

# LOG-BASED SOC PLATFORM SECURITY INCIDENT REPORT

Incident Batch Size: 1

## Incident Summary

Time	Severity	Rule	Source IP	IOC
02/Nov/2025:12:01:05 +0530	INFO	XSS	5.6.7.8	NO

## IP Intelligence & Enrichment

Primary IP	5.6.7.8
Private IP	NO
Country	DE
Region	Hamburg
City	Hamburg
Organization	AS6805 Telefonica Germany GmbH & Co.OHG
ASN	UNKNOWN
Source	CACHE

## Evidence Samples

```
5.6.7.8 - - [02/Nov/2025:12:01:05 +0530] "GET /search?q=<script>alert(1)</script>
HTTP/1.1" 200 310 "-" "Mozilla/5.0 (X11; Linux x86_64)"
```

Generated by Log-Based SOC Platform | UTC 2026-01-11T06:43:17.499085