|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Decorativa | | | | |
|  |  |  | |  |
| Report sulla Violazione della Sicurezza  DATA :04/11/2023 | | |
| EPICODE.INTERNAL | |  |

In data 03/11/2023, nell'azienda epicode.internal è stato effettuato un controllo delle vulnerabilità . L'attaccante(pen tester) ha utilizzato una combinazione di SQL injection, il tool John the Ripper e un attacco XSS stored per ottenere credenziali utente, password e catturare cookie di sessione.

Questo report offre un'analisi dettagliata dell'attacco, dei danni

subiti e delle azioni intraprese per mitigare il problema.

**Dettagli dell'Attacco:**

**Tipo di Attacco:** SQL Injection per fornire credenziali seguito da un attacco a dizionario sulle password in hash con John the Ripper. Inoltre, un attacco XSS stored è stato utilizzato per catturare cookie di sessione.

**Data di Rilevamento:** Roma 03/11/2023 epicode.internal

**Descrizione dell'Attacco:** L'attaccante è riuscito a iniettare query SQL malevole in un'applicazione web vulnerabile, ottenendo l'accesso non autorizzato al database. Successivamente, ha utilizzato il tool John the Ripper per decifrare le password degli utenti. In parallelo, è stato eseguito un attacco XSS stored che ha catturato cookie di sessione degli utenti e li ha inviati a un server Python creato dall'attaccante.

## Danni e Impatti:

**Accesso non Autorizzato:** L'attaccante ha ottenuto l'accesso a informazioni sensibili e dati dell'azienda.

**Compromissione delle Credenziali:** Le credenziali utente e le password sono state compromesse.

**Violazione della Privacy:** I cookie di sessione catturati possono essere utilizzati per impersonare gli utenti e accedere alle loro sessioni.

**Potenziale Perdita di Dati:** Potenziale per la perdita di dati sensibili e riservati.

**Rischi per la Reputazione:** Il compromesso delle credenziali e la violazione della privacy degli utenti potrebbero influire negativamente sulla reputazione dell'azienda.

**Analisi della Sicurezza:**

**Vulnerabilità Riscontrate:** L'attacco è stato possibile a causa di vulnerabilità sia nel sistema di gestione delle query SQL dell'applicazione web che nella gestione dei cookie di sessione.

**Azioni di Sicurezza Precedenti:** Descrizione delle misure di sicurezza in atto prima dell'attacco.

**Raccomandazioni di Sicurezza:** Proposte di miglioramento delle misure di sicurezza, inclusi aggiornamenti del sistema, formazione del personale e miglioramento delle procedure di gestione dei cookie di sessione.

Conclusioni:

È necessario implementare misure di sicurezza robuste sul database SQL, poiché attualmente è vulnerabile alle injection. Inoltre, è essenziale impedire a individui malevoli di modificare il codice HTML del font per evitare che aggiungano script nella casella di testo.

**Cosa Fare:**

È fondamentale reclutare programmatori esperti per identificare e correggere le vulnerabilità legate alle SQL injection e XSS per implementare misure che limitino l'inserimento di script dannosi nelle pagine web dell'azienda.

Questo può includere l'applicazione di restrizioni sui caratteri consentiti per prevenire l'inserimento di script malevoli e il controllo per impedire la modifica del codice HTML del font, al fine di proteggere l'integrità delle pagine web contro eventuali manipolazioni non autorizzate.

"È essenziale promuovere la formazione e la consapevolezza tra il personale aziendale. Garantire che tutti, compresi gli sviluppatori e il personale, acquisiscano conoscenze approfondite riguardo ai rischi legati agli attacchi XSS e alla corretta attuazione delle pratiche di sicurezza."

.

.

## A CURA DI:

### GABRIELE TORTORA

|  |
| --- |
|  |