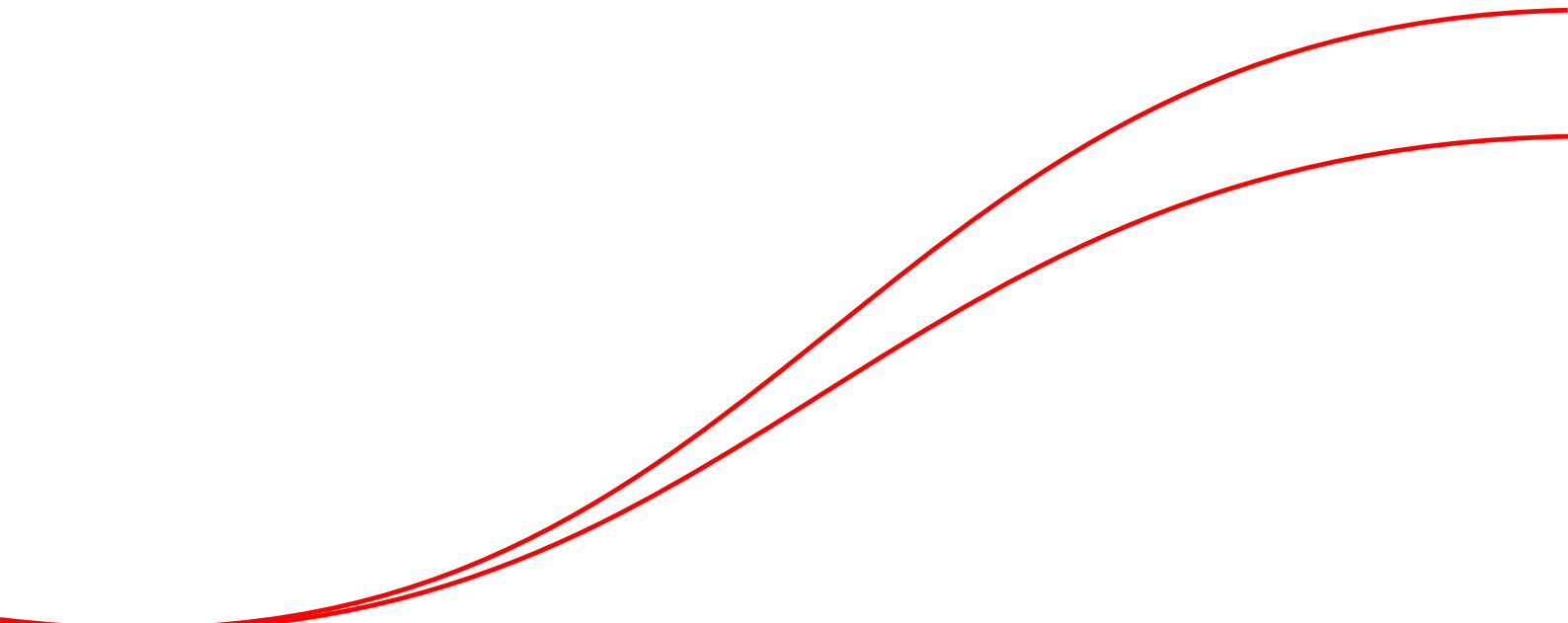


# WAPT

## Web Application Penetration Test



# Web Application Penetration Testing (WAPT)

Il servizio di *Web Application Penetration Testing* è uno dei servizi di sicurezza applicativa (*Application Security Assessment*) proposti da ISGroup.

Le applicazioni web sono ormai prevalenti e sempre più sofisticate oltre ad essere critiche per tutti i *business* basati sul web.

Verranno analizzati i componenti critici di un portale web, un'applicazione *E-Commerce* o una piattaforma web.

Utilizzando tecniche manuali e centinaia di strumenti appropriati il *tester* è in grado di identificare problematiche evidenti e nascoste.

Come per le applicazioni *client/server* le applicazioni web generalmente soffrono di gestione impropria delle richieste del *client* e mancata o impropria validazione e controllo da parte dello sviluppatore.

Data la natura delle applicazioni web, esse sono completamente esposte ed accessibili, questo rende la "sicurezza tramite segretezza" (*security through obscurity*) impossibile e necessario codice applicativo resistente.

In secondo luogo le applicazioni web processano dati da richieste *HTTP*, un protocollo che permette una miriade di encoding e incapsulazioni diverse.

## Descrizione del servizio

Un *Web Application Penetration Test* è la simulazione di un attaccante nei confronti di un sito, portale o applicazione web. Il *testing* inizialmente consiste nello scoprire e identificare tutte le risorse esposte sul *target*.

A questo punto prima di testare le applicazioni web vere e proprie viene controllata l'infrastruttura alla ricerca di vulnerabilità note e non.

Successivamente con l'ausilio di *tool* e manualmente ogni parametro viene testato con valori predefiniti e vengono provate le tecniche di attacco generiche per la data piattaforma.

In parallelo il *tester* effettua un'analisi della business logic per verificare che non vi siano problematiche concettuali.

Una volta individuati dei punti di attacco (*entry point*) validi si procede al tentativo di attacco che ha come obiettivo la compromissione più profonda ed estesa possibile.

Dato il livello di accesso ottenuto si tenderà di compiere azioni non ammesse, prelevare dati dal *database* di *backend*, prelevare file o sorgenti dal disco, modificare informazioni e laddove possibile ottenere il pieno controllo della macchina e di quelle limitrofe.

## Output

Il *Report* è un documento semplice e dettagliato che riassume i risultati dell'attività ed è suddiviso in tre differenti aree come precedentemente descritto:

### **Executive Summary**

All'inizio del *Report* e di lunghezza non superiore ad una pagina, è il riassunto di alto livello destinato al *Management*.

### **Vulnerability Details**

La parte tecnica che descrive nel dettaglio le vulnerabilità riscontrate e il loro impatto, dedicata al *Security Manager*.

### **Remediation Plan**

Sezione tecnica con istruzioni precise su come risolvere le problematiche identificate, dedicata al *System Administrator*.

## Richiedi servizi di Web Application Penetration Testing

Lavorare con noi è molto semplice, chiamando il numero +39-045-4853232 o spedendo una mail a [sales@isgroup.it](mailto:sales@isgroup.it) potremo conoscerci e discutere delle vostre necessità di fornitura di servizi di *IT Security*.