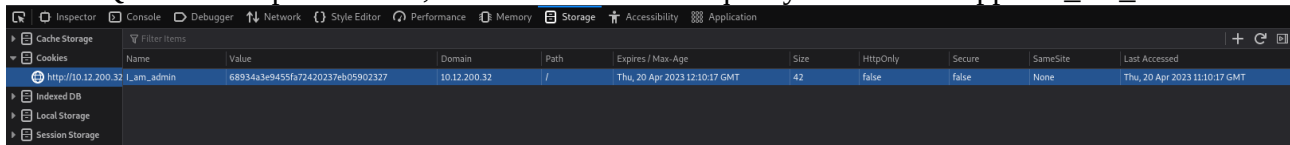


Cookie Forgery

L'idée est modifier voir meme de créer un cookie qui simule la connexion à un compte sur le site

Exploration

Quand on inspecte le site, on découvre très vite qu'il y a un cookie appelé I_am_admin



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
I_am_admin	68934a3e9455fa72420237eb05902327	10.12.200.32	/	Thu, 20 Apr 2023 12:10:17 GMT	42	false	false	None	Thu, 20 Apr 2023 11:10:17 GMT

Offensive

On remarque rapidement l'attribut "secure" dont la valeur est "false". La valeur du cookie est « false » en md5 : <https://md5.gromweb.com/?md5=68934a3e9455fa72420237eb05902327>

On change cette valeur par « true » en md5 : b326b5062b2f0e69046810717534cb09
on charge une nouvelle page.

Faille

L'existence d'un cookie propre à la connexion lors de la « simple visite »

Mitigation

Ne pas mettre de nom aussi évident à un cookie, ne pas un créer un juste à la visite mais au pire une fois la connexion établie et uniquement par rapport au compte sur lequel on est connecté et non à un quelconque compte admin. Mettre une durée de vie aux cookies.

Sources

- <https://md5.gromweb.com/?md5=68934a3e9455fa72420237eb05902327>