IMPLEMENTASI METODE *HYBRID SCAN* UNTUK *INFORMATION GATHERING* DAN PENGUJIAN SISTEM MENGGUNAKAN *SQL INJECTION* BERBASIS *WEBSITE*

SKRIPSI

Disusun oleh:

Randi Rai

H1051171064

PROGRAM STUDI REKAYASA SISTEM KOMPUTER

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS TANJUNGPURA PONTIANAK

2025

IMPLEMENTASI METODE *HYBRID SCAN* UNTUK *INFORMATION GATHERING* DAN PENGUJIAN SISTEM MENGGUNAKAN *SQL INJECTION* BERBASIS *WEBSITE*

SKRIPSI

Sebagai Salah Satu Syarat untuk Memperoleh Gelar Sarjana Komputer pada Program Studi Rekayasa Sistem Komputer

Disusun oleh:

Randi Rai

H1051171064

PROGRAM STUDI REKAYASA SISTEM KOMPUTER

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS TANJUNGPURA PONTIANAK

2025

LEMBAR PENGESAHAN

Judul Tugas Akhir : Implementasi Metode *Hybrid Scan* Untuk *Information Gathering* dan Pengujian Sistem Menggunakan *SQL Injection* Berbasis *Website*.
Nama Mahasiswa : Randi Rai
NIM : H1051171057
Jurusan/Program Studi : Rekayasa Sistem Komputer
Tanggal Lulus : 30 Juli 2024
SK Pembimbing : No.656/UN22.8/TD.06/Tanggal 14 Februari 2023
SK Penguji : No.2177/UN22.8/TD.06/Tanggal 29 Juli 2024

Dosen Pembimbing

Pembimbing I	Pembimbing II
Ikhwan Ruslianto, S.Kom., M.Cs.	Kasliono, S.Mat., M.Cs.
NIP. 198607012014041001	NIP. 199306202022031005

Dosen Penguji

Ketua Penguji	Anggota Penguji
Dwi Marisa Midyanti, S.T., M.Cs.	Hafiz Muhardi, S.T., M.Kom.
NIP. 198003192015042001	NIP. 199007232023211017

Pimpinan Sidang (merangkap anggota penguji)	Sekretaris Sidang (merangkap anggota penguji)
Ikhwan Ruslianto, S.Kom., M.Cs.	Kasliono, S.Mat., MCs.
NIP. 198607012014041001	NIP. 199306202022031005

Mengesahkan
Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Tanjungpura

Prof. Dr. Gusrizal, S.Si., M.Si.
NIP. 197108022000031001

PERNYATAAN INTEGRITAS AKADEMIK

Saya yang bertanda tangan di bawah ini:

Nama	: Randi Rai
NIM	: H1051171064
Program Studi	: Rekayasa Sistem Komputer
Fakultas	: Matematika dan Ilmu Pengetahuan Alam
Judul Skripsi	: Implementasi Metode *Hybrid scan* untuk *Information Gathering* dan Pengujian Sistem Menggunakan *SQL Injection* Berbasis *Website*

Menyatakan bahwa seluruh komponen dan isi dalam skripsi ini adalah hasil karya saya sendiri, dan tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun. Apabila di kemudian hari terbukti bahwa ada beberapa bagian dari karya ini adalah bukan hasil saya sendiri, maka saya akan siap menanggung resiko dan konsekuensi apapun.

Demikian pernyataan ini saya buat, semoga dapat dipergunakan sebagaimana mestinya.

Pontianak, 18 Juli 2024



Randi Rai
NIM. H1051171064

IMPLEMENTASI METODE *HYBRID SCAN* UNTUK *INFORMATION GATHERING* DAN PENGUJIAN SISTEM MENGGUNAKAN *SQL INJECTION* BERBASIS *WEBSITE*

ABSTRAK

Teknologi informasi dan komunikasi mengalami kemajuan pesat, yang diiringi dengan tantangan keamanan. Salah satu ancaman yang sering dihadapi oleh situs web adalah *SQL Injection*, yang termasuk dalam ancaman paling serius dalam daftar kerentanan web. Kemudian kerentanan pada *website* juga dapat ditemukan pada tahap awal, yaitu *information gathering*. Namun, dalam melakukan *information gathering* dan pengujian keamanan, masih diperlukan banyak alat yang berbeda untuk mendapatkan informasi yang diinginkan. Selain itu, hasil dari alat-alat tersebut umumnya berbasis *Command Line Interface* (CLI). Oleh karena itu, pada penelitian ini dibangun sistem dengan metode *hybrid scan* berbasis *website* untuk mempermudah tahap *information gathering* dan pengujian kerentanan *SQL Injection*. Metode *hybrid scan* menggabungkan pemindaian aktif dan pasif. Pemindaian aktif memanfaatkan subfinder, dig, theharvester, curl, host, nmap, whatweb, LBD, dan pengujian dengan *Sqlmap*. Sedangkan pemindaian pasif memanfaatkan API Shodan, API ViewDNS. dan API Diffbot. Hasil pengujian pada 5 web menunjukkan bahwa semua web yang diuji berhasil didapatkan informasi terkait subdomain, alamat IP, URL, host yang aktif, sistem operasi, teknologi, serta status *Load Balancing* dan port yang terbuka. Hasil deteksi kerentanan *SQL Injection* pada web pertama menunjukkan kerentanan tingkat sedang, sedangkan web kedua dan ketiga memiliki kerentanan tinggi, web keempat dan kelima tidak rentan. Waktu yang dibutuhkan untuk proses ini berkisar antara 4 hingga 33 menit.

Kata Kunci: *SQL Injection, hybrid scan, information gathering*

IMPLEMENTASI METODE *HYBRID SCAN* UNTUK *INFORMATION GATHERING* DAN PENGUJIAN SISTEM MENGGUNAKAN *SQL INJECTION* BERBASIS *WEBSITE*

ABSTRACT

Information and communication technology has advanced rapidly, accompanied by security challenges. One of the threats often faced by websites is SQL Injection, which is among the most serious threats in the web vulnerability list. Furthermore, website vulnerabilities can also be found at an early stage, namely information gathering. However, in conducting information gathering and security testing, many different tools are still needed to obtain the desired information. Additionally, the results from these tools are generally based on the Command Line Interface (CLI). *Therefore, in this research, a system with a website-based hybrid scan method was built to facilitate the information gathering stage and SQL Injection vulnerability testing. The hybrid scan method combines active and passive scanning. Active scanning utilizes subfinder, dig, theharvester, curl, host, nmap, whatweb,* LBD*, and testing with Sqlmap. Meanwhile, passive scanning utilizes the* Shodan API*,* API ViewDNS*, and the* Diffbot API*. Test results on* 5 *websites showed that all tested websites successfully provided information related to subdomains,* IP *addresses,* URL*s, active hosts, operating systems, technologies, as well as Load Balancing status and open ports. The SQL Injection vulnerability detection results on the first website showed a medium level of vulnerability, while the second and third websites had high vulnerabilities, and the fourth and fifth websites were not vulnerable. The time required for this process ranged from 4 to 33 minute*.

Keywords*: SQL Injection, hybrid scan, information gathering*

PRAKATA

Segala puji dan syukur kepada Allah SWT, atas segala rahmat dan karunia yang melimpah sehingga penulis dapat menyelesaikan skripsi yang berjudul "Implementasi Metode *Hybrid scan* untuk *Information Gathering* dan Pengujian Sistem Menggunakan *SQL Injection* Berbasis *Website*".

Tujuan dari penyusunan skripsi ini guna memenuhi salah satu syarat untuk memperoleh gelar sarjana komputer pada Program Studi Rekayasa Sistem Komputer Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Tanjungpura.

Penulis menyadari bahwa dalam penyusunan skripsi ini terdapat banyak bimbingan, petunjuk, saran, maupun dorongan moril dari berbagai pihak. Oleh karena itu, penulis ingin menyampaikan ucapan terima kasih kepada yang terhormat:

1. Bapak Dr. Gusrizal, S.Si., M.Si., selaku Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Tanjungpura.
2. Bapak Ikhwan Ruslianto, S.Kom., M.Cs., selaku Ketua Jurusan/Program Studi Rekayasa Sistem Komputer dan selaku dosen pembimbing pertama yang telah meluangkan waktu dan pikiran untuk membimbing, memberikan nasehat serta masukan dan saran dalam menyelesaikan skripsi.
3. Bapak Kasliono, S.Mat., M.Cs., selaku dosen pembimbing kedua yang telah memberikan waktu, tenaga, petunjuk, bimbingan, dan pengarahan dalam penyusunan skripsi ini.
4. Ibu Dwi Marisa Midyanti, S.T., M.Cs., selaku dosen penguji pertama dan selaku pembimbing akademik yang telah memberikan arahan, masukan, serta saran dalam menyelesaikan skripsi dan bimbingan akademik selama perkuliahan.
5. Bapak Hafiz Muhardi, S.T., M.Kom., selaku dosen penguji kedua yang telah memberikan arahan, masukan, serta saran dalam menyelesaikan skripsi.
6. Seluruh dosen serta staf jurusaan Rekayasa Sistem Komputer Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Tanjungpura.

7. Kedua orang tua penulis, Junaedi dan Siti Khadijah yang selalu memberikan kasih sayang, doa, nasehat, serta atas kesabarannya yang luar biasa dalam setiap langkah hidup penulis, yang merupakan anugrah terbesar dalam hidup. Penulis berharap dapat menjadi anak yang dapat dibanggakan.
8. Keluarga besar mahasiswa Sistem Komputer 2017 yang selalu memberi bantuan, nasehat, mengingatkan dan saran dalam pengerjaan skripsi.
9. Pihak-pihak yang tidak dapat disebutkan satu per satu yang turut membantu dalam penyusunan skripsi ini.

Penulis menyadari bahwa skripsi ini masih banyak terdapat kekurangan. Oleh karena itu, kritik dan saran yang bersifat membangun akan penulis terima dengan senang hati. Semoga skripsi ini bermanfaat bagi penulis maupun pembaca.

Pontianak, 18 Juli 2024

Randi Rai
NIM. H1051171064

DAFTAR ISI

LEMBAR PENGESAHAN ..... **Kesalahan! Bookmark tidak ditentukan.**
PERNYATAAN INTEGRITAS AKADEMIK**Kesalahan! Bookmark tidak ditentukan.**
ABSTRAK iv
ABSTRACT v
PRAKATA vi
DAFTAR ISI viii
DAFTAR GAMBAR x
DAFTAR TABEL xiii
DAFTAR KODE PROGRAM xiv
BAB 1 PENDAHULUAN 1
1.1. Latar Belakang 1
1.2. Rumusan Masalah 3
1.3. Batasan Masalah 3
1.4. Tujuan Penelitian 3
1.5. Manfaat Penelitian 4
1.6. Sistematika Penulisan 4
BAB 2 LANDASAN TEORI 7
2.1. Perbandingan dengan penelitian terdahulu 7
2.2. *Hybrid scan* 8
2.3. *Information Gathering* 9
2.4. Subfinder 9
2.5. Dig 10
2.6. TheHarvester 10
2.7. Curl 11
2.8. Host 11
2.9. *Network Mapper* (NMAP) 12
2.10. WhatWeb 12
2.11. *Load Balancing Detector* (LBD) 13
2.12. *Penetration Testing* 13
2.13. *SQL Injection* 14
2.14. Laravel 17
2.15. *Website* 18
BAB 3 METODE PENELITIAN 19
3.1. Studi Literatur 19
3.2. Pengumpulan Data 20
3.3. Analisis Kebutuhan 20
3.4. Perancangan Sistem 22

3.5. Implementasi 22
3.6. Pengujian 23
3.7. Analisis dan Pembahasan 24
3.8. Kesimpulan dan Saran 24
BAB 4 PERANCANGAN 25
4.1. Deskripsi Sistem 25
4.2. Perancangan Sistem 26
4.3. Perancangan Perangkat Lunak 30
4.4. Perancangan Basis Data 32
BAB 5 IMPLEMENTASI, PENGUJIAN DAN PEMBAHASAN 34
5.1. Implementasi *Hybrid scan* 34
5.2. Implementasi Sistem 34
5.3. Kode Program 37
5.4. Pengujian Sistem 42
BAB 6 PENUTUP 70
6.1. Kesimpulan 70
6.2. Saran 71
DAFTAR PUSTAKA 72

DAFTAR GAMBAR

Gambar 2.1. Cara kerja *SQL Injection* 15
Gambar 3.1. Diagram Alir Penelitian 19
Gambar 3.2. *Website* Error Potensi Rentan..... 20
Gambar 4.1. Arsitektur Secara Umum..... 25
Gambar 4.2. Arsitektur *Hybrid scan* 26
Gambar 4.3. Alur Proses *Information Gathering*..... 27
Gambar 4.4. Alur Proses *SQL Injection*..... 29
Gambar 4..5. Halaman *Login* 31
Gambar 4.6. Halaman Penggunaan..... 31
Gambar 4.7. Halaman Hasil..... 32
Gambar 5.1. Halaman *Login* 35
Gambar 5.2. Halaman Penggunaan..... 36
Gambar 5.3. Halaman hasil..... 36
Gambar 5.4. Input Domain, Url dan Perintah Web Pertama 43
Gambar 5.5. Hasil Sub Domain Web Pertama..... 44
Gambar 5.6. Hasil *Reverse* IP 44
Gambar 5.7. Hasil *Page link extraction* 44
Gambar 5.8. Hasil *Check live host* 45
Gambar 5.9. Hasil Convert IP Domain..... 45
Gambar 5.10. Hasil OS *Version*..... 45
Gambar 5.11. Hasil Web Teknologi. 46
Gambar 5.12. Hasil *Load Balancing Detector*..... 46
Gambar 5.13. Hasil Port *Scanning*..... 46
Gambar 5.14. Hasil *SQL Injection* 47
Gambar 5.15. Input Domain, Url dan Target kedua 48
Gambar 5.16. Hasil Sub Domain Target Kedua 49
Gambar 5.17. Hasil *Reverse* IP Target Kedua 49
Gambar 5.18. Hasil *Page link extraction* Target Kedua..... 50
Gambar 5.19. Hasil *Check live host* Target Kedua..... 50
Gambar 5.20. Hasil Convert IP Domain Target Kedua 50

Gambar 5.21. Hasil OS *Version* Target Kedua 50
Gambar 5.22. Hasil Web Teknologi Target Kedua..... 51
Gambar 5.23. Hasil *Load Balancing Detector* Target Kedua 51
Gambar 5.24. Hasil Port *Scanning* Target Kedua 51
Gambar 5.25. Hasil *SQL Injection* Target Kedua 52
Gambar 5.26. Input Domain, Url dan Target Ketiga 53
Gambar 5.27. Hasil Sub Domain Target Ketiga 54
Gambar 5.28. Hasil *Reverse* IP Target Ketiga 54
Gambar 5.29. Hasil *Page link extraction* Target Ketiga 54
Gambar 5.30. Hasil *Check live host* Target Ketiga 55
Gambar 5.31. Hasil Convert IP Domain Target Ketiga 55
Gambar 5.32. Hasil OS *Version* Target Ketiga..... 55
Gambar 5.33. Hasil Web Teknologi Target Ketiga 56
Gambar 5.34. Hasil *Load Balancing Detector* Target Ketiga..... 56
Gambar 5.35. Hasil Port *Scanning* Target Ketiga..... 56
Gambar 5.36. Hasil *SQL Injection* Target Kedua 57
Gambar 5.37. Input Domain, Url dan Target Keempat..... 58
Gambar 5.38. Hasil Sub Domain Target Keempat 58
Gambar 5.39. Hasil *Reverse* IP Target Keempat 59
Gambar 5.40. Hasil *Page link extraction* Target Keempat 59
Gambar 5.41. Hasil *Check live host* Target Keempat 60
Gambar 5.42. Hasil Convert IP Domain Target Keempat 60
Gambar 5.43. Hasil OS *Version* Target Keempat..... 60
Gambar 5.44. Hasil Web Teknologi Target Keempat..... 60
Gambar 5.45. Hasil *Load Balancing Detector* Target Keempat..... 61
Gambar 5.46. Hasil Port *Scanning* Target Keempat..... 61
Gambar 5.47. Hasil *SQL Injection* Target Keempat 62
Gambar 5.48. Input Domain, Url dan Target Kelima 62
Gambar 5.49. Hasil Sub Domain Target Kelima 63
Gambar 5.50. Hasil *Reverse* IP Target Kelima..... 63
Gambar 5.51. Hasil *Page link extraction* Target Kelima..... 63
Gambar 5.52. Hasil *Check live host* Target Kelima..... 64

Gambar 5.53. Hasil Convert IP Domain Target Kelima 64
Gambar 5.54. Hasil OS *Version* Target Kelima 64
Gambar 5.55. Hasil Web Teknologi Target Kelima 65
Gambar 5.56. Hasil *Load Balancing Detector* Target Kelima 65
Gambar 5.57. Hasil Port *Scanning* Target Kelima 65
Gambar 5.58. Hasil *SQL Injection* Target Kelima 66

DAFTAR TABEL

Tabel 2.1. Perbandingan dengan Penelitian Terdahulu 7
Tabel 2.2. Perbandingan dengan Penelitian terdahulu Lanjutan 8
Tabel 4.1. Tabel Users. 32
Tabel 4.2. Tabel Results. 33
Tabel 5.1. Tabel *Information Gathering* 67
Tabel 5.2. Tabel *Information Gathering* Lanjutan 67
Tabel 5.3. Tabel *SQL Injection* 67
Tabel 5.4. Tabel Hasil Pengujian Blackbox 68
Tabel 5.5. Tabel Hasil Pengujian Black Box Lanjutan 68

DAFTAR KODE PROGRAM

Kode Program 5.1. Program Menjalankan *Sub domain enumeration* 37
Kode Program 5.2. Program menjalankan tools dig 37
Kode Program 5.3. Program menjalankan tools theHarvester..... 38
Kode Program 5.4. Program menjalankan tools 38
Kode Program 5.5. Program menjalankan tools host..... 38
Kode Program 5.6. Program menjalankan os *version*..... 39
Kode Program 5.7. Program menjalankan web teknologi 39
Kode Program 5.8. Program menjalankan *Load Balancing* 39
Kode Program 5.9. Program menjalankan port *scanning* 40
Kode Program 5.10. Program menjalankan *SQL Injection*..... 40
Kode Program 5.11. Program API *sub domain enumeration* 41
Kode Program 5.12. Program menjalankan API *Reverse* ip..... 41
Kode Program 5.13. Program menjalankan API *page link extraction*..... 42

BAB 1
PENDAHULUAN

1.1. Latar Belakang

Dalam era modernisasi, perkembangan teknologi informasi dan komunikasi terus mengalami kemajuan yang signifikan seiring dengan perubahan zaman. Teknologi ini digunakan untuk mengelola, memproses, memperoleh, menyusun, dan menyimpan data melalui berbagai metode dengan tujuan menghasilkan informasi yang berkualitas dan sesuai dengan fakta(Dan, 2023). Walaupun teknologi informasi dan komunikasi memfasilitasi akses informasi bagi masyarakat, kemajuan ini juga membawa konsekuensi negatif, terutama dalam aspek keamanan informasi.

Keamanan informasi adalah tindakan perlindungan yang bertujuan untuk menjaga berbagai jenis informasi dari penyalahgunaan oleh pihak-pihak yang tidak bertanggung jawab(Dalimunthe & Sahren, 2020). Dalam menghadapi perkembangan teknologi, keamanan informasi menjadi tantangan signifikan bagi masyarakat dan pengembang situs web. Tidak ada jaminan pasti terkait keamanan sistem digital, dan sering kali terdapat celah yang dapat dimanfaatkan untuk menyerang sistem situs web, yang berpotensi menimbulkan kerugian bagi pemiliknya. Ancaman keamanan dapat mengancam integritas, kerahasiaan, dan ketersediaan data. Oleh karena itu, penting untuk melindungi sistem berbasis digital dengan mempertimbangkan ketiga aspek tersebut.

Salah satu ancaman yang sering dihadapi oleh situs web adalah *SQL Injection*, yang termasuk dalam ancaman paling serius dalam daftar kerentanan situs web(Friadi & Septian, 2021). Serangan ini mengeksploitasi celah pada *query* dengan menyisipkan pernyataan *SQL*. Pemilik *website* sering kali tidak menyadari kerentanan ini, sehingga menganggap keamanan situs mereka telah sepenuhnya terjamin. *SQL Injection* dapat mencuri data administrator dan bahkan menguasai situs web karena *input* pengguna yang tidak divalidasi. Serangan ini berbahaya karena memungkinkan penyerang untuk memanipulasi data dalam *database*, mengakibatkan kerugian signifikan bagi pemilik *website*.

Kemudian kerentanan pada *website* juga dapat ditemukan pada tahap awal, yaitu *information gathering*. Tahap ini melibatkan pengumpulan informasi seperti status atau tipe jaringan, jenis sistem operasi yang digunakan, rentang alamat IP yang digunakan, port yang terbuka, dan server DNS yang digunakan. *Information gathering* juga dapat digunakan untuk mengidentifikasi kepemilikan suatu sistem (Zeeshan et al., 2017).

Namun, dalam melakukan *Information gathering* dan pengujian sistem menggunakan teknik *SQL Injection*, masih diperlukan banyak alat yang berbeda untuk mendapatkan informasi yang diinginkan. Selain itu, hasil dari alat-alat tersebut umumnya berbasis *Command Line Interface* (CLI). Untuk mengatasi masalah ini, diperlukan implementasi metode *hybrid scan* untuk mendapatkan informasi yang diinginkan dan mempermudah proses *Information gathering* serta pengujian sistem menggunakan *SQL Injection* dengan menggunakan antarmuka pengguna berbasis *website*.

Penelitian terkait metode *hybrid scan* yang relevan dengan penelitian ini adalah "Pengembangan Aplikasi *Information Gathering* Menggunakan Metode *Hybrid scan* Berbasis *Graphical User Interface*" yang dilakukan oleh(Riasetiawan et al., 2021). Penelitian ini menghasilkan pengembangan aplikasi atau alat bantu pengujian keamanan sistem dan jaringan komputer yang komprehensif dan dilengkapi dengan laporan yang memudahkan tim manajemen dan teknis. Pengembangan ini dilakukan menggunakan bahasa pemrograman Python dengan modul untuk menghasilkan aplikasi berbasis *Graphical User Interface* (GUI). Fokus pengembangan aplikasi tersebut adalah pada tahap *Information gathering* yang menggunakan metode *hybrid scan*, yaitu pemindaian pasif dan aktif. Pemindaian pasif menggunakan 11 *Application Programming Interface* (API), sedangkan pemindaian aktif menggunakan modul *Socket* Python dan beberapa perangkat bawaan yang berjalan di GNI/Linux.

Penelitian terkait *SQL Injection* yang relevan dengan penelitian ini adalah "*Web Application Penetration Testing Using SQL Injection Attack*" yang dilakukan oleh (Alanda et al., 2021). Penelitian ini melakukan pengujian pada sepuluh situs web secara acak dengan mencari celah untuk menguji keamanan menggunakan serangan *SQL Injection*. Hasil pengujian menunjukkan bahwa 80% dari situs web

yang diuji memiliki kelemahan terhadap *SQL Injection*. Penelitian ini menegaskan bahwa *SQL Injection* masih merupakan ancaman umum bagi aplikasi web.

Penelitian lain yang relevan dengan pengujian keamanan sistem adalah "Pengembangan Aplikasi *Information gathering* Berbasis HybridApps"(Setiawan et al., 2022). Penelitian ini melakukan *information gathering* dengan menggunakan aplikasi sudomy yang masih berbasis CLI, sehingga dibuat berbasis *website*.

Berdasarkan latar belakang tersebut, penelitian ini dilakukan dengan judul "Implementasi Metode *Hybrid scan* untuk *Information gathering* dan Pengujian Sistem Menggunakan *SQL Injection* Berbasis *Website*". Sistem ini bertujuan untuk mempermudah pengguna dalam melakukan *Information gathering* dan pengujian keamanan sebuah *website* menggunakan Teknik *SQL Injection*. Pengguna hanya perlu membuka aplikasi *website*, memasukkan nama domain atau alamat IP *website* yang ingin diambil informasinya, dan menguji keamanan *website* tersebut menggunakan teknik *SQL Injection*.

1.2. Rumusan Masalah

Adapun rumusan masalah dari penelitian ini adalah:

1. Berapa lama waktu yang dibutuhkan *website* dalam melakukan *infomation gathering* dan pengujian kerentanan target terhadap *SQL Injection* ?
2. Bagaimana kerentanan *website* terhadap serangan *SQL Injection* ?

1.3. Batasan Masalah

Adapun batasan masalah dari penelitian ini adalah:

1. Metode yang digunakan yaitu *Hybrid scan* dalam melakukan *information gathering*.
2. Pengujian dilakukan pada 5 *website* yang telah dipilih.
3. Aplikasi yang dibangun berbasis *website*.
4. Menguji keamanan sistem menggunakan teknik *SQL Injection*.

1.4. Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah:

1. Mengetahui waktu yang dibutuhkan *website* dalam melakukan *information gathering* dan pengujian kerentanan *SQL Injection*.
2. Mengetahui bagaimana kerentanan *website* terhadap serangan *SQL Injection*.

1.5. Manfaat Penelitian

Manfaat dari penelitian ini adalah memberikan kemudahan bagi pengguna dalam melakukan *Information gathering* dan Pengujian sistem menggunakan teknik *SQL Injection*. Dengan demikian, penelitian ini memiliki tujuan untuk meningkatkan pemahaman pengguna terkait keamanan suatu *website* terhadap *SQL Injection*. Dengan menggunakan metode yang diimplementasikan dalam penelitian ini, pengguna dapat mengumpulkan informasi yang relevan dan melakukan pengujian sistem dengan lebih efisien. Hasil dari penelitian ini akan memberikan wawasan yang lebih baik mengenai tingkat keamanan *website* terhadap serangan *SQL Injection*, memungkinkan pengguna untuk mengambil tindakan yang sesuai dalam meningkatkan keamanan *website* tersebut. Dengan adanya penelitian ini, pengguna juga akan dapat mengidentifikasi potensi kerentanan dan menerapkan tindakan pencegahan yang efektif untuk melindungi *website* dari serangan *SQL Injection*.

1.6. Sistematika Penulisan

Adapun sistematika penulisan dari penelitian ini adalah:

BAB 1 PENDAHULUAN

Dalam bab pendahuluan berisi tentang latar belakang penelitian yang menjelaskan permasalahan dan alasan kenapa penelitian ini dilakukan. Rumusan masalah penelitian disusun secara deskriptif dengan permasalahan pada kerentanan suatu *website* terhapat serangan *SQL Injection* dan sulitnya dalam melakukan *information gathering*, dengan solusi permasalahan yaitu dibangun sistem menggunakan metode *hybrid scan* dalam melakukan *information gathering*, dan deteksi kerentanan *SQL Injection* secara otomatis sebagai salah satu solusi permasalahan yang ada. Batasan masalah penelitian dibuat agar tidak menyimpang dari tujuan penelitian. Tujuan penelitian yang dibuat menjawab pertanyaan dari

rumusan masalah penelitian ini. Manfaat penelitian yaitu keuntungan yang diperoleh pihak tertentu setelah penelitian selesai dilakukan dan sistematika penulisan memaparkan gambaran umum isi penelitian pada setiap bab.

BAB 2 LANDASAN TEORI

Dalam bab landasan teori memuat pembahasan tentang dasar teori serta landasan pikiran pendukung yang digunakan dalam pembuatan dan perancangan perangkat sebagai landasan penulisan pada penelitian ini. Dasar teori yang dimuat dalam bab ini merujuk pada referensi pustaka seperti jurnal, buku, buku elektronik atau *e-book* dan artikel ilmiah yang dapat mendukung bahasan penelitian ini. Pembahasan landasan teori yang dibuat berupa perbandingan terhadap penelitian yang menjadi referensi dari penelitian ini, teori-teori pendukung seperti *hybrid scan*, *penetration testing*, *information gathering*, *SQL Injection*, dan perangkat lunak pendukung yaitu Subfinder, dig, theHarvester, Nmap, Whatweb, Sqlmap, Aplikasi *Website*, dan Laravel. Landasan teori dibuat agar mendukung pemahaman sehingga peneliti dapat memahami penelitan yang dibuat dalam perspektif yang benar.

BAB 3 METODE PENELITIAN

Dalam bab metode penelitian menguraikan rencana dan prosedur kegiatan penelitan yang dilakukan sehingga proses pengerjaan penelitan dapat berjalan secara sistematis. Metode penelitan pada penelitian ini dimulai dengan melakukan studi literatur, berikutnya dilakukan metode pengumpulan data, kemudian dilakukan analisis kebutuhan penelitan berupa perangkat lunak yang digunakan, kemudian dilakukan perancangan sistem yang dibuat berdasarkan teori pendukung dan perangkat lunak yang dibutuhkan, tahap berikutnya adalah melakukan implementasi dan tahap terkahir pada penelitian ini dilakukan pengujian sistem yang telah dibuat.

BAB 4 PERANCANGAN

Bab perancangan berisi tahapan-tahapan yang dilakukan untuk merancang sistem. Perancangan terdiri dari deskripsi sistem, perancangan perangkat lunak, perancangan antarmuka, dan perancangan pengujian.

BAB 5 IMPLEMENTASI, PENGUJIAN DAN PEMBAHASAN

Bab implementasi, pengujian dan pembahasan berisi tahapan-tahapan yang dilakukan untuk mengimplementasikan, menguji dan membahas sistem. Tahapan implementasi, pengujian dan pembahasan terdiri dari implementasi sistem, kode program, pengujian sistem dan pembahasan.

BAB 6 PENUTUP

Dalam bab penutup berisi pemaparan kesimpulan dari pembahasan masalah yang telah diuraikan pada bab sebelumnya serta saran-saran untuk penelitian lebih lanjut agar dapat dikembangkan menjadi lebih baik.