

## DAFTAR GAMBAR

<b>Gambar I. 1</b> Struktur Pengerjaan.....	15
<b>Gambar II.1</b> Metode OWASP TOP 10 .....	23
<b>Gambar II.2</b> Logo Kali Linux .....	28
<b>Gambar II.3</b> OWASP ZAP (Zed Attack Proxy) .....	29
<b>Gambar II.4</b> Tools <i>WhoIs</i> .....	29
<b>Gambar II.5</b> Tampilan Tools Nikto .....	30
<b>Gambar II.6</b> Tampilan <i>Tools BurpSuite</i> .....	30
<b>Gambar II.7</b> Tampilan Tools dirsearch.....	31
<b>Gambar II.8</b> Tampilan Tools DIRB .....	32
<b>Gambar II.9</b> Tampilan gambar Tools Wappalhyzer .....	32
<b>Gambar II.10</b> Tampilan gambar Tools Curl .....	33
<b>Gambar II.11</b> Tampilan gambar Tools NMAP .....	33
<b>Gambar III. 1</b> Sistematika Pengujian.....	<b>34</b>
<b>Gambar IV. 1</b> Website PTPN 11 .....	43
<b>Gambar IV. 2</b> Teknologi yang dipakai PTPN 11 .....	44
<b>Gambar IV. 3</b> NSLOOKUP untuk mengetahui ip website .....	45
<b>Gambar IV. 4</b> NSLOOKUP untuk mengetahui firewall .....	45
<b>Gambar IV. 5</b> Whois untuk mengetahui hostinger website .....	46
<b>Gambar IV. 6</b> Hasil Scan nmap untuk mengetahui port yang terbuka.....	46
<b>Gambar IV. 7</b> hasil Scanning kerentanan OWASP ZAP .....	47
<b>Gambar IV. 8</b> hasil scan kerentanan Nikto .....	48
<b>Gambar IV. 9</b> Searching using Robot.txt .....	49
<b>Gambar IV. 10</b> pencarian directori tersembunyi dengan Dirsearch .....	50
<b>Gambar IV. 11</b> penggalan directori Curl -v.....	50
<b>Gambar IV. 12</b> Pencarian Directori tersembunyi dengan Dirb.....	51
<b>Gambar IV. 13</b> Access to System/Database.....	52
<b>Gambar IV. 14</b> Contoh parameter Injection.....	53
<b>Gambar IV. 15</b> Injection pada laman login website.....	53
<b>Gambar IV. 16</b> Injection pada laman login website pajak PTPN .....	54
<b>Gambar IV. 17</b> Injection Result username and password.....	54
<b>Gambar IV. 18</b> Contoh Insecure design .....	55
<b>Gambar IV. 19</b> Result Insecure Design dari website pajak PTPN 11.....	56
<b>Gambar IV. 20</b> Result Misconfiguration pada website pajak PTPN 11.....	57
<b>Gambar IV. 21</b> hasil Scanning teknologi dengan Wappalyzer .....	58
<b>Gambar IV. 22</b> Payload Password pengujian serangan brute force .....	59
<b>Gambar IV. 23</b> hasil dari Brute force gagal dengan lokasi yang tidak berpindah .....	59
<b>Gambar IV. 24</b> Brute force berhasil dengan berpindanya lokasi ke halaman utama .....	60
<b>Gambar IV. 25</b> Intercep Cookie untuk dilakukanya decode .....	61
<b>Gambar IV. 26</b> mengirim Cookie ke decoder .....	62
<b>Gambar IV. 27</b> hasil Decode Cookie .....	62
<b>Gambar IV. 28</b> Network link Menu user admin .....	63
<b>Gambar IV. 29</b> Copy link pada akun user.....	64
<b>Gambar IV. 30</b> akun user berhasil menambah akun admin .....	65

<b>Gambar IV. 31</b> Payload username dan Passoword .....	66
<b>Gambar IV. 32</b> hasil dari brute force gagal.....	67
<b>Gambar IV. 33</b> hasil dari brute force berhasil.....	67
<b>Gambar IV. 34</b> Log visitor Pajak PTPN 11 .....	68
<b>Gambar IV. 35</b> Https History Seacrh Burp suite.....	69