Status of Vulnerable Points Discovered

during CERTIN for SCEA, Pune as on 5th Feb 2024

Ser	Issue Details	Resolved Rounds				Remarks
		Level	1st	2nd	3	
1	Error Based SQL Injection	High	YES	YES		**Completed**
2	Cross Site Scripting	High	No	YES		**Completed**
3	HTML Injection	High	No	YES		**Completed**
4	Iframe Injection	High	No	YES		**Completed**
5	Authentication Bypass	High	No	No		Fixed
6	Session Fixation	High	No	No		Fixed
7	Improper Input Validation	Medium	No	No		CSP Implemented
8	HTTP OPTIONS Methods Allowed	Medium	No	No		Method Stopped CORS Applied
9	Content Security Policy Bypass	Medium	YES	YES		**Completed**
10	Server Leaks Information via "X-Asp Net- Version" & "Server" Header	Medium	No	No		Server Sealed
11	Missing X-Frame-Options Header	Medium	YES	YES		**Completed**
12	Insecure Transport Layer Security Protocol version 1.0 supported	Low	No	No		Added 1.3
13	HTTP Strict Transport Security Header Not Set	Low	YES	YES		**Completed**
14	Missing X-Content-Type-Options Header	Low	YES	YES		**Completed**
15	Improper Cache Control Header Set	Low	No	No		Set No Cache
16	Cookie without Secure flag	Low	No	No		Removed Cookie
17	Cookie without Same Site Attribute	Low	No	No		Removed Cookie
18	Unrestricted Upload of File with Dangerous Type	Medium	No	No		Allow pdf /Images only
19	Vulnerable and Outdated Components	Medium	No	YES		**Completed**
20	Clear text Transmission of Sensitive Information	Medium	No	No		Encrypted Now