DFIR-AI Forensic Report

Narrative Summary
Incident Summary:

Multiple web security events were detected involving various IP addresses. Notably, SQL injection attempts wer

Event Timeline

2026-01-06 10:09:22.907969+00:00 - WAF_CORRELATION detected from 91.107.124.38
2026-01-06 10:09:22.911831+00:00 - WAF_CORRELATION detected from 91.107.124.38
2026-01-06 10:09:22.911908+00:00 - SQL_INJECTION detected from 91.107.124.38
2026-01-06 10:09:22.916467+00:00 - ACCESS_DENIED detected from 157.20.32.130
2026-01-06 10:09:22.916648+00:00 - ACCESS_DENIED detected from 157.20.32.130
2026-01-06 10:09:22.927701+00:00 - Network communication observed
2026-01-06 10:09:22.927943+00:00 - ACCESS_DENIED detected from 157.20.32.130
2026-01-06 10:09:22.928098+00:00 - Network communication observed
2026-01-06 10:09:22.928238+00:00 - Network communication observed
2026-01-06 10:09:22.928453+00:00 - Network communication observed
2026-01-06 10:09:22.928582+00:00 - Network communication observed
2026-01-06 10:09:22.938519+00:00 - Network communication observed
2026-01-06 10:09:22.938672+00:00 - Network communication observed
2026-01-06 10:09:22.938893+00:00 - Network communication observed
2026-01-06 10:09:22.939110+00:00 - Network communication observed
2026-01-06 10:09:22.939336+00:00 - ACCESS_DENIED detected from 222.252.11.23
2026-01-06 10:09:22.939541+00:00 - ACCESS_DENIED detected from 118.70.190.36
2026-01-06 10:09:22.955742+00:00 - ACCESS_DENIED detected from 222.252.11.23
2026-01-06 10:09:22.956010+00:00 - ACCESS_DENIED detected from 118.70.190.36
2026-01-06 10:09:22.956259+00:00 - ACCESS_DENIED detected from 222.252.11.23
2026-01-06 10:09:22.956465+00:00 - ACCESS_DENIED detected from 222.252.11.133
2026-01-06 10:09:22.964393+00:00 - ACCESS_DENIED detected from 160.191.139.216
2026-01-06 10:09:22.964647+00:00 - ACCESS_DENIED detected from 160.191.139.216
2026-01-06 10:09:22.964868+00:00 - ACCESS_DENIED detected from 160.191.139.216
2026-01-06 10:09:22.965077+00:00 - ACCESS_DENIED detected from 160.191.139.216
2026-01-06 10:09:22.965361+00:00 - ACCESS_DENIED detected from 160.191.139.216
2026-01-06 10:09:22.965634+00:00 - ACCESS_DENIED detected from 160.191.139.216
2026-01-06 10:09:22.965899+00:00 - ACCESS_DENIED detected from 81.88.49.27
2026-01-06 10:09:22.966157+00:00 - ACCESS_DENIED detected from 81.88.49.27
2026-01-06 10:09:22.970376+00:00 - ACCESS_DENIED detected from 81.88.49.27
2026-01-06 10:09:22.970717+00:00 - ACCESS_DENIED detected from 81.88.49.27
2026-01-06 10:09:22.971166+00:00 - ACCESS_DENIED detected from 81.88.49.27
2026-01-06 10:09:22.971430+00:00 - ACCESS_DENIED detected from 81.88.49.27
2026-01-06 10:09:22.971949+00:00 - WAF_CORRELATION detected from 173.199.123.6
2026-01-06 10:09:22.972538+00:00 - WAF_CORRELATION detected from 173.199.123.6
2026-01-06 10:09:22.972632+00:00 - SQL_INJECTION detected from 173.199.123.6
2026-01-06 10:09:22.973010+00:00 - PROTOCOL_ABUSE detected from 204.76.203.18
2026-01-06 10:09:22.974055+00:00 - PROTOCOL_ABUSE detected from 154.82.150.126
2026-01-06 10:09:22.974587+00:00 - PROTOCOL_ABUSE detected from 154.82.171.11
2026-01-06 10:09:22.975070+00:00 - PROTOCOL_ABUSE detected from 156.239.204.135
2026-01-06 10:09:22.975899+00:00 - PROTOCOL_ABUSE detected from 154.82.169.248
2026-01-06 10:09:22.976500+00:00 - PROTOCOL_ABUSE detected from 156.239.206.170
2026-01-06 10:09:22.976834+00:00 - LFI detected from 51.38.109.223
2026-01-06 10:09:22.977213+00:00 - LFI detected from 51.38.109.223
2026-01-06 10:09:22.977489+00:00 - LFI detected from 51.38.109.223
2026-01-06 10:09:22.981316+00:00 - WAF_CORRELATION detected from 41.90.64.136
2026-01-06 10:09:22.983488+00:00 - WAF_CORRELATION detected from 41.90.64.136
2026-01-06 10:09:22.984368+00:00 - PROTOCOL_ABUSE detected from 41.90.64.136
2026-01-06 10:09:22.984756+00:00 - ACCESS_DENIED detected from 66.240.223.230
2026-01-06 10:09:22.985100+00:00 - ACCESS_DENIED detected from 66.240.223.230
2026-01-06 10:09:22.985447+00:00 - ACCESS_DENIED detected from 66.240.223.230
2026-01-06 10:09:22.985772+00:00 - ACCESS_DENIED detected from 66.240.223.230
2026-01-06 10:09:22.986051+00:00 - ACCESS_DENIED detected from 66.240.223.230
2026-01-06 10:09:22.986413+00:00 - ACCESS_DENIED detected from 66.240.223.230
2026-01-06 10:09:22.986802+00:00 - LFI detected from 157.20.32.130
2026-01-06 10:09:22.987774+00:00 - LFI detected from 157.20.32.130
2026-01-06 10:09:22.988151+00:00 - LFI detected from 157.20.32.130
2026-01-06 10:09:22.988584+00:00 - LFI detected from 157.20.32.130
2026-01-06 10:09:22.989367+00:00 - LFI detected from 157.20.32.130
2026-01-06 10:09:22.990073+00:00 - LFI detected from 157.20.32.130
2026-01-06 10:09:22.990362+00:00 - ACCESS_DENIED detected from 174.142.31.70
2026-01-06 10:09:22.990701+00:00 - ACCESS_DENIED detected from 174.142.31.70

2026-01-06 10:09:22.990920+00:00 - ACCESS_DENIED detected from 174.142.31.70
2026-01-06 10:09:22.991415+00:00 - WAF_CORRELATION detected from 45.227.162.235
2026-01-06 10:09:22.991656+00:00 - ACCESS_DENIED detected from 174.142.31.70
2026-01-06 10:09:22.992288+00:00 - WAF_CORRELATION detected from 45.227.162.235
2026-01-06 10:09:22.992372+00:00 - SQL_INJECTION detected from 45.227.162.235
2026-01-06 10:09:22.992857+00:00 - ACCESS_DENIED detected from 174.142.31.70
2026-01-06 10:09:22.993155+00:00 - ACCESS_DENIED detected from 174.142.31.70
2026-01-06 10:09:22.993487+00:00 - LFI detected from 157.20.32.130
2026-01-06 10:09:22.994048+00:00 - LFI detected from 157.20.32.130
2026-01-06 10:09:22.994481+00:00 - LFI detected from 157.20.32.130
2026-01-06 10:09:22.994770+00:00 - LFI detected from 157.20.32.130
2026-01-06 10:09:22.995146+00:00 - LFI detected from 157.20.32.130
2026-01-06 10:09:22.995418+00:00 - LFI detected from 157.20.32.130
2026-01-06 10:09:22.995852+00:00 - ACCESS_DENIED detected from 194.195.245.44
2026-01-06 10:09:22.996237+00:00 - ACCESS_DENIED detected from 194.195.245.44
2026-01-06 10:09:22.996677+00:00 - ACCESS_DENIED detected from 194.195.245.44
2026-01-06 10:09:22.996984+00:00 - ACCESS_DENIED detected from 194.195.245.44
2026-01-06 10:09:22.997264+00:00 - ACCESS_DENIED detected from 194.195.245.44
2026-01-06 10:09:22.997849+00:00 - Network communication observed
2026-01-06 10:09:22.998117+00:00 - ACCESS_DENIED detected from 194.195.245.44
2026-01-06 10:09:22.998767+00:00 - PROTOCOL_ABUSE detected from 34.78.138.227
2026-01-06 10:09:22.999468+00:00 - WAF_CORRELATION detected from 34.82.67.239
2026-01-06 10:09:22.999981+00:00 - WAF_CORRELATION detected from 34.82.67.239
2026-01-06 10:09:23.000512+00:00 - PROTOCOL_ABUSE detected from 34.82.67.239
2026-01-06 10:09:23.001086+00:00 - WAF_CORRELATION detected from 54.37.118.70
2026-01-06 10:09:23.001545+00:00 - WAF_CORRELATION detected from 54.37.118.70
2026-01-06 10:09:23.001649+00:00 - SQL_INJECTION detected from 54.37.118.70
2026-01-06 10:09:23.002095+00:00 - WAF_CORRELATION detected from 93.123.109.135
2026-01-06 10:09:23.002410+00:00 - LFI detected from 93.123.109.135
2026-01-06 10:09:23.002782+00:00 - LFI detected from 93.123.109.135
2026-01-06 10:09:23.003103+00:00 - LFI detected from 93.123.109.135
2026-01-06 10:09:23.003345+00:00 - LFI detected from 93.123.109.135
2026-01-06 10:09:23.003590+00:00 - LFI detected from 93.123.109.135
2026-01-06 10:09:23.003798+00:00 - LFI detected from 93.123.109.135
2026-01-06 10:09:23.004024+00:00 - LFI detected from 93.123.109.135
2026-01-06 10:09:23.004503+00:00 - WAF_CORRELATION detected from 93.123.109.135
2026-01-06 10:09:23.004716+00:00 - LFI detected from 93.123.109.135
2026-01-06 10:09:23.004942+00:00 - LFI detected from 93.123.109.135

Hash Summary