BAB II

KAJIAN PUSTAKA

A. Tinjauan Pustaka

Penelitian yang dilakukan oleh Andria dan Ridho Pamungkas hasil *penetration testing* tersebut mendapatkan celah kerentanan *SQL Injection* yang dapat melihat stuktur *database* pada web servernya, tetapi pada penelitian ini tidak dieksploitasi lebih lanjut untuk mencari adanya informasi sensitif pada isi *database* tersebut (Andria & Pamungkas, 2021). Pada penelitian ini hanya berfokus *database* dengan menggunakan penyerangan *SQL Injection* saja dan hanya berbasis aplikasi android yaitu *Termux.*

Selanjutnya penelitian yang dilakukan oleh Marcell Dwi Purnomo dan Ahmad Chusyairi yang mengkonfirmasi kebenarannya melalui pengujian menggunakan metode *penetration testing* berdasarkan standar NIST SP 800-115 dengan tahapan *planning*, *discovery*, *attack*, dan *reporting* berhasil mengidentifikasi dua kerentanan pada *website* DPPPA (Dinas Pemberdayaan Perempuan dan Perlindungan Anak), yaitu *sensitive information disclosure* dan *SQL Injection*. Dalam menggunakan metode *penetration testing* ini peneliti mendapatkan celah kerentanan *sensitive information disclosure* yang dapat melihat *directory form login* menuju ke *back end* dan celah kerentanan *SQL Injection* yang dapat mengetahui *informasi sensitif* seperti *username* dan *password* yang bisa di salah

gunakan (Purnomo et al., 2024). Pada penelitian ini dilakukan analisa celah dan saran perbaikan keamanan untuk *website* DPPPA dan peneliti juga mengharapkan agar pemilik sistem melakukan perbaikan dan evaluasi terhadap sistem yang mereka miliki sesuai dengan hasil yang didapatkan dari penelitian.

Penelitian yang dilakukan oleh Dennis Nigel Cunong, Muhardi Saputra, Warih Puspitasari, bahwa hasil penelitian yang dilakukan pada *website* pemerintahan daerah XYZ masih memiliki banyak celah keamanan yang dapat dimanfaatkan oleh peretas untuk melakukan penyerangan terhadap *website*. Terdapat 1 celah keamanan dengan resiko tinggi, 4 celah keamanan dengan resiko sedang, dan 9 celah keamanan dengan celah keamanan dengan resiko rendah. Dengan ditemukannya semua celah keamanan dapat membentu pemerintahan daerah XYZ untuk mengembangkan *website* degan mudah (Cunong et al., 2020). Pada penelitian ini melakukan dengan metode PTES pada *website* pemerintahan XYZ dan dengan hasil tersebut disarankan untuk menggunakan berbagai tools dan metode yang berbeda untuk menemukan celah keamanan yang berbeda.

Penelitian selanjutnya yang dilakukan oleh Rubenson Christian Silaban, Erick Wijaya dengan judul Analisis Kerentanan *Website* Menggunakan Metode NIST SP 800-115 Dan Owasp Di Diskominfo Kabupaten Bandung. pengujian dapat disimpulkan bawa keamanan *website* yang dikelola oleh Diskominfo Kabupaten Bandung rentan terhadap

kerentanan *SQL Injection* dan dapat dengan mudah di eksploitasi oleh pihak yang tidak bertanggung jawab. Sehingga diperlukan antisipasi untuk menanggulangi kerentanan tersebut (Silaban & Wijaya, 2021). Pada penelitian ini dilakukan analisa dan manajemen resiko terkait kerentanan pada *website*, dan juga dilakukan mitigasi terhadap kerentanan yang terdapat dalam *website.*

Penelitian yang ditulis oleh Finka Mambo, Dwi Yuniarto, David Setiadi dengan judul Evaluasi Keamanan *Website* dengan Menggunakan Metode NIST SP 800-115. Pada penelitian ini yaitu mencari kerentanan yang ada di dalam *website* Fakultas Teknologi Informasi (fti.unsap.ac.id) dan melakukan analisis apa saja dampak yang ada jika ancaman tersebut ada di dalam *website* dengan metode yang digunakan NIST SP 800-115 yang terbagi menjadi 4 tipe dalam melakukan pengujian terdiri dari *planning, discovery, attack, reporting* (Mambo et al., 2024). Pada pengujian ini tidak ditemukan kerentanan pada *website* Fakultas Teknologi Informasi dan disarankan untuk menambah beberapa metode untuk menambah serangan.

Selanjutnya penelitian yang dilakukan oleh Tika Astriani, Avon Budiyono, Adityas Widjajarto dengan judul Analisa Kerentanan Pada *Vulnerable Docker* Menggunakan *Scanner Openvas* dan *Docker Scan* Dengan Acuan Standar NIST 800-115 dengan hasil bahwa di dapatkan 7 *Vulnerabilty,* sedangkan hasil yang diperoleh menggunakan *Docker Scan* di dapatkan 8 *Vulnerability* yang di kategorikan dalam *threat level High, Medium* dan *Low*. Dengan di lakukannya klasifikasi hasil dari *vulnerabilty*

scanning berdasarkan frekuensi penggunaan tiap *walktrough*, hasil *vulnerability* dengan nilai perhitungan resiko tertinggi sebesar terdapat pada *WordPress User IDs* and *User* (Astriani, 2021). Pada penelitian ini hanya menggunakan *Scanner Openvas* dan *Docker Scan* saja untuk melakukan pengujian dan analisa.

B. Landasan Teori

1. Analisis

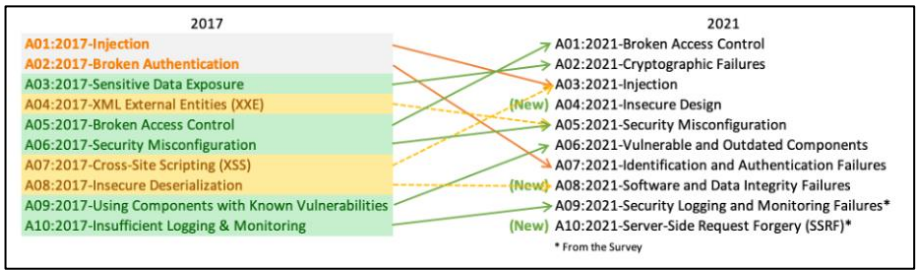
   Secara umum analisis adalah tindakan mengamati suatu objek dengan cara mendeskripsikan bagian-bagian penyusunnya dan menyusun kembali komponen-komponen tersebut agar dapat dipelajari secara detail. Dalam arti lain, analisis adalah kemampuan untuk memecah atau mendeskripsikan suatu dokumen menjadi komponen-komponen yang lebih kecil untuk memudahkan pemahaman dan pembelajaran (Syafitri, 2020).

   Menurut peneliti, sesuai dengan judul yang di ambil, analisis merupakan proses sistematis yang bertujuan untuk mengidentifikasi, mengevaluasi, dan memahami berbagai celah keamanan pada *website* yang memungkinkan pengujian dilakukan baik dari perspektif pengguna eksternal tanpa akses sistem.

2. Risiko Keamanan

   Risiko keamanan adalah potensi terjadinya ancaman terhadap sistem informasi akibat adanya kerentanan, yaitu celah pada perangkat lunak, perangkat keras, atau prosedur yang dapat dieksploitasi oleh

pihak tidak berwenang. Kerentanan ini umumnya disebabkan oleh kesalahan konfigurasi, kode yang tidak aman, atau sistem yang tidak diperbarui, dan dapat menimbulkan dampak serius bagi operasional organisasi.



Gambar 2.1 10 Risiko Keamanan Aplikasi Web Teratas
Sumber: (owasp.org)

OWASP Top 10 merupakan daftar sepuluh besar risiko keamanan aplikasi web yang paling umum, dan secara berkala diperbarui untuk mencerminkan tren serta ancaman terbaru. Dibandingkan versi 2017, OWASP Top 10 edisi 2021 menunjukkan perubahan signifikan, baik dalam struktur maupun penamaannya. Misalnya, kategori *Injection* yang sebelumnya berada di posisi pertama kini turun ke posisi ketiga, sedangkan *Broken Access Control* naik menjadi ancaman paling umum berdasarkan data pengujian terhadap 94% aplikasi. Kategori baru juga ditambahkan, seperti *Insecure Design* (A04:2021) dan *Software and Data Integrity Failures* (A08:2021), menandakan pergeseran fokus dari sekadar kelemahan implementasi ke desain dan integritas proses. Selain itu, beberapa kategori lama seperti *Sensitive Data Exposure* dan *Insecure Deserialization* kini dikonsolidasikan ke dalam kategori yang

lebih luas. Perubahan ini mencerminkan kebutuhan akan pendekatan yang lebih menyeluruh dalam pengembangan aplikasi yang aman.

Dalam manajemen risiko siber, pengelompokan risiko ke dalam empat tingkatan *Low, Medium, High*, dan *Extremely High* merupakan strategi untuk menilai ancaman berdasarkan terjadinya dan dampaknya. Menurut (Cyberinsight, 2023), risiko *Low* memiliki dan dampak minimal sehingga cukup dipantau, sementara *Medium* menunjukkan potensi gangguan yang memerlukan kontrol. Risiko *High* membutuhkan respons cepat karena dampaknya signifikan, dan *Extremely High* harus menjadi prioritas utama karena terjadinya tinggi serta dampaknya sangat besar.

Tabel 2.1 Tingkatan Risiko

Kategori Risiko	Rentang Probabilitas	Deskripsi
Low (Rendah)	< 5 %	Risiko dengan sangat kecil terjadi dan/atau dampaknya minimal.
Medium (Sedang)	5 % – 25 %	Risiko dengan dampak sedang; memerlukan pemantauan rutin.
High (Tinggi)	25 % – 75 %	Risiko tinggi dan/atau dampak signifikan; butuh tindakan.
Extreme (Sangat Tinggi)	> 75 %	Risiko sangat tinggi dan dampak yang sangat besar; prioritas utama mitigasi.

3. *Website*

Website adalah kumpulan halaman yang dirancang untuk menyampaikan informasi dalam berbagai format, seperti teks, gambar statis maupun bergerak, animasi, suara, atau kombinasi dari elemen-elemen tersebut. Halaman-halaman ini dapat bersifat statis atau dinamis dan diorganisasikan dalam struktur yang saling terhubung dengan jaringan tautan (Annaufal et al., 2025).

Gambar 2.2 Contoh *Website*
Sumber: (disparbudpora.pacitankab.go.id/)

Website merupakan suatu media yang dapat menyampaikan dan memperoleh informasi kapanpun dan dimanapun. *Website* menggunakan protokol *Hypertext Transfer Protocol* (HTTP) untuk dapat diakses melalui web browser, sedangkan dokumen pada *website* disimpan dalam web server (Cunong et al., 2020).

Cara kerja website melalui interaksi antara berbagai komponen utama yang saling terhubung untuk menyajikan informasi kepada pengguna secara real-time. Alur kerjanya dapat dijelaskan dalam tahapan berikut:

a. *Server*

Server adalah komputer atau infrastruktur yang menyimpan dan menyajikan konten dari *website* kepada pengguna.

b. DNS (*Domain Name System*)

DNS berfungsi mengonversi alamat URL seperti www.contoh.com menjadi alamat IP numerik agar dapat dipahami oleh server.

c. *Web Browser*

Browser merupakan aplikasi yang digunakan pengguna untuk mengakses dan menampilkan halaman web, seperti *Google Chrome, Mozilla Firefox,* dan *Microsoft Edge.*

d. Bahasa Pemrograman

Website dibangun dengan berbagai bahasa pemrograman seperti *HTML, CSS, JavaScript, PHP,* dan bahasa pendukung lainnya

e. *Database*

Database berperan sebagai tempat penyimpanan data di server yang dibutuhkan untuk menyajikan informasi di dalam *website*.

f. Protokol (HTTP/HTTPS)

Protokol HTTP atau HTTPS digunakan untuk mengirim dan menerima data antara server dengan peramban, sehingga memungkinkan pertukaran informasi secara aman.

g. Media

Media seperti gambar, video, dan audio digunakan untuk menyajikan konten visual dan multimedia, sehingga website menjadi lebih menarik dan komunikatif.

Dengan berinteraksi dengan semua unsur tersebut, website dapat berfungsi untuk menyajikan konten yang terstruktur, menarik dan interaktif kepada pengguna melalui web browser.

4. *Cybersecurity*

Dunia siber merupakan media elektronik dan jaringan komputer tempat terjadinya komunikasi secara daring. Dewi Triwahyun mengatakan bahwa konsep keamanan siber tidak lagi hanya menyentuh ranah teknologi, tetapi telah menjadi ancaman bagi keamanan nasional. Keamanan siber membahas masalah keamanan informasi bagi pemerintah, organisasi, dan urusan individu yang terkait dengan teknologi TIK, dan khususnya teknologi internet (Budiman, 2022).

Cybersecurity adalah sebuah mekanisme yang dibuat untuk melindungi suatu kerahasiaan, integritas, dan ketersediaan informasi. Dan mekanisme ini dibuat untuk melindungi hal tersebut dari serangan yang dilakukan di dunia Internet yang sering disebut sebagai *cyber-attack* (Riyandhika & Pratama, 2020).

Keamanan siber merupakan seperangkat alat, pedoman, prinsip keamanan, perlindungan, rekomendasi, strategi pengelolaan peluang, pergerakan, pelatihan, aplikasi kelas satu, jaminan, dan informasi yang

mencakup pengetahuan teknis (Putra et al., 2024). Keamanan siber juga mencakup semua proses yang dilakukan untuk menjaga dan mengurangi perlindungan data, integritas, dan ketersediaan data yang ada. Proses ini memerlukan perlindungan setiap sistem informasi dari berbagai serangan fisik dan siber.

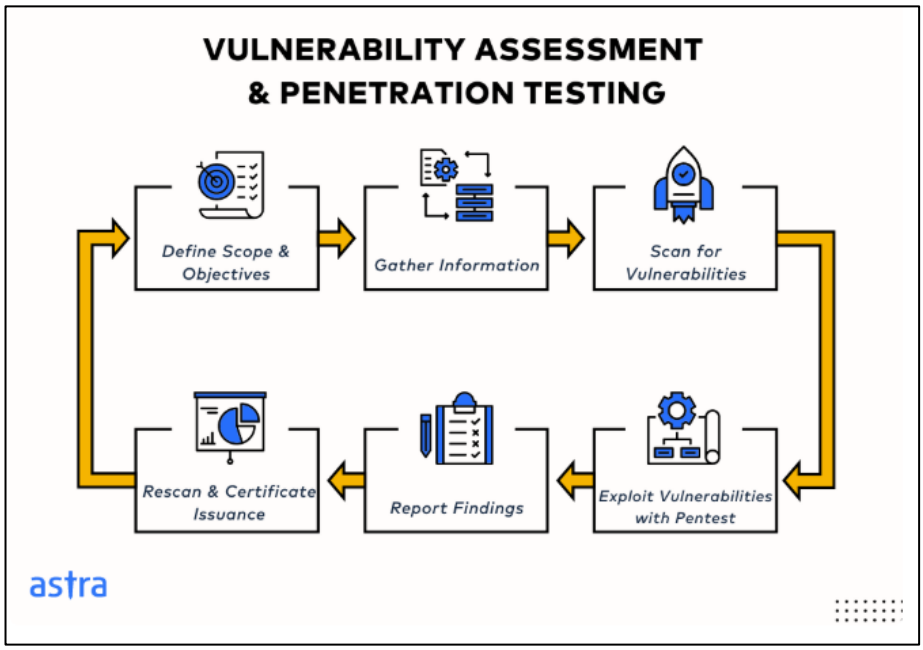
5. *Vulnerability Assessment and Penetration testing* (VAPT)

Dalam praktik keamanan sistem informasi, dua pendekatan utama yang digunakan adalah *vulnerability assessment* dan *penetration testing*. *Vulnerability Assessment* merupakan proses identifikasi dan pemindaian terhadap sistem, perangkat lunak, maupun jaringan dengan tujuan untuk menemukan potensi celah atau kelemahan keamanan. Celah-celah tersebut berisiko dimanfaatkan oleh pihak tidak bertanggung jawab sebagai pintu masuk *(backdoor)* untuk melakukan serangan terhadap sistem target (Yaqi, 2023).

Sedangkan *Penetration testing* adalah langkah lanjutan dari *Vulnerability Assessment* yaitu untuk mengevaluasi sistem untuk kerentanan, konfigurasi yang buruk, serta kelemahan perangkat keras dan perangkat lunak, serta masalah teknis sistem informasi yang sedang diuji. Tujuan utama penetration testing adalah untuk menemukan dan mengatasi kerentanan dalam infrastruktur jaringan sehingga dapat menunjukkan betapa rentannya jaringan tersebut. Pengujian penetrasi langsung telah terbukti dapat meningkatkan keamanan situs web. Selain itu, pengujian penetrasi juga dapat digunakan untuk menilai kebijakan

keamanan suatu organisasi, tingkat kesadaran karyawan tentang persyaratan keamanan, dan kemampuan organisasi untuk menemukan serta menangani masalah keamanan (Gustiyono et al., 2024).

Penetration Testing adalah proses yang terstruktur untuk menguji basis komputasi organisasi yang meliputi perangkat keras atau *hardware*, perangkat lunak atau *software*, dan manusia. Proses ini meliputi analisis seluruh bagian dari sistem untuk mencari kerentanan, seperti konfigurasi sistem, kesalahan pada software dan hardware, dan lain-lain. Penetration testing juga membantu mengidentifikasi tingkat kesulitan penyerang untuk menembus ke dalam sistem (Maherza et al., 2023).

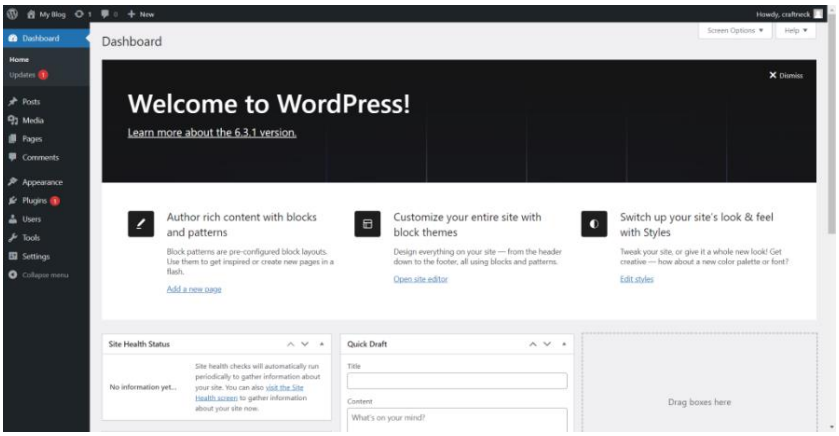


Gambar 2.3 *Vulnerability Assessment and Penetration testing* (VAPT)
Sumber: (www.getastra.com)

Pendekatan kombinasi ini dikenal sebagai *Vulnerability Assessment & Penetration Testing* (VAPT) telah banyak digunakan, khususnya dalam pengamanan sistem pemerintah dan *e-Government*, karena memberikan gambaran lengkap mengenai risiko serta kemampuan organisasi dalam menanggulanginya.

6. *WordPress*

WordPress adalah *CMS open-source* yang mendukung lebih dari 40% dari semua situs web di internet. Keamanan *WordPress* bergantung pada berbagai faktor termasuk pembaruan perangkat lunak penggunaan *Plugin* dan tema yang aman, serta konfigurasi yang tepat (Ramadhani et al., 2024).

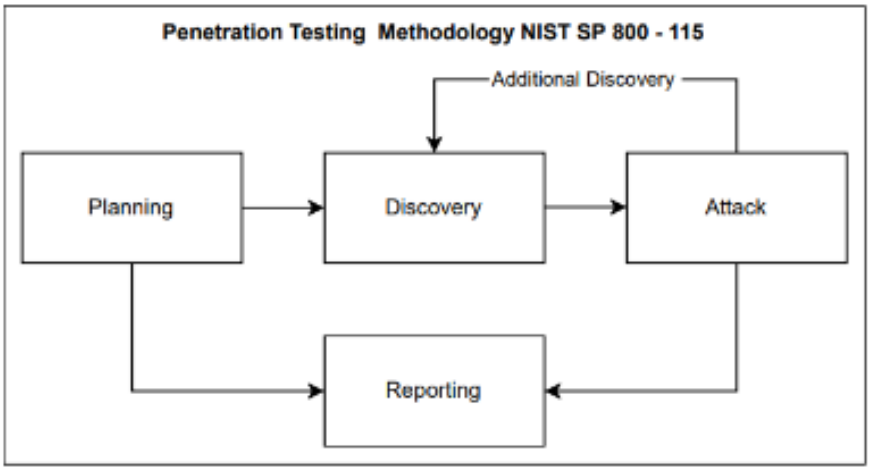


Gambar 2.4 Dashboard *WordPress*
Sumber: (bdthemes.com/)

7. *National Institute of Standards and Technology SP* 800-115

National Institute of Standards and Technology atau NIST adalah sebuah perusahaan keamanan informasi yang dikembangkan oleh pemerintah Amerika Serikat untuk membuat dan mendorong

pengukuran, standar, dan teknologi. Menurut *National Institute of Standards and Technology (NIST)* dalam dokumen *Special Publication* 800-115 dengan judul "*Technical Guide to Information Security Testing and Assessment*" yang digunakan untuk menguji kerentanan situs dalam penetration testing serta memberikan rekomendasi solusi dalam menangani kerentanan yang ditemukan. Pengujian keamanan dilakukan melalui empat langkah utama, yaitu *Planning, Discovery, Attack,* dan *Reporting*. Berikut adalah penjelasan dari setiap langkah tersebut:



Gambar 2.5 Metode NIST SP 800-115
Sumber: (Karen Scarfone et al., 2020)

Berdasarkan gambar diatas maka tahapan-tahapan pada metode NIST adalah sebagai berikut:

a. *Planning* (Perencanaan)

Pada tahap *planning*, peraturan dan hasil yang diharapkan akan didiskusikan dan disetujui oleh kedua pihak, yaitu peneliti dan target. Contoh peraturan yang akan didiskusikan adalah tujuan dilakukannya *penetration testing*, scope atau ruang lingkup, rentang

waktu pengujian, serta hasil yang diharapkan. Tidak ada pengujian yang dilakukan pada tahap ini.

b. *Discovery* (Penemuan)

Merupakan proses pengumpulan informasi tentang sistem target. *Discovery* dilakukan dengan dua pendekatan, yakni secara pasif dan aktif. Pendekatan pasif melibatkan pengumpulan data dari sumber terbuka tanpa menyentuh sistem target secara langsung, sedangkan pendekatan aktif dilakukan dengan melakukan interaksi langsung terhadap sistem, seperti scanning port, deteksi layanan, dan enumerasi kerentanan. Informasi yang diperoleh dari tahap ini akan digunakan untuk menentukan teknik serangan yang tepat di tahap berikutnya.

c. *Attack* (Penyerangan)

Tahap *attack* merupakan fase pelaksanaan di mana penguji berupaya memanfaatkan kerentanan yang telah ditemukan sebelumnya. Tujuan utamanya adalah mensimulasikan serangan nyata agar organisasi dapat memahami potensi dampak dari celah keamanan tersebut. Seluruh proses dilakukan secara hati-hati dan dalam batasan yang telah disepakati, guna menghindari kerusakan sistem. Dalam beberapa kasus, penguji juga melakukan tindak lanjut berupa *post-exploitation* untuk menilai sejauh mana sistem dapat dikendalikan setelah serangan berhasil.

d. *Reporting* (Pelaporan)

Reporting merupakan tahapan dokumentasi dari seluruh hasil pengujian. Laporan ini menyajikan temuan secara terperinci, mulai dari ringkasan eksekutif hingga detail teknis kerentanan yang ditemukan, bukti *eksploitasi*, dampak risiko, serta rekomendasi perbaikan yang perlu dilakukan oleh organisasi. Laporan ini berfungsi sebagai dasar bagi pengambilan keputusan dan peningkatan sistem keamanan ke depannya.

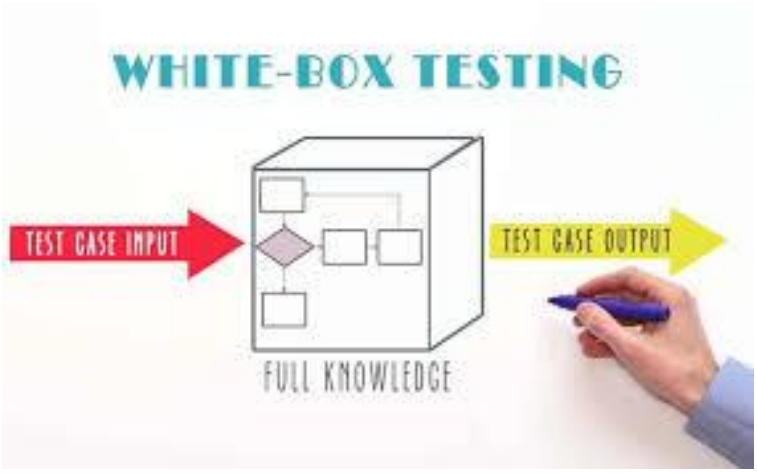
8. *Kali Linux*

Kali Linux adalah distribusi *Linux* berbasis *Debian* yang berfokus pada pengujian penetrasi tingkat lanjut dan peretasan etis. *Linux* sendiri berisikan beberapa alat yang ditujukan untuk berbagai macam tugas keamanan informasi, seperti pengujian penetrasi, pemeriksaan keamanan, komputer *forensik*, dan rekayasa terbalik (Farmadika et al., 2024).

Gambar 2.6 Tampilan Awal Linux

9. *White Box*

White box testing (juga dikenal sebagai *clear box testing, glass box testing, transparent box testing, dan structural testing*) adalah metode pengujian *software* yang menguji struktur internal atau cara kerja suatu aplikasi, yang bertentangan dengan fungsinya (yaitu *black-box testing*). Dalam *white-box testing*, perspektif internal sistem, serta keterampilan pemrograman, digunakan untuk merancang kasus pengujian (Wintana et al., 2022).



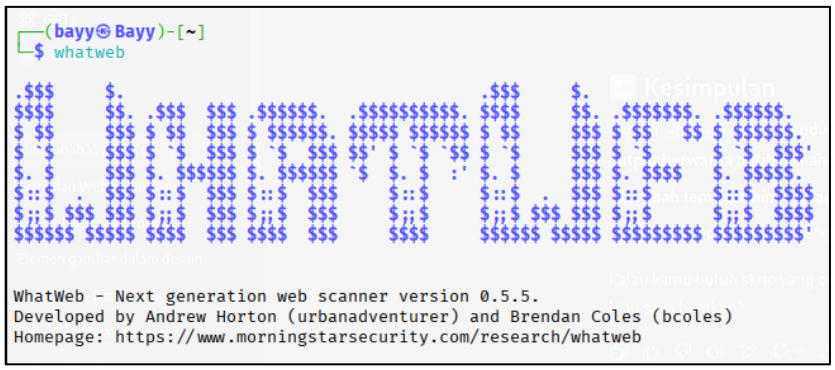
Gambar 2.7 Gambar White Box Testing
Sumber: (www.itbox.id)

White box testing adalah pengujian perangkat lunak pada tingkat alur kode program, apakah masukan dan keluaran yang sesuai dengan spesifikasi yang dibutuhkan, dan pengujian yang didasarkan pada pengujian design program secara prosedural, secara strctural, pengujian berbasis logika atau pengujian berbasis kode (Nurfauziah & Jamaliyah, 2022). Pengujian ini dimulai dengan memberikan data uji tertentu *(test case input)*, lalu diperhatikan bagaimana data tersebut diproses oleh

program *(full knowledge)*, dan hasil akhirnya diperiksa *(test case output)* untuk memastikan apakah program berjalan sesuai dengan yang seharusnya. Dengan metode ini, kesalahan atau bug yang tersembunyi dalam logika program dapat ditemukan lebih mudah.

10. *Whatweb*

WhatWeb adalah alat pemindai web generasi terbaru yang digunakan untuk mengidentifikasi berbagai teknologi yang digunakan oleh suatu situs web.



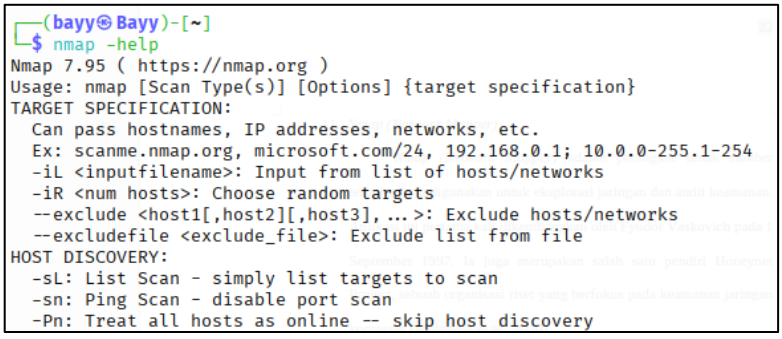
Gambar 2.8 Tools *Whatweb*

WhatWeb dapat dijalankan dalam mode cepat dan tersembunyi untuk pemindaian ringan, atau dalam mode menyeluruh untuk menghasilkan deteksi yang lebih lengkap meskipun dengan waktu yang lebih lama. Saat browser mengakses suatu halaman web, terdapat sejumlah informasi yang dapat diambil untuk mengenali teknologi di balik situs tersebut. Jika informasi tersebut tidak cukup, WhatWeb memungkinkan pengguna untuk menginterogasi lebih lanjut guna memperoleh detail yang dibutuhkan, sehingga alat ini sangat berguna

dalam tahap enumerasi teknologi selama proses pengujian penetrasi. (Supendi, 2023).

11. *Nmap (Network Mapper)*

Nmap (Network Mapper) adalah perangkat lunak sumber terbuka yang digunakan untuk eksplorasi jaringan dan audit keamanan. Aplikasi ini pertama kali dikembangkan oleh Fyodor Vaskovich pada 1 September 1997. Ia juga merupakan salah satu pendiri Honeynet Project, sebuah organisasi riset yang berfokus pada keamanan jaringan komputer (Muhyidin et al., 2020).

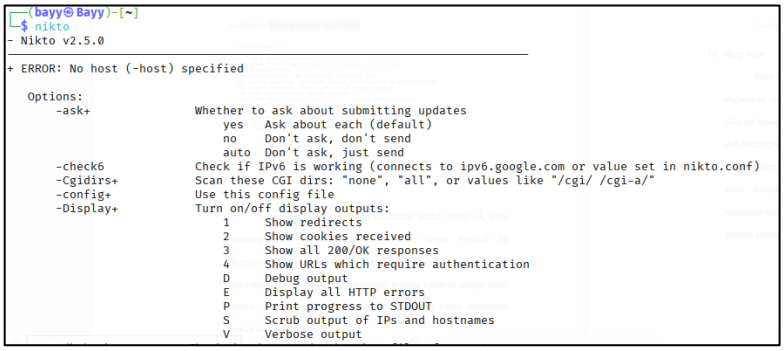


Gambar 2.9 *Tools Nmap*

Salah satu opsi yang umum digunakan adalah *Nmap* -A, yang memungkinkan pemindaian agresif terhadap target. Perintah ini digunakan untuk mendeteksi sistem operasi, versi layanan, skrip pendukung, serta melakukan traceroute. Karena hasilnya sangat rinci, teknik ini efektif untuk mengumpulkan informasi teknis mendalam terkait host yang dipindai.

12. *Nikto*

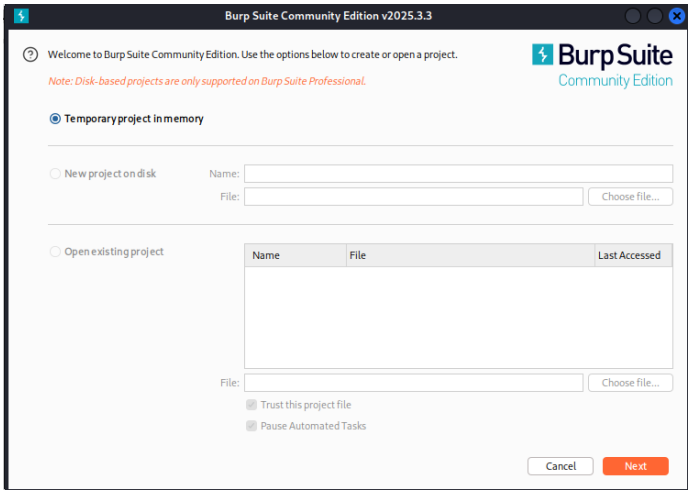
Nikto merupakan alat pemindaian web server yang digunakan untuk melakukan penilaian keamanan terhadap aplikasi web. Tool ini mampu mendeteksi berbagai kerentanan umum, termasuk pemindaian terhadap lebih dari 6.700 file atau program yang berpotensi berbahaya. *Nikto* juga dapat mengidentifikasi konfigurasi server yang lemah, file tersembunyi, serta versi perangkat lunak yang rentan, sehingga sangat berguna dalam tahap awal pengujian penetrasi. (Muhyidin et al., 2020).



Gambar 2.10 Tools Nikto

13. *Burp Suite*

Burp Suite merupakan alat uji keamanan aplikasi web yang digunakan untuk menganalisis lalu lintas data antara klien dan server. Alat ini bekerja dengan cara mencegat (*intercept*) permintaan (*request*) dan tanggapan (*response*) melalui jalur proxy yang telah dikonfigurasi. Dengan demikian, seluruh komunikasi antara browser atau aplikasi klien dengan server akan melalui *Burp Suite* terlebih dahulu, memungkinkan analisis, modifikasi, dan pengujian terhadap berbagai potensi kerentanan aplikasi web (Awanda Alviansyah, 2021).



Gambar 2.11 *Tools Burp Suite*

C. Keaslian Penelitian

Tabel 2.1 Keaslian Penelitian

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
1.	*Penetration Testing Database* Menggunakan Metode *SQL Injection Via SQLMap* di *Termux*	Andria, Ridho Pamungkas. IJAI *(Indonesian Journal of Applied Informatics). 2021*	Untuk pengujian keamanan *database web server* dan membantu pengelola atau admin situs *web* untuk dapat memeriksa adanya celah kerentanan *database* yang dapat dieskploitasi oleh peretas.	Pada penelitian ini ditemukan hasil temuan celah keamanan yang disebut dengan *SQL Injection* yaitu sebuah celah keamanan di lapisan basis data di dalam aplikasi.	Ada saran yang diberikan oleh peneliti dari melakukan yaitu menggunakan *parameterized query* atau *prepared statement*, memberikan batasan hak akses, melakukan validasi *input* pengguna, memberikan *enkripsi* basis data dan menyembunyikan pesan *error*.	Penelitian sebelumnya berfokus pada eksploitasi basis data menggunakan *SQL Injection* dan berhasil memperoleh beberapa tabel dari situs target. Dalam penelitian ini, pendekatannya diperluas dengan tidak hanya menggunakan *SQL Injection*, tetapi juga memanfaatkan tools lain seperti *Hydra*, *Burp Suite*, *Clickjacking*, dan *WPScan* untuk mengidentifikasi kerentanan secara lebih menyeluruh.

Tabel 2.1 Keaslian Penelitian						
No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
2.	Pengujian Keamanan Sistem Mengunakan Metode *Penetration Testing* di Website Diskominfostandi Kota Bekasi	Marcell Dwi Purnomo, Ahmad Chusyairi	Pengujian keamanan pada website Dinas Pemberdayaan Perempuan dan Perlindungan Anak (DPPPA) Kota, sehingga dapat dilakukan pencegahan agar terhindar dari ancaman akses orang yang tidak bertanggung jawab maupun pencurian data.	Dalam menggunakan metode *penetration testing* ini peneliti mendapatkan celah kerentanan *sensitive information disclosure* yang dapat melihat *directory form login* menuju ke *back end* dan celah kerentanan *SQL Injection* yang dapat mengetahui informasi sensitif seperti *username* dan *password* yang bisa di salahgunakan, Penilaian risiko menggunakan CVSS versi 3.1 menunjukkan *SQL Injection* memiliki nilai *critical* dan *sensitive information disclosure* bernilai *medium*, dan dilanjutkan memberi solusi perbaikan yang tepat untuk kedua	penelitian ini tidak dieksploitasi lebih lanjut untuk mencari adanya informasi sensitif pada isi database dan penelitian ini tidak menggunakan Common Vulnerability Scoring System (CVSS) untuk menentukan nilai tingkat keparahan pada kerentanannya	Penelitian oleh Marcell Dwi Purnomo dan Ahmad Chusyairi mengidentifikasi dua kerentanan utama, yaitu SQL Injection dan Sensitive Information Disclosure, pada website DPPPA Kota Bekasi, dan mengevaluasi tingkat risikonya menggunakan CVSS v3.1. Sementara itu, penelitian ini tidak hanya mengevaluasi berdasarkan CVSS, tetapi juga menggunakan standar NIST SP 800-115 untuk membentuk alur pengujian sistematis, dengan eksploitasi

Tabel 2.1 Keaslian Penelitian						
No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
				kerentanan tersebut agar meningkatkan keamanan website DPPPA		tambahan seperti enumerasi akun melalui REST API, analisis Clickjacking, dan simulasi subdomain takeover, sehingga menghasilkan temuan yang lebih kompleks.
3.	Analisis Resiko Keamanan Terhadap *Website* Dinas Penanaman Modal Dan Pelayanan Terpadu Satu Pintu Pemerintahan XYZ Menggunakan Standar *Penetration Testing Execution Standard (PTES)*	Dennis Nigel Cunong, Muhardi Saputra, Warih Puspitasari	Menemukan celah keamanan dan penanganan celah kemanan tersebut agar website tersebut dapat dioptimalkan dalam pemeliharaannya dengan cara mengontrol kerentanan keamanan *website* dengan *vulnerability assessment* and *penetration testing*	Bahwa *website* pemerintahan daerah XYZ masih memiliki banyak celah keamanan yang dapat dimanfaatkan oleh peretas untuk melakukan penyerangan terhadap website. Terdapat 1 celah keamanan dengan resiko tinggi, 4 celah keamanan dengan resiko sedang, dan 9 celah keamanan dengan celah keamanan dengan resiko rendah	Disarankan untuk menggunakan berbagai *tools* dan metode yang berbeda untuk menemukan celah keamanan yang ber beda. Penelitian ini juga dapat menjadi referensi untuk semua orang dalam melakukan audit keamanan suatu website, baik dari segi metode maupun *tools* yang digunakan	Penelitian oleh Dennis Nigel Cunong dkk. menggunakan metode PTES untuk menemukan total 14 celah keamanan pada website pemerintahan daerah XYZ dengan tingkat risiko yang bervariasi. Penelitian ini menyarankan penggunaan metode dan tools yang lebih beragam. Penelitian Anda menggunakan pendekatan berbasis NIST SP 800-115

Tabel 2.1 Keaslian Penelitian						
No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
						secara sistematis, serta menerapkan eksploitasi yang lebih variatif seperti WPScan, Burp Suite, dan eksploitasi REST API, sehingga memberikan cakupan analisis yang lebih dalam pada aspek aplikasi web.
4.	Analisis Kerentanan *Website* Menggunakan Metode *NIST SP 800-115* Dan Owasp Di Diskominfo Kabupaten Bandung	Rubenson Christian Silaban, Erick Wijaya	Dapat membatu menanggulangi penyerangan terhadap *website* yang dikelola oleh Dinas Komunikasi, Informatika dan Statistika Kabupaten Bandung	Keamanan *website* Diskominfo rentan terhadap kerentanan *SQL Injection* dan dapat dengan mudah di eksploitasi oleh pihak yang tidak bertanggung jawab. Sehingga diperlukan antisipasi untuk menanggulangi kerentanan tersebut	1). Perlu ditambahkan *Tools* pendukung tambahan yang kompatibel dengan *OS Windows, 2)* Ditambahkannya fitur yang dapat membaca hasil *Scanning Vulnerabily*, *3)* Dapat dilakukan pengembangan aplikasi serupa untuk *platform OS linux*	Rubenson Christian Silaban dan Erick Wijaya menemukan kerentanan *SQL Injection* pada website Diskominfo Kabupaten Bandung menggunakan pendekatan NIST dan OWASP, dan menyarankan penambahan tools pendukung. Penelitian ini melangkah lebih jauh dengan

Tabel 2.1 Keaslian Penelitian						
No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
						penerapan penuh tahapan NIST SP 800-115 dan penggunaan tools eksploratif, serta eksploitasi tambahan seperti *Clickjacking*, analisis header keamanan HTTP, dan eksploitasi file publik yang rentan.
5.	Evaluasi Keamanan *Website* dengan Menggunakan Metode *NIST SP 800-115*	Finka Mambo, Dwi Yuniarto, David Setiadi. Jurnal Penelitian Mahasiswa. Volume 3, Nomor 4, Tahun 2024	Mencari kerentanan yang ada di dalam website Fakultas Teknologi Informasi (fti.unsap.ac.id) dan melakukan analisis apa saja dampak yang ada jika ancaman tersebut ada di dalam website dengan metode yang digunakan *NIST SP 800-115*	Keamanan yang ada pada website fti.unsap.ac.id masih dibilang aman karena dari hasil melakukan pengujian belum menemukan kerentanan karena sistem yang ada pada website tersebut terdapat firewall yang mampu menghalangi serangan	Dapat dilakukan pengujian ulang baik dari pihak Fakultas Teknologi Informasi maupun dari penguji yang lain pada website supaya dapat menemukan celah keamanan yang lebih mendalam. Serta melakukan pengujian dengan menambahkan beberapa metode sebagai penunujang untuk menemukan kerentanan	Penelitian oleh Finka Mambo dkk. menyimpulkan bahwa website Fakultas Teknologi Informasi UNSAP relatif aman karena tidak ditemukan kerentanan dalam pengujian awal yang dilakukan dengan metode NIST SP 800-115. Sebaliknya, penelitian ini berhasil mengidentifikasi berbagai kerentanan

Tabel 2.1 Keaslian Penelitian						
No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
						aktif dan pasif pada dua domain berbeda, serta menyajikan pemetaan tingkat risiko berbasis CVSS v3.1 sebagai dasar rekomendasi mitigasi teknis.
6.	Analisa Kerentanan Pada *Vulnerable Docker* Menggunakan *Scanner Openvas* Dan *Docker Scan* Dengan Acuan Standar NIST 800-115	Tika Astriani, Avon Budiyono, Adityas Widjajarto. Jurnal Teknik Informatika dan Sistem Informasi. Desember 2021	Analisis mengenai kerentanan pada *Docker* dengan menggunakan *software opensource* sebagai *vulnerability scanner* dan standar NIST 800-115	Bedasarkan *software open source OpenVAS* bahwa di dapatkan hasil 7 *Vulnerabilty*, Sedangkan hasil yang diperoleh menggunakan *Docker Scan* di dapatkan 8 *Vulnerability* yang di kategorikan dalam *threat level High, Medium* dan *Low*. Dengan di lakukannya klasifikasi hasil dari *Vulnerabilty scanning* berdasarkan frekuensi penggunaan tiap *walktrough*, hasil *vulnerability* dengan nilai perhitungan resiko tertinggi sebesar	1. Perlu dilakukannya penelitian lebih spesifik dengan menggunakan software lainnya. 2. Melakukan lebih banyak pengujian menggunakan walkthrough dengan skala lebih luas. 3. Disarankan menggunakan *open source vulnerability* selain *OpenVAS* untuk melakukan	Penelitian oleh Tika Astriani dkk. menganalisis kerentanan pada Docker menggunakan OpenVAS dan Docker Scan berdasarkan standar NIST SP 800-115, dengan hasil 7–8 kerentanan pada level risiko berbeda. Penelitian ini menyarankan eksplorasi tools dan metode lain. Berbeda dengan itu,

Tabel 2.1 Keaslian Penelitian						
No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
				terdapat pada *WordPress User IDs and User*.	*vulnerability assessment.* 4. Melakukan analisa dengan menggunakan selain standar NIST 800-115, seperti PTES ataupun OWASP.	penelitian ini fokus pada aplikasi web berbasis *WordPress*, dengan eksploitasi langsung menggunakan berbagai tools seperti WPScan, Burp Suite, Hydra, dan teknik *Clickjacking*, untuk menemukan kerentanan yang lebih kompleks dan relevan dengan sistem pemerintahan.