

# Fuzz Testing

İsmail Dönmez, [ismail@pardus.org.tr](mailto:ismail@pardus.org.tr)

6 Mayıs 2007

## Yazılımlar neden bu kadar güvensiz?

- İnsanların güvenliği düşünmemesi
- Gün geçtikçe gelişen güvenlik açığı bulma metodları
- 0-Day Konsepti

## Güvenlik neden hep ikinci planda?

- Kötü niyetli kullanıcı yoktur fikri
- Kapalı kodlu yazılımda güvenlik açığı zor bulunur düşüncesi
- Projelerin zaman açısından kısıtlı olması

## Yeni geliştirilen güvenlik açığı bulma metodları

- Fuzz Testing ( Bu sunumun amacı!)
- Otomatik güvenlik açığı testi (Metasploit, Own the shell)
- Pen Testing

## 0-Day (Zero Day)

- Windows Vista'da açık bulmak 300 dolar ve üzeri
- Zero Day Initiative (ZDI) , 3COM
- iDefense, eEYE ve diğer benzeri şirketlerin programları

## Fuzz Testing'in kısa hikayesi

- Bilinen ilk kullanımı 90'ların başında
- Wisconsin Üniversite'sinde 1990 yılında yapılan Fuzz Testing çalışmasında **2000**'e yakın hata bulundu
- Hatalı programlar arasında **df,ls,login(!)** gibi konsol programları vardı

## Fuzz hayatımıza nasıl girdi?

- Month Of Kernel Bugs (2007)
- 30 gün içinde 30 kritik güvenlik açığı
- Linux çekirdeğinde 11, MacOSX çekirdeğinde 9 güvenlik açığı
- Fuzz testing artık aydınlığa çıktı
- Month of XXX Bugs konsepti başladı

## Programlar nasıl exploit edilir?

- Programı çökert
- Program çöktüğü anda kontrolü ele geçiren bir program yaz (exploit)
- Profit!

## Fuzz Testing nasıl çalışır?

- Programa doğru gibi gözükten rastgele input gönder
- Bunu otomatikleştirip başarı şansını arttır
- Program çöktüğü anda bir exploit şansı doğar

## Fuzz Testing başarı hikayeleri

- Month of Kernel Bugs, 30 kritik güvenlik açığı
- Month of Apple Bugs, 1'i hala çık 31 kritik güvenlik açığı
- Firefox 2.0.0.3'ün çıkışının ertelenmesine sebep olan hatalar (Michal Zalewski)
- Tek ortak noktaları: Fuzzed!

## Fuzz Testing neden bu kadar başarılı?

- Programcılar sadece olağan inputları test ediyor
- Otomatik!
- Hızlı!
- İnternette birden fazla fuzz testing programı var

## Enter ZZUF

- Samuel Hocevar tarafından yazılmış bir fuzz programı
- İlk çıkışında MPlayer, FFmpeg, VLC olmak üzere birçok multimedia programında onlarca açık buldu
- Özgür yazılım (DWTFYWTPPL lisanslı)
- <http://sam.zoy.org/zzuf>

## Elleri kirletme zamanı

```
[cartman@southpark] [02:14:17]
[~]> zzuf -s0:1500 -r0.01 -c2 file /bin/ls
/bin/ls: ERROR: Cannot allocate memory for note
/bin/ls: ERROR: Cannot allocate memory for note
/bin/ls: ERROR: Cannot allocate memory for note
/bin/ls: ERROR: Cannot allocate memory for note
/bin/ls: ERROR: Cannot allocate memory for note
/bin/ls: ERROR: Cannot allocate memory for note
```

## Seçenekleri biraz daha inceleyelim

- -s 0:1500 , 0 ile 1500 arası rastgele bir seed kullan
- -r0.01 , dosyanın sadece yüzde birlik kısmını fuzz et
- -c2 , program iki kere çöktükten sonra çık

## Referanslar

- ZZUF, <http://sam.zoy.org/zzuf>
- Fuzz Revisited,  
<ftp://www.cs.wisc.edu/paradyn/fuzz-revisited/>
- Metasploit , <http://www.metasploit.org>
- MOKB, <http://projects.info-pull.com/mokb/>
- MOAB, <http://projects.info-pull.com/moab/>

Ohhhh ya!

Sorularınız?