Alexander Ticket

Note: This report has been sanitized for public sharing.

All internal IPs, hostnames, and Splunk URLs have been redacted or replaced with simulated values.

Report was originally prepared for Jira; internal console links are not publicly accessible. Query references shown for context

QRadar ID: **55225**

Description

Multiple XSS probe attempts detected. ET WEB_SERVER Script tag in URI targeting `/search.php` from 77.111.246.36.

Victim:

[internal web server] - redacted-domain.local

1 Encoded log:

```
"/search.php?searchdata=%3Cscript%3Ealert%28%27You+are+HACKED%21%27%29%3C%2Fscript%3E&search="
```

1 Decoded log:

```
/search.php?searchdata=&lt;script&gt;alert('You are HACKED!')&lt;/script&gt;&search=
```

2 Encoded log:

```
"/search.php?searchdata=%3Cscript%3Ealert%28%27You+are+HACKED%21%27%29%3C%2Fscript%3E&search="
```

2 Decoded log:

```
/search.php?searchdata=&lt;script&gt;alert('You are HACKED!')&lt;/script&gt;&search=
```

3 Encoded log:

```
"/search.php?searchdata=%3Cscript%3Edocument.body.innerHTML+%3D+%27You+have+been+hacked%21%27%3B%3C%2Fscript%3E&search="
```

3 Decoded log:

```
/search.php?searchdata=&lt;script&gt;document.body.innerHTML = 'You have been hacked!';&lt;/script&gt;&search=
```

4 Encoded log:

```
"/search.php?searchdata=%3Cscript%3Ealert%28%27You+are+HACKED%21%27%29%3C%2Fscript%3E&search="
```

4 Decoded log:

```
/search.php?searchdata=&lt;script&gt;alert('You are HACKED!')&lt;/script&gt;&search=
```

5 Encoded log:

```
"/search.php?searchdata=%3Cscript%3E+++for%28let+i+%3D+0%3B+i+%3C+100%3B+i%2B%2B%29+%7B+++++alert%28%27This+is+XSS+%27+%2B+i%29%3B+++%7D+%3C%2Fscript%3E&search="
```

5 Decoded log:

```
/search.php?searchdata=&lt;script&gt; for(let i = 0; i &lt; 100; i++) { alert('This is XSS ' + i); } &lt;/script&gt;&search=
```

6 Encoded log:

```
"/search.php?searchdata=%3Cscript%3E+++for%28let+i+%3D+0%3B+i+%3C+100%3B+i%2B%2B%29+%7B+++++alert%28%27This+is+XSS+%27+%2B+i%29%3B+++%7D+%3C%2Fscript%3E&search="
```

6 Decoded log:

```
/search.php?searchdata=&lt;script&gt;   for(let i = 0; i &lt; 100; i++) {    alert('This is XSS ' + i);   }&lt;/script&gt;&search=
```

7 Encoded log:

```
"/search.php?searchdata=%3Cscript%3Ealert%28%27You+are+HACKED%21%27%29%3C%2Fscript%3E&search="
```

7 Decoded log:

```
/search.php?searchdata=&lt;script&gt;alert('You are HACKED!')&lt;/script&gt;&search=
```

8 Encoded log:

```
"/search.php?searchdata=%3Cscript%3E+++for%28let+i+%3D+0%3B+i+%3C+5%3B+i%2B%2B%29+%7B+++++alert%28%27This+is+XSS+%27+%2B+i%29%3B+++%7D+%3C%2Fscript%3E&search="
```

8 Decoded log:

```
/search.php?searchdata=&lt;script&gt; for(let i = 0; i &lt; 5; i++) { alert('This is XSS ' + i); } &lt;/script&gt;&search=
```

ATTACKER INFO:

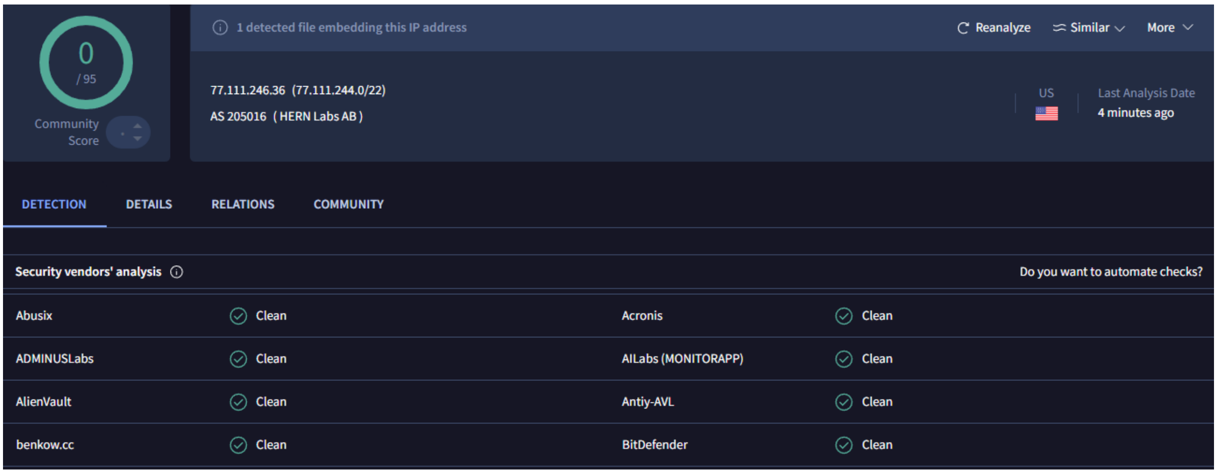
IP: `77.111.246.36` `multiple source ports observed:` `22963, 25031, 50207, 23257, 17709, 36057, 19281, 14815`

User Agent: "The User-Agent string identifies as a common browser (Mozilla/5.0 ... OPR/120.0.0.0). Although it resembles a legitimate Opera/Chrome UA, the value is identical across all requests and may be spoofed. This suggests the requests were likely generated by an automated script or tool (UA spoofing), and used for reconnaissance/probing rather than normal interactive user activity."

ANALYST INVESTIGATION:

Virus Total Result: **[here|https://www.virustotal.com/gui/ip-address/77.111.246.36/detection]**

Security Vendors' Analysis from Virus Total: **Analysis from VirusTotal: 0/94 vendors flagged this IP as malicious — no current reputation hits. Activity is still suspicious based on observed XSS attempts.**



1 detected file embedding this IP address

77.111.246.36 (77.111.244.0/22)
AS 205016 (HERN Labs AB)

US

Last Analysis Date
4 minutes ago

Security vendors' analysis

Do you want to automate checks?

Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AILabs (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	Antiy-AVL	✓ Clean
benkow.cc	✓ Clean	BitDefender	✓ Clean

Talos Intelligence:

REPUTATION DETAILS:

Email Reputation: *Poor*

Web Reputation: *Unknown*

BLOCK LISTS:

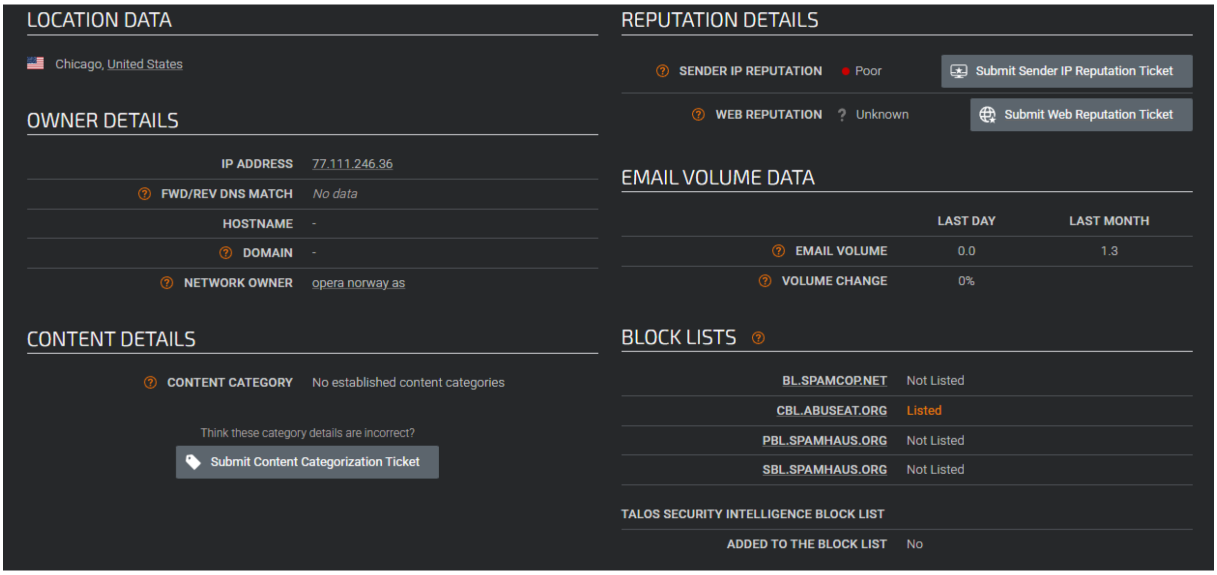
Talos Security Intelligence Block List

cbl.abuseat.org = Listed

Added to the Block List = No

Status = Good

Talos Result:
[here|https://talosintelligence.com/reputation_center/lookup?search=77.111.246.36]



LOCATION DATA

Chicago, United States

OWNER DETAILS

IP ADDRESS	77.111.246.36
FWD/REV DNS MATCH	*No data*
HOSTNAME	-
DOMAIN	-
NETWORK OWNER	opera norway as

CONTENT DETAILS

CONTENT CATEGORY	No established content categories

Think these category details are incorrect?

Submit Content Categorization Ticket

REPUTATION DETAILS

SENDER IP REPUTATION	● Poor
WEB REPUTATION	? Unknown

Submit Sender IP Reputation Ticket
Submit Web Reputation Ticket

EMAIL VOLUME DATA

	LAST DAY	LAST MONTH
EMAIL VOLUME	0.0	1.3
VOLUME CHANGE	0%	

BLOCK LISTS

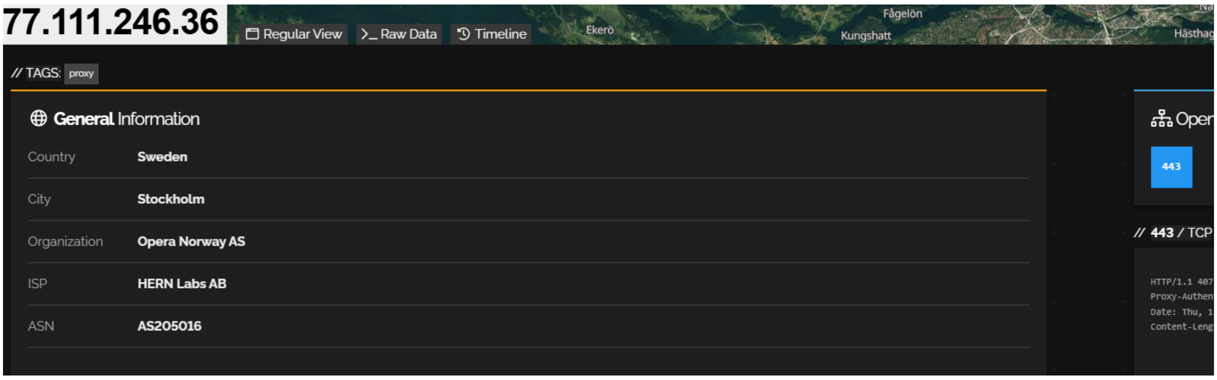
BL.SPAMCOP.NET	Not Listed
CBL.ABUSEAT.ORG	Listed
PBL.SPAMHAUS.ORG	Not Listed
SBL.SPAMHAUS.ORG	Not Listed

TALOS SECURITY INTELLIGENCE BLOCK LIST

ADDED TO THE BLOCK LIST	No

ShodanResult: **[here|https://www.shodan.io/host/77.111.246.36]**

Open Ports: 443



77.111.246.36

// TAGS: proxy

General Information

Country	Sweden
City	Stockholm
Organization	Opera Norway AS
ISP	HERN Labs AB
ASN	AS205016

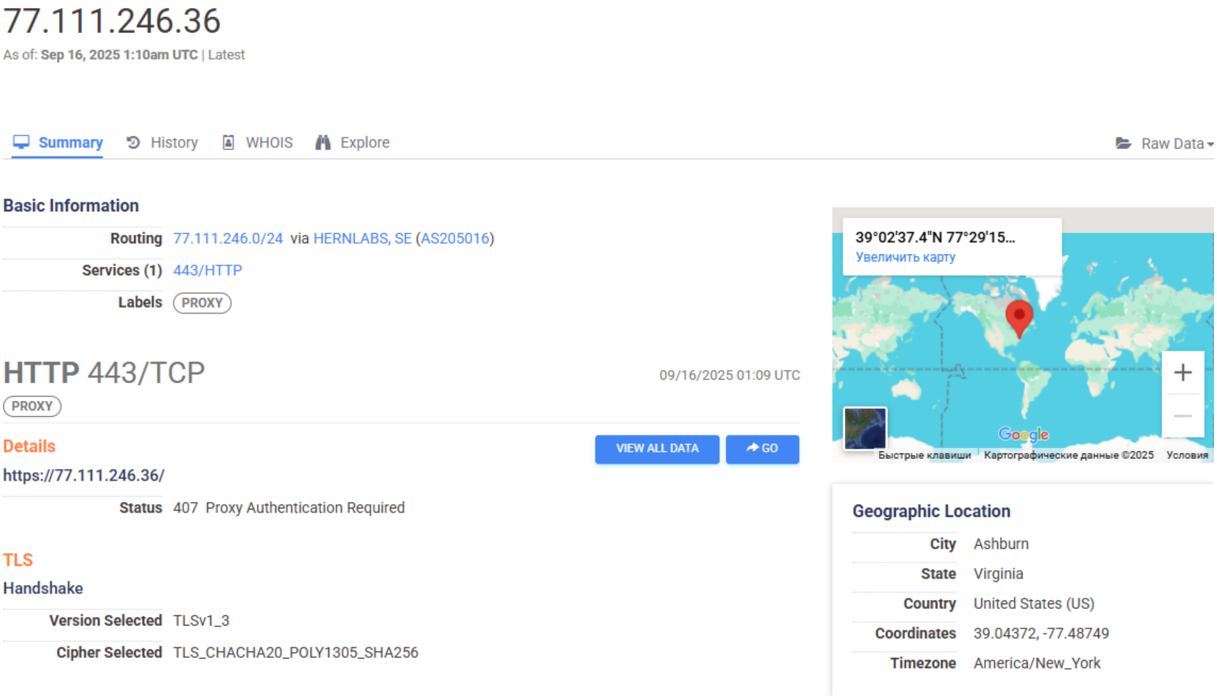
Open

443

// 443 / TCP

```
HTTP/1.1 407
Proxy-Authen
Date: Thu, 1
Content-Leng
```

CensysResult: **[here|**https://search.censys.io/hosts/77.111.246.36**]**



77.111.246.36

As of: Sep 16, 2025 1:10am UTC | Latest

Basic Information

Routing	77.111.246.0/24 via HERNLABS, SE (AS205016)
Services (1)	443/HTTP
Labels	PROXY

HTTP 443/TCP

PROXY

09/16/2025 01:09 UTC

Details

https://77.111.246.36/

Status 407 Proxy Authentication Required

TLS

Handshake

Version Selected	TLSv1_3
Cipher Selected	TLS_CHACHA20_POLY1305_SHA256

Geographic Location

City	Ashburn
State	Virginia
Country	United States (US)
Coordinates	39.04372, -77.48749
Timezone	America/New_York

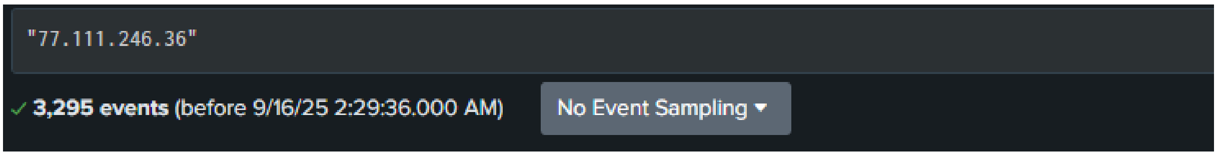
Splunk Investigation: A total of **3,295 events** were identified during the analysis for source IP **77.111.246.36**.

To structure the investigation, the following filters were applied step-by-step:

Step 1: Search `"77.111.246.36"` → **3,295 events** (baseline volume).

Result 1: Splunk search — internal link (not accessible)

↓↓↓



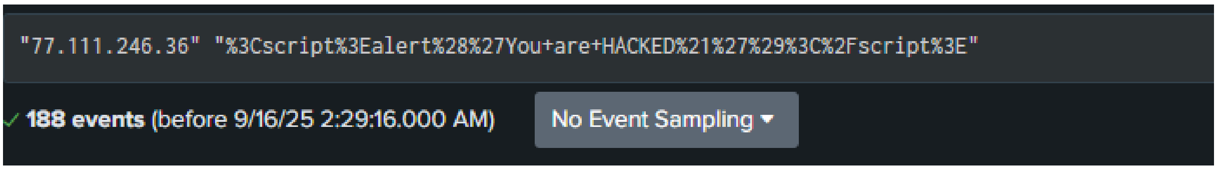
```
"77.111.246.36"
```

✓ **3,295 events** (before 9/16/25 2:29:36.000 AM)

Step 2: Search with encoded XSS payload `"%3Cscript%3Ealert%28%27You+are+HACKED%21%27%29%3C%2Fscript%3E"` → **188 events** matched (XSS activity targeting `/search.php`).

Result 2: Splunk search — internal link (not accessible)

↓↓↓



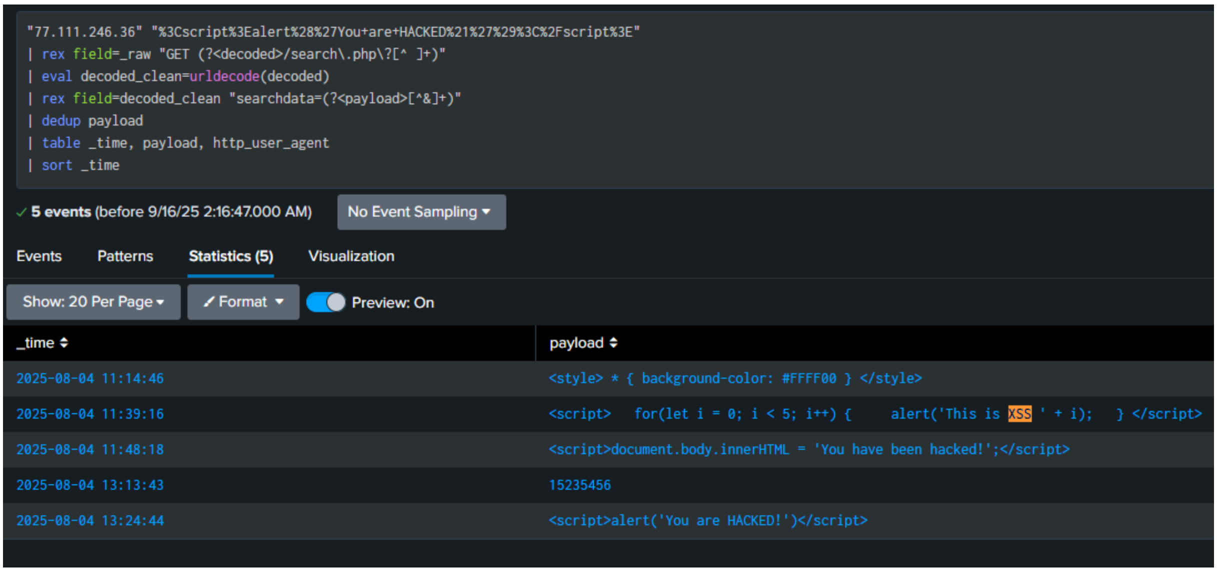
```
"77.111.246.36" "%3Cscript%3Ealert%28%27You+are+HACKED%21%27%29%3C%2Fscript%3E"
```

✓ **188 events** (before 9/16/25 2:29:16.000 AM)

Step 3: URL decoding + deduplication of `searchdata` parameter → **5 unique payloads** identified .

Result 3: Splunk search — internal link (not accessible)

↓↓↓



```
"77.111.246.36" "%3Cscript%3Ealert%28%27You+are+HACKED%21%27%29%3C%2Fscript%3E"
| rex field=_raw "GET (?<decoded>/search\.php\?[^ ]+)"
| eval decoded_clean=urldecode(decoded)
| rex field=decoded_clean "searchdata=(?<payload>[^&]+)"
| dedup payload
| table _time, payload, http_user_agent
| sort _time
```

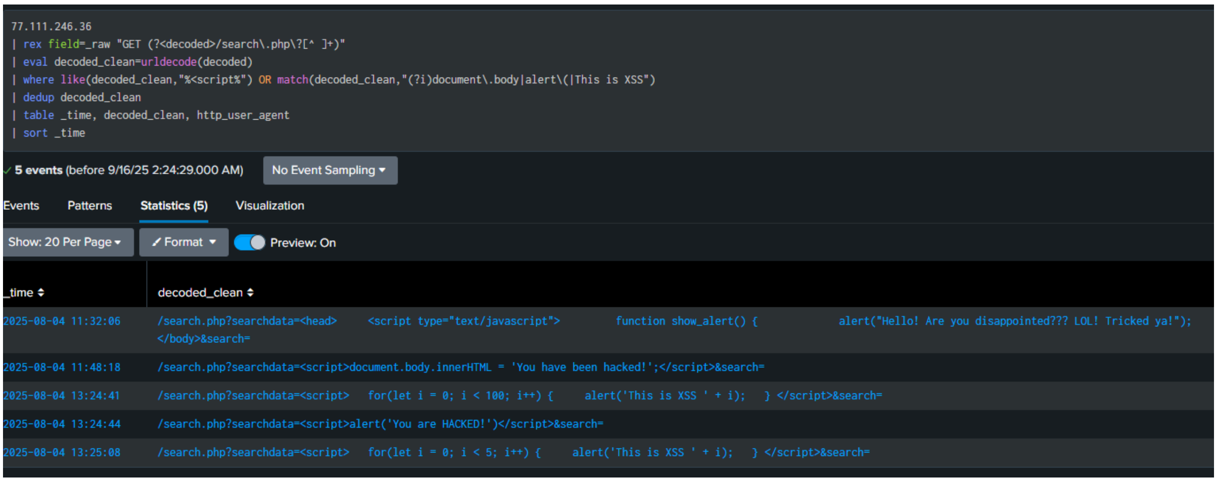
✓ **5 events** (before 9/16/25 2:16:47.000 AM)

_time	payload
2025-08-04 11:14:46	`<style> * { background-color: #FFFF00 } </style>`
2025-08-04 11:39:16	`<script>   for(let i = 0; i < 5; i++) {     alert('This is XSS ' + i);   } </script>`
2025-08-04 11:48:18	`<script>document.body.innerHTML = 'You have been hacked!';</script>`
2025-08-04 13:13:43	15235456
2025-08-04 13:24:44	`<script>alert('You are HACKED!')</script>`

Step 4: Pattern-based search (`<script>`, `document.body`, `alert()`, `This is XSS`) confirmed the same 5 unique decoded requests.

Result 4: Splunk search — internal link (not accessible)

↓↓↓



```
77.111.246.36
| rex field=_raw "GET (?<decoded>/search\.php\?[^ ]+)"
| eval decoded_clean=urldecode(decoded)
| where like(decoded_clean,"%<script%") OR match(decoded_clean,"(?i)document\.body|alert\(|This is XSS")
| dedup decoded_clean
| table _time, decoded_clean, http_user_agent
| sort _time
```

✓ **5 events** (before 9/16/25 2:24:29.000 AM)

_time	decoded_clean
2025-08-04 11:32:06	`/search.php?searchdata=<head>   <script type="text/javascript">     function show_alert() {       alert("Hello! Are you disappointed??? LOL! Tricked ya!"); </body>&search=`
2025-08-04 11:48:18	`/search.php?searchdata=<script>document.body.innerHTML = 'You have been hacked!';</script>&search=`
2025-08-04 13:24:41	`/search.php?searchdata=<script>   for(let i = 0; i < 100; i++) {     alert('This is XSS ' + i);   } </script>&search=`
2025-08-04 13:24:44	`/search.php?searchdata=<script>alert('You are HACKED!')</script>&search=`
2025-08-04 13:25:08	`/search.php?searchdata=<script>   for(let i = 0; i < 5; i++) {     alert('This is XSS ' + i);   } </script>&search=`

1 Raw Data:

```
<168>suricata[8969]: {"timestamp":"2025-08-04T10:36:08.384875-0400","flow_id":1478859335168381,"in_iface":"eth0","event_type":"alert","src_ip":"77.111.246.36","src_port":22963,"dest_ip":" [internal web server IP] ","dest_port":80,"proto":"TCP","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":2009714,"rev":5,"signature":"ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt","category":"Web Application Attack","severity":1},"http":{"hostname":" redacted-domain.local","url":"\/search.php?searchdata=%3Cscript%3Ealert%28%27You+are+HACKED%21%27%29%3C%2Fscript%3E&search=","http_user_agent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/135.0.0.0 Safari\/537.36 OPR\/120.0.0.0","http_content_type":"text\/html","http_refer":" <redacted-splunk-instance>/search","http_method":"GET","protocol":"HTTP\/1.1","status":200,"length":1140}}
```

2 Raw Data:

```
<168>suricata[8969]: {"timestamp":"2025-08-04T10:42:24.435707-0400","flow_id":673467092456935,"in_iface":"eth0","event_type":"alert","src_ip":"77.111.246.36","src_port":25031,"dest_ip":" [internal web server IP] ","dest_port":80,"proto":"TCP","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":2009714,"rev":5,"signature":"ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt","category":"Web Application Attack","severity":1},"http":{"hostname":" redacted-domain.local","url":"\/search.php?searchdata=%3Cscript%3Ealert%28%27You+are+HACKED%21%27%29%3C%2Fscript%3E&search=","http_user_agent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/135.0.0.0 Safari\/537.36 OPR\/120.0.0.0","http_content_type":"text\/html","http_refer":" <redacted-splunk-instance>/search %3Cscript%3Ealert%28%27You+are+HACKED%21%27%29%3C%2Fscript%3E&search=","http_method":"GET","protocol":"HTTP\/1.1","status":200,"length":1140}}
```

3 Raw Data:

```
<168>suricata[8969]: {"timestamp":"2025-08-04T10:48:18.615233-0400","flow_id":1307726411071864,"in_iface":"eth0","event_type":"alert","src_ip":"77.111.246.36","src_port":50207,"dest_ip":" [internal web server IP] ","dest_port":80,"proto":"TCP","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":2009714,"rev":5,"signature":"ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt","category":"Web Application Attack","severity":1},"http":{"hostname":" redacted-domain.local","url":"\/search.php?searchdata=%3Cscript%3Edocument.body.innerHTML+%3D+%27You+have+been+hacked%21%27%3B%3C%2Fscript%3E&search=","http_user_agent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/135.0.0.0 Safari\/537.36 OPR\/120.0.0.0","http_content_type":"text\/html","http_refer":" <redacted-splunk-instance>/search%3Cscript%3Ealert%28%27You+are+HACKED%21%27%29%3C%2Fscript%3E&search=","http_method":"GET","protocol":"HTTP\/1.1","status":200,"length":1140}}
```

4 Raw Data:

```
<168>suricata[8969]: {"timestamp":"2025-08-04T10:48:23.254472-
0400","flow_id":1344534281162747,"in_iface":"eth0","event_type":"alert","src_ip":"77.111.246.36","src_port":23257,"des
t_ip":" [internal web server IP]
","dest_port":80,"proto":"TCP","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":2009714,"rev":5,"signature":"
ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt","category":"Web Application
Attack","severity":1},"http":{"hostname":" redacted-
domain.local","url":"\/search.php?searchdata=%3Cscript%3Ealert%28%27You+are+HACKED%21%27%29%3C%2Fscri
pt%3E&search=","http_user_agent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like
Gecko) Chrome\/135.0.0.0 Safari\/537.36 OPR\/120.0.0.0","http_content_type":"text\/html","http_refer":" <redacted-splunk-
instance>/search%3Cscript%3Ealert%28%27You+are+HACKED%21%27%29%3C%2Fscript%3E&search=","http_metho
d":"GET","protocol":"HTTP\/1.1","status":200,"length":1140}}
```

5 Raw Data:

```
<168>suricata[8969]: {"timestamp":"2025-08-04T12:23:43.098485-
0400","flow_id":1894784391081469,"in_iface":"eth0","event_type":"alert","src_ip":"77.111.246.36","src_port":17709,"des
t_ip":" [internal web server IP]
","dest_port":80,"proto":"TCP","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":2009714,"rev":5,"signature":"
ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt","category":"Web Application
Attack","severity":1},"http":{"hostname":" redacted-
domain.local","url":"\/search.php?searchdata=%3Cscript%3E+++for%28let+i+%3D+0%3B+i+%3C+100%3B+i%2B%2
B%29+%7B+++++alert%28%27This+is+XSS+%27+%2B+i%29%3B+++%7D+%3C%2Fscript%3E&search=","http_us
er_agent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/135.0.0.0
Safari\/537.36 OPR\/120.0.0.0","http_content_type":"text\/html","http_refer":" <redacted-splunk-
instance>/search125&search=","http_method":"GET","protocol":"HTTP\/1.1","status":200,"length":1140}}
```

6 Raw Data:

```
<168>suricata[8969]: {"timestamp":"2025-08-04T12:24:41.348561-
0400","flow_id":799911331826998,"in_iface":"eth0","event_type":"alert","src_ip":"77.111.246.36","src_port":36057,"dest
_ip":" [internal web server IP]
","dest_port":80,"proto":"TCP","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":2009714,"rev":5,"signature":"
ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt","category":"Web Application
Attack","severity":1},"http":{"hostname":" redacted-
domain.local","url":"\/search.php?searchdata=%3Cscript%3E+++for%28let+i+%3D+0%3B+i+%3C+100%3B+i%2B%2
B%29+%7B+++++alert%28%27This+is+XSS+%27+%2B+i%29%3B+++%7D+%3C%2Fscript%3E&search=","http_us
er_agent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/135.0.0.0
Safari\/537.36
OPR\/120.0.0.0","http_content_type":"text\/html","http_method":"GET","protocol":"HTTP\/1.1","status":200,"length":1140
}}
```

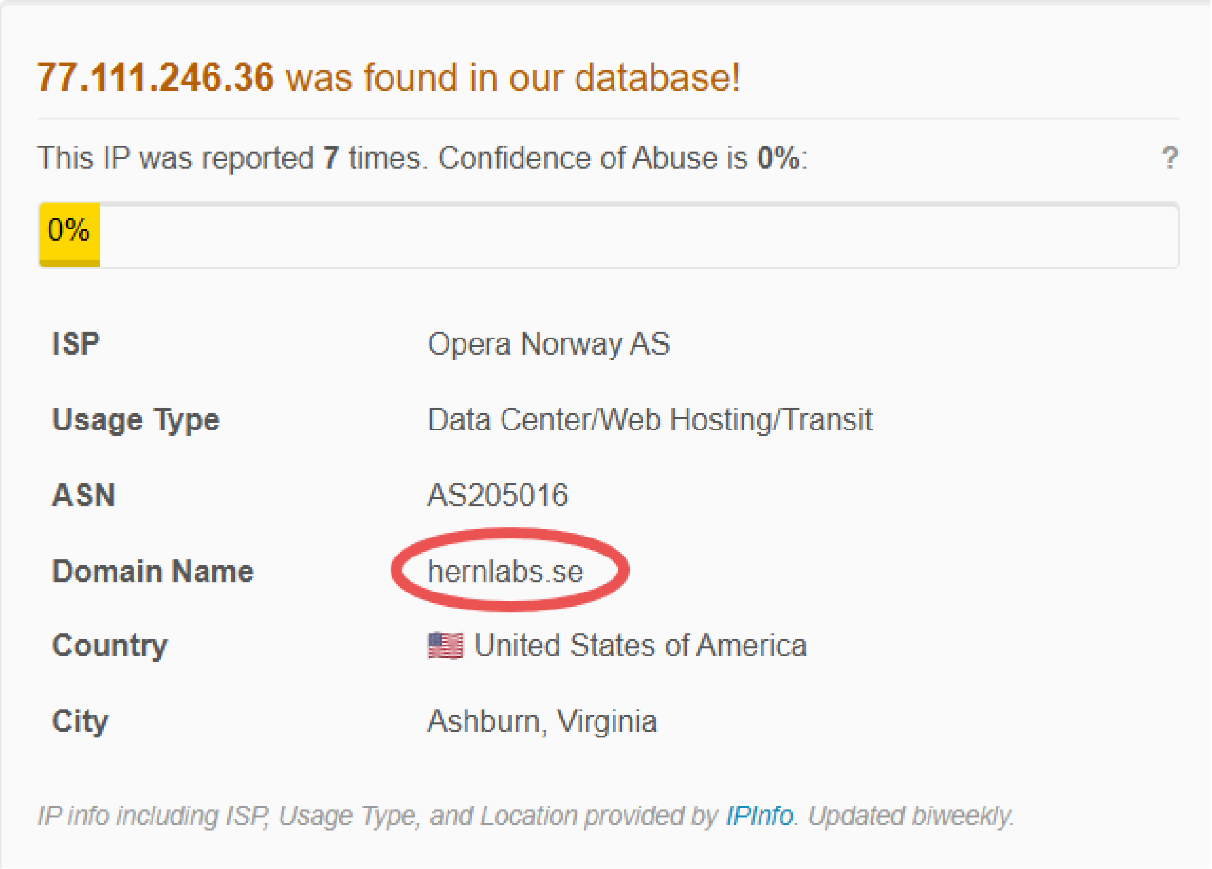
7 Raw Data:

```
<168>suricata[8969]: {"timestamp":"2025-08-04T12:24:44.328196-
0400","flow_id":1188661706905498,"in_iface":"eth0","event_type":"alert","src_ip":"77.111.246.36","src_port":19281,"des
t_ip":" [internal web server IP]
","dest_port":80,"proto":"TCP","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":2009714,"rev":5,"signature":"
ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt","category":"Web Application
Attack","severity":1},"http":{"hostname":" redacted-
domain.local","url":"\/search.php?searchdata=%3Cscript%3Ealert%28%27You+are+HACKED%21%27%29%3C%2Fscri
pt%3E&search=","http_user_agent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like
Gecko) Chrome\/135.0.0.0 Safari\/537.36 OPR\/120.0.0.0","http_refer":" <redacted-splunk-
instance>/search121315&search=","http_method":"GET","protocol":"HTTP\/1.1","length":0}}
```

8 Raw Data:

```
<168>suricata[8969]: {"timestamp":"2025-08-04T12:25:08.805250-
0400","flow_id":1469754433135928,"in_iface":"eth0","event_type":"alert","src_ip":"77.111.246.36","src_port":14815,"des
t_ip":" [internal web server IP]
","dest_port":80,"proto":"TCP","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":2009714,"rev":5,"signature":"
ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt","category":"Web Application
Attack","severity":1},"http":{"hostname":" redacted-
domain.local","url":"\/search.php?searchdata=%3Cscript%3E+++for%28let+i+%3D+0%3B+i+%3C+5%3B+i%2B%2B
%29+%7B+++++alert%28%27This+is+XSS+%27+%2B+i%29%3B+++%7D+%3C%2Fscript%3E&search=","http_use
r_agent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/135.0.0.0
Safari\/537.36 OPR\/120.0.0.0","http_content_type":"text\/html","http_refer":" <redacted-splunk-
instance>/search","http_method":"GET","protocol":"HTTP\/1.1","status":200,"length":1140}}
```

Additional Findings:



77.111.246.36 was found in our database!

This IP was reported **7** times. Confidence of Abuse is **0%**: ?

0%

ISP	Opera Norway AS
Usage Type	Data Center/Web Hosting/Transit
ASN	AS205016
Domain Name	hernlabs.se
Country	United States of America
City	Ashburn, Virginia

IP info including ISP, Usage Type, and Location provided by IPInfo. Updated biweekly.

77.111.246.36 is an IP address from within our whitelist belonging to the subnet 77.111.246.0/24, which we identify as: **"Opera built-in browser VPN"**.

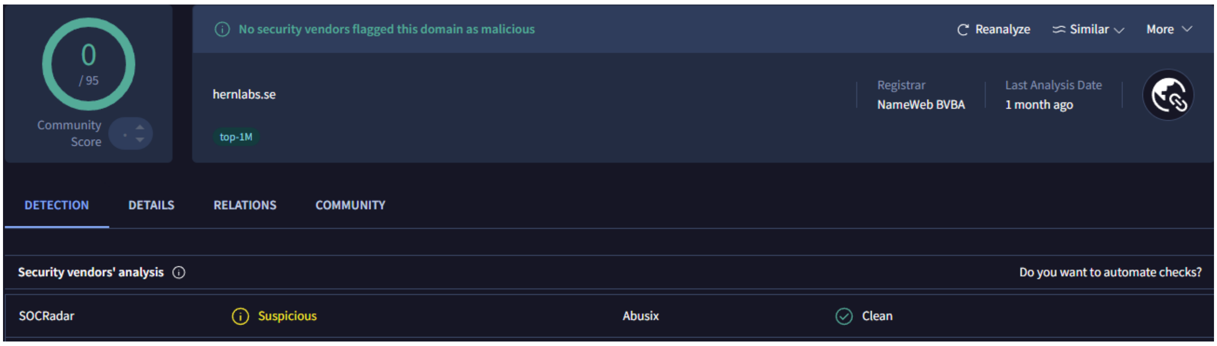
Whitelisted netblocks are typically owned by trusted entities, such as Google or Microsoft who may use them for search engine spiders. However, these same entities sometimes also provide cloud servers and mail services which are easily abused.

ResultAbuseIPDB: **[here|https://www.abuseipdb.com/check/77.111.246.36]**

The source IP **77.111.246.36** resolves to the domain **hernlabs.se**.

This domain was checked on **VirusTotal**, and the result showed:

[here|https://www.virustotal.com/gui/ip-address/77.111.246.36/details]



0 / 95 Community Score

No security vendors flagged this domain as malicious

hernlabs.se

top-1M

Registrar: NameWeb BVBA

Last Analysis Date: 1 month ago

Security vendors' analysis

SOCRadar	Suspicious	Abusix	Clean

This indicates that the domain is **likely legitimate**, but the *Suspicious* flag suggests further monitoring is recommended.

Investigation of QRadar Alert ID 55225 and subsequent Splunk/Suricata log review shows automated XSS probing activity originating from source IP 77.111.246.36 targeting `/search.php` on [internal web server IP] (redacted-domain.local).

Summary of findings

- **Baseline: 3,295 events observed from source IP 77.111.246.36 (selected time range).**
- **Filtered XSS hits: 188 events matched the encoded payload `%3Cscript%3Ealert%28%27You+are+HACKED%21%27%29%3C%2Fscript%3E`.**
- **Unique payloads: After URL decoding and deduplication of the `searchdata` parameter, 5 distinct XSS payloads were identified (examples include `alert('You are HACKED!')`, DOM modification `document.body.innerHTML = 'You have been hacked!'`, and looped alert injections).**
- **Raw evidence: 8 Suricata alerts (attached) mapped to these payloads; several payloads repeated across multiple source ports/timestamps — consistent with automated scanning.**

Attack details

- **Vector: Reflected XSS attempts via the `searchdata` parameter on `/search.php`.**
- **Payload types: `<script>alert(...)</script>`, DOM-manipulation (`document.body.innerHTML`), inline `<style>` injection, and looped JavaScript alerts — all intended to test for improper output encoding/reflection.**
- **User-Agent: `Mozilla/5.0 ... OPR/120.0.0.0` (identical across requests). UA appears browser-like but likely spoofed; behavior consistent with**

automation.

- **Observed behaviour: Multiple requests from same IP with varying source ports (22963, 25031, 50207, 23257, 17709, 36057, 19281, 14815) — repeated probing rather than single manual request.**

Detection context

- **Signature triggered: ET WEB_SERVER — *Script tag in URI, Possible Cross Site Scripting Attempt* (signature_id 2009714).**
- **Suricata events: 8 raw Suricata alerts captured (attached).**
- Splunk correlation: narrow filter → 188 matched events; decode + dedup → 5 unique payloads.

Threat intelligence

- **Domain/IP resolution: IP resolves to domain hernlabs.se (associated with Opera/Opera VPN infrastructure). Source IP appears within a whitelisted subnet used by Opera's built-in VPN.**
- **VirusTotal: 0/94 vendors flagged the IP as malicious (no current TI hits).**
- **Cisco Talos: Web reputation *Unknown*, Email reputation *Poor*; listed on `cbl.abuseat.org` but not blocked.**
- **Shodan / Censys: Minimal exposure observed (Shodan shows port 443 open).**
- **Interpretation: Lack of TI hits (VT=0/94) indicates no broad known malicious reputation, but SOCRadar/SOC signals and observed behavior (automated XSS probes) warrant suspicion — likely abuse of legitimate VPN/proxy infrastructure.**

Assessment

- **Likely actor behavior: Automated reconnaissance / mass XSS probing leveraging VPN exit node to obscure origin. Identical UA and repeated payload patterns strongly indicate scripted tooling rather than interactive user activity.**
- **Probable intent: Identify reflected XSS vulnerabilities in `/search.php` for possible later exploitation (proof-of-concept payloads observed).**
- **Immediate impact observed: No evidence of successful exploitation in the logs reviewed (no signs of server-side compromise). Impact currently limited to reconnaissance/probing attempts.**

Risk rating

- **Risk: Medium — Confirmed malicious probing (XSS) but no confirmed successful compromise.**
- **Likelihood of further attempts: High — repeated probes over time and variety of payloads suggest ongoing scanning.**

Impact if Successful

- **Remote Code Execution (RCE):** Exploitation of XSS could allow execution of arbitrary JavaScript, potentially leading to full compromise if chained with other bugs.
- **Session Hijacking:** Theft of session cookies or tokens could result in account takeover.
- **Data Exfiltration:** Attacker could access sensitive data from the DOM or trigger unauthorized requests (CSRF).
- **Defacement / Phishing:** Injected scripts could modify page content, serve phishing forms, or deliver malware.
- **Persistence & Lateral Movement:** Successful exploitation could lead to web shells or backdoors for deeper network access.

Mini Attack Visualization:

[QRadar Alert ID 55225 — ET WEB_SERVER Script tag in URI (XSS)]

↓

[Analyst pivots into logs — source IP 77.111.246.36]

↓

[Baseline traffic from IP: 3,295 events (all indexes/time range)]

↓

[Filtered by encoded XSS payload `%3Cscript%3Ealert(...)%3C%2Fscript%3E` → 188 matched events]

↓

[Suricata raw alerts (attached): 8 events mapped to these matches]

↓

[URL decoded + `searchdata` extracted → deduplicated → 5 unique XSS payloads]

↓

[Target: [internal web server IP] — redacted-domain.local]

↓

[Observed payload types: `alert()` popups, DOM manipulation (`document.body.innerHTML`), looped alerts, inline `<style>`]

↓

[User-Agent: `Mozilla/5.0 ... OPR/120.0.0.0` — identical across requests (likely scripted)]

↓

[Source behavior: multiple ephemeral source ports observed (22963,25031,50207,23257,17709,36057,19281,14815) — repeated automated probing]

↓

[Detection: Suricata SID 2009714 triggered — “ET WEB_SERVER Script tag in URI, Possible XSS”]

↓

[Threat Intel: IP resolves to hernlabs.se (Opera/VPN infrastructure); VirusTotal 0/94; Talos: mixed/unknown; Shodan shows port 443 open]

↓

[Conclusion: Automated XSS reconnaissance from a VPN/proxy exit node. Recommend blocking/rate-limit, collect HTTP responses, and dev review of `/search.php` for proper encoding]

Recommended Actions:

1. Immediate Containment & Monitoring

- **Network Controls:**
  - Closely monitor traffic from **77.111.246.36** and the broader **77.111.246.0/24 Opera VPN subnet**.
  - If probing continues, consider temporary rate-limiting or blocking this IP/subnet at the firewall, WAF, or load balancer level to reduce noise and potential exploitation attempts.
- **Evidence Collection:**
  - Capture and review HTTP response bodies for a sample of the 188 XSS events to verify if payloads were reflected (potentially exploitable) or sanitized.
  - Archive the 8 Suricata raw JSON alerts and the deduplicated payload table (5 unique payloads) for incident documentation and possible dev team review.

2. Application Security Hardening

- **Code Review:**
  - Conduct secure code review of `/search.php` focusing on the `searchdata` parameter — ensure robust **input validation** and **output encoding** (HTML-encoding of special characters).
  - Implement server-side checks to block `<script>` tags and other malicious payload patterns before rendering responses.
- **Security Headers:**
  - Deploy or review **Content Security Policy (CSP)** headers to restrict inline script execution.
  - Ensure X-XSS-Protection or equivalent browser defenses are configured (or modern replacements like CSP/Trusted Types).
- **WAF Rules:**
  - Update or enable WAF rules/signatures to detect and block reflected XSS attempts in query parameters.
  - Configure normalization of double-encoded payloads to avoid bypasses.

3. SOC Detection & Alerting

- **Splunk Correlation:**
  - Build or refine a correlation search that decodes `searchdata`, matches on `<script>` or known XSS payload patterns, and deduplicates payloads for easier triage.
  - Trigger alerts when multiple unique payloads are observed from a single IP within a short time window — a strong indicator of automated scanning.
- **Threat Intelligence Feeds:**
  - Continue monitoring **VirusTotal, Cisco Talos, AbuseIPDB, SOCRadar** for changes in the IP/domain reputation.
  - Add the IP/domain to a watchlist to detect recurring activity from the same VPN exit node or associated infrastructure.

4. Awareness & Process Improvements

- **Dev Team Notification:**
  - Share investigation findings, including the 5 unique decoded payloads, with the web/app dev team for replication testing and patch validation.
  - Recommend adding automated regression tests to catch reflected XSS before deployment.
- **AppSec Testing:**
  - Schedule periodic DAST scans or pen-tests on "redacted-domain.local" and especially `/search.php` to validate mitigations and check for other injection points.
- **Documentation:**
  - Record this incident in the internal knowledge base as an example of XSS probing from Opera VPN IP ranges, including links to Splunk searches, TI results, and Suricata alerts.

5. Long-Term Security Strategy

- **User Impact Protection:**
  - Apply proper session cookie flags (HttpOnly, Secure, SameSite) to reduce the risk of session theft if XSS occurs.
- **Visibility & Logging:**

  - Ensure full HTTP request/response logging for `/search.php` during high-risk windows to aid in future investigations.

- **Continuous Improvement:**
  - Evaluate adding runtime protection (RASP) or advanced WAF with virtual patching capabilities to mitigate 0-day XSS attempts.