BAB III

METODOLOGI PENELITIAN

3.1 Subjek dan Objek Penelitian

Subjek penelitian ini adalah *Website* Pemerintah Daerah di Indonesia yang digunakan untuk analisis kerentanan yang ada dalam *website* tersebut. Supaya kedepannya *website* pemerintah daerah yang digunakan lebih aman dan terhindar dari pihak yang tidak bertanggung jawab yang masuk tanpa sepengetahuan dari admin. Adapun objek penelitian ini yaitu analisis *website* pemerintah daerah.

3.2 Alat dan Bahan Penelitian

3.2.1 Alat Penelitian

Adapun alat yang digunakan dalam pelaksanaan penelitian yaitu terdiri dari perangkat keras *(hardware)* dan perangkat lunak *(software)* yaitu:

1. Perangkat Keras *(Hardware)*
   a. Laptop Lenovo G-400

      Laptop digunakan untuk menulis laporan, menganalisis, mengolah data dan juga untuk melakukan pengujian terhadap *website* pemerintah daerah.
2. Perangkat Lunak *(Software)*
   a. Sistem operasi

      Sistem operasi yang digunakan peneliti yaitu Kali Linux versi 2021, untuk melakukan *scanning vulnerability* dan melakukan pentesting terhadap *website* pemerintah daerah.
   b. NMAP

      NMAP digunakan untuk membantu identifikasi *por*t pada *website* pemerintah daerah.
   c. Dirbuster

      Dirbuster digunakan untuk melakukan *scanning directory* yang ada pada *website* pemerintah daerah.

d. Burpsuite

BurpSuite merupakan aplikasi open source yang digunakan untuk menguji keamanan sebuah website. Pada penelitian in burpsuite digunakan untuk melakukan serangan *payload* pada *website* pemerintah daerah.

e. WPScan

WPScan adalah salah satu tool open source yang digunakan untuk melakukan pemindaian keamanan pada WordPress.

f. Wappalyzer

Wappalyzer adalah sebuah extension atau add-on browser yang digunakan untuk menganalisis teknologi yang digunakan pada suatu situs web.

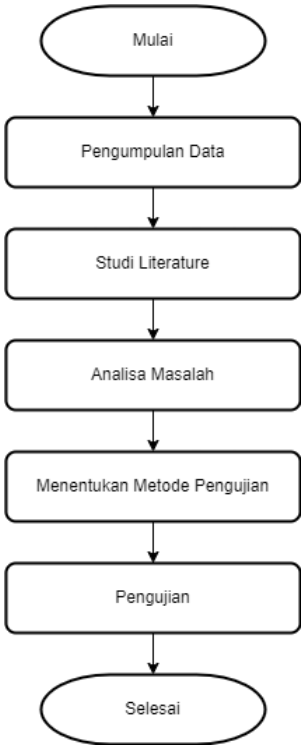
3.2.2 Bahan Penelitian

Bahan penelitian yang gunakan ialah berupa *website* pemerintah daerah yang akan dilakukan perbandingan dan analisis keamanan dan kerentanannya. Beberapa sampel *website* yang digunakan antara lain dengan istilah penamaan sebagai berikut:

1. Website Pemkab BR (Bootstrap)
2. Website Pemkab DK (Bootstrap)
3. Website Pemkab PBG (Bootstrap)
4. Website Pemkab RBG (Wordpress)
5. Website Pemkab BJR (Wordpress)
6. Website Pemkab CMS (Wordpress)

3.3 Diagram Alur Penelitian

Pada alur peneliti memaparkan tahapan kerja yang akan dilakukan. Alur penelitian ini digunakan sebagai pedoman selama melakukan penelitian agar hasil yang diperoleh tidak menyimpang dari tujuan. Tahapan-tahapan kerja tersebut disusun dalan bentuk *flowchart* seperti pada gambar 3.1.



Gambar 3. 1 Diagram Alur Penelitian

3.3.1 Pengumpulan Data

Pada tahap ini peneliti mengumpulkan data yang dapat menunjang kebutuhan dalam melakukan penelitian ini seperti data serangan siber yang terjadi di Indonesia. Pengumpulan data dilakukan dengan cara membaca jurnal penelitian sebelumnya serta informasi yang didapatkan dari *wbsite* resmi.

3.3.2 Studi Literature

Studi literature dilakukan mengingat pentingnya sebuah sebuah *studi literature* yang dapat menunjang ilmu teori ataupun praktiknya dalam penelitian yang dilakukan. *Studi literature* yang dilakukan berkaintan dengan tema yang sama baik dari penelitian sebelumnya, buku-buku, jurnal dan informasi dari internet yang memilki kerterkaitan dengan penelitian ini.

3.3.3 Analisa Masalah

Pada tahap ini peneliti melakukan analisa permasalahan yang terjadi di lapangan yang dianggap bisa dilakukan untuk penelitian, peneliti menemukan

beberapa masalah pada website kabupaten yang digunakan sebagai sempel pada penelitian ini.

3.3.4 Menentukan Metode Pengujian

Pada tahap ini peneliti menetukan metode apa yang akan peneliti gunakan dalam melakukan uji coba keamanan pada *website* pemerintah daeran DK, BR, CMS, BJR, PBG, dan RBG. Peneliti memilih metode Penetration Testing Execution Standard karena metode PTES menyediakan kerangka kerja kerja yang terstruktur dan terdokumentasi dengan baik untuk melaksanakan pengujian penetrasi, PTES memastikan konsistensi dalam pelaksanaan pengujian penetrasi, PTES secara teratur diperbarui untuk mencerminkan perkembangan dalam ancaman keamanan dan teknologi.

3.3.5 Pengujian

Pada tahap ini peneliti mulai melakukan pengujian dengan metode *Penetration Testing Execution Standard* (PTES). Dalam metode PTES terdapat 7 tahapan seperti *Pre-engagement Interaction, Intelegence Gathering, Threat modeling, Vulnerability Analysis, Exploitation, Post Exploitation* dan *Reposrting*.

Pada tahap *Pre-engagement Interaction* peneliti melakuakan kegiatan berupa identifikasi masalah yang terdapat pada *wesite* pemerintah daerah yang dijadikan sempel. Selanjutnya pada tahap *Intelegence Gathering* peneliti mengumpulkan informasi yamg meliputi informasi tentang url, parameter input, jenis teknologi yang digunakan dan informasi terkait lainnya menggunakan *tools* NMAP, WPScan, dan Wappalyzer yang dibutuhkan saat melakukan PTES.

Selanjutnya pada tahap *Threat Modeling* peneliti melakukan pendekatan pemodelan untuk memudahkan memahami kerentanan yang akan ditemukan pada pengujian ini. Selanjutnya *Vulnerabillity Analysis* peneliti melakukan analisa kerentanan yang ada pada *website* pemerintah daerah yang dijadikan sempel. Tahap selanjutnya *Exploitation*, pada tahap ini lakukan

serangan berupa *Cross Site Scripting* (XSS) dan *vulnerability dorking*. *Post Exploitation* tahap ini melibatkan pemanfaatan akses yang diperoleh dari tahap *exploitation* untuk mendapatkan informasi atau data yang diinginkan. Tahap terakhir yaitu *Reporting*, pada tahap ini peneliti menuliskan hasil analisis pengujian yang dilakukan pada *website* pemerintah daerah.