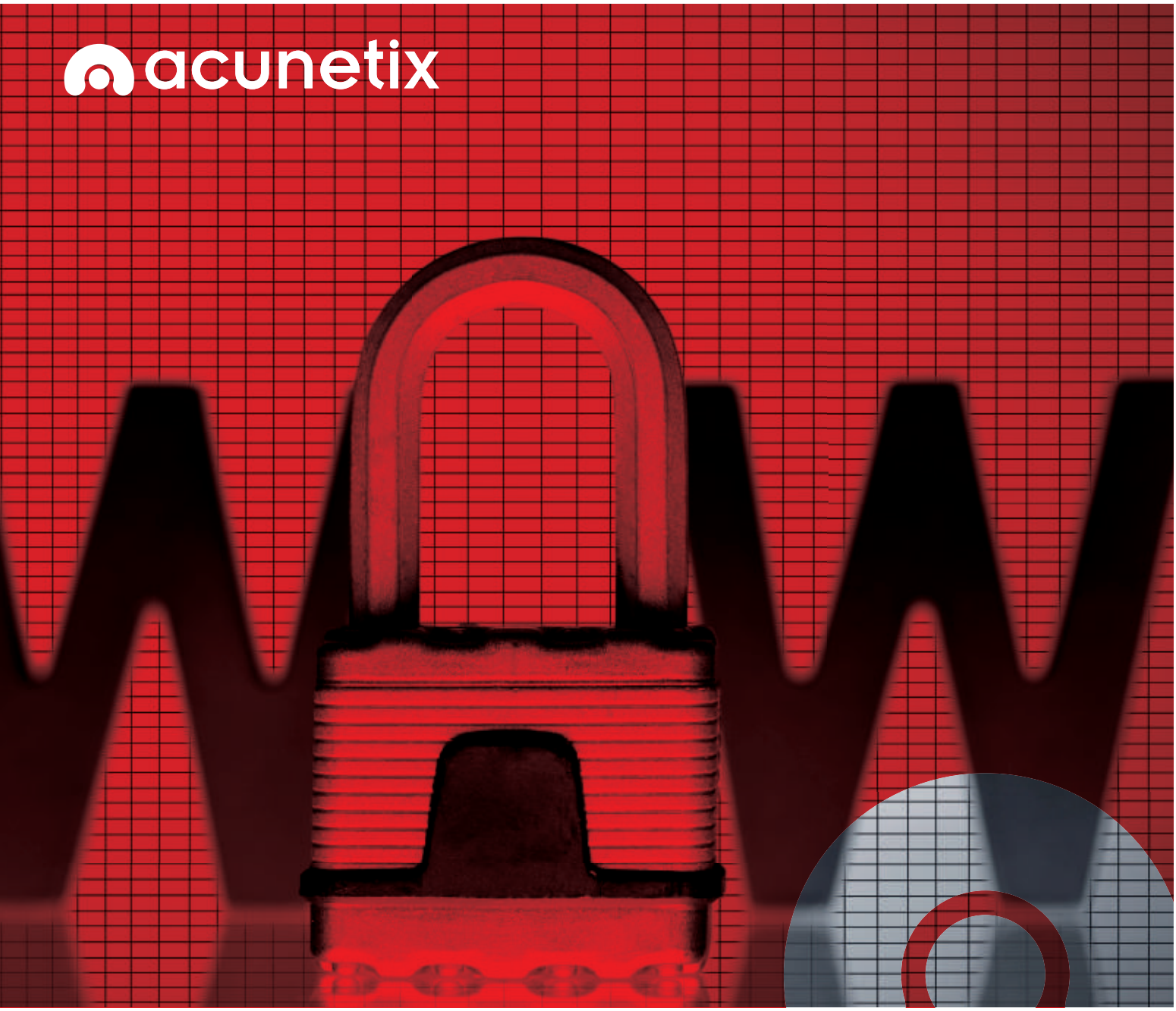
acunetix



IL VOSTRO WEB VULNERABILITY SCANNER RIESCE A TENERE LONTANI GLI HACKER?

Verifica la sicurezza del tuo sito web con Acunetix Web Vulnerability Scanner v9

Circa il 70% dei siti web hanno vulnerabilità che possono portare al furto di dati aziendali sensibili, come numeri di carte di credito o liste di clienti. Gli hacker stanno concentrando i loro sforzi sulle applicazioni web-based: carrelli, moduli, pagine di login, contenuti dinamici, o semplicemente errori umani.

Accessibili 24/7 da qualsiasi parte del mondo, le applicazioni web non sicure offrono agli hacker un facile accesso ai database aziendali di backend, e gli permettono di effettuare attività illegali usando i siti da loro compromessi.

Firewall, SSL e Server Locked-Down: futili precauzioni dal Web Application Hacking!

Gli attacchi alle applicazioni Web, lanciati sulla porta 80/443, passano attraverso il firewall, il sistema operativo e la sicurezza a livello di rete, per finire dritti al cuore delle vostre applicazioni e dati aziendali. Le applicazioni fatte su misura sono spesso non sufficientemente testate, hanno vulnerabilità non conosciute e sono quindi facili prede per gli hacker.

VERIFICATE SE IL VOSTRO SITO WEB SIA SICURO PRIMA CHE GLI HACKER scarichino dati sensibili, commettano un crimine usando il vostro sito come piattaforma di lancio, e mettano in pericolo il vostro business. Acunetix Web Vulnerability Scanner v9 esegue la scansione del vostro sito web, analizza automaticamente le applicazioni e trova vulnerabilità pericolose per il vostro business online come SQL injection e Cross Site Scripting.
Report precisi indicano esattamente dove si debbano modificare le applicazioni web, permettendovi di proteggere il vostro business da potenziali e prossimi attacchi.

ACUNETIX – Un Leader mondiale in Web Application Security

Acunetix è un pioniere della tecnologia web application security scanning,su cui i suoi ingegneri si sono focalizzati a partire dal 1997, sviluppandoun vantaggio tecnologico nell'analisi di siti web e identificazione di vulnera-bilità.

LE NUOVE TECNOLOGIE PORTANO ALLA LUCE NUOVI RISCHI DI SICUREZZA. ACUNETIX RISPONDE ALLA SFIDA CON LA PIU' COMPLETA TECNOLOGIA DI SCANSIONE SUL MERCATO.

Scansione Completa di vulnerabilità SQL Injectione Cross Site Scripting (XSS)

Acunetix WVS è il leader di mercato indiscusso per l'identificazione di vulnerabilità SQL Injection e XSS.

Acumonitor

Con la versione 9, è possibile scoprire nuove forme di XSS, come il Blind XSS e il DOM-based XSS. Per scoprire queste vulnerabilità serve un motore di scansione evoluto e sofisticato. Le tecnologie tradizionali di crawling e scanning non sono più sufficienti. Con **ACUMONITOR**, un nuovo servizio esclusivo per i Clienti Acunetix, sarete sempre un passo avanti agli hacker e scoprirete vulnerabilità come Blind XSS e Mail Header Injection (vulnerabilità che altri prodotti non riescono a trovare). Inoltre, Acunetix può vantarsi di tecniche avanzate di interpretazione JavaScript, che migliorano in modo drastico la scoperta automatica delle vulnerabilità XSS DOM-based.

Remediation Veloce grazie all'innovativa tecnologia AcuSensor

La nostra tecnologia proprietaria allo stato dell'arte garantisce un più alto livello di identificazione delle vulnerabilità, riduzione dei falsi positivi, e indicazione esatta di dove si trova la vulnerabilità all'interno del codice sorgente. Rimediare diventa quindi un'operazione molto rapida.

Supporto Completo di HTML5 con Acunetix DeepScan

La tecnologia DeepScan utilizza lo stesso motore di rendering di Chrome e Safari, ed è in grado di interpretare siti e applicazioni web che utilizzano tecnologie HTML5 e JavaScript, come applicazioni AJAX e Single Page.

Scansione Automatica di Aree Protette da Password

Acunetix Web Vulnerability Scanner è in grado di riempire automaticamente form web e di autenticarsi su login web. La maggior parte dei web vulnerability scanner non possono fare questo, oppure devono usare scripting complessi per testare pagine del genere. Acunetix è diverso: con lo strumento di registrazione macro Login Sequence Recorder, è possibile registrare una sequenza di login, un processo di compilazione moduli o una specifica sequenza di crawling.Lo scanner eseguirà nuovamente la sequenza durante il processo di scansio-ne e riempirà moduli web, effettuando il logon alle aree protette in modo automatico.

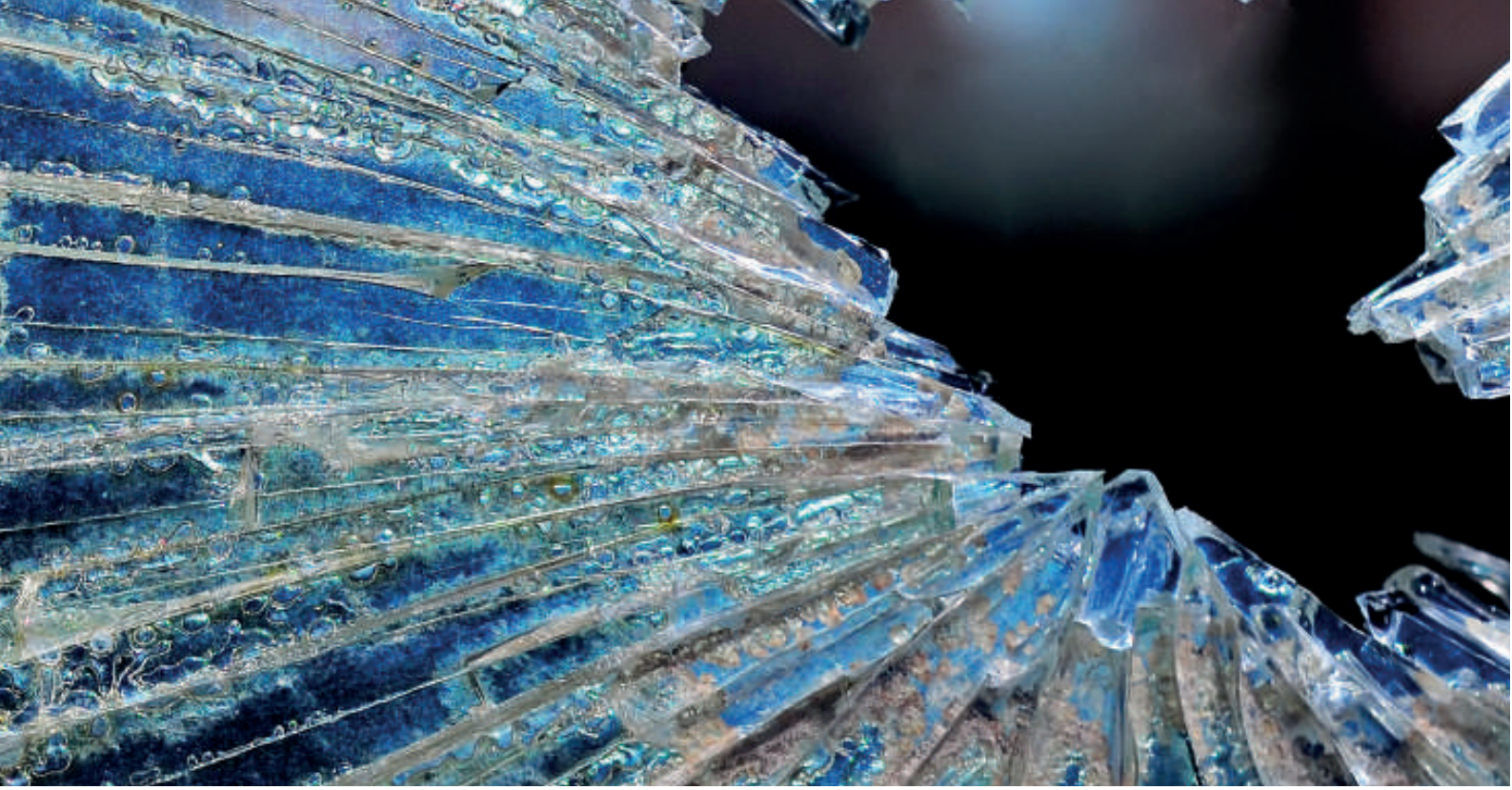
Scansione di Siti Multipli in ogni momento e luogo

Effettuate la scansione fino ad un massimo di 10 siti contemporaneamente dallo stesso computer. Acunetix WVS include un'interfaccia web-based per effettuare scansioni immediate oppure per pianificare le scansioni, offrendo i risultati in qualunque momento, da qualsiasi luogo.

Report Completi per la Compliance

La vostra applicazione web è conforme ai requisiti di compliance?Lasciate che Acunetix WVS vi aiuti, con i suoi moduli di reporting dettagliatiche coprono una vasta gamma di standard, tra cui:

- CWE/SANS Top 25 Most Dangerous Software Errors
- The Health Insurance Portability and Accountability Act (HIPAA)
- International Standard - ISO 2700
- NIST Special Publication 800-53 - Recommended Security Controls for Federal Information Systems
- OWASP TOP 10 2013
- Payment Card Industry Data Security Standard version 2.0
- Sarbanes-Oxley Act
- DISA STIG Web Security
- Web Application Security Consortium: Threat Classification



Fermare i Search Engine degli Hacker

Acunetix lancia le sue query dal Google Hacking Database (GHDB) verso il contenuto del vostro sito web, identificando dati sensibili o target a rischio prima che sia un search engine di un hacker a farlo.

Identificazione Automatica di Pagina Personalizzata "404 Error Page"

Determina automaticamente se viene utilizzata una pagina personalizzata di errore 404, e la identifica senza aver bisogno che nessun pattern di riconoscimento venga configurato prima della scansione.

Scansione delle Porte e Alert di Rete

Acunetix Web Vulnerability Scanner esegue delle scansioni sulle porte verso il web server che ospita il sito web, e identifica automaticamente i servizi di rete che sono in esecuzione su porte aperte, lanciando una serie di test di network security verso questi servizi. Utilizzando la documentazione sull'SDK fornita da Acunetix, è possibile anche sviluppare degli alert di sicurezza personalizzati.

Tra i controlli di security già compresi nel prodotto troviamo:

- Test per password deboli su FTP, IMAP, server SQL , POP3, Socks, SSH, Telnet e altre vulnerabilità DNS quali Open Zone Transfer, Open Recursion, Cache Poisoning;
- Test di accesso FTP come verifica della possibilità di accesso anonymous, lista delle directory FTP writable, controlli di sicurezza per Proxy Server mal configurati;
- Controlli su SNMP Community String deboli;
- Controlli su cifrature SSL deboli;
- E molti altri controlli di sicurezza sofisticati.

Strumenti Avanzati di Penetration Testing

Oltre al suo motore di scansione automatico, Acunetix include strumenti evoluti per consentire ai penetration tester di effettuare verifiche di sicurezza raffinate sulle applicazioni web:

- HTTP Editor – Costruisce richieste HTTP/HTTPS e analizza la risposta del web server.
- HTTP Sniffer – Intercetta, mantiene il log e modifica tutto il traffico HTTP/HTTPS, rivelando tutti i dati inviati da un'applicazione web.
- HTTP Fuzzer – Effettua test di fuzzing sofisticati, per verificare i meccanismi di validazione dell'input delle applicazioni web, e la gestione di dati casuali inaspettati e/o invalidi. Con il rule builder integrato, è possibile testare migliaia di parametri di input. Test che solitamente richiedono giorni per essere effettuati manualmente, si possono concludere in pochi minuti.
- Blind SQL Injector – Uno strumento automatico di estrazione dei dati da un database, ideale per i penetration tester che desiderano svolgere ulteriori test manualmente.

Ulteriori Funzionalita' Avanzate

- Identifica le vulnerabilità HTTP Parameter Pollution (HPP).
- Supporta gli header HTTP personalizzati nelle scanzioni automatiche.
- Supporta credenziali multiple di autenticazione HTTP.
- Profili utente personalizzati, per effettuare scansioni con diverse opzioni e identità.
- Generatore di Report personalizzati.
- Compara diverse scansioni, rilevando le differenze.
- Effettua nuovamente una verifica dei cambiamenti sul sito web grazie alla funzione rescan.
- Supporta l meccanismi di autenticazione CAPTCHA, Single Sign-On e Two Factor.
- Scopre le directory con permessi deboli e se siano abilitati processi HTTP potenzialmente pericolosi.
- Genera una lista di risposte HTTP non frequenti quali internal server error, HTTP 500, etc.
- Lista dei falsi positivi personalizzabile.
- Audit di sicurezza della configurazione del web server.
- Auto importazione delle regole di riscrittura di IIS 7 direttamente dal file web.config.
- Può effettuare la scansione di una specifica vulnerabilità per verificarne la remediation.
- Test di vulnerabilità di Upload Automatici di File.

acunetix

DOVE TROVARCI:

Website: www.acunetix.com
Acunetix Blog: www.acunetix.com/blog
Facebook: www.facebook.com/acunetix
Twitter: twitter.com/acunetix

CONTACT INFORMATION:

Acunetix (Malta)
Level 6, Portomaso Business Tower
STJ4011 St Julians
Tel: +44 (0)330 202 0190
Fax: +44 (0)330 202 0191
Email: sales@acunetix.com

Acunetix (UK)
Unit 2, St Johns Mews,
13 St Johns Road, Hampton Wick
KT1 4AN, Kingston Upon Thames
Tel: +44 (0)330 202 0190
Fax: +44 (0)330 202 0191
Email: sales@acunetix.com

Acunetix (USA)
Tel: (+1) 404 990 3280
Fax: (+1) 404 990 3279
Email: salesusa@acunetix.com