Hi,
I am a security researcher and I founded this vulnerability in your website.

Vulnerability : Content Spoofing

I Found a SubDomain which is Vulnerable to Plain text Content Spoofing.

Poc:
https://www.afternic.com///We%20are%20moved%20to%20URL:%20www.evil.com%2f
Steps to reproduce:
1: Just browse this target on any browser
2: Target: https://www.afternic.com/
3: add any content after For example: this is not available anymore pls check WWW.EVIL.COM because this site
4: Now browser reflect the content or text .

Fix :
Use Predefined 404 page , with fixed error content
It can be fixed by adding the following to the web server config:
ErrorDocument 404 "File not found."

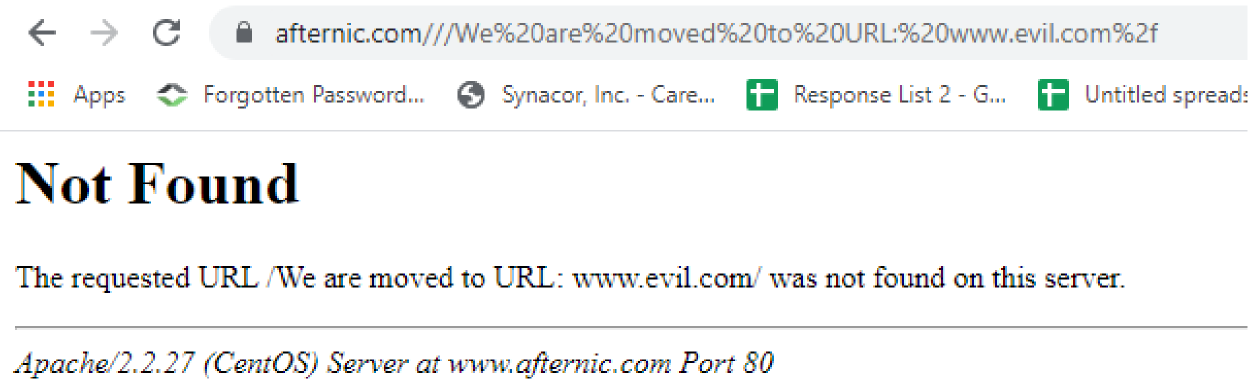
Impact
Application allows users to inject any text content on the 404 not found webpage.

References:
https://www.owasp.org/index.php/Content_Spoofing

Note :
I am also attaching a screen shot as proof of concept.

Waiting for your response.

Regards,
Iqtidar hadi



afternic.com///We%20are%20moved%20to%20URL:%20www.evil.com%2f

Not Found

The requested URL /We are moved to URL: www.evil.com/ was not found on this server.

Apache/2.2.27 (CentOS) Server at www.afternic.com Port 80