PRAETORIAN

FaceTec Web Browser SDK Security Assessment

OWASP ASVS Level 1: Opportunistic

Praetorian benchmarked the security posture of FaceTec's Web Browser SDK against OWASP Application Security Verification Standard (ASVS) Level 1: Opportunistic.

Product Security Evaluation Performed by Independent Experts

This document confirms the results of the recent security evaluation undertaken by FaceTec and performed by Praetorian. Between the dates of January 27, 2020 and February 5, 2020, Praetorian benchmarked the security posture of FaceTec's Web Browser SDK via its Spoof Bounty Page against OWASP Application Security Verification Standard (ASVS) Level 1: Opportunistic. During the assessment, Praetorian identified **0** critical risk issues, **0** high risk issue, **0** medium risk issues, **0** low risk issues, and **0** informational issues. One additional high risk issue was identified. This issue was verified to be mitigated in the latest version of the Spoof Bounty Page.

As FaceTec's Web Browser SDK's code bases continues to change, so too will their overall security posture. Such changes will affect the validity of Praetorian's findings and this letter. Therefore, any statements made by Praetorian only describe a "snapshot" in time. Praetorian would like to thank FaceTec for this opportunity to help the organization evaluate its current security posture.

facetec

Cole Hecht
Practice Manager, Praetorian
cole.hecht@praetorian.com
(214) 901-9031 Phone

Issued date
FEBRUARY 21, 2020

Guided by OWASP Application Security Verification Standard (ASVS)

|