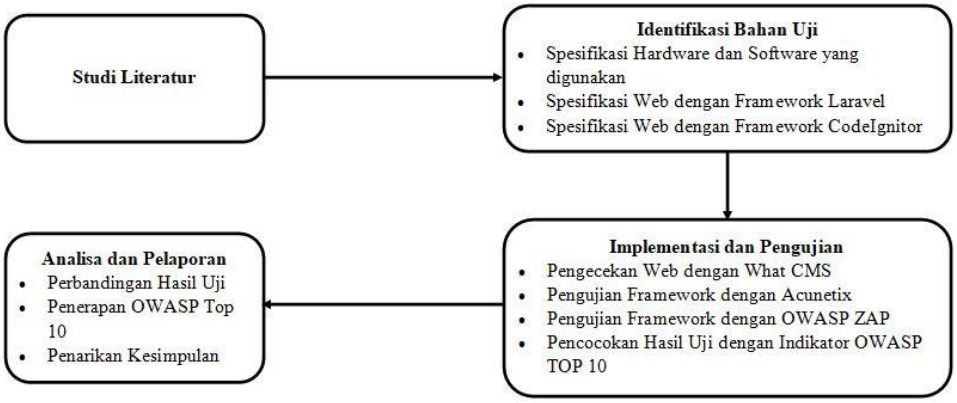
BAB III

METODOLOGI PENELITIAN

3.1 Tahapan Penelitian



Gambar 3.1 Tahapan Penelitian

Gambar 3.1 menjelaskan mengenai tahapan-tahapan dalam melakukan penelitian untuk menganalisa perbandingan keamanan web *Laravel* dan *Codeigniter* dengan *Acunetix* dan *Open Web Application Security Project Zed Attack Proxy* (OWASP ZAP).

3.1.1 Studi Literatur

Studi literatur merupakan tahapan awal untuk memulai penelitian dengan mengumpulkan bahan atau materi-materi yang berkaitan dengan penelitian yang akan dilakukan untuk dijadikan rujukan mengenai keamanan web *laravel* dan *codeigniter* dengan *acunetix* dan OWASP ZAP serta metode OWASP Top 10 yang menjadi parameter perbandingan. Pengumpulan referensi dilakukan di

perpustakaan, melalui *website* ataupun melalui karya tulis ilmiah yang sudah di publikasi pada internet secara resmi.

3.1.2 Identifikasi Bahan Uji

Penelitian dilakukan dengan menggunakan laptop pribadi dan bahan uji yang digunakan merupakan web dengan *framework Laravel* dan *CodeIgniter*. Kebutuhan *hardware* dan *software* yang digunakan pada penelitian terdapat pada tabel 3.1, sedangkan untuk spesifikasi web dengan *framework Laravel* terdapat pada tabel 3.2, spesifikasi web dengan *framework CodeIgniter* terdapat pada tabel 3.3, dan klasifikasi kerentanan menggunakan indikator OWASP TOP 10.

Tabel 3.1. Spesfikasi *Hardware* dan *Software* yang digunakan

No	Alat dan bahan	Keterangan
1	Laptop	ASUS Intel Core i7-6700HQ CPU @2.60Ghz 8GB DDR4
2	*Acunetix*	*Tools* untuk *scanning* agar mengetahui bugs atau celah keamanan yang ada diaplikasi web.
3	OWASP ZAP	*Tools* untuk *scanning* agar mengetahui bugs atau celah keamanan yang ada diaplikasi web.
4	OWASP Top 10	*Penetration test* untuk *checklist* standar keamanan aplikasi web

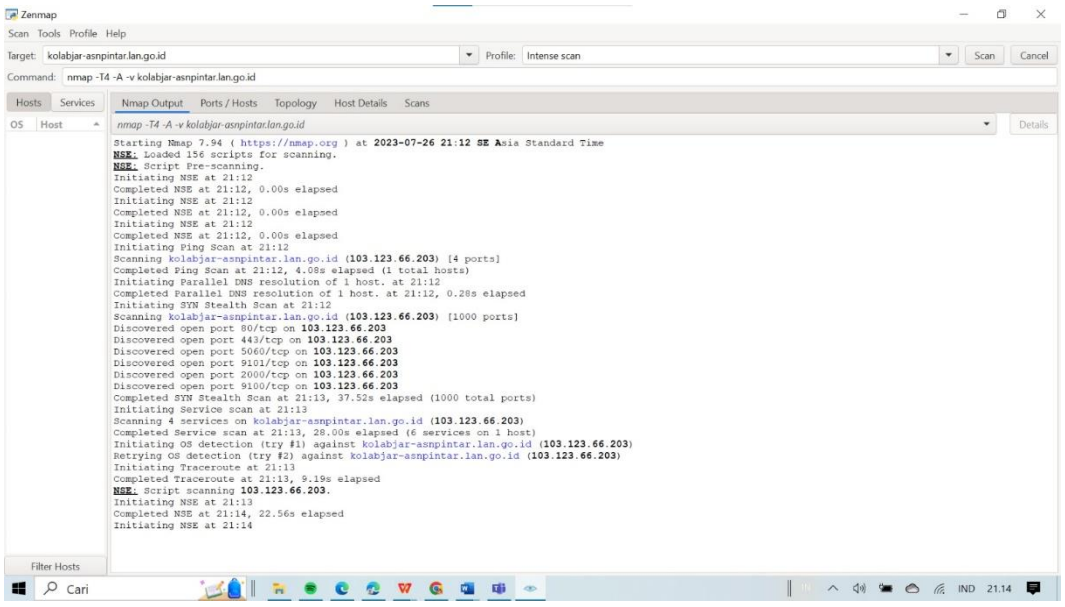
Tabel 3.2. Spesfikasi Web dengan *Framework Laravel*

Website: kolabjar-asnpintar.lan.go.id		
No.	Kategori	*Software*
1	Web *Framework*	*Laravel*
2	*Programing Language*	PHP
3	*Web Server*	Nginx
4	*Address*	36.67.50.251

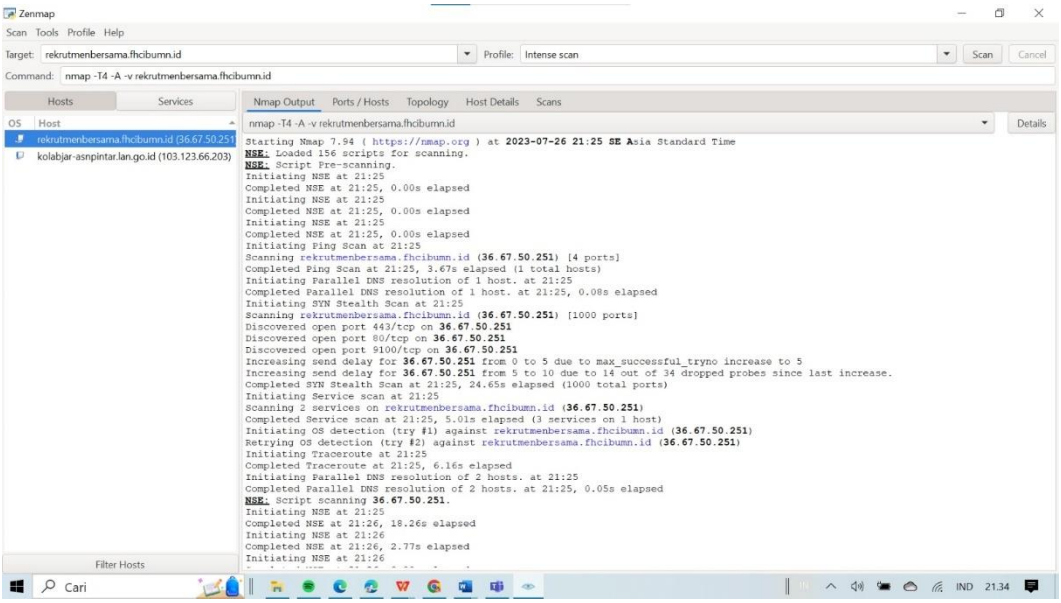
Tabel 3.3. Spesfikasi Web dengan *Framework CodeIgnitor*

Website: rekrutmenbersama.fhcibumn.id		
No.	Kategori	*Software*
1	Web *Framework*	*CodeIgniter*
2	*Programing Language*	PHP
3	*Web Server*	Nginx
4	*Address*	103.123.66.203

Nmap (*Network Mapper*) adalah sebuah *tool open source* untuk eksplorasi dan audit keamanan jaringan. *Output* Nmap merupakan sebuah daftar target *host* yang diperiksa dan informasi tambahan sesuai dengan opsi yang digunakan (Bayu et al., 2020).

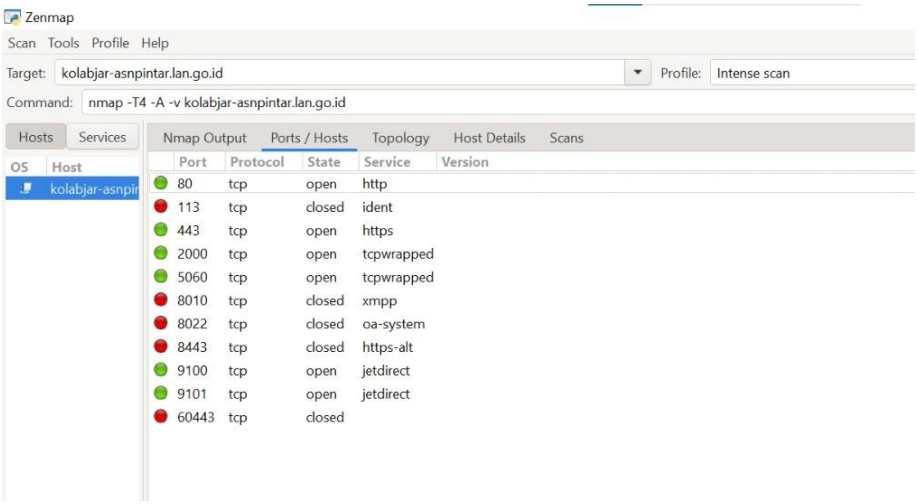


Gambar 3.2 Pengujian Nmap Web kolabjar-asnpintar.lan.go.id

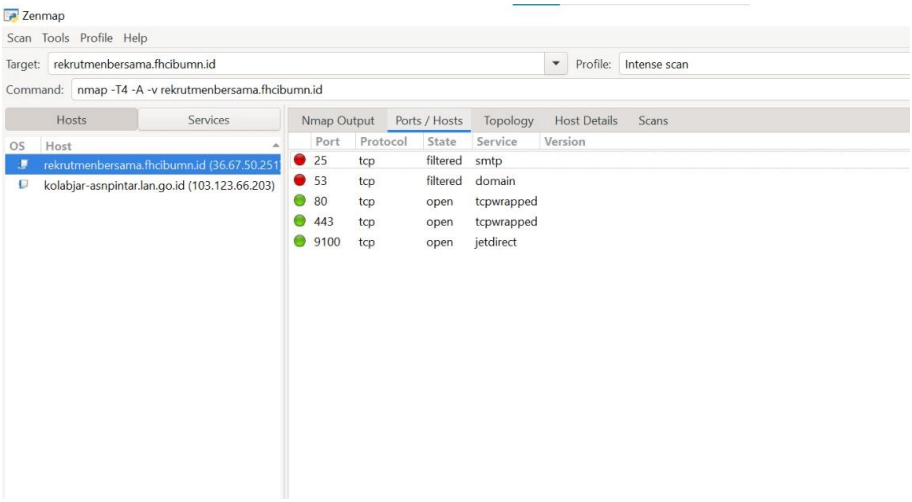


Gambar 3.3 Pengujian Nmap Web rekrutmenbersama.fhcibumn.id

Dari proses *scanning* jaringan menggunakan *software* Nmap pada *website:* kolabjar-asnpintar.lan.go.id dapat diketahui Ip Address alamat tersebut yaitu 103.123.66.203, seperti pada gambar 3.2, sedangkan pada *website*: rekrutmenbersama.fhcibumn.id diketahui Ip Address alamat tersebut yaitu 36.67.50.251 , seperti pada gambar 3.3.



Gambar 3.4 Hasil *Port Scanning* Web kolabjar-asnpintar.lan.go.id



Gambar 3.5 Hasil *Port Scanning* Web rekrutmenbersama.fhcibumn.id

Pada gambar 3.4 merupakan hasil dari *scanning* yang dilakukan oleh Nmap pada *website* kolabjar-asnpintar.lan.go.id. Pada hasil menunjukan beberapa *port* yang terbuka (open) dan ter-*filtered. Port* tersebut diantaranya *port* 80/tcp http, 443/tcp https, 2000/tcp tcpwrapped, 5060/tcp tcpwrapped, 9100/tcp jetdirect, 9101/tcp jetdirect merupakan *port* yang terbuka dan *Port* 113/tcp ident, 8010/tcp xmpp, 8022/tcp oa-system, 8443/tcp https-alt, 60443/tcp merupakan *port* yang ter-*filtered.*

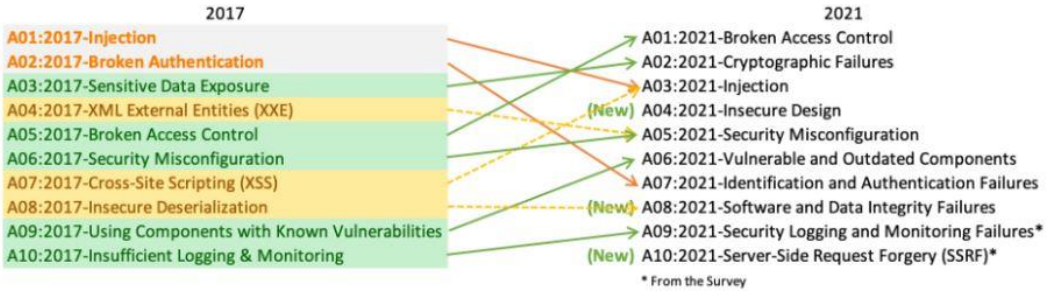
Pada gambar 3.5 merupakan hasil dari *scanning* yang dilakukan pada *website* rekrutmenbersama.fhcibumn.id. Hasilnya menunjukan beberapa *port* diantaranya *port* 80/tcp tcpwrapped, 443/tcp tcpwrapped, 9100/tcp jetdirect yang merupakakan *port* terbuka (*open*) dan *port* 25/tcp smtp, 53/tcp domain merupakan *port* yang ter-*filtered.*

Pada tabel 3.4 dibawah merupakan komparasi *port-port* yang terbuka dari hasil *scanning* yang dilakukan menggunakan Nmap pada kedua *website* tersebut.

Tabel 3.4 Komparasi *Open Port* Berdasarkan Nmap

No.	Port	kolabjar-asnpintar.lan.go.id	rekrutmenbersama.fhcibumn.id
1	Open port 80/tcp	V	V
2	Open port 443/tcp	V	V
3	Open port 2000/tcp	V	
4	Open port 5060/tcp	V	
5	Open port 9100/tcp	V	V
6	Open port 9101/tcp	V	

Berdasarkan situs resmi OWASP bahwasanya indikator OWASP Top 10 terdapat perubahan pada tahun 2021 terhadap indicator pada tahun 2017. Mengacu pada perubahan indikator tersebut maka akan digunakan indikator OWASP Top 10 pada tahun 2021 untuk mengikuti keterbaharuan indikator. Indikator terbaru pada OWASP Top 10 berdasarkan situs resmi OWASP terdapat pada gambar 3.6.



Gambar 3.6 Indikator OWASP Top 10

Komparasi kelebihan dan kekurangan dari *tools Acunetix* dan OWASP ZAP terdapat pada Tabel 3.4 berdasarkan *Source Forge* (Sourceforge.com, 2023), dan sumber dari SaaSHub terdapat pada Tabel 3.4 (Saashub.com, 2023).

Tabel 3.5 Komparasi *Acunetix* dan OWASP ZAP (*Source Forge*)

No.	Category	Acunetix	OWASP ZAP
1	Application Security	V	V
2	Dynamic Application Security Testing	V	V
3	Penetration Testing	V	V
4	Computer Security	V	
5	Cyber Security	V	
6	IP Scanners	V	
7	IT Security	V	
8	Network Security	V	
9	Vulnerability Management	V	
10	Vulnerability Scanners	V	
11	Website Security	V	

Tabel 3.6 Komparasi *Acunetix* dan OWASP ZAP (SaaSHub)

No.	Category	In percentage (%)	
		Acunetix	OWASP ZAP
1	Cyber Security	100	0
2	Monitoring Tools	66	34
3	Ethical Hacking	100	0
4	Security & Privacy	0	100

3.1.3 Implementasi dan Pengujian

Tahap implementasi dimulai dengan melakukan proses identifikasi web yang akan digunakan sebagai bahan uji yaitu situs web rekrutmen BUMN dan situs web kolabjar dengan menggunakan situs web "*What CMS is This Site Using?*". Tahap selanjutnya yaitu melakukan pengujian dengan menggunakan Acunetix pada kedua website tersebut sehingga didapatkan hasil kerentanannya, begitu juga dilakukan dengan menggunakan OWASP ZAP sehingga didapatkan hasil kerentanannya, kemudian dilakukan pengklasifikasian dengan OWASP TOP 10 untuk hasil pengujian menggunakan *Acunetix* dan OWASP ZAP.

Penggunaan aplikasi *Acunetix* dan OWASP ZAP hanya dengan memasukkan halaman web dari rekrutmen BUMN dan kolabjar kemudian aplikasi akan langsung melakukan *penetration test* dan didapatkan hasil dari pengujian yang dilakukan pada kedua aplikasi tersebut, yang kemudian akan dilakukan penarikan kesimpulan setelah dilakukannya pengklasifikasian dengan indikator OWASP TOP 10.

3.1.4 Analisa dan Pelaporan

Hasil pengujian akan dianalisa dan dibandingkan tingkat kerentanan keamanan web mana yang lebih rentan antara kedua *framework* tersebut, yaitu *laravel* dan *codeigniter* dari hasil klasifikasi berdasarkan indikator OWASP TOP 10. Tahap berikutnya setelah didapatkan hasil perbandingan kemudian dilakukan penarikan kesimpulan untuk hasil pengujian manakah *framework* yang lebih rentan.