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: 54773

Description

Trojan detected, preceded by web exploit. RCE and directory traversal attempts targeting the web server.

Victim:

[internal web server] - redacted-domain.local

1 Encoded log:

"/hello.world?%ADd+allow_url_include%3d1+%ADd+auto_prepend_file%3dphp://input"

1 Decoded log:

/hello.world?-d allow_url_include=1 -d auto_prepend_file=php://input

2 Encoded log:

%2Findex.php%3Flang%3D..%2F..%2F..%2F..%2F..%2F..%2F..%2Ftmp%2Findex1

2 Decoded log:

/index.php?lang=../../../../../../../tmp/index1

ATTACKER INFO:

IP: `188.128.39.37` on port 46216

User Agent: "Custom-AsyncHttpClient" (seems to be a custom or fake user agent). The full browser and operating system details are missing, likely due to the use of automated tools or scripts that do not include standard browser/OS headers.

ANALYST INVESTIGATION:

Virus Total Result: **[here|https://www.virustotal.com/gui/ip-address/188.128.39.37]**

Security Vendors' Analysis from Virus Total: 10**/94 security vendors flagged this IP address as malicious**

Brief Community Comments:

- **SSH Brute-Force Attack: Attempted unauthorized SSH logins to a honeypot hosted in Sweden, targeting usernames like `root` and others. Logged on 2025-04-28.**
- **PHPUnit Exploitation: Made multiple requests to known PHP vulnerabilities (e.g., `/eval-stdin.php`) and directory traversal attempts (e.g., `/index.php?lang=../../../../../../../../tmp/index1`).**
- **Shell Execution Attempts: Sent POST requests attempting to execute system commands via `/cgi-bin` paths (e.g., `%32%65%32%65/.../bin/sh`).**

The IP has been classified as malicious due to aggressive login attempts and exploitation of PHP vulnerabilities.

[Result here|https://www.virustotal.com/gui/ip-address/188.128.39.37/community]

Talos Intelligence:

REPUTATION DETAILS:

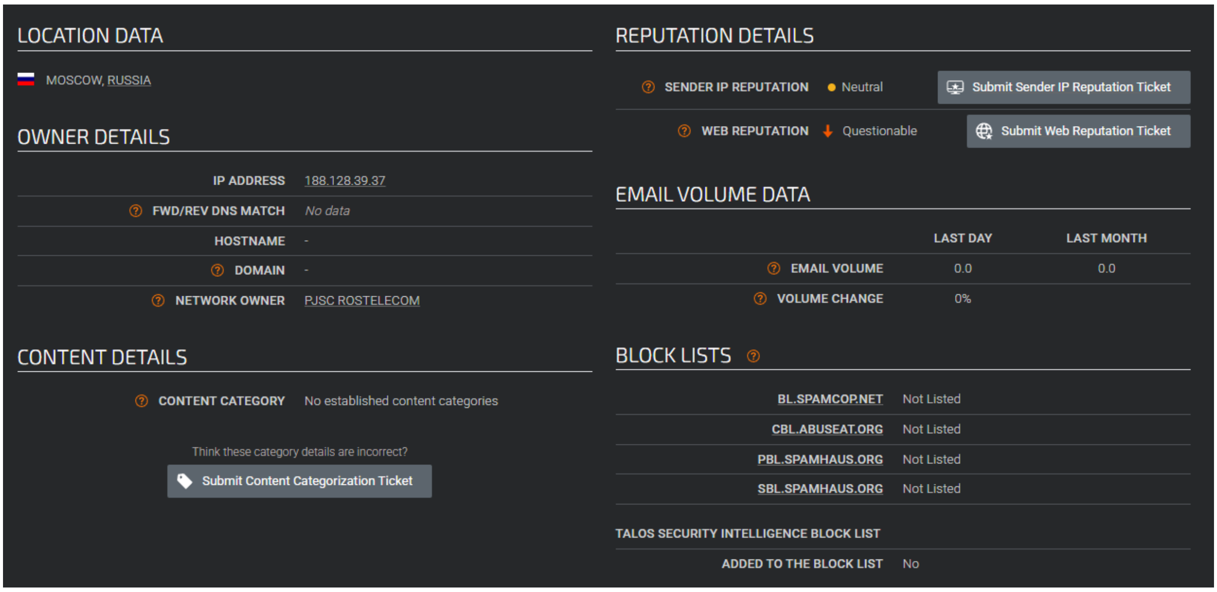
Email Reputation: *Neutral*

Web Reputation: *Questionable*

BLOCK LISTS:

Added to the Block List: *No*

Talos Result:
[here|https://talosintelligence.com/reputation_center/lookup?search=188.128.39.37]



LOCATION DATA

MOSCOW, RUSSIA

OWNER DETAILS

IP ADDRESS	188.128.39.37
FWD/REV DNS MATCH	No data
HOSTNAME	-
DOMAIN	-
NETWORK OWNER	PJSC ROSTELECOM

CONTENT DETAILS

CONTENT CATEGORY No established content categories

Think these category details are incorrect?

Submit Content Categorization Ticket

REPUTATION DETAILS

SENDER IP REPUTATION	● Neutral	Submit Sender IP Reputation Ticket
WEB REPUTATION	↓ Questionable	Submit Web Reputation Ticket

EMAIL VOLUME DATA

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

BLOCK LISTS

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

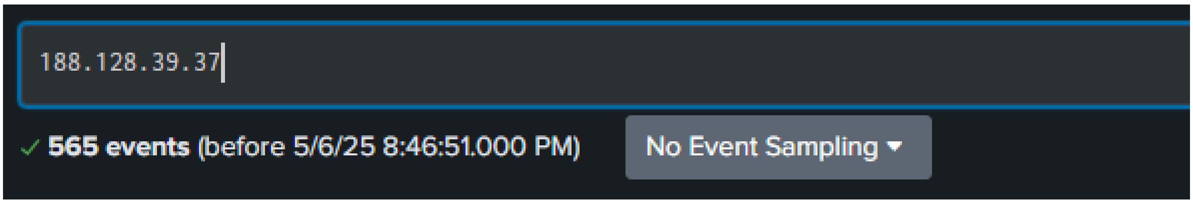
TALOS SECURITY INTELLIGENCE BLOCK LIST

ADDED TO THE BLOCK LIST No

ShodanResult: **[here|https://www.shodan.io/search?query=188.128.39.37]**

Open Ports: 80

Splunk Investigation: **A total of 565 logs were found, and after analyzing them with different identifiers, it was determined that 17 logs were associated with the identifier /hello.world, and 52 logs were linked to the identifier /index.php.**

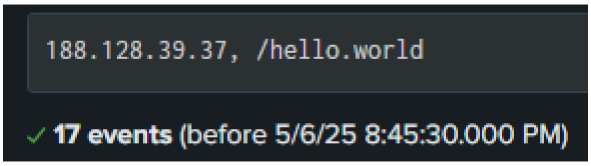


188.128.39.37

✓ **565 events** (before 5/6/25 8:46:51.000 PM)

↑↑↑

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

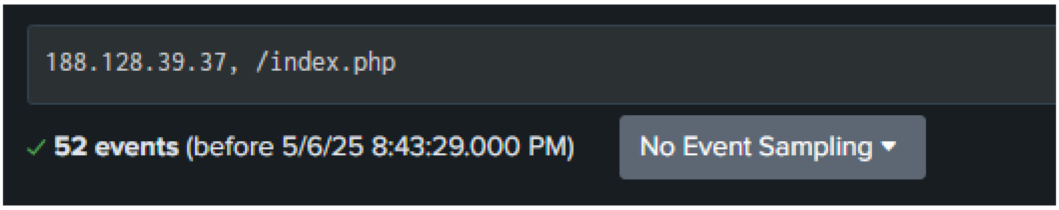


188.128.39.37, /hello.world

✓ **17 events** (before 5/6/25 8:45:30.000 PM)

↑↑↑

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



188.128.39.37, /index.php

✓ **52 events** (before 5/6/25 8:43:29.000 PM)

↑↑↑

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

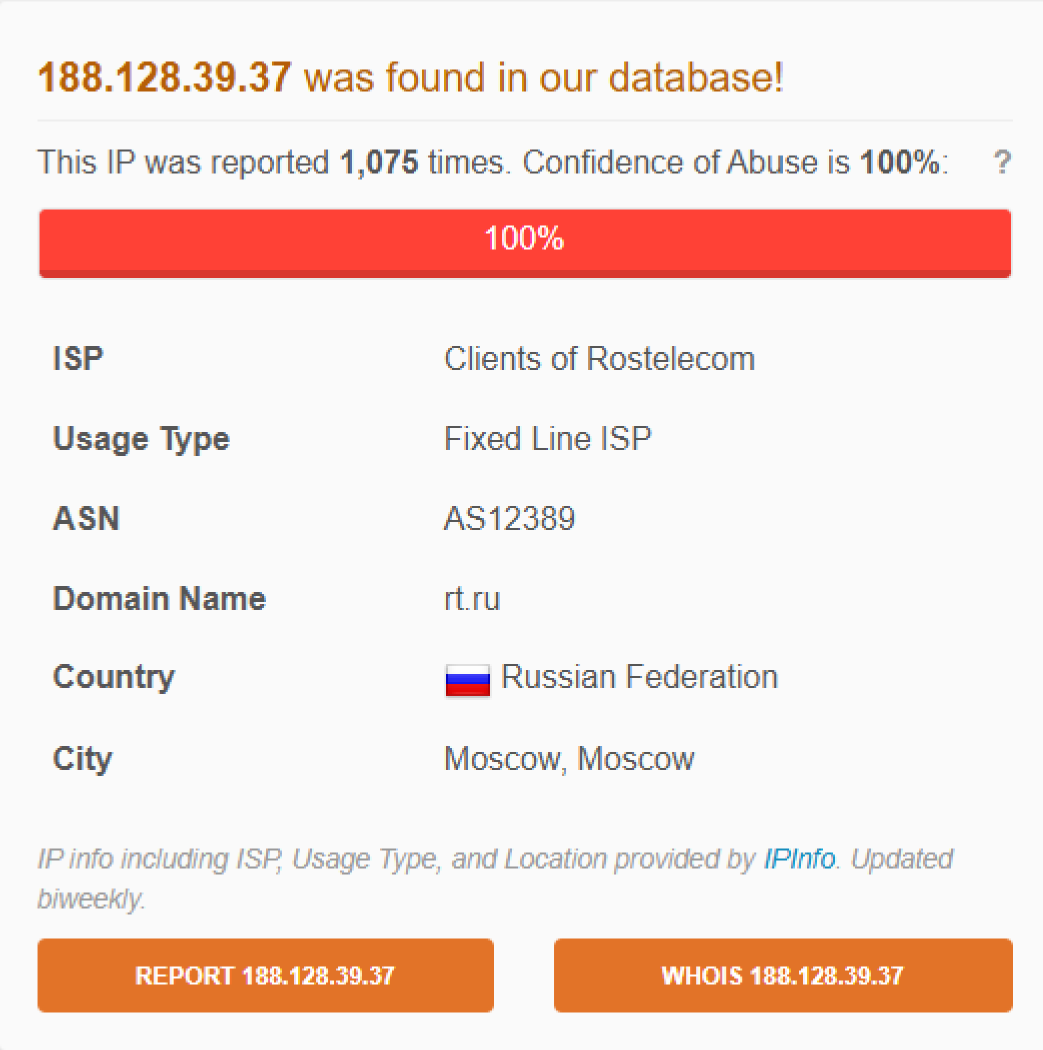
1 Raw Data:

```
<168>suricata[1541]: {"timestamp":"2025-05-04T10:07:02.255326-
0400","flow_id":1014544097237946,"in_iface":"eth0","event_type":"alert","src_ip":"188.128.39.37","src_port":46216,"d
est_ip":" [internal web server]","dest_port":80,"proto":"TCP","http":{"hostname":" [internal web server]
","url":"\/hello.world?%ADd+allow_url_include%3d1+%ADd+auto_prepend_file%3dphp:\/\/input","http_user_agent":"C
ustom-
AsyncHttpClient","http_content_type":"text\/html","http_method":"POST","protocol":"HTTP\/1.1","status":403,"length":2
79},"tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":2016977,"rev":3,"signature":"ET WEB_SERVER
allow_url_include PHP config option in uri","category":"A Network Trojan was detected","severity":1}}
```

2 Raw Data:

```
<168>suricata[1541]: {"timestamp":"2025-05-04T10:07:05.128061-0400","flow_id":1014544097237946,"in_iface":"eth0","event_type":"alert","src_ip":"188.128.39.37","src_port":46216,"dest_ip":" [internal web server]","dest_port":80,"proto":"TCP","tx_id":41,"alert":{"action":"allowed","gid":1,"signature_id":3000001,"rev":6,"signature":"ET WEB_SERVER Directory Traversal Attempt","category":"Web Application Attack","severity":1},"http":{"hostname":" [internal web server] ","url":"\/index.php?lang=..\/..\/..\/..\/..\/..\/..\/..\/tmp\/index1","http_user_agent":"Custom-AsyncHttpClient","http_content_type":"text\/html","http_method":"GET","protocol":"HTTP\/1.1","status":403,"length":279}}
```

Additional Findings:



188.128.39.37 was found in our database!

This IP was reported **1,075** times. Confidence of Abuse is **100%**: ?

100%

ISP	Clients of Rostelecom
Usage Type	Fixed Line ISP
ASN	AS12389
Domain Name	rt.ru
Country	Russian Federation
City	Moscow, Moscow

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

This IP address has been reported a total of **1,075** times from 491 distinct sources. 188.128.39.37 was first reported on April 24th 2025, and the most recent report was **3 hours ago**.

ResultAbuseIPDB: **[here|https://www.abuseipdb.com/check/188.128.39.37]**

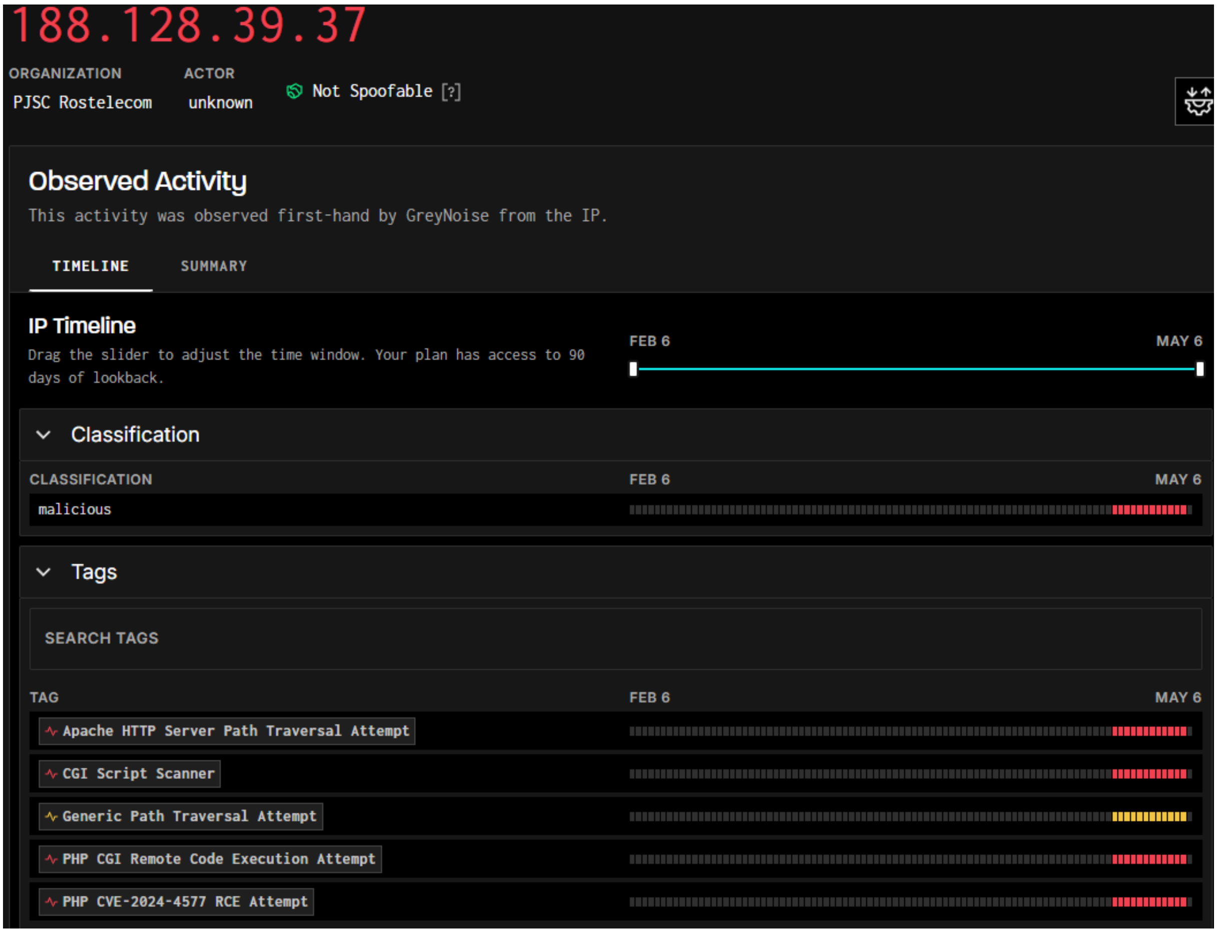
GreyNoise:

From April 24th to May 5th, hacker attacks were observed from the IP address **188.128.39.37** targeting various vulnerabilities, as detected by **GreyNoise**. The attacks include:

- **Apache HTTP Server Path Traversal Attempt**
- **CGI Script Scanner**
- **Generic Path Traversal Attempt**
- **PHP CGI Remote Code Execution Attempt**
- **PHP CVE-2024-4577 RCE Attempt**

These activities indicate aggressive attempts to exploit server vulnerabilities.

greynoise Result: **[here**↓ ↓ ↓|https://viz.greynoise.io/ip/188.128.39.37**]**



188.128.39.37

ORGANIZATION
PJSC Rostelecom

ACTOR
unknown

Not Spoofable [?]

Observed Activity

This activity was observed first-hand by GreyNoise from the IP.

IP Timeline

Drag the slider to adjust the time window. Your plan has access to 90 days of lookback.

Classification

CLASSIFICATION	FEB 6	MAY 6
malicious		

Tags

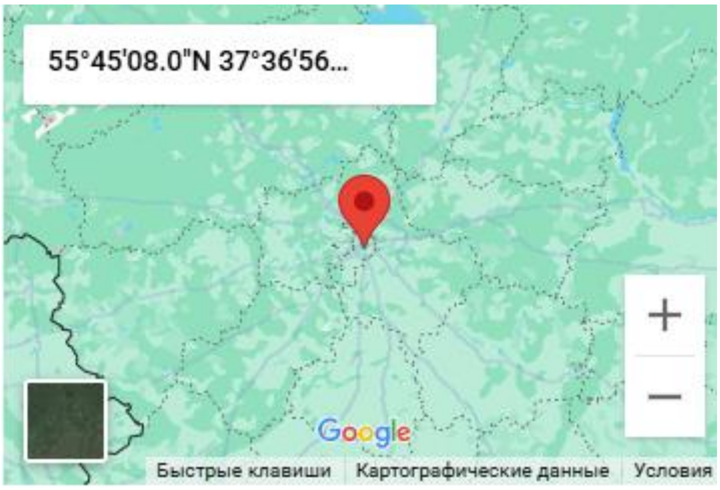
SEARCH TAGS

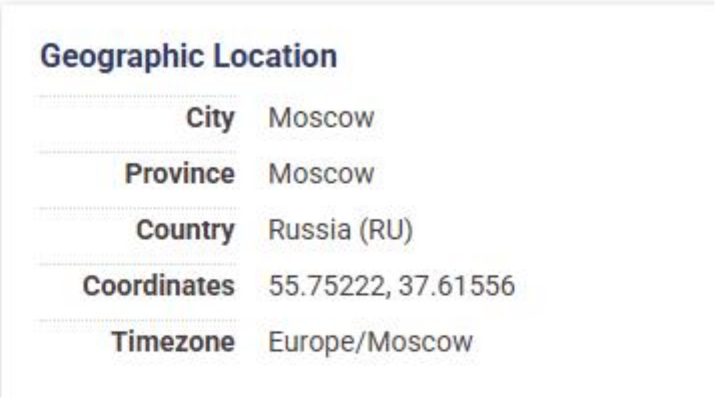
TAG	FEB 6	MAY 6
Apache HTTP Server Path Traversal Attempt		
CGI Script Scanner		
Generic Path Traversal Attempt		
PHP CGI Remote Code Execution Attempt		
PHP CVE-2024-4577 RCE Attempt		

Cencys:

Routing : 188.128.0.0/17 via ROSTELECOM-AS PJSC Rostelecom. Technical Team, RU (AS12389)

CencysResult: **[here** ↓ ↓ ↓|https://search.censys.io/hosts/188.128.39.37**]**





Geographic Location

City	Moscow
Province	Moscow
Country	Russia (RU)
Coordinates	55.75222, 37.61556
Timezone	Europe/Moscow

ANALYST ASSESSMENT

The analysis of network traffic logs reveals that the IP address **188.128.39.37** attempted two distinct web application attacks targeting a web server.

1. **Attempt 1: PHP Configuration Manipulation**
   The first attempt was identified as an attack aimed at exploiting the **allow_url_include** PHP configuration option, which could enable remote code execution. This was attempted via a **POST** request to the URL `/hello.world?%ADd+allow_url_include%3d1+%ADd+auto_prepend_file%3dphp://input` on port 80. The request was made using a custom user-agent, **Custom-AsyncHttpClient**, indicating the use of an automated tool. The attack was categorized under "A Network Trojan was detected" by the system.

2. **Attempt 2: Directory Traversal Attack**
   The second attempt was a **Directory Traversal** attack targeting the web application on the server. The attacker attempted to access files outside the intended directory using the URL `/index.php?lang=../../../../../../../../tmp/index1` via a **GET** request on port 80. This type of attack is commonly used to exploit vulnerabilities in web applications that fail to properly sanitize user inputs and restrict file access. The request was again made using the same user-agent, **Custom-AsyncHttpClient**.

Both of these attacks were detected on port 80 of the destination server ([internal web server]), and the system flagged them with a **severity level 8**. The attacker appears to be using automated tools to perform these exploits.

Attack Details:

1. PHP Configuration Manipulation Attempt

- **Request Details**:
  The attacker from IP address **188.128.39.37** made an **HTTP POST** request to the following URL:

  `/hello.world?%ADd+allow_url_include%3d1+%ADd+auto_prepend_file%3dphp://input`

- **Objective**:
  The goal of this attack was to **modify PHP configuration settings remotely**, enabling dangerous directives such as:

  - `allow_url_include=1`: Allows inclusion of remote files, opening the door for remote code execution.

  - `auto_prepend_file=php://input`: Forces PHP to execute raw input data as code before processing the script.

- **Method**: **POST** – Indicates data was sent to the server with the intent to modify configuration or execute payloads.

- **User-Agent**: **Custom-AsyncHttpClient** – Suggests an automated script/tool was used.

- **Content-Type**: `text/html` – Implies the attacker expected the server to respond in HTML format.

- **HTTP Status**: **403 Forbidden** – The request was blocked by the server, meaning the attack was unsuccessful.
- **Request Length**: **279 bytes**
- **Category**: `A Network Trojan was detected`

2. Directory Traversal Attempt

- **Request Details**:
  The same attacker (188.128.39.37) made an **HTTP GET** request to the following URL:
  `/index.php?lang=../../../../../../../../tmp/index1`
- **Objective**:
  This is a classic **directory traversal attack**, where the attacker attempts to break out of the web server's root directory by using multiple `../` sequences to access arbitrary files on the system (e.g., `/tmp/index1`).
  If successful, it could expose sensitive files or scripts and potentially lead to **remote code execution or file inclusion**.
- **Method**: **GET** – The attacker was trying to retrieve or execute an unauthorized file.
- **User-Agent**: **Custom-AsyncHttpClient** – Again indicating the use of automated tooling.
- **Content-Type**: `text/html`
- **HTTP Status**: **403 Forbidden** – The server rejected the attempt.
- **Request Length**: **279 bytes**
- **Category:** `Web Application Attack`

The goals of these attacks were:

1. /hello.world?...

Goal: Remote Code Execution (RCE)
The attacker tried to enable PHP settings to execute code sent in the request, aiming to run arbitrary commands on the server.

---

2. /index.php?...lang=../../../../../tmp/index1

Goal: Local File Inclusion (LFI) / Directory Traversal
The attacker attempted to include a file outside the web directory, possibly to access or execute malicious code.

○

Detection Context:

The attacks were detected by the following Suricata signatures:

- `ET WEB_SERVER allow_url_include PHP config option in uri` – indicating a Remote Code Execution (RCE) attempt.
- `ET WEB_SERVER Directory Traversal Attempt` – indicating an attempt to exploit a Local File Inclusion (LFI) vulnerability.

Unusual URL Access:

- The first request targeted the URL `/hello.world?%ADd+allow_url_include=1+%ADd+auto_prepend_file=php://input`, aiming to inject malicious PHP code.
- The second request accessed `/index.php?lang=../../../../../../tmp/index1`, a classic directory traversal attempt to read sensitive files.

Suspicious User Agent:
Both requests used the `Custom-AsyncHttpClient` user agent, often associated with scripted or automated attacks.

403 Forbidden Status:
The server returned a `403 Forbidden` HTTP status for both requests, meaning the attack was blocked and did not succeed.

Traffic Anomalies:
The source IP `188.128.39.37` is considered suspicious and has been flagged by threat intelligence sources such as GreyNoise for prior malicious behavior.

Impact if Successful:

1.Remote Code Execution (RCE): If the `allow_url_include` and `auto_prepend_file` parameters had been accepted, the attacker could have executed arbitrary PHP code on the server, potentially taking full control.

Sensitive File Access: The directory traversal attempt could have allowed the attacker to access critical files outside the web root (e.g., configuration files, credentials).

Server Compromise: Successful exploitation could lead to backdoor installation, data exfiltration, or use of the server in further attacks.

Privilege Escalation: Gaining execution capability or reading system files could be leveraged to escalate privileges within the environment.

Mini Attack Visualization:

[QRadar Alert ID 54773 — ET WEB_SERVER allow_url_include / Directory Traversal]

↓

[Analyst pivots into logs — source IP 188.128.39.37]

↓

[Baseline traffic from IP: 565 events (time range/search scope)]

↓

[Filtered by target URIs → hits: 69 events total]

- /hello.world?%ADd+allow_url_include%3d1+%ADd+auto_prepend_file%3dphp://input → 17 matched events
- /index.php?lang=../../../../../../../tmp/index1 → 52 matched events

↓

[Suricata raw alerts (attached): 2 SIDs mapped to these matches]

- SID 2016977 — "ET WEB_SERVER allow_url_include PHP config option in uri"
- SID 3000001 — "ET WEB_SERVER Directory Traversal Attempt"

↓

[Payloads decoded + extracted → deduplicated → unique payload examples]

- `-d allow_url_include=1 -d auto_prepend_file=php://input` (attempt to force PHP to execute request body)
- `lang=../../../../../../../../tmp/index1` (classic directory traversal / LFI)

↓

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

↓

[Observed payload intent / types]

- PHP configuration manipulation → attempt to enable remote include / execute `php://input` (RCE vector)
- Directory traversal / LFI → attempt to include/read files outside webroot

↓

[User-Agent: "Custom-AsyncHttpClient" — consistent across requests (likely scripted)]

↓

[Source behavior: multiple ephemeral source ports observed (single TCP sessions), automated tooling characteristics — repeated probing, patterning]

↓

[Detection / Response]

- HTTP Response: 403 Forbidden for observed requests (blocked)
- Alerts: Suricata + QRadar correlated (QRadar ID 54773)
- Splunk: 565 total logs; filtered counts as above (17 + 52)

↓

[Threat Intelligence & Reputation]

- VirusTotal: multiple community reports; 10/94 vendors flagged as malicious
- GreyNoise: observed scanning / PHP exploit activity
- Talos: poor / questionable reputation; listed in blocklists (CBL.abuseat.org)
- AbuseIPDB: numerous reports (1,075 reports / 491 sources in dataset)

↓

[Conclusion / Immediate Recommendations]

- Conclusion: Automated exploit attempts observed combining PHP config abuse (allow_url_include / auto_prepend_file) and directory traversal (LFI). All attempts returned 403 — no confirmed code execution, but high risk if protections fail.
- Immediate actions: block source IP (188.128.39.37), create WAF rule for the specific payload patterns, review PHP configuration (ensure `allow_url_include = Off`,

`auto_prepend_file` not user-controllable), and add Splunk saved search + alert for similar payloads.

- Forensics: collect webserver access & error logs for timestamps of matched events, search for any successful 200 responses to similar patterns, hunt for webshells or unexpected files in `/tmp` and webroot, consider host isolation if suspicious artifacts found.

ACTION

1. **Block the Attacker's IP (188.128.39.37)**
   Immediately block the IP address 188.128.39.37 to prevent further exploitation attempts.

2. **Review and Secure PHP Configuration**
   The attacker attempted to exploit PHP configuration settings (`allow_url_include` and `auto_prepend_file`) via the `/hello.world` URL. Ensure these settings are disabled in the PHP configuration to prevent Remote Code Execution (RCE) vulnerabilities.
3. **Prevent Directory Traversal:**
   Sanitize all user inputs to prevent directory traversal, especially on URLs like `/index.php`.

4. **Monitor Suspicious User-Agent:**
   Block or flag requests with the user-agent `Custom-AsyncHttpClient` and monitor for similar automated attack attempts.

5. **Check Logs and Alerts:**
   Investigate logs for more suspicious activity from the same IP or similar attack methods.

6. **Update and Patch Systems:**
   Ensure the server and PHP are updated with the latest security patches.

7. **Improve Access Control:**
   Tighten access controls and set up alerts for suspicious access attempts.