**Report: Analisi di Sicurezza e Test di Penetrazione su un'Applicazione Web**

**1. Introduzione**

In questo report, documenteremo l'analisi di sicurezza condotta su un'applicazione web vulnerabile utilizzando strumenti di penetration testing come Kali Linux e Burp Suite. L'obiettivo del test è stato identificare e sfruttare vulnerabilità comuni in un ambiente controllato per migliorare le pratiche di sicurezza.

**2. Preparazione dell'Ambiente di Test**

Prima di iniziare i test, è stato configurato un ambiente di test locale utilizzando Damn Vulnerable Web Application (DVWA).

* **Installazione e Configurazione di DVWA**: Abbiamo clonato il repository DVWA da GitHub e configurato l'applicazione sulla macchina Kali Linux. Sono stati impostati i permessi delle directory e modificati i file di configurazione necessari per collegarsi al database MySQL locale.
* A screenshot of a computer program

  Description automatically generated
* **Configurazione del Database**: Utilizzando il comando service mysql start, il servizio MySQL è stato avviato. È stato creato un utente di database specifico e assegnati i privilegi necessari.
  + A screenshot of a computer

    Description automatically generated
* **Configurazione del Server Web Apache**: Utilizzato il comando service apache2 start per avviare il servizio Apache. Abbiamo modificato il file php.ini nella directory Apache2 per abilitare le opzioni allow\_url\_fopen e allow\_url\_include.
  + A screenshot of a computer program

    Description automatically generated

**3. Test di Penetrazione con Burp Suite**

Dopo aver configurato l'ambiente, è stato utilizzato Burp Suite per condurre i test di penetrazione sull'applicazione DVWA.

* **Intercettazione e Modifica delle Richieste HTTP**: Abbiamo utilizzato Burp Suite per intercettare le richieste di login all'applicazione. Sono stati modificati i parametri di login per testare la risposta dell'applicazione a credenziali errate o manipolate.
  + A screenshot of a computer

    Description automatically generated
* **Sfruttamento delle Vulnerabilità Identificate**: Dopo aver modificato i campi delle richieste HTTP, sono state inviate ripetutamente utilizzando la funzione "Repeater" di Burp Suite per osservare come l'applicazione gestisce diverse tipologie di input.
  + A screenshot of a computer

    Description automatically generated
* **Analisi dei Risultati**: Le risposte HTTP ottenute hanno indicato che l'applicazione era vulnerabile a diverse tipologie di attacchi, tra cui SQL Injection e Cross-Site Scripting (XSS).
  + A screenshot of a computer

    Description automatically generated

**4. Conclusione**

Il test di penetrazione ha dimostrato l'importanza della sicurezza delle applicazioni web e ha fornito preziose informazioni su come queste possono essere vulnerabili a vari tipi di attacchi. La pratica e l'uso di strumenti come Burp Suite sono essenziali per identificare e mitigare tali rischi in modo efficace.