INFORIS : JURNAL INFORMATIKA DAN SISTEM INFORMASI
Volume 1 Nomor 1 (...) ..-..
DOI: ...
https://istech.biteks.my.id/index.php/inforis/index
E-ISSN .....

Pendeteksi Serangan Brute Force pada Keamanan Website Berbasis Mobile

Muh. Satriawan[1], La Ode Ferlin yarlin[2], Justam[2]

[1]Program Studi Kecerdasan buatan, Universitas Kristen Indonesia Palulus
Jl. Perintis Kemerdekaan No.Km.13, Daya, Kec. Tamalanrea, Kota Makassar, Sulawesi Selatan 90245
[2]Program Studi Teknik Informatika, Universitas Mega Buana Palopo
Jl. Luminda, Wara, Palopo Kota, South Sulawesi 91913
muhsatriawan@ukipaulus.ac.id*

ABSTRACT

The Internet makes the availability and exchange of information faster. However, the internet has potential dangers that are ready to happen at any time. The potential danger is in the form of attacks that can damage the confidentiality, authenticity and availability of information. The purpose of this study is to create a Mobile-based Brute Force Attack Detection Application to improve webiste security protection, as well as provide a website early handling mechanism in the form of temporary deactivation of detected users used by attackers to enter the system, in making the application the author uses the black box testing method. by testing the function of the application that the author succeeded in making so that all the features in the application are in accordance with the design that the author has made. With this Brute Force attack detection application, it is hoped that administrators can more easily handle in the event of a brute force attack and protect website users from criminal attempts committed by entering or infiltrating a website system illegally, without permission or without the knowledge of the owner. websites that he entered (illegal access) from attackers (attackers).

Keywords: *Internet, Hacking, Brute Force Attacks*

ABSTRAK

Internet membuat ketersediaan dan pertukaran informasi menjadi lebih cepat. Akan tetapi, internet mempunyai potensi bahaya yang siap terjadi kapan saja. Potensi bahaya tersebut berupa serangan yang dapat merusak kerahasiaan, keaslian dan ketersediaan dari informasi. Tujuan dalam penelitian ini adalah membuat sebuah Aplikasi Pendeteksi Serangan Brute Force berbasis Mobile untuk meningkatkan proteksi keamanan website, serta menyediakan mekanisme penanganan dini website berupa penonaktifan sementara user yang terdeteksi digunakan oleh penyerang untuk masuk ke dalam system. Metode pengujian aplikasi yang digunakan untuk menguji fungsional yaitu black box. Hasil dari penelitian ini adalah administrator akan lebih mudah dalam melakukan penanganan apabila terjadi serangan brute force dan melindungi pengguna website dari upaya kejahatan yang dilakukan dengan memasuki atau menyusup ke dalam suatu sistem

website secara tidak sah, tanpa izin atau tanpa sepengatahuan dari pemilik website yang dimasukinya (ilegal access) dari penyerang (attacker).
Kata Kunci: Internet, Hacking, Serangan Brute Force

PENDAHULUAN

Pada era perkembangan teknologi yang semakin cepat dengan berbagai macam fungsi yang di tawarkan, sehingga menuntut untuk meningkatnya kualitas keamanan pada suatu sistem online maupun website, karena bocornya suatu informasi pada pihak yang tidak berkepentingan dapat menimbulkan suatu kerugian bagi pemilik informasi, karena pada era sekarang semakin terbukanya pengetahuan tentang cracking maupun hacking, dan semakin mudahnya untuk mendapatkan tool yang dapat di gunakan untuk melakukan serangan pada server. Salah satu teknik serangan yang dapat menyerang server adalah, serangan brute force dimana akibat yang di timbulkan seorang penyerang mendapatkan hak akses pada server.

Proteksi terhadap sistem online maupun website sangat mengandalkan kehadiran administrator untuk melakukan monitoring terhadap website tersebut. Administrator akan melakukan monitoring terhadap aktifitas-aktifitas yang mencurigakan dari website tersebut namun administrator tidak dapat melakukan monitoring secara terus menerus terhadap sistem online tersebut, dikarenakan keterbatasan sumber daya dan waktu yang dimiliki administrator tersebut. Sedangkan potensi serangan terhadap website bisa terjadi kapan saja. Termasuk dalam upaya-upaya illegal access dari attacker dalam hal ini teknik brute force. Belum adanya mekanisme notifikasi terhadap administrator apabila ada upaya illegal access ke dalam sistem online tersebut selain mengandalkan monitoring yang dilakukan administrator, model proteksi juga bisa memanfaatkan teknologi notifikasi yang terus berkembang saat ini. Apabila sistem online mendeteksi upaya illegal access yang terdeteksi oleh sistem secara langsung akan mengirimkan notifikasi kepada administrator melalui gawai yang dimiliki administrator. Selain mengandalkan monitoring berupa notifikasi, administrator dapat melakukan proteksi dini melalui aplikasi yang terdapat pada gawai. Proteksi dini berupa penonaktifan sementara user yang terdeteksi melakukan upaya illegal access serta administrator dapat melakukan pengaktifan kembali user yang telah diblokir melalui aplikasi android administrator.

METODE PENELITIAN

WAKTU DAN LOKASI PENELITIAN

Penelitian ini dilakukan di bulan Desember 2024 sampai Februari 2025. Bertempat di Universitas Dipa Makassar, yang beralamat di Jalan Perintis Kemerdekaan IX Kota Makassar.

HASIL DAN PEMBAHASAN

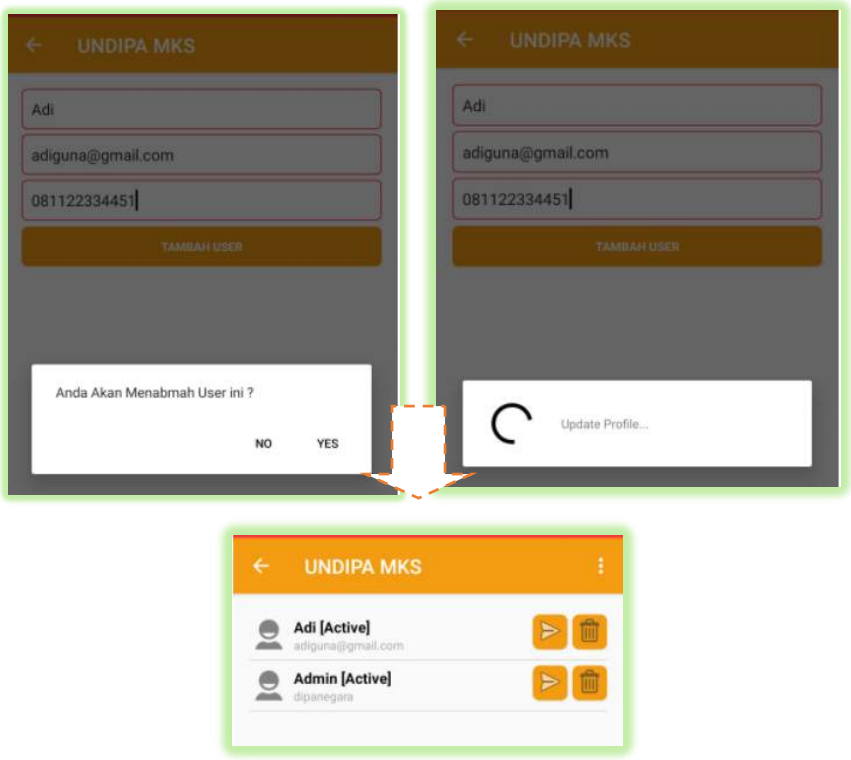
Pengujian Black Box

1. Pada tahap validasi sistem ini, peneliti akan menguji fungsional dari aplikasi yang dibangun :

Fungsi Menyimpan Identitas Data User

Tabel 1. Pengujian Menyimpan Identitas Data User

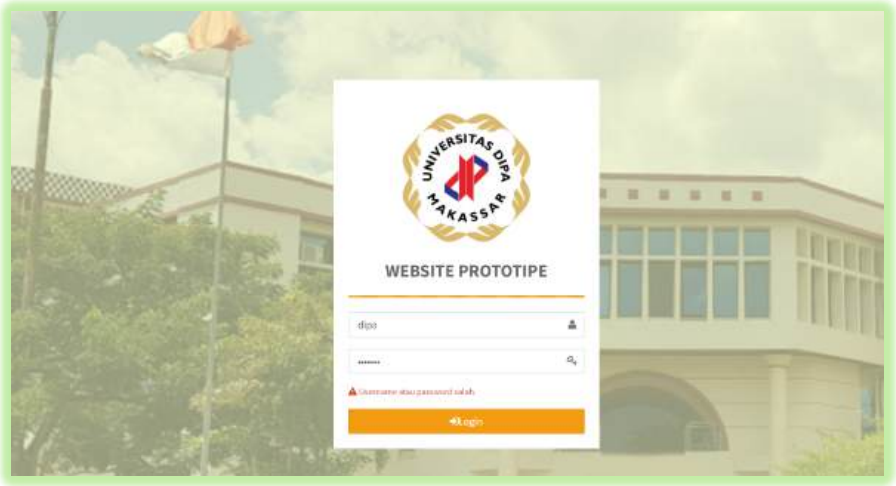
Test Factor	Hasil	Keterangan
Fungsi Menyimpan Biodata Data User	✓	Berhasil Menyimpan dengan indikator aplikasi tampilnya data pada halaman daftar Data User
Antarmuka		
		

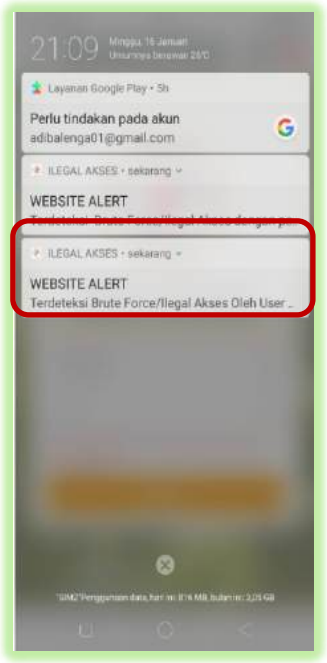


Pengujian Input Notifikasi Website Protection

Tabel 2. Pengujian Fungsi input Website Protection

Test Factor	Hasil	Keterangan
Menguji Notifikasi Web Protection	✓	Berhasil Mengirim Pesan Notifikasi ke administrator
Antarmuka		

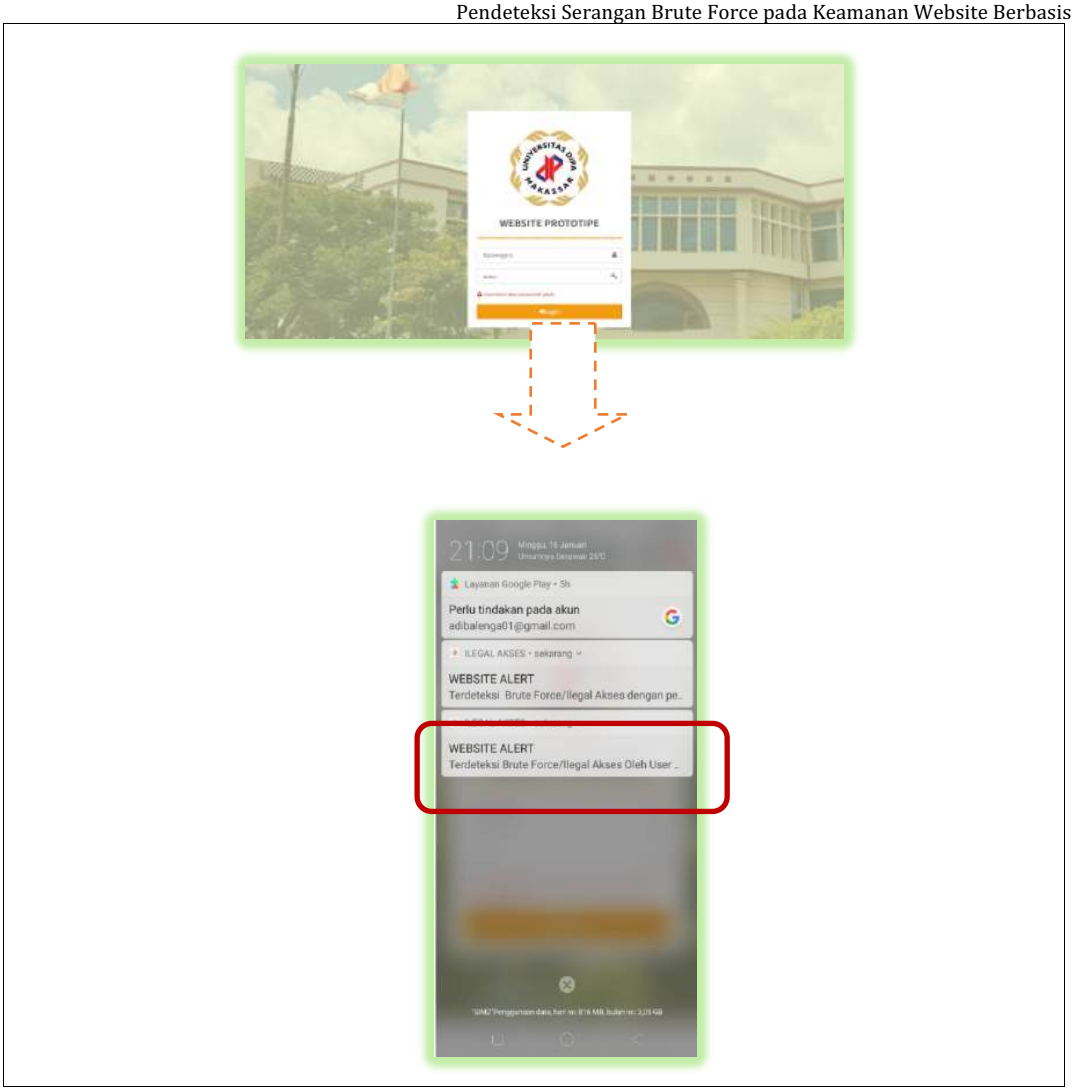




Pengujian Notifikasi User Detection

Tabel 3. Pengujian Fungsi Kirim Notifikasi user Terdeteksi

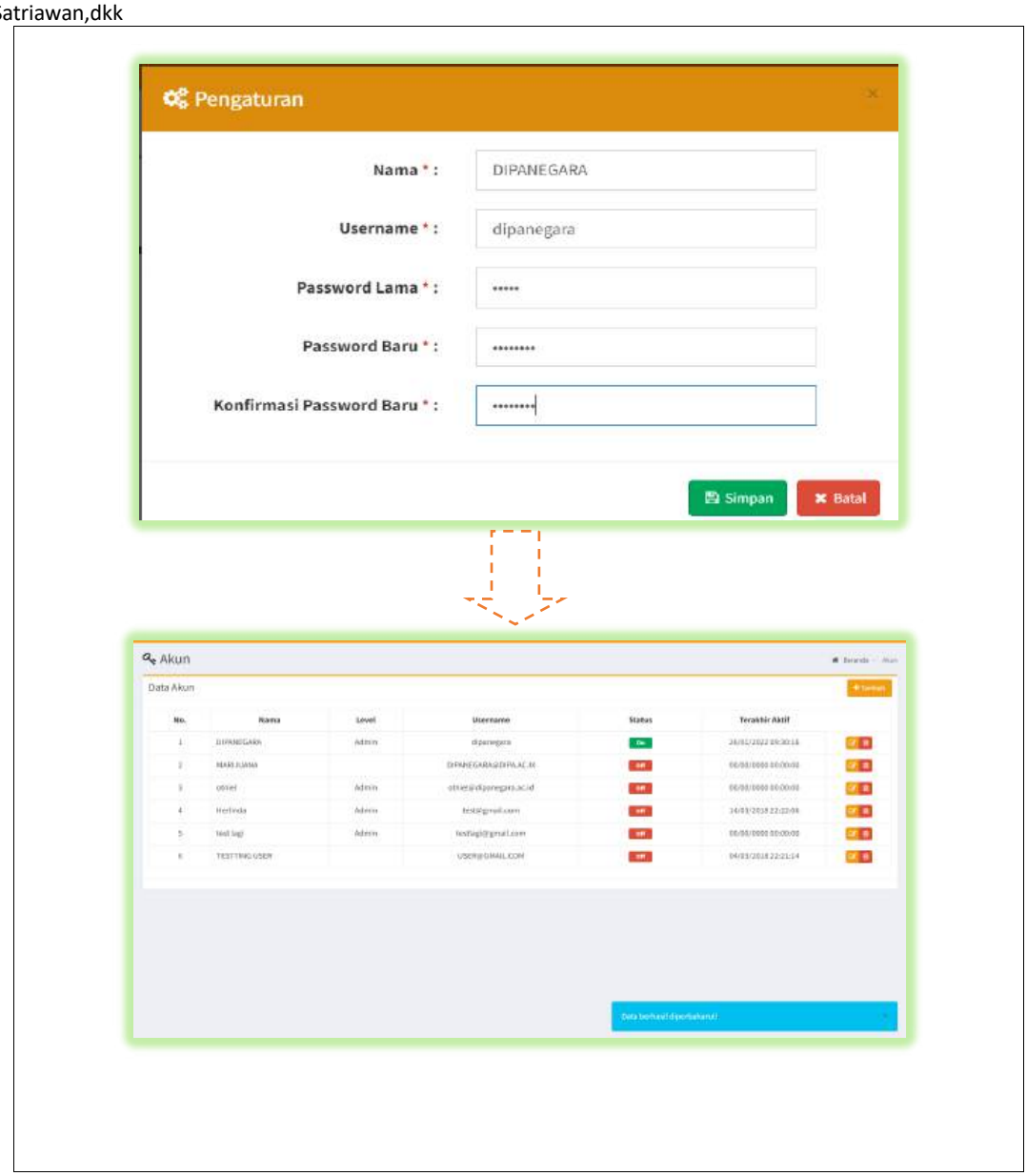
Test Factor	Hasil	Keterangan
Menguji Notifikasi User Protection	✓	Berhasil Mengirim Pesan Notifikasi ke administrator
Antarmuka		



Edit Data user

Tabel 4. Pengujian Fungsi Edit Data user

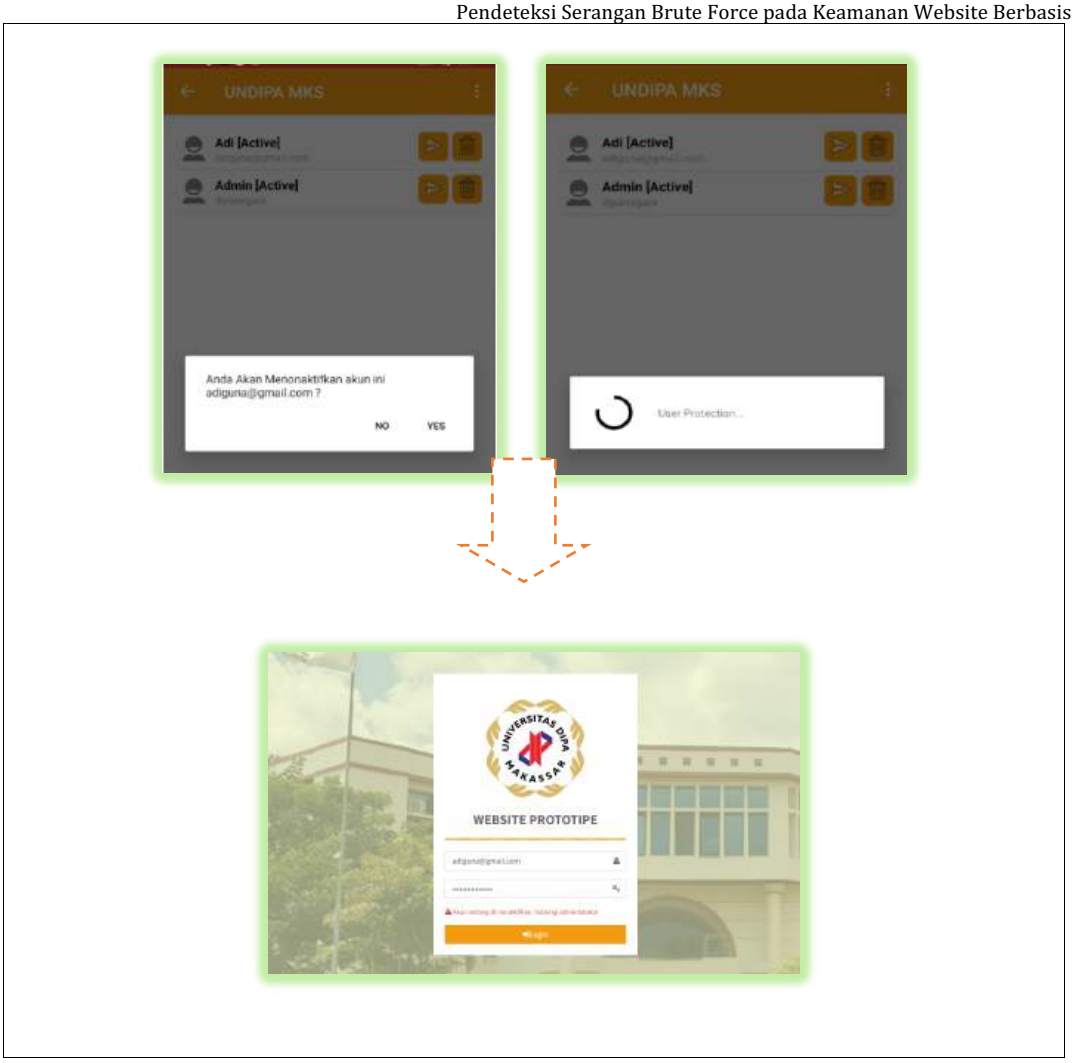
Test Factor	Hasil	Keterangan
Fungsi Mengedit data user	✓	Berhasil Mengedit data dan password user berhasil diubah
Antarmuka		



Fungsi Nonaktifkan User

Tabel 5. Pengujian fungsi nonaktif user

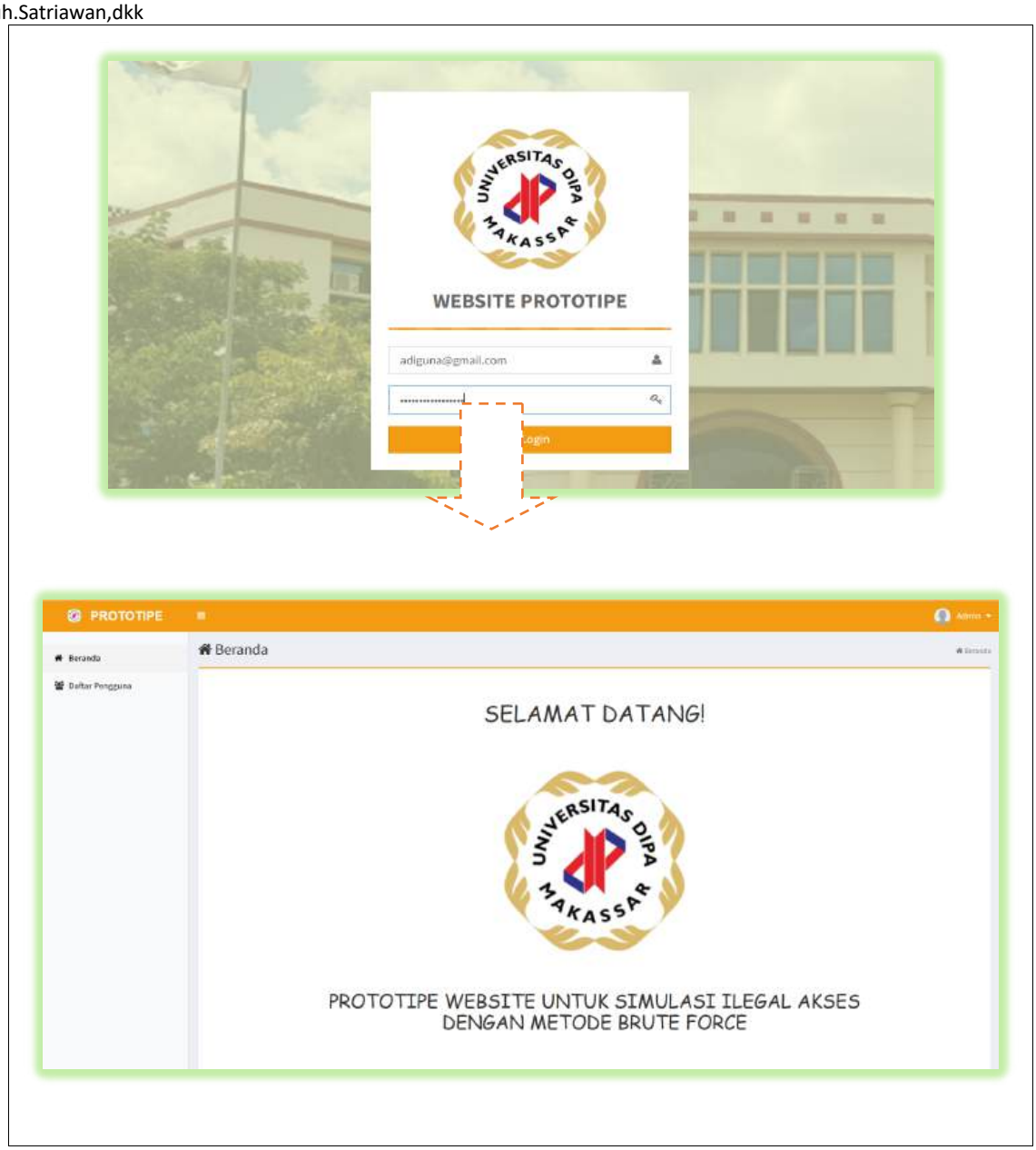
Test Factor	Hasil	Keterangan
Aplikasi harus bisa Mendisable User dari Aplikasi Android	✓	Aplikasi berhasil mendisable User dari aplikasi android
Antarmuka		



Fungsi Login Administrator

Tabel 6. Pengujian Login Administrator

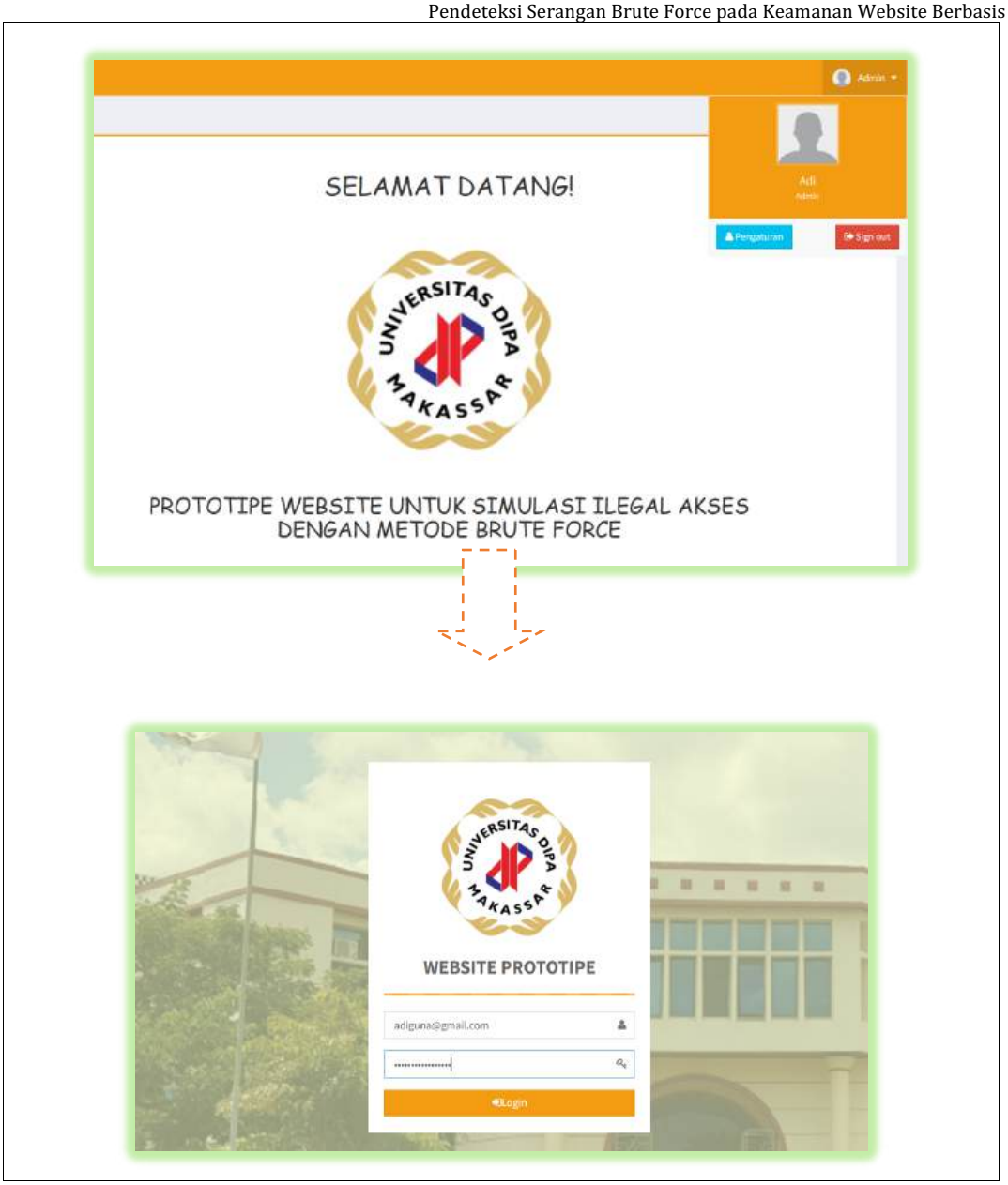
Test Factor	Hasil	Keterangan
Aplikasi harus dapat menampilkan menu utama	✓	Setelah login aplikasi berhasil menampilkan menu beranda pada aplikasi web
Antarmuka		



Fungsi Logout

Tabel 7. Pengujian Fungsi Logout dari Aplikasi

Test Factor	Hasil	Keterangan
Menguji fungsi Logout	✓	Berhasil Logout dengan indikator bahwa akan tampil Halaman Login
Antarmuka		



Fungsi Login Android

Tabel 8. Pengujian Fungsi Login android

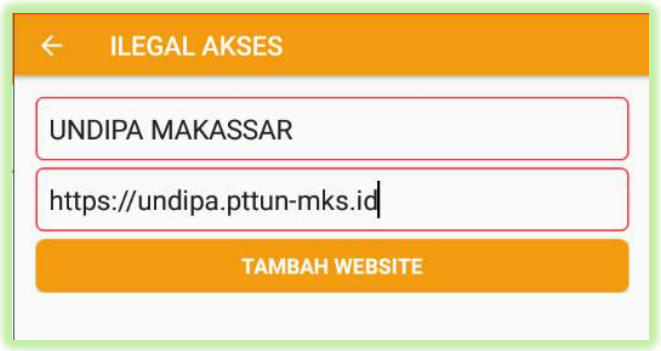
Test Factor	Hasil	Keterangan
Menguji fungsi Login Android	✓	Berhasil Login ke android dengan indikator tampil ke halaman utama android
Antarmuka		

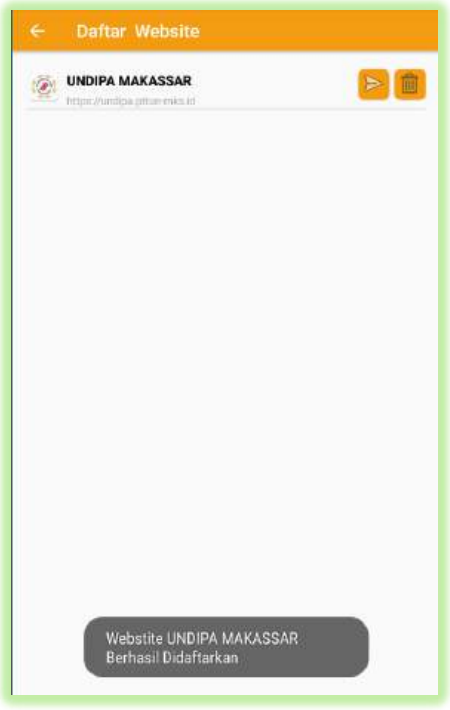
Fungsi Daftar Url Website

Tabel 9. Pengujian Fungsi Input URL Website

Test Factor	Hasil	Keterangan
Menguji fungsi input url website	✓	Berhasil menambahkan url website dengan indikator

		tampil pada halaman daftar website
Antarmuka		

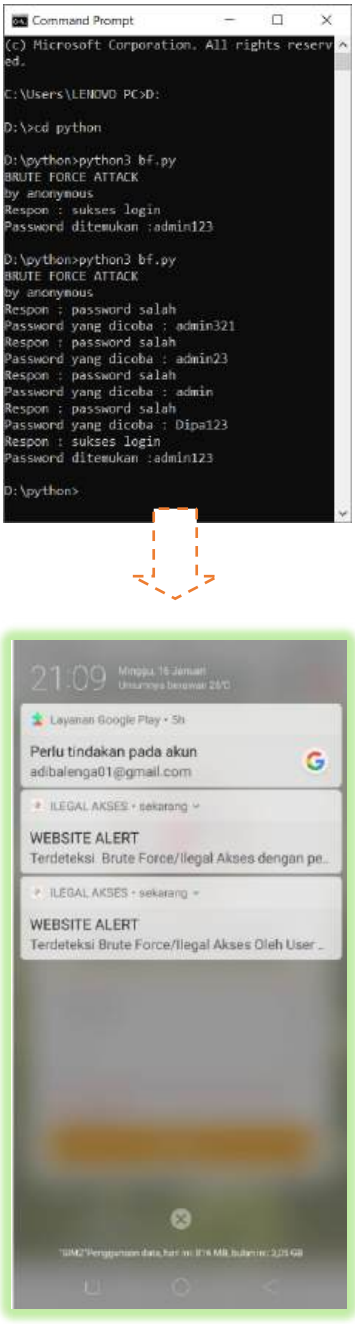




Fungsi Notifikasi Serangan Brute Force

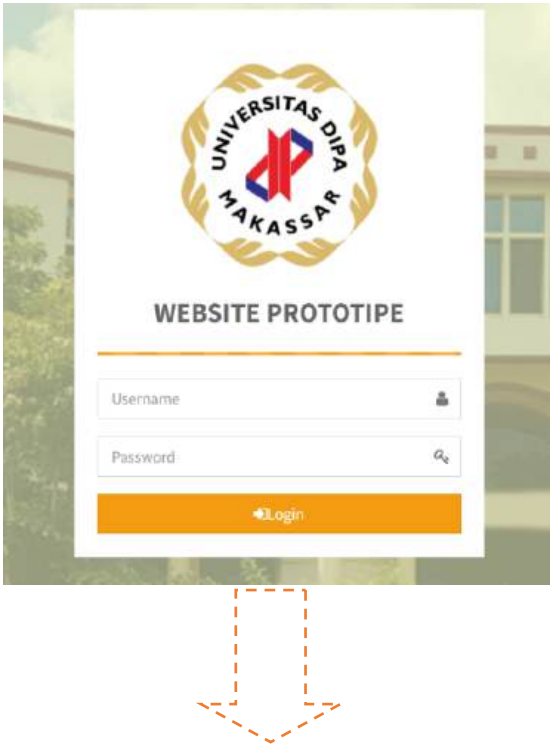
Tabel 10. Pengujian Fungsi Notifikasi Serangan Brute Force

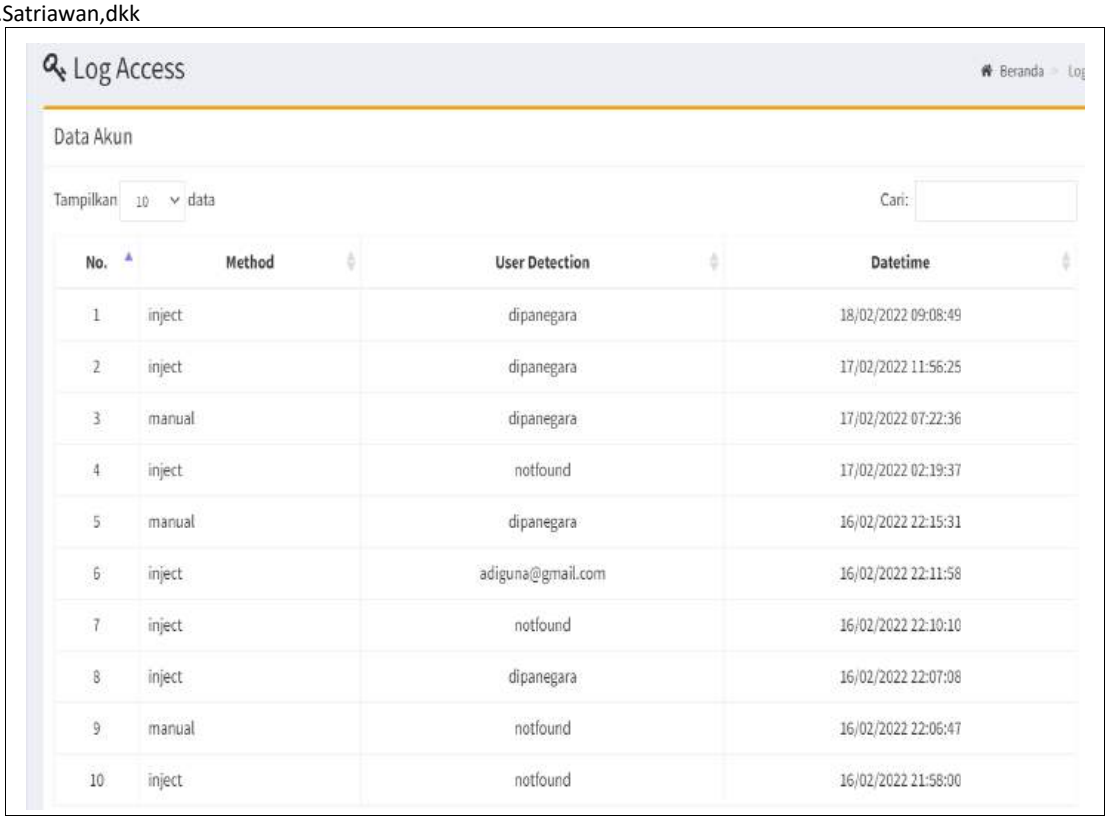
Test Factor	Hasil	Keterangan
Menguji fungsi notifikasi saat serangan brute force	✓	Berhasil mengirimkan notifikasi saat serangan brute force terjadi
Antarmuka		



Fungsi log *Access*

Tabel 11. Pengujian Fungsi log access

Test Factor	Hasil	Keterangan
Fungsi log access	✓	Berhasil mendeteksi user yang mencoba masuk ke dalam website
Antarmuka		
		



KESIMPULAN

Berdasarkan hasil pengujian aplikasi Pendeteksi Serangan Brute Force Pada Keamanan Website Berbasis Mobile maka diketahui bahwa:

1. Hasil pengujian fungsional dari sistem ini berjalan dengan benar sesuai dengan fungsional yang diinginkan.
2. Aplikasi dapat digunakan untuk melakukan penanganan dini terhadap serangan brute force dengan menggunakan peranti mobile.
3. Aplikasi berhasil menggunakan teknologi *firebase* dalam penanganan notifikasi secara real time ke perangkat mobile android administrator yang telah didaftarkan.

Daftar Pustaka

Doel, M. (2016). *Panduan Hacking Website dengan Kali Linux*. Elex Media Komputindo.

Krisbiantoro, D., Kom, M., Abda'u, P. D., & Kom, M. (2021). *DASAR PEMROGRAMAN WEB dengan bahasa HTML, PHP, dan Database MySQL* (Vol. 1). Zahira Media Publisher.

Muslihudin, M. (2016). *Analisis Dan Perancangan Sistem Informasi Menggunakan Model Terstruktur Dan UML*. Penerbit Andi.

Riandari, F., & Fahmi, H. (2019). *Rekayasa Perangkat Lunak*.

Riswaya, A. R. (2016). Sistem Keamanan Web Dengan Menggunakan Kriptografi Message Digest 5/Md5 Pada Koperasi Mitra Sejahtera Bandung. *Jurnal Computech & Bisnis*, *7*(1), 30–41.

Rohmansyah, R. R., & Nurwasito, H. (2017). Pengembangan Aplikasi Mobile untuk Sistem Keamanan Kantor Menggunakan NFC (Near Field Communication) dan Wi-Fi (Studi Kasus: PT. Rahmi Ida Nusantara). *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer E-ISSN*, *2548*, 964X.

Rosa, A. S. (2016). *Rekayasa perangkat lunak terstruktur dan berorientasi objek*. informatika.

Sari, I. Y., Muttaqin, M., Jamaludin, J., Simarmata, J., Rahman, M. A., Iskandar, A., Pakpahan, A. F., Abdul Karim, S., Giap, Y. C., & Hazriani, H. (2020). *Keamanan Data dan Informasi*. Yayasan Kita Menulis.

Utomo, D., Sholeh, M., & Avorizano, A. (2017). Membangun Sistem Mobile Monitoring Keamanan Web Aplikasi Menggunakan Suricata dan Bot Telegram Channel. *Prosiding Seminar Nasional Teknoka*, *2*, I81–I87.

Yudhanto, Y., & Wijayanto, A. (2018). *Mudah Membuat dan Berbisnis Aplikasi Android dengan Android Studio*. Elex Media Komputindo.

Profil Penulis

Muh. Satriawan adalah dosen pada Program Studi Kecerdasan Buatan, Universitas Kristen Indonesia Paulus, Makassar. Fokus penelitian meliputi pembelajaran mesin, pengolahan citra digital, kemanan komputer dan jaringan, dan penerapan kecerdasan buatan di bidang pertanian serta industri kreatif.