LinkedIn: Kelvin Kimotho

Solution

This challenge required the knowledge of how to interfere with session cookies. I accessed the website first.
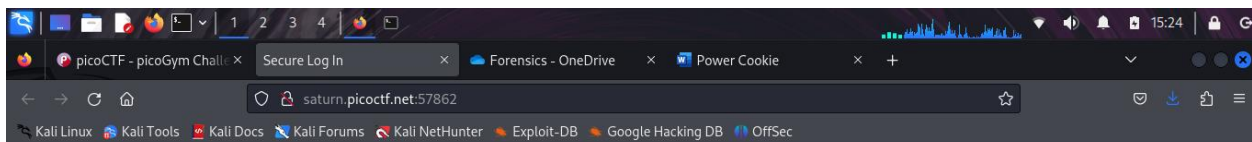
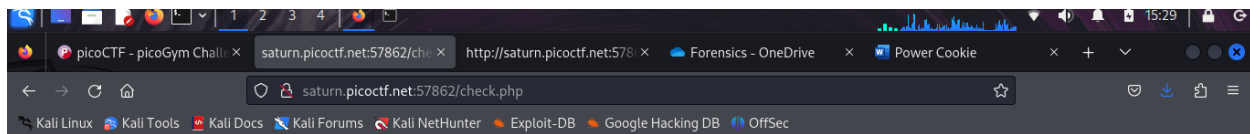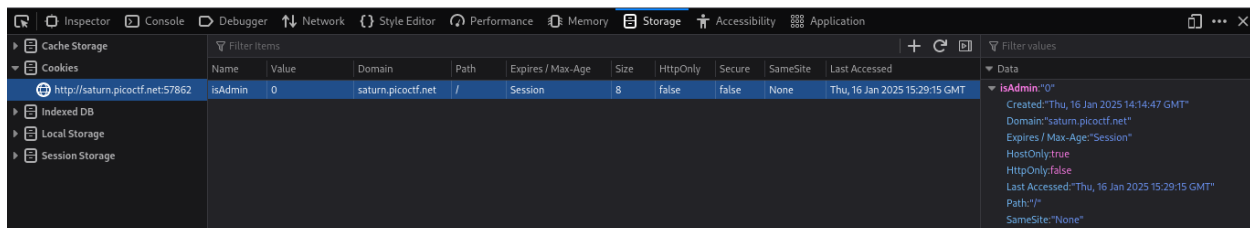I examined the website source code where guest.js file gave me a hint that an admin had cookie value of 0.
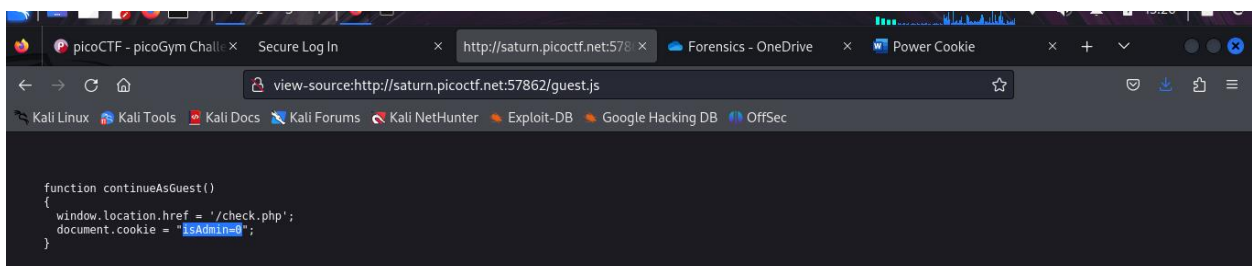
I went ahead modify the cookie values randomly and a cookie value of 1 gave me the flag.

We apologize, but we have no guest services at the moment.

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
isAdmin	0	saturn.picoctf.net	/	Session	8	false	false	None	Thu, 16 Jan 2025 15:29:15 GMT

▼ isAdmin:"0"
  Created:"Thu, 16 Jan 2025 14:14:47 GMT"
  Domain:"saturn.picoctf.net"
  Expires / Max-Age:"Session"
  HostOnly:true
  HttpOnly:false
  Last Accessed:"Thu, 16 Jan 2025 15:29:15 GMT"
  Path:"/"
  SameSite:"None"

I changed the value to 1 then refreshed the page and that's how i found the flag

picoCTF{gr4d3_A_c00k13_65fd1e1a}.

picoCTF{gr4d3_A_c00k13_65fd1e1a}

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
isAdmin	1	saturn.picoctf.net	/	Session	8	false	false	None	Thu, 16 Jan 2025 15:31:13 GMT