help with session key on project 2

You are subscribed. Unsubscribe

UNRESOLVED

sessionnKeyDecodingPassword × + Add Tag

Sort replies by: Oldest first Newest first Most popular

Karen West . 4 hours ago

Note: This is NOT the real password on KarenWest15@gmail.com in session key decoded below:
Session Key:

SSOid=S2FyZW5XZXN0MTVAZ21haWwuY29tOmExNTgyYTRkOTdhMjM0M2NhZWFmM2ZiMTc3OTIxNTEyOkth%0AcmVuIFdlc3Q6VQ%3D%3D%0A

Base 64 Decode of above session key:
KarenWest15@gmail.com:a1582a4d97a2343caeaf3fb177921512:KaÐ&VâvW7C¥PÜ=ÃÐ

Session Keys:
First Field: email address -- KarenWest15@gmail.com
Second Field: MD5 hash of password -- I used: KarShayAlbany65 (15 bytes) -- MD5 hashed ??
Thrid Field: userID -- ??
Fourth Field: role -- ?? -- U (common user, not admin) ??

Second Field (MD5 hash of password: a1582a4d97a2343caeaf3fb177921512)

gave: 25 8c b3 e2 28 e7 5b 57 06 18 8a e6 23 2d b2 8d (16 bytes -- my password is 15 bytes - so is it a carriage return at end?)
Looking at ASCII chart - some bytes make no sense - since ASCII only goes to 0x7F in the table of valid chars.
So for chars not in ASCII table I put ? below:
From ASCII table, I get: % ? ? ? (? [W ACK(acknowledge) CAN(cancel) ? ? # - ? ?

From Extended ASCII table, I get: % (Latin capital ligature OE) (Superscript three - cubed)
(Latin small letter a with circumflex) (Latin small letter c with cedilla) [W ACK(acknowledge) CAN(cancel)
(Latin capital letter S with caron) (Latin small letter ae) # - (Superscript two - squared) (nothing for byte 16)

UTF-8 encoding table and Unicode characters -- don't help either.

If someone could help lead me in the direction of where I'm going wrong to obtain the 2nd field of the session key - which should be according to the quiz --the MD5 encoded password I wrote above (not my real password for this account so no worries there).

I ran the 2nd field (after the first colon, before the 2nd colon) through the MD5 hash and it gave what I shared above. I tried to see what that meant to see how it could be my password and it made no sense. If you have any ideas here, please let me know. Thank you!

↑ 0 ↓ · flag

 Karen West . 4 hours ago

Actually - I meant session cookie in the subject part of the question. ;-)

I did forget to ask however another part of this question - once I deciper the session cookies's parts - how do you know the name of the key for the session cookie? Where do you find that?

↑ 0 ↓ · flag

Anonymous . 3 hours ago

Hint: A cookie consists of a **key:value** pair
You are staring right at the answer ;)

↑ 0 ↓ · flag

 Karen West . 2 hours ago

So when you enter the answer, you enter the base 64 decoded key? My email address?
I'm guessing you just write the words "email address" as the key? Thanks for clarifying the format: XXX:YYY:ZZZ, and I'm assuming the key part is the first field, the email address.

↑ 0 ↓ · flag

Anonymous . an hour ago

Nope! Like I said you are staring right at the answer.

You might want to re-watch a couple of videos relating to this topic, because you are using the wrong terminology(in your OP) ;)
I suggest you also take a look at the HTTP headers and see what a cookie is.

↑ 0 ↓ · flag

 Karen West . 33 minutes ago

I actually did that 2 days ago - and what I found was the server returns to the client:
set-cookie: key = value; options; ...
set-cookie: edition = us; expires = Wed, 18-Feb-2015 08:20:34 GMT; path = /; domain = .zdnet.com
This lecture video / notes said that "edition" was a key and "us" was a value. expires tells you how long the cookie can be used, the cookie is only good in the domain of .zdnet.com and the client should send any future requests to <domain>/<path>, and it is also available to any resource within subdirectory of /.

I then saw that the HTTP header from server to client on first visit was:
set-cookie: edition=us; expires = ...
set-cookie: session-zdnet_production = 590b97fpinqe4bg6lde4dvvqll; path = /; domain = zdnet.com

and on a sub-sequent visit the HTTP header was:
http://zdnet.com/

GET/HTTP/1.1
Host: zdnet.com
o
o
o
Cookie: session-zdnet_production = 590b97fpinqe4bg6lde4dvvqll; zdregion = MT15LjlumT15LjEMzplczpjZDJmNW

I know that in the case of the session cookie, after you authenticate, subsequent actions provide the cookie (so you do not have to authenticate each time).

However - I'm still not sure what I'm supposed to enter for the answer to the question on the bad store quiz, the key name of the session cookie, and the key name of the cart cookie.

Would it be something like (for session cookie key): session-emailAddress,
or for the cart cookie's key: cart-integer ??

Have I already reviewed what you were recommending from lecture, or is this it, and I should know the answer of what to write from the above? I looked at the slides from the lecture video I watched awhile back for the above.

Sorry - it seems that I'm the only person in this class who does not understand these things that well!

↑ 0 ↓ · flag

+ Comment

Anonymous . 4 hours ago

You already identified the fields after decoding the base64 string. As far as I remember, you don't need to do anything further...

I see that you are somewhat confused about the md5 hash
a1582a4d97a2343caeaf3fb177921512 is the md5 hash of **KarShayAlbany65**

You need to *decrypt* the hash to get back your password.
Instead, it seems that you hashed **a1582a4d97a2343caeaf3fb177921512** using md5 to **258cb3e228e75b5706188ae6232db28d.**
Which is why it isn't making any sense.

0 · flag

 Karen West . 2 hours ago

Thank you. I am guessing that we have no means to decrypt (?), and with the help I've been given here, I believe the key is the first field in the cookie, the email address, which is all we need to answer the question, not to decrypt the password or any of the other fields in this cookie?

0 · flag

+ Comment

New post

To ensure a positive and productive discussion, please read our forum posting policies before posting.

B | I | Link | <code> | Pic | Math | Edit: Rich | Preview

Resolve thread

This thread is marked as unresolved. If the problem is fixed, please check the above box and make a post to let staff know that they no longer need to monitor this thread.

Make this post anonymous to other students

Subscribe to this thread at the same time

Add post