E-Arogya - Feature #265

Feature # 235 (New): [Security Audit Round 2]

[Security Audit Round 2] Host Header Injection

01/05/2024 01:02 PM - Kalyan Battula

Status:	Resolved	**Start date:**	01/05/2024
Priority:	High	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0:00 hour
Target version:	Security Audit	**Spent time:**	0:00 hour
Deployed In:		**Category:**	

Description

Host Header Injection
observation : New
CWE : CWE-20
Description :
A web server commonly hosts several web applications on the same IP address, referring to each application via the virtual host. In an incoming HTTP request, web servers often dispatch the request to the target virtual host based on the value supplied in the Host header. Without proper validation of the header value, the attacker can supply invalid input to cause the web server to:
Dispatch requests to the first virtual host on the list.
Perform a redirect to an attacker-controlled domain.
Perform web cache poisoning.
Manipulate password reset functionality.
Allow access to virtual hosts that were not intended to be externally accessible.
Affected Path(s) :
/(WebServer)
Impact :
Possible attacks like Cache poisoining, Password reset functionality abuse, redirection, etc.
Evidence/Proof Of Concept :
Step 1: Access any path in the application and change the host header to a third party malicious site. It was observed that the application was getting re-directed to the attacker injected host there making the application vulnerable to host header injection.
clipboard-202405011302-2xltc.png

Recommendation :
The web application should use the SERVER_NAME instead of the Host header. It should also create a dummy vhost that catches all requests with unrecognized Host headers. This can also be done under Nginx by specifying a non-wildcard SERVER_NAME, and under Apache by using a non-wildcard serverName and turning the UseCanonicalName directive on. Consult references for detailed information.

History

#1 - 03/05/2024 05:27 AM - Sivakanth Kesiraju

- Target version set to Security Audit

#2 - 10/05/2024 07:18 AM - Harish Beechani

- Status changed from New to Resolved

Files

clipboard-202405011302-2xltc.png	67.4 KB	01/05/2024	Kalyan Battula