

Esercizio S5L2

Analisi OSINT della Sicurezza delle Informazioni sul Sito Web dell'Accademia di Belle Arti di Macerata

Obiettivo della ricerca

Questa ricerca OSINT (Open Source Intelligence) mira a identificare e analizzare le esposizioni di dati sensibili attraverso il sito web dell'Accademia di Belle Arti di Macerata, valutando il rispetto delle normative sulla privacy e sicurezza informatica.

Metodologia utilizzata

Per condurre questa analisi sono state impiegate tecniche di Google Hacking, in particolare gli operatori di ricerca site:, inurl:, e l'uso combinato degli operatori booleani per affinare la ricerca di informazioni pubblicamente accessibili ma sensibili.

Metodologia

Dettagli delle Query Utilizzate

Query 1: site:abamc.it inurl:curriculum vitae

Obiettivo: Identificare i curriculum vitae dei professori.

Query 2: site:abamc.it + "codice fiscale" + "email" + pdf

Obiettivo: Cercare pagine che contengono codici fiscali ed e-mail dei professori.

Maltego: Utilizzato per scoprire ulteriori DNS e sottodomini non rilevabili tramite ricerca Google diretta. Un esempio specifico è stato il DNS relativo alle timbrature del personale, un punto di dati potenzialmente sensibile.

Risultati Attesi e Realizzati

Si prevedeva di scoprire informazioni generalmente pubbliche, quali biografie o pubblicazioni accademiche. Inaspettatamente, sono stati trovati dati altamente sensibili, inclusi dettagli personali e finanziari.

Risultati

Descrizione dei Dati Trovati

Dati da google hacking: Il sito ha esposto dettagli sensibili come codici fiscali, e-mail, indirizzi di residenza e informazioni sui pagamenti e sulle mansioni dei professori, questi dati erano accessibili senza alcuna forma di autenticazione o protezione.

Dati da Maltego: Identificazione di sottodomini come quello delle timbrature del personale, dove si possono registrare orari e altre informazioni sensibili dei dipendenti.

Implicazioni di Sicurezza

L'esposizione di tali informazioni mette a rischio la privacy degli individui coinvolti e potrebbe portare a violazioni di dati, frodi, o altri attacchi informatici.

L'analisi quindi ha evidenziato una significativa esposizione di dati sensibili attraverso il sito web dell'accademia, che non solo viola le normative sulla privacy ma espone anche l'istituzione a rischi legali e di sicurezza.