Strumenti

Paros – un web pen tester free

Sistema operativo: *Multipiattaforma*
Homepage: *http://www.parosproxy.org/index.shtml*
Licenza: *Open Source*

Con la crescita delle web applications e dei CMS, gratuiti o a pagamento, i nostri dati sono sempre più esposti ad attacchi e rischi, per questo motivo associazioni come l'OWASP (*Open Web Application Security Project – http://www.owasp.org*) e il *Web Application Security Consortium* (WASC – *http://www.webappsec.org/*) tendono sempre a rilasciare nuove linee guida al fine di prevenire molti bugs di sicurezza nei software online, che compongono le web applications.

Per perseguire questo obbiettivo si dovrebbero testare manualmente tutte le vulnerabilità, alle quali il sito web può essere esposto, quindi provare con numerosi pen test (penetration test).

Molti sono i software che permettono di eseguire tanti pen test automaticamente, tra i più famosi ricordiamo Nessus, MS Baseline,WebScarab and Sprajax, Burp,WhiteHat Sentinel e WebInspect, ma in quest'articolo parleremo di Paros Proxy un programma sviluppato da un gruppo di professionisti esperti di sicurezza IT, che vantano anni di eseperienza nel campo delle applicazioni web e mirano a:

- Sviluppare una metodologia standard per la sicurezza delle applicazioni web,
- Sviluppare delle linee guida per i web developers,
- Esprimere la loro visione sui problemi di sicurezza sul web.

La loro società è la Milescan (*http://www.milescan.com*) ma per la loro creaturina Paros c'è il sito dedicato: *http://www.parosproxy.org/index.shtml*.

Il Paros è un HTTP/HTTPS proxy server tutto sviluppato in Java e che è in grado di intercettare e modificati tutti i dati scambiati tra il client ed il server, inclusi i cookies e i campi dei forms. Ingolositi? Bene, allora passiamo alla fase operativa!

Dopo aver scaricato ed installato il programma, passiamo subito all'azione.

- *Primo passo*: Configurare il proprio web browser con con connessione attraverso proxy server ed inserire come host il localhost e la porta è la 8080 (la porta di default sulla quale lavorerà Paros, anche se poi dalle opzioni di Paros sarà possibile cambiarla).
- *Secondo passo*: Lanciamo Paros.
- *Terzo passo*: Navighiamo sul sito che vogliamo esaminare.

Questi tre step vi fanno immaginare la facilità d'uso del programma, però ci sono delle considerazioni da fare.

Paros ha un motore di spidering del sito molto potente, quindi cerchiamo di settare bene il livello di profondità che lo spider deve percorrere, altrimenti andiamo a testare anche siti che non interessano la nostra analisi.

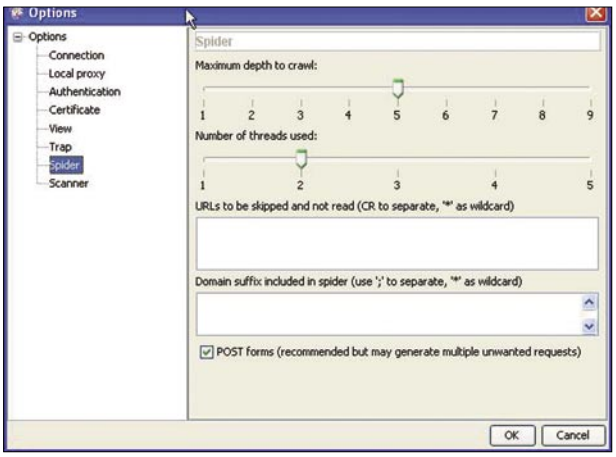

Fig. 1: *Configurazione dello spider*

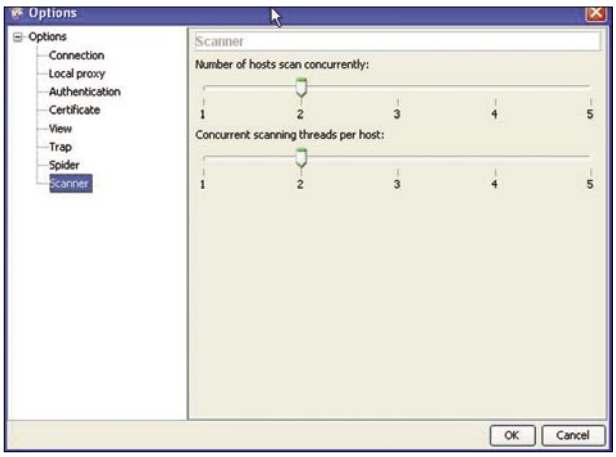

Fig. 2: *Configurazione dello scanner*

Anche lo Scanner va configurato, perché dopo che il proxy avrà navigato tutti i link presenti sul sito target (*spider*), si dovrà procedere alla fase di scanning per individuare le vulnerabilità e cliccando su Analyse e poi Scan Policy possiamo selezionare che tipo di vulnerabilità vogliamo analizzare.

Quando lo spider e lo scanner di Paros sono in azione, lascieranno sul server attaccato parecchie tracce di attività massiccia, quindi NON usatelo mai su siti dai quali non siete stati autorizzati.

Per questo motivo ci sono dei siti fatti apposta per sperimentare le vostre abilità hacker come: *http://hackme.ntobjectives.com*.

Appena siete sul sito vedrete che nella sezione Sites di Paros, ci sarà l'url del sito bersaglio, ma anche altri url relativi ai siti linkati (es. i banner di google, ecc.). Per fare pulizia basta selezionare gli url estranei e col secondo tasto del mouse scegliere l'opzione Delete from View o Purge from DB, così da avere sotto il mirino solo il necessario.

A questo punto selezioniamo l'url (es. *http://hackme.ntobjectives.com/*) e iniziamo lo Spidering per visualizzare tutta la gerarchia di cartelle e files del sito e poi usiamo lo Scan per individuare le possibili falle. Dopo un pò di tempo avremo la lista degli Alert che ci diranno quante vulnerabilità di tipo *Low* (file obsoleti), *Medium* (directory browsing and cross-site scripting), *High* (SQL injection).

Dalla Figura 2 evinciamo subito che il sito attaccato ha vulnerabilità Medie e Alte, c'è la directory delle immagini che è sfogliabile ed una serie di files con form che hanno attivata la funzione di autocompletamento, cosa da evitare, perché se lasciate la vostra postazione sguarnita, qualcuno potrebbe, con un semplice doppio click del mouse in una casella del form, far apparire i vostri dati recentemente inseriti e quindi entrare tranquillamente.

Inoltre vediamo una serie di links che portano alle pagini vulnerabili alla SQL-Injection, la bellezza di questo programma è che si può cliccare sul l'Alert della pagina vulnerabile e modificare i paramentri per poi re-inviare la pagina modificata per poter vedere i risultati.

Altra funzione molto carina è il TOOL di codifica/decodifica per i vari tipi di encoding, URL, BAS64, SHA1, MD5, che potrebbero risultare molto utili per decodificare, per esempio, un account file codificato con BASE64.

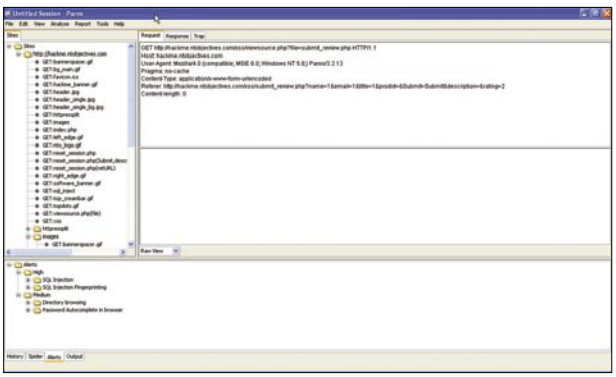

Fig. 3: *Dopo lo scanning*

Per finire, Paros, permette di generare un report HTML organizzato e facilmente comprensibile, che riassume tutte le vulnerabilità individuate.

The Last but not the Least è una caratteristica, *simpatica*, del Paros , ossia la possibilità di impostare un gateway di uscita, così usando gateway di anonimizzazione IP, tipo JAP (*http://anon.inf.tu-dresden.de/*),si potrebbero sferrare dei *test* in maniera del tutto coperta, impostando da *TOOLS --> OPTIONS --> CONNECTIONS ---> USE AN OUTGOING PROXY SERVER* ed impostare il localhost sulla porta di ascolto di JAP, in questo modo il browser usa PAROS come gateway sulla porta X (es. 8080) e Paros usa JAP sulla porta Y (es. 4001) per uscire sul web, rendendovi praticamente invisibili.

Certo che con l'uso di questi Pen Test automatizzati l'hardening delle web applications diventa più semplice e doveroso, poichè spesso si tende a proteggere le reti interne, snobbando il web , che invece è la parte più esposta di tutto il sistema informativo.

Ma come allenarsi ad usare il PAROS?

Possiamo provarlo sul localhost (127.0.0.1) oppure c'è CD-Rom da scaricare BADSTORE (*http://www.badstore.net/*) un sito di e-commerce che gira in un ambiente *Trinux* (Linux), una volta scaricata l'immagine ISO dal sito, basterà lanciare il VMServer (*http://www.vmware.com*) e montare l'immagine creando una macchina virtuale con le seguenti opzioni:

- Sistema operativo: *OTHER LINUX*,
- Scheda di rete: *HOST ONLY – A private network shared with the host*,
- CD-ROM: *Use ISO IMAGE* (così non siamo costretti a masterizzare l'immagine su cd).

A questo punto basta fare *PLAY* e la macchina virtuale si avvierà, al termine della procedura di boot si visualizzerà il prompt bash qui basterà lanciare il comando ifconfig per vedere l'indirizzo IP della macchina virtuale es: 192.168.147.128 quindi ritorniamo sul nostro Windows e apriamo il browser su questo indirizzo: *http://192.168.147.128/cgi-bin/badstore.cgi* (chiaramente l'indirizzo è *http://IP_DELLA_TUA_MACCHINAVIRTUALE/cgi-bin/badstore.cgi*), nel caso vogliate impostare a mano indirizzo IP diverso servirà solamente digitare il comando: `ifconfig eth0 up xxx.xxx.xxx.xx netmask yyy.yyy.yyy.yyy broadcast xxx.xxx.xxx.255` (dove *xxx* sono i numeri che sceglierete voi).

Badstore include Apache web server, un'applicazione CGI (*Common Gateway Interface*), ed una implementazione completa di MySQL con un database con tabelle multiple, insomma BadStore.net is not a simulation, ma una vera e proprio web application su un server reale con un database reale.

Bene adesso avete un intero sito di e-commerce da torturare.....BUON DIVERTIMENTO!

Per saperne di più ed effettuare il download: *http://www.parosproxy.org/index.shtml*.

Nanni Bassetti