|  |  |
| --- | --- |
| WEB APP HACKING | |
| 04/11/2023Cyber Security &  Ethical Hacking | Ivan Galati |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  | INTRODUZIONE Il presente report documenta i risultati del Penetration Testing condotto su un’applicazione web e un web server su una macchina Metasploitable con DVWA. Lo scopo di questo test è valutare la sicurezza ed identificare potenziali vulnerabilità. | |  |
|  |  | |  |
|  | METODOLOGIA Il Penetration Testing è stato condotto utilizzando attacchi XSS Stored e SQL Injection Blind per simulare minacce di parte di un Black Hat. Gli obiettivi principali erano identificare vulnerabilità che potrebbero permettere a un attaccante di ottenere informazioni sensibili, come credenziali di accesso e cookie di sessione.   VULNERABILITÀ XSS STORED Durante il test, è stata identificata una vulnerabilità XSS Stored nell'applicazione web. Questa vulnerabilità consente a un attaccante di iniettare script malevoli all'interno delle pagine web, mettendo a rischio gli utenti del sito.  Raccomandazioni: Implementare una sanitizzazione degli input per prevenire attacchi XSS. | VULNERABILITÀ SQLI BLIND  È stata identificata una vulnerabilità SQL Injection Blind nell'applicazione web. Questa vulnerabilità potrebbe consentire a un attaccante di estrarre informazioni sensibili dal database sfruttando query SQL malevoli. Raccomandazioni: Applicare misure di sicurezza per prevenire attacchi SQL Injection, come la validazione dei dati dell'utente. CONCLUSIONI E RACCOMANDAZIONI Il Penetration Testing ha rivelato due vulnerabilità critiche. Bisogna affrontare queste vulnerabilità per garantire la sicurezza degli utenti e dei dati sensibili. Eseguire una revisione completa del codice dell'applicazione web per individuare e correggere tutte le vulnerabilità XSS.  Implementare controlli di validazione degli input e sanitizzazione dei dati per prevenire attacchi SQL Injection. |  |

Ivan Galati

Data:04/11/2023