

LOG-BASED SOC PLATFORM SECURITY INCIDENT REPORT

Incident Summary

Incident Time	02/Nov/2025:12:01:30 +0530
Severity	High
Threat Rule	XSS
Source IP	13.13.13.13
IOC Confirmed	NO

IP Intelligence & Enrichment

Private IP	NO
Country	GR
Region	Attica
City	Athens
Organization	AS22390 XEROX CORPORATION
ASN	UNKNOWN
Source	CACHE

Normalized Payload

```
get /page.php?img=<img src=x onerror=alert(1)> http/1.1
```

Raw Log Evidence

```
13.13.13.13 - - [02/Nov/2025:12:01:30 +0530] "GET /page.php?img=<img src=x onerror=alert(1)> HTTP/1.1" 200 201 "-" "Mozilla/5.0"
```

Response Actions

Firewall Action	No Firewall Action
Email Alert	Not Sent
PDF Report	Generated