LinkedIn: Kelvin Kimotho

Description

Can you get the flag?

Additional details will be available after launching your challenge instance.

instance on demand.
Its current status is:
NOT_RUNNING

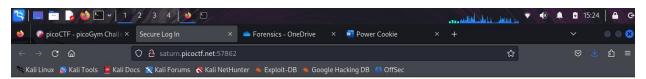
Launch
Instance

Hints ?

Do you know how to modify cookies?

Solution

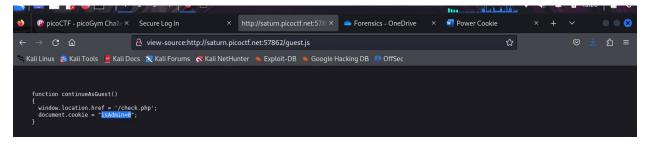
This challenge required the knowledge of how to interfere with session cookies. I accessed the website first.



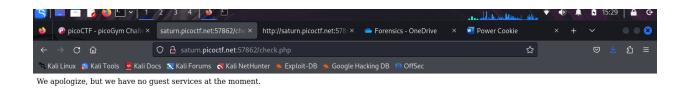
Online Gradebook

Continue as guest

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.



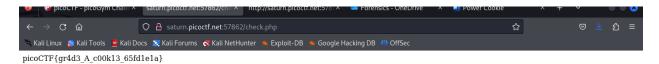
Canal Control Console
Debugger
↑ Network
() Style Editor
C) Performance
() Memory
Storage
† Accessibility
※ Application

Cookies
Name
Value
Domain
Path
Espires / Max-Age
Size
Http://statum.picoctf.net-S7862
Last Accessed
✓ Data

Thtp://statum.picoctf.net-S7862
Is Admin
0
saturn.picoctf.net
/ Session
8
false
None
Thu,16 Jan 2025 15:29:15 GMT

Domain: Statum.picoctf.net
Path
Session Storage
Session Storage
Http://statum.picoctf.net
Path
Session Storage
Http://statum.picoctf.net

I changed the value to 1 then refreshed the page and that's how i found the flag picoCTF{gr4d3_A_c00k13_65fd1e1a}.



Character
Console
Debugger
↑ Network
() Style Editor
Q Performance
⊕ Storage
↑ Accessibility
※ Application
⊕ Application

⊕ Codeke Storage
Value
Domain
Path
Expires / Max-Age
Size
Http/Only
Secure
SameSite
Last Accessed

⊕ Indexed DB
⊕ Indexed DB
⊕ Code Storage
None
Thu, 16 Jan 2025 15:31:13 GMT

**Bession Storage*

**Bession Storage*

**Bession Storage*

**Bession Storage*

**Accessibility
※ Application
● Storage
† Accessibility
※ Application

• Path
Expires / Max-Age
Size
HttpOnly
Secure
SameSite
Last Accessed

• Balse
False
None
Thu, 16 Jan 2025 15:31:13 GMT