Fuzz Testing

Onur Yılmaz, Ağustos 2009, WGT E-Dergi 1. Sayı

Bir uygulamada zafiyet tespit edebilmek için uygulamaya rastgele veriler göndererek, uygulamanın farklı isteklere verdiği cevapları analiz etmek isteyebiliriz. Bu rastgele veri gönderme işlemine fuzzing (fuzz testing), bu işlemi yapmaya yarayan araçlara ise fuzzer denilmektedir.

Fuzz testing; test yapılacak uygulamanın arka planında ki işlevsel ve yazılımsal özellikler bilinmediğinden ve gönderilen verilerin uygulamada oluşturduğu etki ve sonuçların analizine dayandığından, uygulama test tekniklerinden black-box kategorisine girmektedir [1,2].

Fuzz testing; yazılım geliştirme ve test süreçlerinde ve ters mühendislik işlemlerinde kullanıldığı gibi, web uygulamalarında zayıflık tespiti veya bilgi toplama amaçlı da kullanılmaktadır. Web uygulamaları için geliştirilmiş olan fuzzing araçlarını (fuzzer) iki kategoride inceleyebiliriz [3];

- **Recursive Fuzzing:** 'Yinelemeli fuzzing' olarakta adlandırabileceğimiz bu teknikte, belirlenmiş karakterler fuzzer aracılığıyla kombinasyonel veriler halinde gönderilecektir. Örneğin; {3,9,6,1) şeklinde belirlediğimiz karakterler;
    - ?id=3961, ?id=3916, ..., ?id=1693 yinelenerek gönderilecek ve her bir dönen sonuç incelenecektir.
- **Replacive Fuzzing:** 'Değiştirmeli fuzzing' olarakta adlandırabileceğimiz bu teknikte ise, seçilmiş değerin / parametrenin değiştirilerek gönderilmesi esastır.

Fuzz Testing konusunda detaylı bilgiye farklı [4] kaynaklardan erişebilirsiniz. Şimdi web uygulamaları için geliştirilmiş olan fuzzer`lara göz atalım [5].

Ferruh Mavituna's Freakin' Simple Fuzzer (FM-FSF)

Ferruh Mavituna tarafından geliştirilen Freakin' Simple Fuzzer (FSF) [6]; web uygulamaları için fuzz testing ve veri toplama işlevlerini yapabilmektedir. Temel düzeyde fuzzing işlemleri ve belirtilen düzenli ifadeye göre veri toplama işlemi yapabilen FSF, plugin yapısını desteklemektedir.

VB.NET ile geliştirilen FSF`i, .NET Framework 3.5 (Windows) ve Mono (OSX ve Linux) sistemlerinde çalıştırabilirsiniz. Kurulumu ve kullanımının çok basit olması nedeniyle tercih edebileceğiniz FSF`in kullanım detaylarına proje sayfasından erişebilirsiniz [7].

WebSlayer

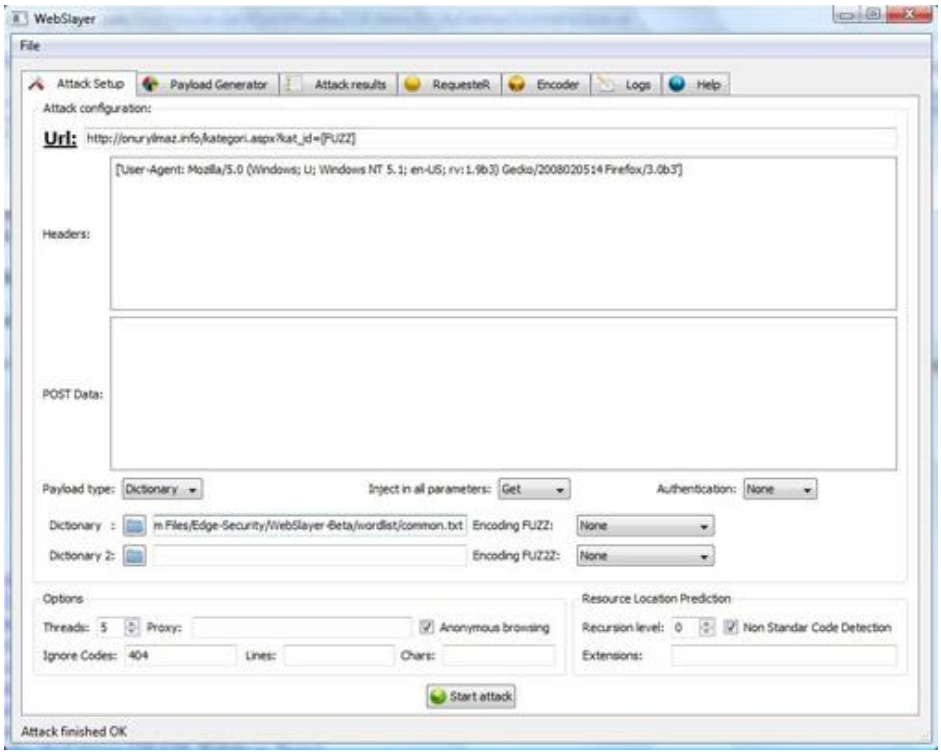
OWASP WebSlayer projesinin ürünü olan WebSlayer [8]; web uygulamaları için hazırlanmış bir fuzz testing ve brute-force uygulamasıdır. WebSlayer ile;

- Dosya ve klasör tespiti,
- Login formlarına brute-force,
- Oturumlara brute-force,
- Parametrelere brute-force,
- XSS ve SQL Injection tespiti ve
- Authentication`lara yönelik brute-force atakları düzenlemek mümkündür.

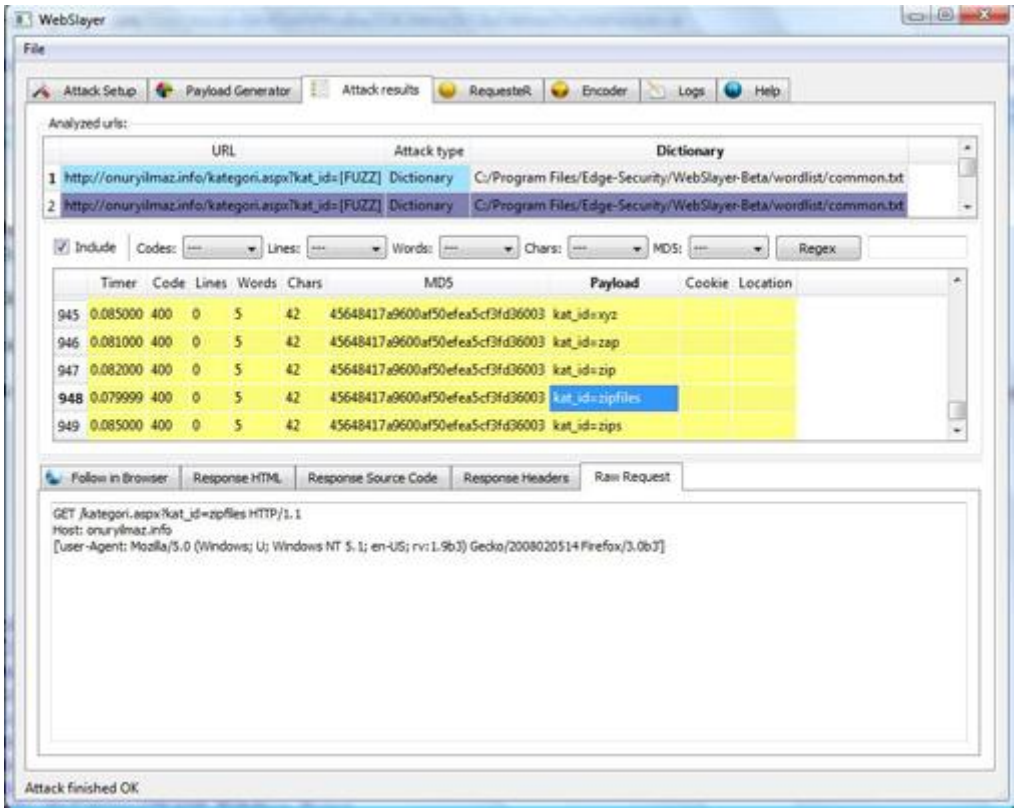
WebSlayer`ın bünyesinde barındırdığı özellikler ise;

- Encoding desteği,
- Get, post ve header`lara yönelik ataklar,
- Authentication desteği,
- Payload desteği,
- Proxy desteğiyle gizlilik,
- Filtreleme,
- Multi Threading olarak sıralanabilir.

WebSlayer ile alakalı detaylı bilgilere proje sayfasından ulaşabileceğiniz gibi [9], belirlenen parametreye seçilen wordlist`teki değerleri post etmek için gerekli temel konfigürasyonları ve test sonuçlarını da görebilirsiniz.



Şekil -1: Konfigürasyon



Şekil - 2: Dönen Sonuçlar

Referanslar

[1] http://en.wikipedia.org/wiki/Black-box_testing
[2] http://docs.google.com/View?id=d4w2g9c_5hc6m7vgj
[3] http://www.owasp.org/index.php/OWASP_Testing_Guide_Appendix_C:_Fuzz_Vectors
[4] http://www.informit.com/store/product.aspx?isbn=0321446119
[5] http://www.dragoslungu.com/2007/05/12/my-favorite-10-web-application-security-fuzzing-tools/
[6] http://code.google.com/p/fm-fsf/
[7] http://code.google.com/p/fm-fsf/w/list
[8] http://code.google.com/p/webslayer/downloads/list
[9] http://www.owasp.org/index.php/Category:OWASP_Webslayer_Project