Tesi - Payment Request API

Daniele Rigon - 857319

3 agosto 2018

Indice

1 SEZIONE PHISHING GENERALE **2**

2 Come difendersi **2**

1 SEZIONE PHISHING GENERALE

Con un attacco XSS, alla chiamata dell'API, invece di questa finestra potrebbe venirne aperta un'altra uguale a quella originale, gestita però dall'attaccante. Essendo identica la vittima sarà convinta di inserire le credenziali in un posto sicuro, mentre invece saranno inviate all'attaccante invece di essere salvate nel browser tramite l'API.

2 Come difendersi

Vi sono diverse metodologie per difendersi da questi tipi di attacchi:

- Una strategia per combattere il phishing è sicuramente quella di istruire le persone a riconoscere gli attacchi e ad affrontarli;
- Dato che il piu delle volte non e facile riconoscere questi attacchi, ci sono anche delle misure anti-phishing implementate nei browsers, come estensioni o toolbar, oltre a diversi software contro il phishing;
- Inoltre, la maggior parte dei siti bersaglio del phishing sono protetti da SSL con una forte crittografia, dove l'URL del sito web è usata come identificativo. Questo dovrebbe in teoria confermare l'autenticità del sito, ma nella pratica è facile da aggirare, sfruttando la vurnerabilita che sta nella user interface (UI) del browser. Nell'url del browser viene poi indicata la connessione utilizzara con diversi colori (blocco verde per certificato EV, scritta https in verde, ecc.).