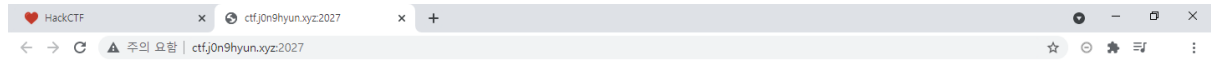


Cookie




개꿀맛 쿠키



들어가보면 맛있는 쿠키가 보인다. 제목이 쿠키니까 쿠키 값을 확인해보자!

개꿀맛 쿠키



Application

Manifest

Service Workers

Storage

Local Storage

Session Storage

IndexedDB

Web SQL

Cookies

Trust Tokens

Cache

Cache Storage

Application Cache

Background Services

Background Fetch

Background Sync

Notifications

Payment Handler

Periodic Background Sync

Push Messaging

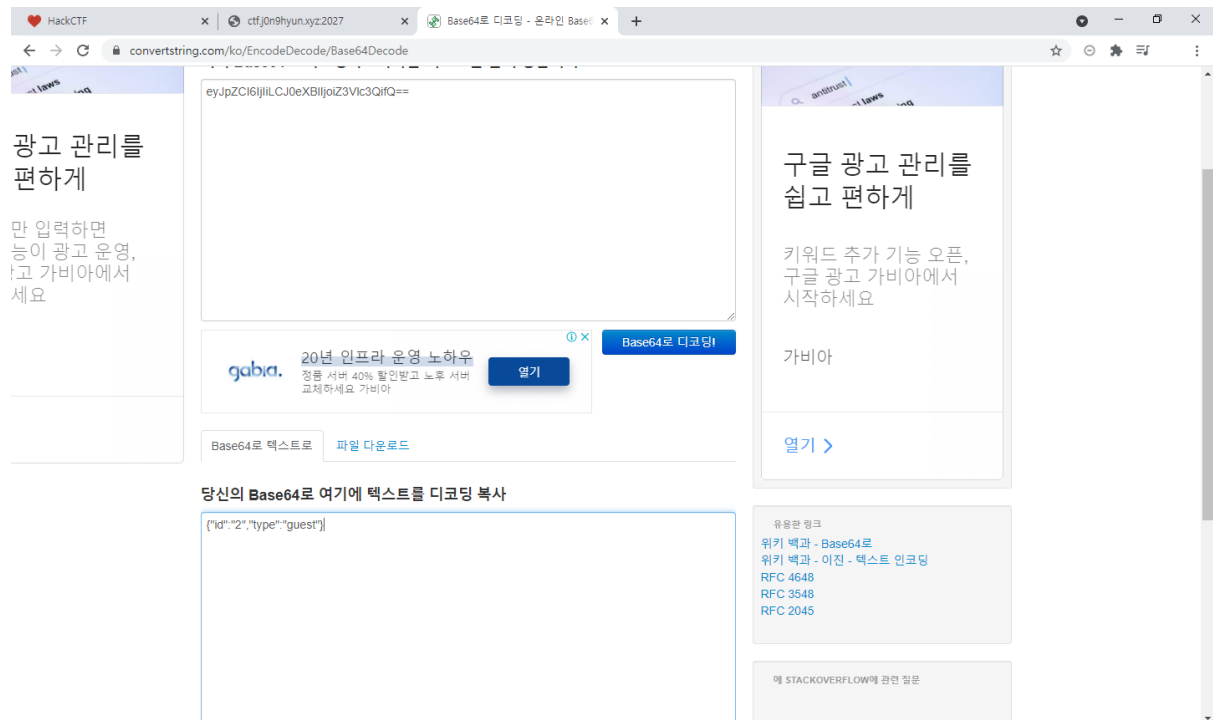
Frames

top

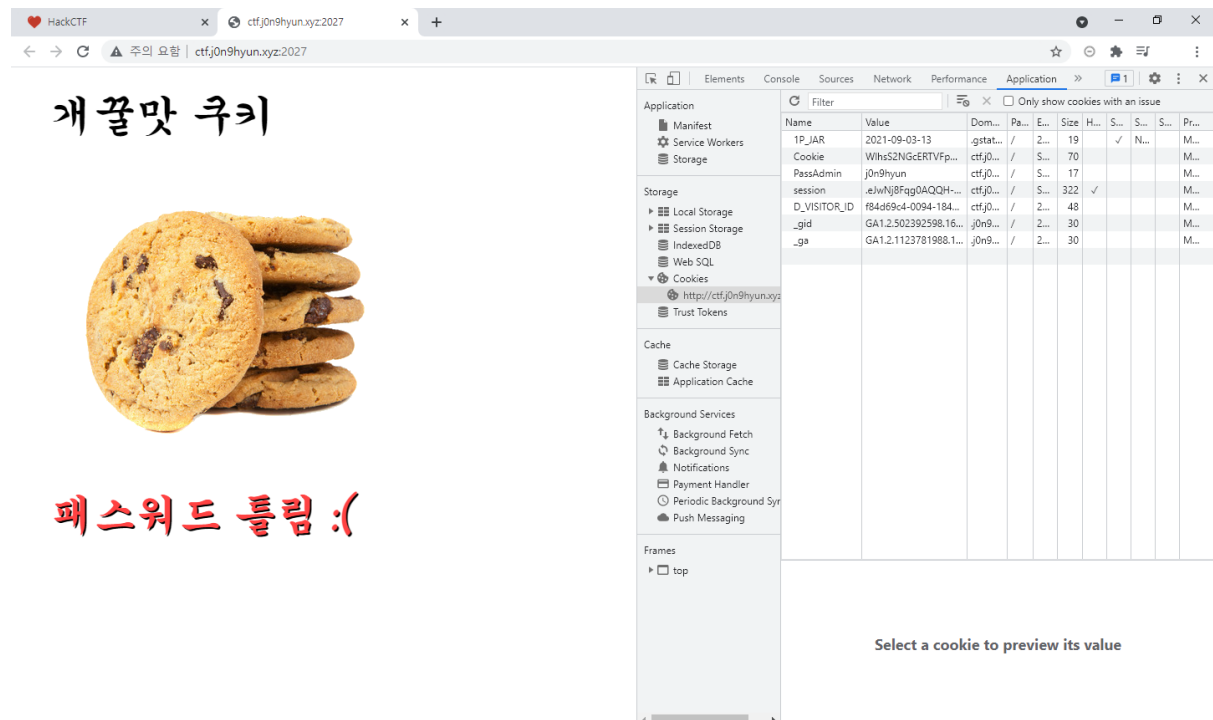
Name	Value	Dom...	Pa...	E...	Size	H...	S...	S...	Pr...
PassAdmin	j0n9hyun	ctfj0...	/	S...	17				M...
session	eJwNj8Fgg0AQQH...	ctfj0...	/	S...	322	✓			M...
_gat_gtag_U...	1	j0n9...	/	2...	25				M...
_gid	GA1.2.502392598.16...	j0n9...	/	2...	30				M...
_ga	GA1.2.1123781988.1...	j0n9...	/	2...	30				M...
D_VISITOR_ID	F84d69c4-0094-184...	ctfj0...	/	2...	48				M...
Cookie	WltzS2NGcERTVfp...	ctfj0...	/	S...	70				M...
1P_JAR	2021-09-03-13	.gstat...	/	2...	19		✓	N...	M...

Select a cookie to preview its value

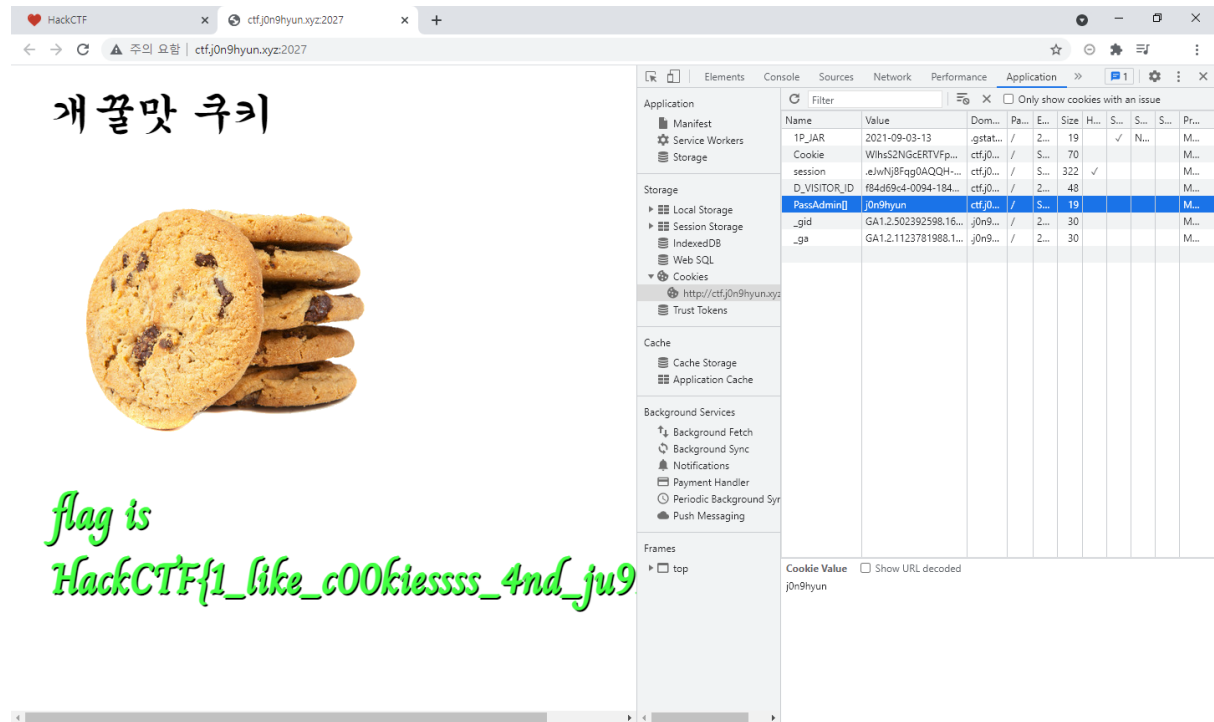
쿠키 값이 암호화 되어 있는 것 같아서 base64 복호화를 해봤다 3번정도 디코딩 하니까 다음과 같은 문자열이 나온다.



디코딩 한 값이 `{"id":"2","type":"guest"}`이므로 `{"id":"1","type":"admin"}`을 3번 인코딩하여 쿠키값에 넣어주자.



넣어주고 나서 f5로 새로고침하면 패스워드가 틀렸단다. Passadmin이라는 쿠키 값이 보이는데 우리가 저 값을 알 리가 없다. 아마도 strcmp의 취약점을 이용하면 될거 같다. 간단히 말하면 배열을 인자로 넣으면 무조건 pass되는 것이다. 그래서 Passadmin을 배열로 바꿔서 새로고침하면 답을 알 수 있다.(Passadmin[])



개꿀맛 쿠키

flag is
HackCTF{1_like_c00kiessss_4nd_ju9

Name	Value	Domain	Path	Expires	Size	HttpOnly	Secure	Session	Priority
1P_IAR	2021-09-03-13	.gstat...	/	2...	19			✓	N...
Cookie	WlHs5ZNGcERTVfp...	ctfj0...	/	S...	70				M...
session	.eJwNj8Fgg0AQQH...	ctfj0...	/	S...	322			✓	M...
D_VISITOR_ID	f84d69c4-0094-184...	ctfj0...	/	2...	48				M...
PassAdmin[]	j0n9hyun	ctfj0...	/	S...	19				M...
_gid	GA1.2.502392598.16...	j0n9...	/	2...	30				M...
_ga	GA1.2.1123781988.1...	j0n9...	/	2...	30				M...

Cookie Value: j0n9hyun