proses Login Attempt Throttling 2 (IP Terblokir).....              | 68 |
| Gambar 4.4.15 Proses Login Attempt Throttling 3 (Password Salah).....            | 68 |
| Gambar 4.4.16 Proses Login Attempt Throttling 4 (Akun Tidak Ditemukan) .....     | 69 |
| Gambar 4.4.17 Proses Login Attempt Throttling 5 (Akun Terkunci).....             | 69 |
| Gambar 4.4.18 Flowchart MFA (TOTP).....                                          | 70 |
| Gambar 4.4.19 Proses OTP 1 (Pengiriman kode OTP ke Email Admin/Aparat) .....     | 71 |
| Gambar 4.4.20 Proses OTP 2 (Opsi Pengiriman kode OTP ke No. Telp) .....          | 71 |
| Gambar 4.4.21 Proses OTP 3 (OTP salah).....                                      | 72 |
| Gambar 4.4.22 Proses OTP 4 (Login Sebagai Aparat) .....                          | 72 |
| Gambar 4.4.23 Proses OTP 5 (Login Sebagai Admin).....                            | 73 |
| Gambar 4.4.24 Flowchart Mekanisme Wajib Ganti Password .....                     | 74 |
| Gambar 4.4.25 Proses Aktivasi Akun 1 (Peringatan Aktivasi Akun) .....            | 75 |
| Gambar 4.4.26 Proses Aktivasi Akun 2 (Input Email dan Password yang kuat).....   | 75 |
| Gambar 4.4.27 Proses Aktivasi Akun 3 (Pemberitahuan password Tidak Kuat).....    | 76 |
| Gambar 4.4.28 Proses Aktivasi Akun 4 (Email Verifikasi Terkirim).....            | 76 |
| Gambar 4.4.29 Proses Aktivasi Akun 5 (Klik Verifikasi Akun pada Email) .....     | 77 |
| Gambar 4.4.30 Proses Aktivasi Akun 6 (Verifikasi Berhasil).....                  | 78 |
| Gambar 4.4.31 Flowchart Masa berlaku Akun Aparat .....                           | 78 |
| Gambar 4.4.32 Pemrosesan Akun tidak Aktif.....                                   | 79 |
| Gambar 4.4.33 Pembatasan Masa Aktif Akun Aparat oleh Admin Desa.....             | 80 |
| Gambar 4.4.34 Penghilangan Tombol Daftar pada halaman Login (sebelum).....       | 81 |
| Gambar 4.4.35 Penghilangan Tombol Daftar pada Halaman Login (sesudah) .....      | 81 |
| Gambar 4.4.36 Masking Username pada Halaman Pendaftaran .....                    | 82 |

|                                                                                     |     |
|-------------------------------------------------------------------------------------|-----|
| Gambar 4.4.37 Halaman Monitoring dan Pendeteksian oleh Admin Desa .....             | 83  |
| Gambar 4.4.38 Halaman Monitoring dan Pengelolaan IP yang terblokir oleh sistem..... | 83  |
| Gambar 4.4.39 Percobaan <i>Hybrid Attack</i> setelah penerapan Mitigasi.....        | 84  |
| Gambar 5.2.1 Proses Pre-Engagement Interactions 1.....                              | 100 |
| Gambar 5.2.2 Proses Pre-Engagement Interactions 2.....                              | 100 |
| Gambar 5.2.3 Penyerahan Surat Izin Penelitian .....                                 | 101 |
| Gambar 5.2.4 Proses Exploitation dengan Hydra.....                                  | 101 |