



SI PUO' ENTRARE NEL TUO SITO?

Meglio controllare con
Acunetix Web Vulnerability Scanner

Controlla la sicurezza del tuo sito web con Acunetix Web Vulnerability Scanner

La sicurezza dei siti Web è oggi, forse, l'aspetto maggiormente trascurato nella policy di sicurezza aziendale dei dati, mentre dovrebbe essere un aspetto prioritario. Infatti, gli hacker stanno concentrando i loro sforzi verso le applicazioni Web-based, come ad esempio moduli online, carrelli della spesa, pagine di login e diregistrazione, contenuti dinamici e così via, da cui poter ricavare informazioni e dati sensibili.

Le applicazioni Web sono disponibili 24 ore su 24, per 7 giorni alla settimana, e controllano dati ed informazioni di valore dal momento che spesso sono in accesso diretto verso dati di backend come il database dei clienti.

I firewall, l'SSL e server "chiusi" sono precauzioni inutili verso l'hacking delle applicazioni Web: Infatti, le difese di sicurezza a livello di rete non offriranno protezione contro tali attacchi, dal momento che questi vengono lanciati sulla porta 80, che deve rimanere aperta.

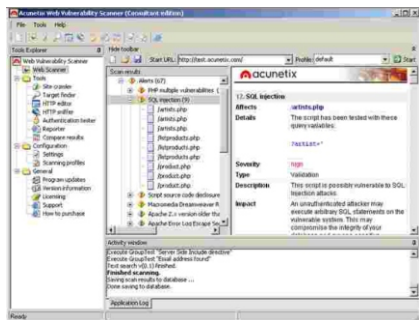
Oltre a ciò, le applicazioni web sono spesso realizzate su misura, e per questo motivo meno testate del software standard pacchettizzato, e più probabilmente hanno vulnerabilità non ancora scoperte.

L'auditing manuale di un sito web per ricercarne le vulnerabilità è virtualmente impossibile: questo tipo di attività va svolta automaticamente e regolarmente.

Gli attacchi alle applicazioni Web rappresentano il 70% di tutti i cyber attack

Caratteristiche

- ✓ Rende sicuro il vostro sito contro gli attacchi web
- ✓ Controlla automaticamente le vulnerabilità di tipo SQL injection e Cross Site Scripting
- ✓ Verifica l'efficacia delle password sulle pagine di autenticazione (moduli HTTP o HTML)
- ✓ Verifica il controllo automatico di shopping cart, moduli, contenuto dinamico ed altre applicazioni web
- ✓ Crea report di security auditing professionali.

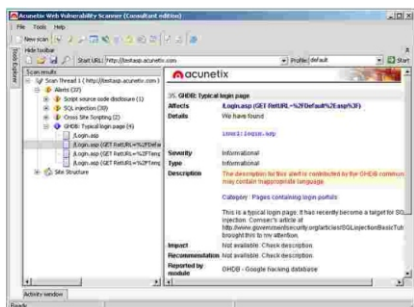


Identifica automaticamente SQL injection, cross site scripting e altre vulnerabilità web

L'SQL injection è una tecnica di hacking che modifica i comandi SQL con l'obiettivo di accedere ai dati presenti nel database. Gli attacchi di tipo cross site scripting permettono ad un hacker di eseguire codici maligni sul browser dei vostri visitatori. Acunetix Web Vulnerability Scanner può verificare e controllare se le vostre applicazioni web siano vulnerabili a entrambe queste tipologie di attacchi. E' possibile trovare ulteriori informazioni su SQL injection e cross site scripting sul sito web Acunetix, alla sezione security centre.

Altre vulnerabilità e attacchi web identificabili

- CLRF injection
- Code Execution
- Directory traversal
- File inclusion
- Input validation
- Authentication

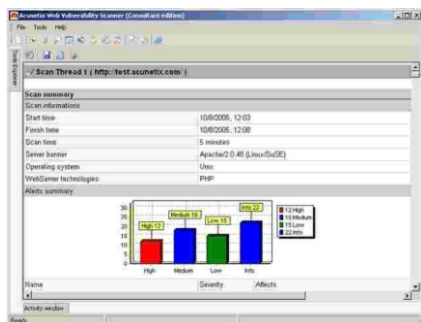


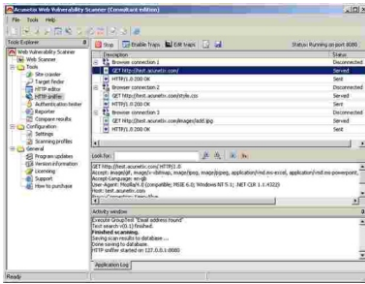
Identifica le vulnerabilità Google hacking

Google hacking è il termine utilizzato nel caso in cui un hacker provi a trovare obiettivi e dati sensibili attraverso query sui motori di ricerca. Il Google Hacking DataBase (GHDB) contiene query che identificano dati sensibili come pagine di logon a portali, log con informazioni sensibili e così via. Acunetix lancia tutte le query del GHDB all'interno del contenuto del vostro sito web alla ricerca di dati sensibili o di target raggiungibili, prima che lo faccia un hacker. Questa caratteristica rende il prodotto Acunetix unico nel mercato.

Generatore di report

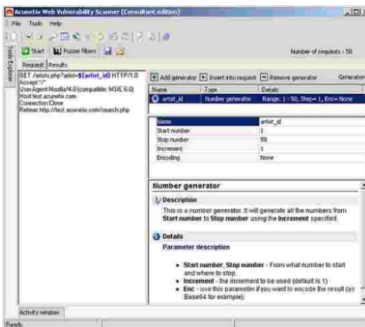
Con il generatore di report è possibile creare velocemente e facilmente dei report professionali che specificano le vulnerabilità identificate e suggeriscono cosa può essere fatto per eliminarle. Oltre a ciò, tutte le sessioni di scansione del sito possono essere salvate in un database MS SQL Server o MS Access per potere sottoporre e memorizzare report personalizzati.





Estendi gli attacchi con lo sniffer e l'editor HTTP

Con l'editor HTTP, è possibile costruire richieste di tipo HTTP e HTTPS, analizzando la risposta del server. Questa funzione ha lo scopo di simulare SQL injection personalizzate e attacchi di tipo cross site scripting. Con lo sniffer HTTP, è possibile effettuare il log, intercettare e modificare tutto il traffico di tipo HTTP/HTTPS, con lo scopo di ottenere una visione approfondita e particolareggiata su quali dati la vostra applicazione web stia trasmettendo.



HTTP fuzzer - Test automatico e basato su regole variabili

Lo strumento HTTP fuzzer permette di creare regole per effettuare test automatici su buffer overflow e input validation. Per esempio, utilizzando l'HTTP fuzzer è possibile creare una regola che rimpiazza la parte variabile in un indirizzo URL (es. `http://test.acunetix.com/listproducts.php?cat=1`) con i numeri 1-999. In questo modo è possibile lanciare 1000 query, controllando solamente i risultati significativi, risparmiando moltissimo tempo rispetto ad un test manuale.

Crawl aree protette da password

Acunetix Web Vulnerability Scanner può essere configurato per effettuare la scansione di sezioni del vostro sito web protette da password con una o più combinazioni user/password. Utilizzando lo strumento login sequence, che funziona in modo simile ad un registratore di macro, è possibile configurare con semplicità il percorso che lo scanner deve crawl, includendo link che non devono essere seguiti, come ad esempio un link di logout.

HTML form filler automatico

L'HTML form filler permette di configurare differenti input che desiderate che il web scanner fornisca quando incontra un form HTML. In questo modo è possibile testare automaticamente il comportamento del vostro sito web di fronte a differenti tipi di input.



Altre caratteristiche

- Test sulla efficacia delle pagine di login lanciando un "dictionary attack"
- Possibilità di creare attacchi web personalizzati o modificare quelli esistenti con il Vulnerability Editor
- Supporta tutte le maggiori tecnologie Web, quali ASP, ASP.NET, PHP e CGI
- Utilizza differenti profili di scansione
- Comparazione fra diverse e successive scansioni per ricercare nuove vulnerabilità
- Effettua facilmente i re-auditing in seguito a cambiamenti sul sito web
- Interpreta file Flash
- Scopre directory con livelli di permission deboli o inadeguati
- Determina se sul sito Web siano abilitati metodi HTTP potenzialmente pericolosi (es. PUT, TRACE, DELETE) e ispeziona i banner in versione HTTP

Requisiti di sistema

- Windows 2000/2003 o Windows XP
- Internet Explorer 5.1 o successivi
- MS SQL Server/access se il database è abilitato
- 200Mb di spazio su disco rigido

Distribuito da

● FORCE

Via Zuretti, 25 - 20125 Milano Italy

Tel. +39 02 45481521

Fax +39 02 67076111

www.dotforce.it

email: acunetix@dotforce.it

