Università degli Studi di Padova

Corso di Laurea in Informatica

Log #4

Azienda:
KIREY Srl

Soranzo Mendez Andrea Jesus
2075539

Indice

Giorno 1

Ordine del giorno:

- Redazione capitolo riguardante l'**Azienda** per la tesi
- Compliance A10 implementata

Note:

La prima parte della giornata è stata impiegata nella redazione della descrizione dell'azienda e nell'analisi del progetto a noi affidato. Successivamente, ho provveduto all'implementazione delle misure di sicurezza per garantire la conformità OWASP A10, configurando i parametri URI su F5 per il rilevamento proattivo degli attacchi SSRF. La giornata si è conclusa con l'analisi della gestione dello userID dinamico e della vulnerabilità IDOR (A4).

Giorno 2

Ordine del giorno:

- Compliance A2,A5,A6 implementata

Note:

Sono riuscito a configurare un server virtuale e a modificare la web application per utilizzare il protocollo HTTPS anziché HTTP. Ciò ha permesso di soddisfare pienamente la compliance A2, che richiede la comunicazione client-server criptata (TLS/SSL). Per le compliance A5 e A6, è stato sufficiente approvare manualmente i requisiti, poiché queste sono attività di competenza del responsabile della sicurezza e dell'implementazione della web application, come l'aggiornamento delle tecnologie e il monitoraggio delle potenziali vulnerabilità.

Giorno 3

Ordine del giorno:

- Compliance A4 implementata
- Installazione di f5-waf-tester
- Troubleshooting IDOR

Note:

Abbiamo implementato manualmente la compliance A4, poiché alcuni requisiti riguardano accorgimenti specifici del team di sviluppatori e non competono all'amministratore del WAF. La maggior parte della giornata è stata dedicata al tentativo di implementare una regola per prevenire un attacco di tipo IDOR (Insecure Direct Object References) nell'ambiente WAF. Non siamo ancora riusciti a implementarla e riteniamo che ciò non sia possibile a causa della struttura attuale della web app, che non lo consente.

Giorno 4

Ordine del giorno:

- Compliance A8,A9 implementata
- Mitigazione attacchi CSRF

Note:

Per quanto riguarda la conformità A8, sono state apportate modifiche manuali per soddisfare requisiti specifici che esulano dalle procedure operative standard. Relativamente al logging A9, è stata presa una decisione strategica per ottimizzare le prestazioni e l'analisi del firewall. Ora, solo i log delle attività sospette o illegali vengono archiviati direttamente sul firewall. Tutti gli altri dati di log vengono reindirizzati a un server esterno dedicato. Ciò garantisce che la memoria del firewall sia utilizzata principalmente per richieste critiche e sospette, le quali sono anche le uniche che possono essere direttamente associate ai suggerimenti di apprendimento visibili tramite GUI del firewall. La giornata si è conclusa con la riuscita attivazione del modulo F5 per la mitigazione degli attacchi CSRF.