



*SERVIZIO DI
PENETRATION TEST
APPLICATIVO*

PENETRATION TEST APP

Datasheet

Le aziende del Gruppo MEET IT



Via di Corticella, 89/2
40128 Bologna BO

+39 051 4070383
www.3cime.com | info@3cime.com



Viale Alcide De Gasperi, 37
33100 Udine UD

+39 0432 524001
infoentonline.it | www.ntonline.it



LE TUE APP SONO DAVVERO SICURE?

Il servizio permette di verificare la sicurezza delle applicazioni esposte in Internet.

Tutte le organizzazioni – private e pubbliche – lavorano ormai su **applicativi sviluppati da terzi**, affidandosi quindi con una fiducia cieca all'operato dei gestori dell'app.

Se si escludono i grandi player – come SAP, Oracle, ecc. – esistono migliaia di sviluppatori software per i quali, fino ad oggi, quello che contava era il risultato applicativo del codice: la sicurezza era semplicemente non considerata.

Questo approccio diventa **pericoloso** quando le applicazioni sono esposte in Internet o, più semplicemente, quando sono utilizzate anche da soggetti esterni. Ricordiamo, infatti, che i pirati informatici possono entrare nelle nostre reti e raggiungere, non solo i dati, ma anche le applicazioni interne.

Il servizio viene erogato come una **verifica una-tantum** delle **applicazioni specifiche** e del loro codice, combinando sistemi di **intelligenza artificiale** e **risorse umane**.

SERVIZIO

Coscienti che spesso gli sviluppatori sono poco attenti ai **bug di sicurezza** delle proprie applicazioni, il sistema va ad **analizzare le righe di codice scritte**, le **librerie utilizzate**, ma anche **API, compilatori web, container** e tutto quello che porta alla realizzazione di un'app realmente sicura.

L'obiettivo del servizio è fornire un quadro completo e chiaro delle **vulnerabilità** e dei **bug** delle applicazioni. Fornisce, infatti:



Elenco delle **vulnerabilità riscontrate**



Elenco delle **fasi applicative da modificare**, con sostituzioni di codice, librerie o altro



Output di configurazione per il nostro servizio WAF as a Service di protezione dell'applicazione da utilizzare nell'attesa che lo sviluppatore applichi le remediation

VISITA IL SITO **MEETIT.CLOUD**

