Università degli Studi di Padova

Corso di Laurea in Informatica

Log #3

Azienda:
KIREY Srl

Soranzo Mendez Andrea Jesus
2075539

Indice

Giorno 1 ..... **2**

Giorno 2 ..... **2**

Giorno 3 ..... **3**

Giorno 4 ..... **3**

Giorno 1

Ordine del giorno:

- Studio del pacchetto **IP Inteligence**: **https://github.com/lukaszknysak/F5-Advanced-Web-Application-Firewall**.
- Selezione di una web app con vulnerabilità note per la configurazione e la validazione del WAF di progetto.

Note:

La ricerca ha individuato le seguenti possibili applicazioni web:

- **bWAPP**
- **BadStore**
- **XVWA - Extreme Vulnerable Web Application**

Giorno 2

Ordine del giorno:

- Reperimento screenshot ed informazioni utili per la tesi
- Call con F5
- Decisione della web app per il progetto

Note:

La nostra call con l'esperto F5 ha risolto con successo alcune domande sulle attack signature e i parameters in modalità enforced. Abbiamo concluso la giornata decidendo per **NodeGoat** come web app vulnerabile per il nostro progetto. Abbiamo anche concordato che, se dovessimo completare le consegne del progetto prima del termine previsto per lo stage, affronteremo la sfida di mettere in sicurezza un'applicazione ancora più complessa. Il progetto consiste del creare una policy che rispetti e mitighi le OWASP Top 10.

Giorno 3

Ordine del giorno

- Prima versione del diagramma dei casi d'uso
- Disegno di rete (semplificato)
- Inizio progetto

Note:

È stata completata la configurazione iniziale e di base per successivamente procedere con l'aggiunta delle regole specifiche per la web app al fine di raggiungere l'obiettivo finale del progetto.

Giorno 4

Ordine del giorno

- Disegno di rete (nel dettaglio)
- Protezione A1,A3 OWASP implementate

Note:

Abbiamo raggiunto il 100% di compliance per le vulnerabilità OWASP A1 e A3. Questo risultato è stato ottenuto grazie all'integrazione di attack signature contro gli attacchi più comuni e rischiosi, alla protezione delle pagine che richiedono autenticazione, e alla definizione di regole precise per i parametri nelle richieste HTTP.