

LOG-BASED SOC PLATFORM SECURITY INCIDENT REPORT

Incident Summary

Incident Time	02/Nov/2025:12:01:07 +0530
Severity	Critical
Threat Rule	Sensitive File Access
Source IP	9.9.9.9
IOC Confirmed	NO

IP Intelligence & Enrichment

Private IP	NO
Country	US
Region	Virginia
City	Ashburn
Organization	AS19281 Quad9
ASN	UNKNOWN
Source	ipinfo.io

Normalized Payload

```
get /profile.php?user=../../../../etc/passwd http/1.1
```

Raw Log Evidence

```
9.9.9.9 - - [02/Nov/2025:12:01:07 +0530] "GET /profile.php?user=../../../../etc/passwd HTTP/1.1" 200 842 "-" "curl/7.68.0"
```

Response Actions

Firewall Action	No Firewall Action
Email Alert	Sent
PDF Report	Generated