Discoverability	Occorre identificare un url che restituisca in output, senza aver subito alcun encoding, un input utente malevolo, precedentemente persistito sul database senza alcuna bonifica.	1

DREAD Score: 10/15 (MEDIO)

7.5.3 Controllo accesso debole per una risorsa

Categoria: Information Disclosure

Descrizione: Una inadeguata protezione dei dati a livello di " SQL Database" può consentire a un attaccante di leggere informazioni non destinate alla divulgazione. Esaminare le impostazioni di autorizzazione.

Contromisure:

- Autenticare tutti gli utenti.
- Mettere in pratica un efficace meccanismo di controllo degli accessi che garantisca che i dati possono essere letti solo da utenti autorizzati.
- Rispettare il principio del minimo privilegio.
- Attuare controlli che seguano correttamente e registrino le azioni degli utenti
- Crittografare i dati.
- Assicurarsi che le utilità o le tecniche di riservatezza dei data store vengano appropriatamente utilizzate in modo che la riservatezza dei dati sia mantenuta e gestita in base alle esigenze aziendali/regole.

Valutazione della priorità della minaccia (Ranking)

DREAD	Descrizione	Score
Damage Potential	La possibilità, senza averne diritto, di leggere i dati all'interno del database dell'applicazione espone potenzialmente l'owner del sistema a violazioni di normative di legge (es. Privacy) o a danno reputazionale o a divulgazione di informazioni di business riservate.	2
Reproducibility	L'attacco può essere condotto in qualunque momento.	3
Exploitability	Per la natura del servizio, l'attacco richiede un'utenza autenticata.	2
Affected Users	100%.	3
Discoverability	Occorre identificare un exploit, attraverso la manomissione dei dati di input, cui il Web Server risulta vulnerabile.	1

DREAD Score: 11/15 (MEDIO)