IMPLEMENTASI *AES* 256 UNTUK PENCEGAHAN *SQL INJECTION* DI PARAMETER ALAMAT URL DI TAHAP *PREPARE STATEMENT*

SKRIPSI

SABILILLAH FAUZAL ADDIM

NIM. 1810511017

PROGRAM STUDI S1 INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

2023

IMPLEMENTASI *AES* 256 UNTUK PENCEGAHAN *SQL INJECTION* DI PARAMETER ALAMAT URL DI TAHAP *PREPARE STATEMENT*

SKRIPSI

Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar

Sarjana Komputer

SABILILLAH FAUZAL ADDIM

NIM. 1810511017

PROGRAM STUDI S1 INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

2023

LEMBAR PERSETUJUAN

LEMBAR PERSETUJUAN

Dengan ini menyatakan bahwa skripsi berikut:

Nama	:	Sabilillah Fauzal Addim
NIM	:	1810511017
Program Studi	:	S1 Informatika
Judul	:	Implementasi AES 256 Untuk Pencegahan SQL Injection di Parameter Alamat URL di tahap Prepare Statment

Sebagai bagian persyaratan yang diperlukan untuk mengikuti ujian Sidang Tugas Akhir/Skripsi pada Program Studi S1 Informatika Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.

Menyetujui,

Dosen Pembimbing

Henki Bayu Seta, S.Kom., MTI

Mengetahui,

Ketua Program Studi

Dr. Widya Cholil, M.I.T

Ditetapkan : **Jakarta**

Tanggal Persetujuan : **18 Oktober 2023**

PERNYATAAN ORISINALITAS

PERNYATAAN ORISINALITAS

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

Nama	: Sabilillah Fauzal Addim
NIM	: 1810511017
Program Studi	: S1 Informatika
Judul	: Implementasi AES 256 Untuk Pencegahan *SQL Injection* di Parameter Alamat URL di tahap *Prepare statement*

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Bogor, 14 Januari 2024

Yang Menyatakan,

Sabilillah Fauzal Addim

PERNYATAAN PERSETUJUAN PUBLIKASI

PERNYATAAN PERSETUJUAN PUBLIKASI

Sebagai civitas akademik Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan di bawah ini:

Nama : Sabilillah Fauzal Addim

NIM : 1810511017

Fakultas : Ilmu Komputer

Program Studi : S1 Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non esklusif (*Non-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul

Implementasi *AES* 256 Untuk Pencegahan *SQL Injection* di Parameter Alamat URL di tahap *Prepare Statement*

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Tugas Akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.Dengan pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Bogor

Pada tanggal : 14 Januari 2024

Yang Menyatakan,

Sabilillah Fauzal Addim

LEMBAR PENGESAHAN

LEMBAR PENGESAHAN

Dengan ini menyatakan bahwa skripsi berikut:

Nama	: Sabilillah Fauzal Addim
NIM	: 1810511017
Program Studi	: S1 Informatika
Judul	: Implementasi AES 256 Untuk Pencegahan *SQL Injection* di Parameter Alamat URL di tahap *Prepare statment*

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana pada Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.

Dr. Didit Widiyanto, S.Kom, M.Si.
Penguji I

Yuni Widiastiwi, S.Kom, M.Si.
Penguji II

Henki Bayu Seta, S.Kom., MTI.
Pembimbing Skripsi

Erly Krisnanik S.Kom., MM.
Plt. Dekan

Dr. Widya Cholil, M.I.T
Kepala Program Studi

Ditetapkan di : Jakarta
Tanggal Ujian : 19 Desember 2023

IMPLEMENTASI *AES* 256 UNTUK PENCEGAHAN *SQL INJECTION* DI PARAMETER ALAMAT URL DI TAHAP *PREPARE STATEMENT*

Oleh Sabilillah Fauzal Addim

ABSTRAK

Dengan pesatnya kemajuan akan teknologi web membuat sebagian kegiatan individu dilakukan di sana. Sehingga aplikasi web menjadi hal penting sebagai pendukung dalam aktivitas individu di internet dalam kesehariannya. Bahaya kebocoran data pada situs web akibat injeksi *SQL* sering ditemui kasusnya dan bahkan menurut organisasi OWASP yang merupakan komunitas yang membahas aplikasi web menetapkan bahwa ancaman injeksi *SQL* berada di urutan ke 3 dari 10 urutan teratasnya. Cara kerja dari ancaman ini akibat hasil *input* pengguna terhadap aplikasi ditampilkan secara jelas dan tidak validasi, ini berpotensi digunakan sebagai area injeksi untuk pernyataan *SQL* berbahaya yang berfungsi mengekstraksi data dari basis data. Sehingga ancaman dari serangan injeksi *SQL* memiliki dampak yang besar sebab penyerang dapat mendapatkan hak akses ke basis data situs web dan informasi pada situs web layaknya pengguna sah. Makalah ini menyajikan pendekatan dalam mengidentifikasi dan mengamankan nilai atau isi di parameter yang di*temp*atkan pada alamat *URL* yang menyorot pada 2 aspek: yang pertama membuat nilai atau isi parameter terjaga kerahasiaannya dengan enkripsi dan langkah kedua melakukan penyiapan pernyataan *SQL* untuk menjaga agar kueri *SQL* tidak menjadi kueri yang berbahaya serta memastikan nilai parameter yang diikat dalam kueri memiliki tipe data yang sesuai dan dimodifikasi dalam bentuk aman sehingga layak untuk dieksekusi.

Kata kunci : *SQL Injection Attack,* Keamanan parameter alamat *URL, AES-256, Prepare Statement.*

ABSTRACT

With the rapid advancement of web technology, some individual activities are carried out there. So that web applications become important as a support for individual activities on the internet in their daily lives. The danger of data leakage on websites due to *SQL injection* is often encountered cases and even according to the OWASP organization which is a community that discusses web applications determines that the threat of *SQL injection* is in 3rd place out of the top 10. The way this threat works is because the results of user *input* to the application are displayed in a clear and invalidated manner, this can potentially be used as an *injection* area for malicious *SQL state*ments that function to extract data from the *database*. Therefore, the threat of *SQL injection* attacks has a great impact because the attacker can gain access rights to the website *database* and information on the website like a legitimate user. This paper presents an approach to identify and secure the values or contents in the parameters placed in the URL address highlighting 2 aspects: the first is to make the parameter values or contents confidential by encryption and the second step is to *prepare SQL state*ments to keep the *SQL* query from becoming a malicious query and ensure that the parameter values bound in the query have appropriate data types and are modified in a safe form so that they are eligible for execution.

***Keywords*: *SQL Injection Attack, Security URL address parameters, AES-256, Prepare Statement*.**

KATA PENGANTAR

Puji dan syukur saya panjatkan ke kehadirat Allah SWT yang selalu melimpahkan rahmat dan karunia-Nya sehingga dapat menyelesaikan penyusunan skripsi yang berjudul "Implementasi *AES* 256 Untuk Pencegahan *SQL Injection* di Parameter Alamat URL di tahap *Prepare Statement*" guna memenuhi syarat dalam memperoleh gelar sarjana pada program studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.

Penulis menyadari banyak pihak yang membantu dan memberi arahan dalam proses menyelesaikan skripsi ini. Sehingga penulis ingin menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Bapak Prof. Dr. Ir. Supriyanto, ST., M.Sc., IPM selaku Dekan Fakultas Ilmu Komputer.
2. Ibu Erly Krisnanik, S.Kom.,MM selaku Wakil Dekan Bidang Akademik Fakultas Ilmu Komputer.
3. Ibu Dr. Widya Cholil, S.Kom., M.I.T. selaku Kepala Program Studi Informatika.
4. Bapak Henki Bayu Seta, S.Kom., MTI. selaku Dosen Pembimbing Skripsi penulis yang telah banyak memberikan arahan dan saran yang sangat membantu dalam penyelesaian skripsi ini.
5. Para Bapak dan Ibu Dosen Fakultas Ilmu Komputer UPN Veteran Jakarta serta para Staf Akademik Fakultas Ilmu Komputer UPN Veteran Jakarta yang telah membantu penulis selama menempuh perkuliahan.
6. Untuk ayah dan ibu yang selalu memberikan dukungan kepada penulis untuk menyelesaikan skripsi.
7. Serta semua pihak yang telah membantu dan tidak dapat disebutkan satu persatu.

Semoga pihak yang membantu mendapat berkah dari Allah SWT. Akhir kata penulis menyadari skripsi ini masih banyak kekurangan , untuk itu penulis berharap dengan kerendahan hati meminta maaf dan mengharapkan saran dan kritik demi pengembangan ke arah yang lebih baik.

Bogor, 20 Oktober 2023

Sabilillah Fauzal Addim

DAFTAR ISI

LEMBAR PERSETUJUAN ii
PERNYATAAN ORISINALITAS iii
PERNYATAAN PERSETUJUAN PUBLIKASI iv
LEMBAR PENGESAHAN v
ABSTRAK vi
ABSTRACT vii
KATA PENGANTAR viii
DAFTAR ISI ix
DAFTAR GAMBAR xii
DAFTAR TABEL xix
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 2
1.3 Ruang Lingkup / Batasan Masalah 2
1.4 Tujuan Penelitian 3
1.5 Luaran yang diharapkan 3
1.6 Manfaat Penelitian 3
1.7 Sistematika Penulisan 4
BAB II TINJAUAN PUSTAKA 5
2.1 Situs Web 5
2.2 URL 5
2.3 Sintak URL 5
2.4 Parameter URL atau Nilai Parameter 7
2.5 Kriptografi 7
2.5.1 Jenis kriptografi 8
2.5.2 AES(Algoritma Rijnadael) 9
2.5.3 Key Expansion 9
2.5.4 Proses Enkripsi 14
2.5.5 Proses Deskripsi 22
2.6 Padding pada AES 24
2.7 Base64 25
2.8 Basis Data 28
2.8.1 Struktur basis data relasional 28

2.8.2 MySQL 29
2.9 Prepare Statement 29
2.9.1 Prepare statement dan SQL injection 33
2.10 SQL Injection Attack 34
2.10.1 Tipe SQL Injection 35
2.11 SQL Map 39
2.12 Cron Job 40
2.13 Penelitian Terkait 43
BAB III METODOLOGI PENELITIAN 50
3.1 Kerangka Pikir 50
3.2 Tahapan penelitian 51
3.2.1 Identifikasi Masalah 51
3.2.2 Studi Literatur 51
3.2.3 Menyiapkan Lingkungan Pengembangan Aplikasi Web 52
3.2.4 Pembuatan Aplikasi Web 53
3.2.5 Pembuatan skenario pengujian 58
3.2.6 Pengujian aplikasi web 59
3.2.7 Dokumentasi 60
3.3 Alat Bantu Penelitian 60
3.3.1 Perangkat Keras 61
3.3.2 Perangkat Lunak 61
3.4 Jadwal Penelitian 62
BAB IV PEMBAHASAN 63
4.1 Implementasi AES 63
4.1.1 Proses Pesan Dan Kunci Sebelum Enkripsi 63
4.1.2 Ekspansi Kunci 64
4.1.3 Proses Enkripsi 76
4.1.4 Encoding Base 64 84
4.1.5 Decode Base 64 87
4.1.6 Proses Deskripsi 88
4.2 Penerapan Enkripsi Nilai Parameter Pada Aplikasi 92
4.3 Penerapan Penjadwalan Penghasilan Kunci AES Pada Aplikasi 96
4.4 Implementasi Prepare Statement 103
4.5 Skenario Pengujian Manual 107
4.6 Skenario Pengujian Otomatis 109

4.7 Pengujian Situs Tanpa Pengamanan 110
4.7.1 Target Parameter 111
4.7.2 Pengujian Manual 112
4.7.3 Pengujian SQL Map 125
4.8 Pengujian Situs Dengan Enkripsi 132
4.8.1 Target Parameter 132
4.8.2 Pengujian Manual 133
4.8.3 Pengujian SQL Map 136
4.9 Pengujian Situs Dengan Prepare Statement 139
4.9.1 Target Parameter 139
4.9.2 Pengujian Manual 139
4.9.3 Pengujian SQL Map 142
4.10 Pengujian Dengan Enkripsi dan Prepare Statament 144
4.10.1 Target Parameter 144
4.10.2 Pengujian Manual 145
4.10.3 Pengujian SQL Map 146
4.11 Hasil Pengujian 149
4.11.1 Hasil Pengujian Situs Tanpa Pengamanan 149
4.11.2 Hasil Pengujian Situs Dengan Enkripsi AES 153
4.11.3 Hasil Pengujian Situs Dengan Prepeare Statment 155
4.11.4 Hasil Pengujian Situs Dengan Enkripsi AES Dan Metode Prepare statement 156
4.11.5 Kesimpulan Pengujian 158
BAB V Penutup 160
5.1 Kesimpulan 160
5.2 Saran 160
DAFTAR PUSTAKA 162
RIWAYAT HIDUP 166

DAFTAR GAMBAR

Gambar 2. 1 Ilustrasi URL dan bagiannya(Gourley, 2002a) 5
Gambar 2. 2 Contoh penulisan sintak alamat url 6
Gambar 2. 3 Contoh letak parameter(Ofiwe, n.d.) 7
Gambar 2. 4 Proses kriptografi(Munir, 2019) 8
Gambar 2. 5 Pseudo code proses *key* expansion *AES* (Rothke, 2007) 10
Gambar 2. 6 Contoh *array* kunci untuk dilakukan ekspansi kunci *AES* 11
Gambar 2. 7 Hasil *Key Expantion* untuk *Round Key* ke-1 12
Gambar 2. 8 Proses enkripsi *AES*(Munir, 2019) 14
Gambar 2. 9 Alur proses *AddRoundKey*(Munir, 2019) 14
Gambar 2. 10 Contoh proses *addroundkey* 15
Gambar 2. 11 Gambar tabel S-Box (Munir, 2019) 15
Gambar 2. 12 Alur Proses *SubBytes*(Munir, 2019) 16
Gambar 2. 13 Conton *state* yang akan dilakukan *subbytes* 16
Gambar 2. 14 Contoh proses berlangsungnya subtitusi *s-box* 16
Gambar 2. 15 Hasil subtitusi *s-box* 17
Gambar 2. 16 Alur proses *ShiftRow*(Munir, 2019) 17
Gambar 2. 17 Contoh kasus untuk *shiftrow* 17
Gambar 2. 18 Penggambaran proses *MixColumns*(Munir, 2019) 18
Gambar 2. 19 contoh kasus untuk *mixcolumn* 18
Gambar 2. 20 Tabel L untuk Mix Columns(Munir, 2019) 20
Gambar 2. 21 Tabel E untuk MixColumns(Munir, 2019) 20
Gambar 2. 22 contoh *addroundkey* dengan *round key*-2 pada putaran Nr-1 21
Gambar 2. 23 Proses deskripsi *AES* pada kasus *AES128* (Guang, 2019) 22
Gambar 2. 24 Alur proses inverse *ShiftRows*(Munir, 2019) 22
Gambar 2. 25 Gambar tabel inversi *S-Box*(Wijaya, 2020) 23
Gambar 2. 26 Proses inversi mix column(Munir, 2019) 23
Gambar 2. 27 Contoh penggunaan *padding*(Wong, 2021) 24
Gambar 2. 28 Contoh pengisian *padding* pada base64(Gourley, 2002b) 25
Gambar 2. 29 Pengelompokan biner per 24 bit(3 huruf)(Arif & Misdram, 2020) 27
Gambar 2. 30 Pemecahan nilai biner 24 bit ke biner per 6 bit dan konversi nilai bit ke indeks base64(Arif & Misdram, 2020) 27
Gambar 2. 31 Contoh bentuk tabel pada basis data relasional(Kurniati et al., 2022). 28
Gambar 2. 32 Konsep hirarki data pada basis data(Supono & Putratama, 2018). 29
Gambar 2. 33 Cara kerja *prepare statment* 32

Gambar 2. 34 Cara kerja escape *string* 33
Gambar 2. 35 Contoh *SQL Injection*(Tajpour et al., 2012) 34
Gambar 2. 36 Tipe *SQL Injection*(Rai et al., 2021) 35
Gambar 2. 37 Contoh kueri Boolean blind *SQL*i 36
Gambar 2. 38 Cara kerja *Error* based *SQL*i 38
Gambar 2. 39 Contoh kueri Union Query *SQL*i(Hlaing & Khaing, 2020) 39
Gambar 2. 40 Penjelasan Nilai pada Level di *sqlmap*(Lee, 2023) 40
Gambar 2. 41 Penjelasan Nilai pada riks di *sqlmap*(Lee, 2023) 40
Gambar 2. 42 Isi dari *cron*tab entry atau disebut *cron* field 41
Gambar 2. 43 Contoh membuat *cron* job di aapanel 42
Gambar 2. 44 Area Task list untuk melihat *cron* job yang sudah dibuat di aapanel 42
Gambar 2. 45 Log status dari *cron* job bernama “tampil tulisan hello” 43

Gambar 3. 1 Diagram kerangka pikir penelitian 50
Gambar 3. 2 Tampilan Menjalankan layanan apache dan my*sql* pada xampp 52
Gambar 3. 3 Tampilan bahasa php telah terinstall pada xampp 52
Gambar 3. 4 Diagram alur implementasi enkripsi dan deskripsi *AES 256* pada nilai parameter alamat *url* 54
Gambar 3. 5 Diagram alur implementasi metode *prepare statement* 56
Gambar 3. 6 Diagram pengujian model pencegahan 59

Gambar 4. 1 Pseudo code proses *key* expansion *AES* (Rothke, 2007) 66
Gambar 4. 2 Contoh proses subtitusi nilai pada *array* dengan tabel s-box 77
Gambar 4. 3 Contoh proses subtitusi nilai pada *array* dengan tabel inversi s-box 89
Gambar 4. 4 Baris kode penyiapan kunci manual dan nilai *input* sebagai plaintex untuk proses enkripsi 92
Gambar 4. 5 Tampilan tombol di situs yang digunakan untuk menghasilkan nilai 93
Gambar 4. 6 Hasil penerapan enkripsi pada nilai parameter filter = fik di situs *AES*.tasabil.my.id 93
Gambar 4. 7 Kode enkripsi *AES* 256 yang di terapkan pada situs yang diteliti 94
Gambar 4. 8 Skrip atau kode php untuk penghasil kunci *AES*-256 97
Gambar 4. 9 Gambar pembuatan *cron* job untuk eksekusi skrip pengahasil kunci(random_kunci.php) di aapanel 99
Gambar 4. 10 *Cron* job bernama “generate *key* buat *AES*” telah dibuat 99
Gambar 4. 11 Log status untuk *cron* job “generate *key* buat *AES*” 100

Gambar 4. 12 Kunci hasil menjalankan skrip penghasil kunci yang dijadwalkan dengan *cron*job pada pukul 16:21 100
Gambar 4. 13 Kunci hasil menjalankan skrip penghasil kunci yang dijadwalkan dengan *cron*job pukul 16.22 101
Gambar 4. 14 Baris kode penyiapan kunci otomatis dan nilai *input* sebagai plaintex untuk proses enkripsi 102
Gambar 4. 15 Hasil penerapan enkripsi pada nilai parameter filter = fik di situs *AES*.tasabil.my.id dengan kunci otomatis 102
Gambar 4. 16 Hasil pengecekan enkripsi dengan cryptotool dengan kasus kunci otomatis 103
Gambar 4. 17 Baris kode proses menghasilkan nilai dari tombol yang dipilih pada browser 104
Gambar 4. 18 Tampilan tombol di situs yang digunakan untuk menghasilkan nilai 104
Gambar 4. 19 Kode baris untuk mengecek parameter filter dan mengirim nilai parameter dikirim ke fungsi catalog 104
Gambar 4. 20 Baris kode untuk melakukan proses *prepare statment* 105
Gambar 4. 21 Proses Debug kueri *SQL* dan nilai parameter fileter = FIK yang diproses dengan *prepare statment* 106
Gambar 4. 22 Tampilan general log berisi kueri *sql* yang dikim ke server hasil metode *prepare state*ment dengan nilai parameter = FIK 107
Gambar 4. 23 *Payload*(konten muatan perintah) *crawling* parameter dengan *SQL Map* pada tasabil.my.id 111
Gambar 4. 24 Hasil ekseskusi dari *payload*(konten muatan perintah) *crawling* parameter dengan *SQL Map* pada tasabil.my.id 111
Gambar 4. 25 Tampilan situs tasabil.my.id sebelum *submit quote* pada alamat *url* 112
Gambar 4. 26 Tampilan situs tasabil.my.id setelah *submit quote* pada alamat tasabil.my.id/info.php?nim=15 112
Gambar 4. 27 Tampilan situs setelah *payload*(konten muatan perintah) logika pada alamat tasabil.my.id/info.php?nim=15 113
Gambar 4. 28 Log pengujian identifikasi kerentanan pada situs tasabil.my.id 113
Gambar 4. 29 Contoh *Payload*(konten muatan perintah) *Order by*(Portswigger, 2021) 114
Gambar 4. 30 *Payload*(konten muatan perintah) pengujian *Order By* indeks = 7(nilai indek tertinggi pada pengujian yang tidak menampilkan *error*) 114
Gambar 4. 31 Pengujian *order by* dengan indeks = 7 pada situs tasabil.my.id 114
Gambar 4. 32 *Payload*(konten muatan perintah) pengujian *Order By* indeks = 8(nilai indek pada pengujian yang tmenampilkan *error*) 115

Gambar 4. 33 Pengujian *order by* menampilkan *error* pada situs tasabil.my.id.....115
Gambar 4. 34 Log pengujian identifikasi jumlah kolom pada situs tasabil.my.id dengan *order by*.....115
Gambar 4. 35 *Payload*(konten muatan perintah) *UNION SELECT NULL*(PortSwigger Ltd, 2020).....116
Gambar 4. 36 *Payload*(konten muatan perintah) pengujian *UNION SELECT* yang tidak menampilkan *error* 116
Gambar 4. 37 Pengujian *UNION SELECT* saat nilai *NULL* tidak menampilkan *error* pada situs tasabil.my.id.....117
Gambar 4. 38 *Payload*(konten muatan perintah) pengujian *UNION SELECT* yang menampilkan *error* 117
Gambar 4. 39 Pengujian *UNION SELECT* saat nilai *NULL* menampilkan *error* pada situs tasabil.my.id.....117
Gambar 4. 40 Log pengujian identifikasi jumlah kolom pada situs tasabil.my.id dengan *union select null* 118
Gambar 4. 41 *Payload(*konten muatan perintah*)* penyisipan karakter pada nilai *NULL* 119
Gambar 4. 42 Tampilan pengujian penyisipan karakter pada nilai pada situs tasabil.my.id 119
Gambar 4. 43 Log pengujian identifikasi kolom pada nilai *null* dengan karakter pada situs tasabil.my.id.....119
Gambar 4. 44 *Payload(*konten muatan perintah*)* untuk menampilkan seluruh tabel pada basis data di my*sql*.....120
Gambar 4. 45 Hasil menampilkan semua tabel dari basis data di browser pada situs tasabil.my.id.....120
Gambar 4. 46 Log pengujian situs untuk mencari nama tabel pada basis data yang diakses parameter nim pada situs tasabil.my.id 121
Gambar 4. 47 *Payload(*konten muatan perintah*)* untuk menampilkan seluruh kolom pada basis data di my*sql*.....121
Gambar 4. 48 Hasil menampikan semua kolom dari basis data di browser pada situs tasabil.my.id.....121
Gambar 4. 49 Log pengujian situs untuk mencari nama kolom pada basis data yang diakses parameter nim pada situs tasabil.my.id 122
Gambar 4. 50 *Payload*(konten muatan perintah) untuk dump data pada situs tasabil.my.id.....123
Gambar 4. 51 Dump data yang ditampilkan di browser pada situs tasabil.my.id.....123
Gambar 4. 52 Tampilan Dashboard dengan akun rama berhasil *login* pada tasabil.my.id dengan data temuan pengujian manual 124

Gambar 4. 53 Log pengujian *dump data* pada basis data yang diakses parameter nim pada situs tasabil.my.id.....124
Gambar 4. 54 *Payload*(konten muatan perintah) untuk enumerasi basis data dan analisis jenis basis data pada alamat tasabil.my.id/info.php?nim=15.....125
Gambar 4. 55 Hasil ekseskusi proses *payload*(konten muatan perintah) enumerasi basis data dan analisis jenis basis data pada alamat tasabil.my.id/info.php?nim=15.....125
Gambar 4. 56 *Payload(*konten muatan *perintah)* enumerasi table dari basis data *sql*_tasabil di situs tasabil.my.id 127
Gambar 4. 57 Hasil ekseskusi proses *payload(*konten muatan perintah*)* enumerasi tabel pada alamat tasabil.my.id/info.php?nim=15.....127
Gambar 4. 58 *Payload*(konten muatan perintah) enumerasi kolom dari tabel user di situs tasabil.my.id.....128
Gambar 4. 59 Hasil ekseskusi proses *payload(*konten muatan perintah*)* enumerasi kolom pada alamat tasabil.my.id/info.php?nim=15.....128
Gambar 4. 60 *Payload*(konten muatan perintah) enumerasi kolom dari tabel user di situs tasabil.my.id.....130
Gambar 4. 61 Hasil ekseskusi proses *payload(*konten muatan perintah*)* dump data pada alamat tasabil.my.id/info.php?nim=15.....130
Gambar 4. 62 Tampilan Dashboard dengan akun admin berhasil *login* pada tasabil.my.id dengan data temuan pengujian *sqlmap* 131
Gambar 4. 63 Cuplikan Log pengujian *SQL Map* pada tasabil.my.id 132
Gambar 4. 64 *Payload*(konten muatan perintah) crawling url dengan *SQL Map* pada *AES*.tasabil.my.id.....132
Gambar 4. 65 Hasil ekseskusi dari *payload*(konten muatan perintah) *crawling* parameter dengan *SQL Map* pada *AES*.tasabil.my.id.....132
Gambar 4. 66 Tampilan situs submit quote pada Alamat *AES*.tasabil.my.id/info.php?nim=W7AEHbNqAebTi8hIRVzLAQ%3D%3D&*key*=MTIz NDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwYWI%3D&flag=1.....134
Gambar 4. 67 Tampilan situs setelah *payload*(konten muatan perintah) logika pada alamat *AES*.tasabil.my.id/info.php?nim=W7AEHbNqAebTi8hIRVzLAQ%3D%3D&*key*=MTIz NDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwYWI%3D&flag=1.....134
Gambar 4. 68 Cuplikan General Log proses identifikasi kerentanan pada situs *AES*.tasabil.my.id saat pengujian manual 135
Gambar 4. 69 *Payload*(konten muatan perintah) untuk enumerasi basis data dan analisis jenis basis data pada alamat

AES.tasabil.my.id/info.php?nim=W7AEHbNqAebTi8hIRVzLAQ%3D%3D&*key*=MTIz NDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwYWI%3D&flag=1.....136
Gambar 4. 70 Hasil ekseskusi proses *payload*(konten muatan perintah) enumerasi basis data dan analisis jenis basis data pada alamat *AES*.tasabil.my.id/info.php?nim=W7AEHbNqAebTi8hIRVzLAQ%3D%3D&*key*=MTIz NDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwYWI%3D&flag=1.....137
Gambar 4. 71 Cuplikan General Log pengujian *SQL Map* pada *AES*.tasabil.my.id.....138
Gambar 4. 72 *Payload*(konten muatan perintah) crawling url dengan *SQL Map* pada stmt.tasabil.my.id.....139
Gambar 4. 73 Hasil ekseskusi dari *payload*(konten muatan perintah) *crawling* parameter dengan *SQL Map* pada stmt.tasabil.my.id.....139
Gambar 4. 74 Tampilan situs sebelum submit quote pada situs stmt.my.id/info.php?nim=15.....140
Gambar 4. 75 Tampilan situs setelah submit quote pada situs stmt.my.id/index.php?nim=15’.....140
Gambar 4. 76 Tampilan situs setelah *payload*(konten muatan perintah) logika pada situs stmt.my.id/info.php?nim=15.....140
Gambar 4. 77 Proses Debug kueri *SQL* dan nilai parameter nim = 15 yang disisipkan *paylod* kutip(‘) 141
Gambar 4. 78 Proses Debug kueri *SQL* dan nilai parameter nim = 15 yang disisipkan *paylod* logika(‘OR 1=1-- -).....141
Gambar 4. 79 Cuplikan General Log identifikasi kerentanan pada situs stmt.tasabil.my.id 142
Gambar 4. 80 *Payload*(konten muatan perintah) untuk enumerasi basis data dan analisis jenis basis data di situs lab101en.my.id/info.php?nim=15 142
Gambar 4. 81 Hasil ekseskusi proses *payload*(konten muatan perintah) enumerasi basis data dan analisis jenis basis data pada alamat stmt.tasabil.my.id/info.php?nim=15.....143
Gambar 4. 82 Log pengujian *SQL Map* pada *AES*.tasabil.my.id 144
Gambar 4. 83 *Payload*(konten muatan perintah) crawling url dengan *SQL Map* pada all.tasabil.my.id.....144
Gambar 4. 84 Hasil ekseskusi dari *payload* crawling parameter dengan *SQL Map* pada all.tasabil.my.id.....144
Gambar 4. 85 Tampilan situs submit quote pada Alamat all.tasabil.my.id/info.php?nim=W7AEHbNqAebTi8hIRVzLAQ%3D%3D&*key*=MTIzN DU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwYWI%3D&flag=1 145

Gambar 4. 86 Tampilan situs setelah *payload*(konten muatan perintah) logika pada alamat all.tasabil.my.id/info.php?nim=W7AEHbNqAebTi8hIRVzLAQ%3D%3D&*key*=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwYWI%3D&flag=1 146
Gambar 4. 87 Log pengujian identifikasi kerentanan pada situs all.tasabil.my.id 146
Gambar 4. 88 *Payload*(konten muatan perintah) untuk enumerasi basis data dan analisis jenis basis data di situs all.tasabil.my.id/info.php?nim=W7AEHbNqAebTi8hIRVzLAQ%3D%3D&*key*=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwYWI%3D&flag=1 147
Gambar 4. 89 Hasil ekseskusi proses *payload* enumerasi basis data dan analisis jenis basis data pada alamat all.tasabil.my.id/info.php?nim=W7AEHbNqAebTi8hIRVzLAQ%3D%3D&*key*=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwYWI%3D&flag=1 147
Gambar 4. 90 Cuplika General Log pengujian *SQL Map* pada all.tasabil.my.id 148

DAFTAR TABEL

Tabel 2. 1 Komponen url dan penjelasanya 6
Tabel 2. 2 Versi *AES*(Munir, 2019) 9
Tabel 2. 3 Tabel Rcon *AES* 10
Tabel 2. 4 Tabel indeks base 64(Gunadhi & Nugraha, 2017) 26
Tabel 2. 5 Penelitian terkait 46

Tabel 3. 1 Jadwal Penelitian 62

Tabel 4. 1 *Payload*(konten muatan perintah) pengujian manual(Portswigger, 2021) 108
Tabel 4. 2 *Payload*(konten muatan perintah) *SQL Map* 110
Tabel 4. 3 Hasil keseluruhan pengujian pada situs tasabil.my.id 149
Tabel 4. 4 Hasil keseluruhan pengujian situs *AES*.tasabil.my.id 153
Tabel 4. 5 Hasil keseluruhan pengujian situs stmt.tasabil.my.id 155
Tabel 4. 6 Hasil keseluruhan pengujian situs all.tasabil.my.id 156
Tabel 4. 7 Tabel Komparasi Pengujian terhadap 4 Aplikasi web 158