**Question 1 - regular expression**

One of the BadStore pages has a hidden form field that establishes a new user’s privilege level. What is the name of this field?

\*A: ([Rr]ole)

Feedback: This field is on the page used to make a new user account

Default Feedback:

**Question 2 - numeric**

How many items for purchase are in BadStore’s database? Use SQL injection on the quick search form field to find out.

\*A: 16.0

Feedback: SQL injection shows there are more items than just those shown on the "What's New?" page

B: 15.0

Feedback: SQL injection shows there are more items than just those shown on the "What's New?" page. You would get 15 if you didn't count the Test item.

Default Feedback:

**Question 3 - checkbox, shuffle, partial credit**

Which of the following operations are suppliers permitted to do? Use SQL injection to bypass authentication, or find a way to create an account as a supplier.

\*A: Upload price list

Feedback: This option is on the "for suppliers only" page

\*B: View existing price list

Feedback: This option is on the "for suppliers only" page

C: Download an activity report

D: Submit monthly bill payment

E: Cancel contract

**Question 4 - regular expression**

Log in as $$\color{red}{\verb|joe@supplier.com|}$$ — this is possible in a variety of ways, including SQL injection. Then look at his previous orders and answer the question: What credit card number did he use to make a purchase of $46.95 (multiple answers are possible, but we will accept all of them) ?

\*A: (4111[- ]\*1111[- ]\*1111[ -]\*1111)

\*B: (5500[- ]\*0000[- ]\*0000[ -]\*0004)

\*C: (3747[- ]\*1000[- ]\*0000[- ]\*0000)

\*D: (4217[- ]\*6399[- ]\*5237[- ]\*2130)

Default Feedback:

**Question 5 - text match**

Get admin privileges and then use the $$\color{red}{\verb|admin|}$$ action to look at the user database. There are two users whose emails have the form *XXX*$$\color{red}{\verb|@whole.biz|}$$; what is the *XXX* portion of **either (but not both)** of the two users? For example, if one of the users is $$\color{red}{\verb|jackie@whole.biz|}$$, the right answer is $$\color{red}{\verb|jackie|}$$. (The answer is case-sensitive.)

\*A: landon

\*B: fred

C: landon fred

Feedback: we only asked for one of them

D: fred landon

Feedback: we only asked for one of them.

Default Feedback:

**Question 6 - regular expression**

BadStore uses cookies to implement *session keys*, once you’ve authenticated, and to track the *contents of the cart*, once you’ve added something to it. You can inspect these cookies in use by BadStore in various ways. One way is to do an XSS attack on the guest book. Get the guest book to run the code $$\color{red}{\verb|<script>alert(document.cookie)</script>|}$$ and it will tell you the current cookies. (Be sure you have popups enabled on your browser or this won’t work.) Alternatively, you can examine the cookies directly using Firefox developer tools. Recall that cookies are pairs *key*=*value*. What is the key name of the session cookie?

\*A: (SS[O0][iI][dD])

Default Feedback:

**Question 7 - regular expression**

BadStore uses cookies to track the *contents of the cart*, once you’ve added something to it. What is the key name of the cookie used for the cart?

\*A: (Cart[Ii][Dd])

Default Feedback:

**Question 8 - checkbox, shuffle, partial credit**

BadStore’s session cookie format is poorly designed because it is uses a predictable structure. In particular, it is an encoded string (with a URL-encoded newline at the end) of concatenated fields separated by colons, i.e., of the form *XXX*:*YYY*:*ZZZ*:etc. Which of the following are the fields that it uses?

\*A: e-mail address

Feedback: This is the first field

\*B: MD5 hash of password

Feedback: This is the second field

C: SHA1 hash of password

Feedback: The password hash uses MD5, not SHA1

\*D: full name

Feedback: This is the third field

E: expiration timeout

Feedback: This is not part of the cookie

\*F: role

Feedback: This is the fourth field

G: integer that counts the number of times ever logged in

Feedback: This is not part of the cookie

H: the number of failed login attempts

Feedback: This is not part of the cookie

**Question 9 - numeric**

BadStore’s cart cookie is also an encoded string with a predictable structure *XXX*:*YYY*:*ZZZ*:etc., and it probably contains information it shouldn’t. Which field (where fields are numbered starting at 1) of the decoded string could an attacker change to give himself a discount on an item’s price?

\*A: 3.0

Feedback: The first field is an integer, the second is the number of items in the cart, and the third is the total price of those items

Default Feedback: