Vulnerability Report: Open Redirect on Nojoto Website

1. Executive Summary:

Vulnerability Type: Open Redirect

Severity: Medium

Reported by: [Your Name]

Date Reported: [Date]

2. Vulnerability Details:

An Open Redirect vulnerability has been identified on the Nojoto website (https://nojoto.com). The vulnerability allows an attacker to craft malicious URLs that, when accessed, can redirect users to external websites. This report provides details of the identified Open Redirect vulnerability and its potential impact.

3. Affected URL and Parameter:

- Affected URL: https://nojoto.com/under-maintenance.php

- Parameter: return

4. Description:

The Open Redirect vulnerability arises from the improper validation of the "return" parameter within the URL. An attacker can craft a malicious link with a manipulated "return" parameter that redirects the user to an external website. This could potentially be abused for phishing attacks or to trick users into visiting malicious content.

5. Proof of Concept (PoC):

Actual link: https://nojoto.com/under-maintenance.php?return=https://nojoto.com/nojoto-for-creator.php

An example of a crafted link exploiting the vulnerability:

https://nojoto.com/under-maintenance.php?return=https://upload.wikimedia.org/wikipedia/commons/b/bc/Alan_Walker_%28cropped%29.jpg
```

In this example, I replaced the original return URL with an arbitrary external URL.
```

6. Impact:

- The potential for phishing attacks by redirecting users to malicious sites.

- Increased risk of users being tricked into accessing harmful content.

7. Recommendations:

- Implement proper input validation and filtering for user-supplied parameters, especially those involved in redirection.

- Use a whitelist approach to allow only specific, trusted domains for redirection.

- Regularly monitor and log security events related to URL redirection.

8 Acknowledgment:

I would like to acknowledge the prompt response and collaboration of the Nojoto website administrators in addressing this security vulnerability.

9. Legal Disclaimer:

This report is submitted in good faith for the purpose of responsible disclosure. The information provided is accurate to the best of my knowledge at the time of reporting.

10. Contact Information:

Binay Kumar Dubey
binaydubey08@gmail.com

Thank you for your attention to this matter. I look forward to your prompt response and the resolution of this vulnerability.

Sincerely,

Binay Kumar Dubey