Vulnerability Report

Title: Blind SSRF Leading to Internal IP Disclosure via DNS-based Interaction
Severity: High – Server-Side Request Forgery (Blind SSRF)
CWE-ID: CWE-918 – Server-Side Request Forgery (SSRF)
CWE-ID (Secondary): CWE-200 – Exposure of Sensitive Information to an Unauthorized Actor

Summary:

A **Blind Server-Side Request Forgery (SSRF)** vulnerability was identified on [Target Site]. By injecting a crafted payload containing an external domain controlled by the researcher, the backend server initiated a DNS request to the supplied address. This resulted in an outbound DNS interaction captured on Burp Collaborator, which revealed an internal IP address and port: `185.31.40.97:28861`.

This confirms that the application processes or forwards attacker-supplied URLs internally, without proper sanitization or restriction. The vulnerability allows an attacker to force the server to make arbitrary network requests, which can be used to interact with internal services not exposed publicly.

Technical Details:

- **Vulnerability Type:** Blind SSRF via DNS interaction
- **Payload Used:** `http://<your-collaborator-id>.burpcollaborator.net`
- **Server Behavior:** The target system issued a DNS request to the supplied domain, indicating that the input was processed on the backend
- **Collaborator Interaction:** The DNS log captured:
- ```
  Source IP: 185.31.40.97
  Port: 28861
  ```

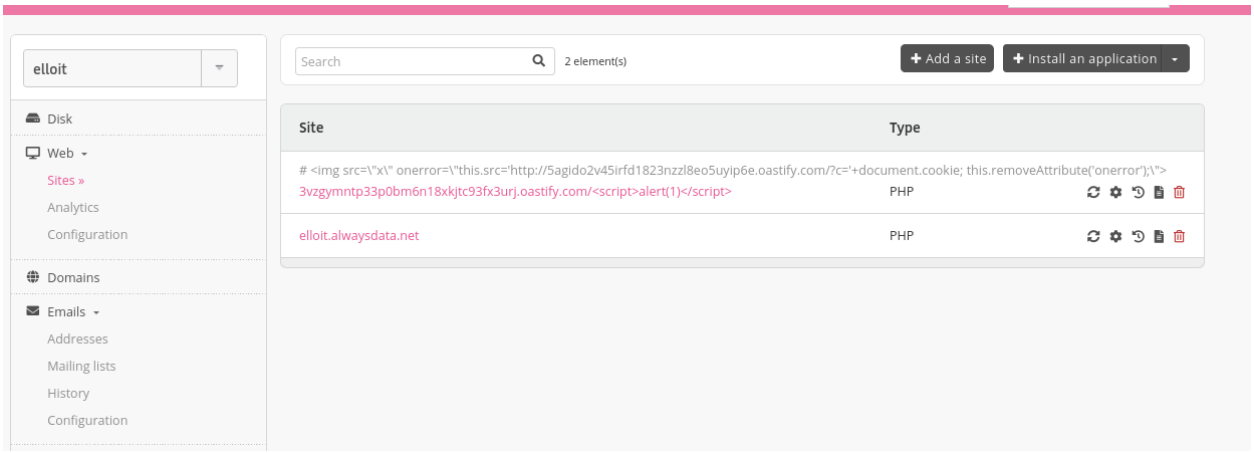
- **Tool Used:** Burp Suite Collaborator
- **Endpoint Affected:** [https://admin.alwaysdata.com/site/]
  ```

Impact:

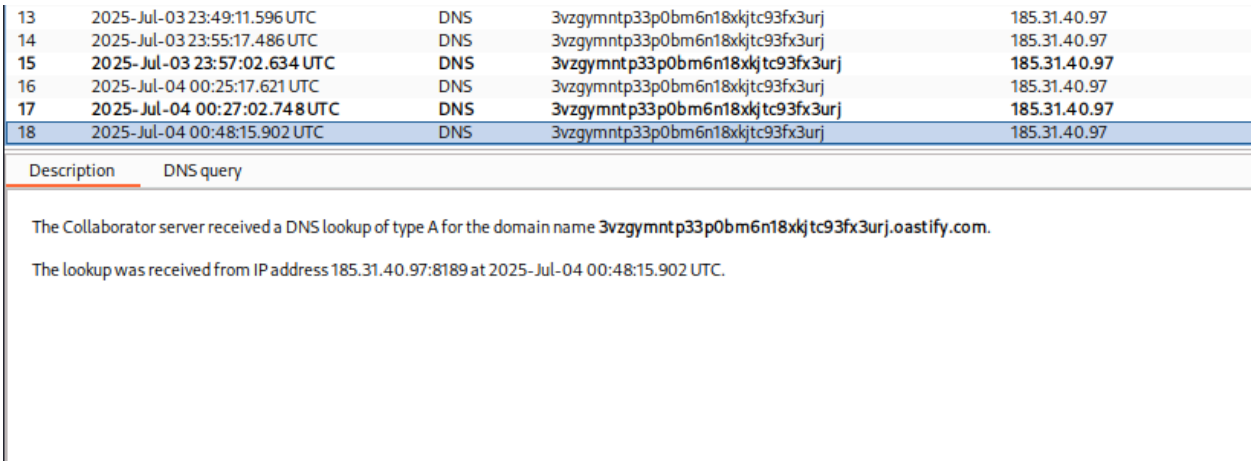
- **Internal Network Exposure:** The internal IP (`185.31.40.97`) indicates backend network information is leaked.
- **Pivot Opportunities:** Attackers may use SSRF to access internal systems/services (e.g., metadata endpoints, admin panels).
- **Enumeration:** Can lead to mapping of internal infrastructure.
- **Further Exploitation:** Depending on server responses, this may be escalated to full SSRF or even RCE depending on exposed internal services.

Steps to Reproduce:

1. Interact with the vulnerable endpoint and inject a payload containing a Burp Collaborator subdomain:



2. Monitor the Collaborator for DNS/HTTP interactions.
3. Observe DNS query resolving with an internal IP in the interaction log:



13	2025-Jul-03 23:49:11.596 UTC	DNS	3vzgymntp33p0bm6n18xkjtc93fx3urj	185.31.40.97
14	2025-Jul-03 23:55:17.486 UTC	DNS	3vzgymntp33p0bm6n18xkjtc93fx3urj	185.31.40.97
15	**2025-Jul-03 23:57:02.634 UTC**	**DNS**	**3vzgymntp33p0bm6n18xkjtc93fx3urj**	**185.31.40.97**
16	2025-Jul-04 00:25:17.621 UTC	DNS	3vzgymntp33p0bm6n18xkjtc93fx3urj	185.31.40.97
17	**2025-Jul-04 00:27:02.748 UTC**	**DNS**	**3vzgymntp33p0bm6n18xkjtc93fx3urj**	**185.31.40.97**
18	2025-Jul-04 00:48:15.902 UTC	DNS	3vzgymntp33p0bm6n18xkjtc93fx3urj	185.31.40.97


```
Source: 185.31.40.97
Port: 28861
```

4. Confirm this is not part of standard application behavior.

Recommendation:

- Validate and sanitize all user-controlled input, especially URLs.
- Use an allowlist for outbound requests from the server.
- Disable direct server access to internal or sensitive resources unless absolutely necessary.
- Log and monitor all outbound network requests to detect anomalies.
- Implement SSRF protection libraries or built-in controls at the framework level.