Opis środiwska testowego W3AF

Ogólny opis funkcjonalności

W3AF (***w**eb **a**pplication **a**ttack and **a**udit **f**ramework*) jest to open-source'owa aplikacja służąca do testowania bezpieczeństwa aplikacji webowych. Została zaimplementowana w języku python. Oprogramowanie to ma za zadanie umożliwiać zindentyfikowanie i wychwycenie luk bezpieczeństwa w aplikacji webowych, poprzez wysyłanie do niej zainfekowanych requestów HTTP. Oprogramowanie jest w stanie przetestować aplikację pod względem ponad 200 najpopularniejszych podatności. Przed uruchomieniem testów, użytkownik powienien znać zarys sposobu działania testowanej aplikacji.

Wersje darmowe/płatne.

W3AF jest rozpowszechniany w wersji darmowej na licencji GPLv2.0.

Sposoby przygotowania testów.

Aplikacja wykonuje testy penetracyjne składające się z trzech etapów, za każdy z nich opowiadają następujące pluginy:

- crawl: dostają od użytkownika na wejściu adres URL, dzięki któremu znajdują nowe formy adresu oraz potencjalne niezabezpieczone miejsca.
- audit: otrzymuje punkty potencjalnego zagrożenia od crawla, po czym przesyła do nich zainfekowane dane w celu zlokalizowania luk w zabezpieczeniach.
- attack: jako wejście otrzymują luki w zabezpieczeniach znalezione przez audit. Mają na celu maksymalnie wykorzystać potencjalne dziury.

Ponadto występują pluginy wspomagające:

- infrastructure: uzyskuje informacje o webowych firewallach, systemie operacyjnym oraz http daemon.
- grep: analizują treść zapytań i odpowiedzi wysyłanych do i z aplikacji, dzięki czemu identyfikują luki bezpieczeństwa.
- output: jest odpowiedzialny za komunikację z użytkownikiem. Zapisuje on dane wyjściowe analizy do pliku *.txt*, *.xml* lub *.html*. Ponadto może on także zapisać do analizy informacje uzyskanie z debugu.
- mangle: pozwala manipulować zapytaniami do serwera i dpowiedziami w oparcu o wyrażenia regularne.

Framework może być konfigurowany na 2 poziomach: globalnej konfiguracji oraz konfiguracji pojedynczych pluginów. Konfiguracja może być zapisana i odtworzona w ramach tak zwanego profilu.

Sposoby prezentacji wyników testów.

Wyniki mogą być wyświetlane na konsoli, zapisywane w formatach txt, xml, html oraz wysyłane przez e-mail.

Stopień aumatyzacji testów.

Testy mogą być odpalane z konsoli użytkownika lub z poziomu interfejsu gui. W celu automatyzacji testów w3af wykorzystuje skrypty. Są to pliki tekstowe zawierające w każdej linii jedno wywołanie komendy z w3af-console. Świetnie sprawdzają się przy wykonywaniu okresowych skanów bezpieczeństwa.