Forums / Assignments Help

project 2 - found some info - any hints on where to go next with it?

✉ You are subscribed. Unsubscribe

? UNRESOLVED

project2Help × + Add Tag

Sort replies by: Oldest first Newest first Most popular

Karen West · 2 days ago

Hi,
I finally started project 2 yesterday and found some information and I'm not really sure where it is leading me, and any hints within the honor code would help at this point - I'm new to the web world.

Queston: Using the Firefox developer tools, I tried to bring up the inspector to modify the login page, and at the hidden field for example "U" in the role section to an "A" but I found I could not modify code - can you modify code?

By poking around I also found info. and I'm wondering where to go next with it - any hints within honor code would be appreciated.

I found within the www.badstore.net/robots.txt web crawler file that there was a directory called "suppliers" and when I took those 4 entries and ran them through the base64 decoder, I found this:

×M5joeuser/password/platnum/192.168.100.56
×M6kroemer/s3Cr3t/gold/10.100.100.1
×M7janeuser/waiting4Friday/172.22.12.19
×M8kbookout/sendmeapo/10.100.100.20

I found no help from this within the supplier login - any hint would be helpful here within honor code!

All the other directories in robots.txt did not lead me to any information. Should they? cgi-bin and upload had nothing. scanbot had some code I did not understand. backup took me to the bad store web page.

```
# /robots.txt file for http://www.badstore.net/
# mail webmaster@badstore.net for constructive criticism

User-agent: badstore_webcrawler
Disallow:

User-agent: googlebot
Disallow: /cgi-bin
Disallow: /scanbot # We like Google

User-agent: *
Disallow: /backup
Disallow: /cgi-bin
Disallow: /supplier
Disallow: /upload
```

In the bad store manual, for the guest book page, it recommended entering some XSS scripts, and the last one is the longest, and that produced this on the bad store web page - some people who had signed the guest book, and it recommended attempting to find out info. using their login name - yet I found nothing.

Guestbook
Wednesday, February 18, 2004 at 07:42:34: Joe Shopper joe@microsoft.com

This is a great site! I'm going to shop here every day.

Wednesday, February 18, 2004 at 11:41:07: John Q. Public jqp@whitehouse.gov

Let me know when the summer items are in.

Friday, February 20, 2004 at 14:05:22: Big Spender billg@microsoft.com

Where's the big ticket items?

Sunday, February 22, 2004 at 06:16:05: Evil Hacker s8n@haxor.com

You have no security! I can own your site in less than 2 minutes. Pay me $100,000 US currency by the end of day Friday, or I will hack you offline and sell the credit card numbers I found on your site. Send the money
direct to my PayPal account.

Another time after I had tried many, many things, so I'm not sure what state badstore was in, I went back to the guest page, entered that same script, and this time an SSOid (cookie) popped up in a little window:

SSOid=S2FyZW5XZXN0MTVAZ21haWwuY29tOjc4MjZjNTEyODk1NGU3YzQ3YjRmY2U0YzkxMzdiMTM1Okth%0AcmVuIFdlc3Q6VQ%3D%3D%0A

I heard that cookie's use MD5 to hash, and when I ran it through that, it gave: 98aa5b76ca22cbc5ccf7b7dfd6ae6605

Can I use that to get info. in some way? Also, how to I get that into the required format of: XXX:YYY:ZZZ:U

How do I know the key of session cookie?
Or is this the cart cookie? If not, any hints on how to find the cart's cookie?

I then did a grep of the file (in the bash shell):
grep admin userdb.MYD

thinking that might give some info from the database file on the badstore VM bash trinux shell:
And that gave me:
System AdministratorA5EBE2294ECD0E0F08EAB7690D2A6EE69black

So I took the hex part:
A5EBE2294ECD0E0F08EAB7690D2A6EE69 (hex)

and that in decimal is:
413545424532323934454344304530463038454142373639304432413645453639 (decimal)

and I thought - could black be a password when I login as admin (no!)
black

So then I ran the hex numbers through:
98e00737aa80919ca5681e801f6111c5a69d7be5 (SHA1 hash of hex)
4554f40afc0b0c9845e6e9c28d0ec820 (MD5 hash of hex)

But I did not know what this would mean, if anything!

I understand that the hidden field on the login page is the "role" and you would want to modify it's value to be "A" for admin privilege, but I could figure out how you could do that.

I tried some SQL injection by entering the tick mark after the login name:
joe@supplier.com' OR 1=1); --
but that did not work as they said it would.

I tried in the quick item search and it always responded with this error message that when I tried to tweak to match what the column headers were in the WhatsNew page, none worked--always this type of error:
SELECT itemnum,sdesc,ldesc,price FROM itemdb WHERE 'Item' IN (itemnum,sdesc,ldesc)

The assignment recommended using the quick item search, but I got nowhere with that.

I saw how to get into the admin portal by modifying the action in the URL to be admin, and I saw all the different actions you can do as admin, but I could not do any of them without the admin privilege.

I saw on the What's New page that there were 8 items on display for sale you could put into your cart, but I'm guessing there are some hidden items, since I did not use any tricks to find that answer.

For the operations that suppliers can do, I logged in and saw that you can:
-upload price lists to badstore.net
-view pricing file on badstore.net
But I had no idea how to find the info. that asked us to find the credit card number joe@supplier.com used for his $46.95 purchase.

Any help within the honor code appreciated! Thank you.

↑ 1 ↓ · flag

Federico Violante · 2 days ago

Hi Karen, first of all, keep calm.

To correctly break the logon, you are using the wrong syntax. You need a well specified record, not ANY record. Watch carefully what you are querying (isn't obvious, I know),

I think you can also break the account in a semi-legitimate way, if you try to reset the password (or else guess it, there are some

"easy" passwords, just a little stronger than most routers' default).
If you become an admin, you can solve all almost of your problems trough the admin menu. There are interesting functions there.

You need (I think) SQL injection only to discover how many products are in the list, but you don't need to logon for this. I don't have BadStore at hand now, but if I remember well, you can find something interesting in the "What's new" page. Also, you had identified the "role" field, try to use it, make an account and then....

It's not much, but is a good starting point, hopefully not in violation of the honor code.

🡅 0 🡇 · flag

+ Comment

Anonymous · 2 days ago

How do I know the key of session cookie?
Or is this the cart cookie? If not, any hints on how to find the cart's cookie?

SSOid=S2FyZW5XZXN0MTVAZ21haWwuY29tOjc4MjZjNTEyODk1NGU3YzQ3YjRmY2U0YzkxMzdiMTM1Okth%0AcmVuIFdlc3Q6VQ%3D%3D%0A

Suggest you review the class notes about key=value.

This will give you the answer for the session key above.

For the cart cookie, you need to check an item to add to your cart and then re-examine your cookie.

You should see two key value pairs.

I think the key for the cart will be very obvious.

↑ 0 ↓ · flag

David F. · 6 hours ago 🔗

Watch out what info you've posted here, Karen! ;)

↑ 0 ↓ · flag

Karen West · 5 hours ago 🔗 ⚙

Why? Are there clues I should not have shared that violate honor code? I guess I don't know enough about what I did and posted to even know that. ;-) I'm still working on it but right now working on getting the quiz that is due tomorrow completed, and then will come back to this. I'm the type student whose obligations are mostly elsewhere with having to borrow a Win7 lap top to do the projects from my 11 year old son, since I could not get them to work on SUSE Linux for some reason (and I know they should have!) My 9 and 11 year old children have been interrupting more than usual with 3 half days last week for parent teacher conferences and this upcoming week 3 days off for Thanksgiving! So I do the best I can. But it sounded to me like something I posted would be helpful to those who like me have not yet completed project 2 that is due tomorrow (are there any students left that have not submitted it yet?) On my end--feels like no--since most posts to the forum that go by are about either future weeks quizzes or the next project - but I don't let it intimidate me, and work hard with the time that I have. I got project 1 to work the night before so hopefully the same will happen for project 2 - we'll see! I have not yet heard from anyone that anything I posted should be "watched out about the info. I posted" !! ;-)

↑ 0 ↓ · flag

Stewart Bell · 5 hours ago 🔗

I think David is referring to the session cookie you posted, more in terms of your own online security than of any honour code violation. When decoded it reveals your (real?) gmail address and encrypted password.

If you didn't use a real gmail account and password then all is okay. Otherwise it might be worth changing your gmail password. Not sure if the encrypted password can be decoded, but.. you know.. just to be on the safe side!

Have you gained admin on the BadStore yet?

↑ 0 ↓ · flag

+ Comment

Dmitry Dulepov Signature Track · a day ago

To find the session cookie, you need the session. To find the cart cookie, you need..... what?

↑ 0 ↓ · flag

+ Comment

Adam Chmielowiec Signature Track · 5 hours ago

as for the ssoid you need to get that id through http://ostermiller.org/calc/encode.html or other calculator to get any meaningful data from it. to get the list of items you can run sql injection attack on the item search field.If you dont know what to type in you might check youtube and badstore manual, it will take you max 5 minutes. to login as an admin to have its priveledges you can also do the same but in other field, you probably know which. All in all you can check youtube videos on badstore and articles on the internet. Those might be very helpful. Oh and how to get a cart cookie. Thing is its way easier than everybody think and describe it is. If you are having recent internet explorer you can click f12 on your keyboard, enter console and type document.cookie and press enter. If you will run this while having something added to the cart you will be supplied with two cookie id's session id and cart id

↑ 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