# Feedback — BadStore quiz

Help

You submitted this quiz on **Sun 23 Nov 2014 2:14 PM PST**. You got a score of **14.00** out of **34.00**. You can attempt again, if you'd like.

### **Question 1**

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?

#### You entered:

role

Your Answer		Score	Explanation
role	~	3.00	This field is on the page used to make a new user account
Total		3.00 / 3.00	

#### **Question 2**

### **Question 3**

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.

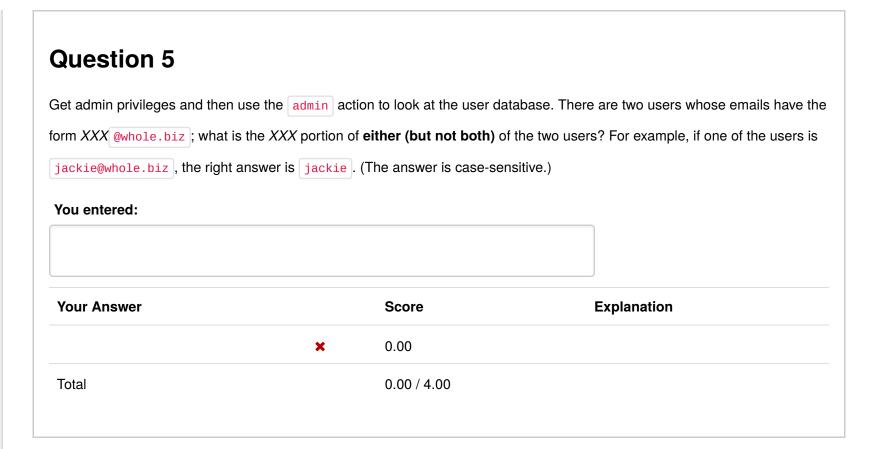
Your Answer		Score	Explanation
View existing price list	•	1.00	This option is on the "for suppliers only" page
Cancel contract	~	1.00	
Download an activity report	~	1.00	

Submit monthly bill payment	~	1.00	
Upload price list	<b>~</b>	1.00	This option is on the "for suppliers only" page
Total		5.00 / 5.00	

Log in as <code>joe@supplier.com</code> — 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)?

#### You entered:

Your Answer		Score	Explanation
	×	0.00	
Total		0.00 / 4.00	



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 <script>alert(document.cookie)</script> and it will tell you

the current cookies. (Be sure you have pop	ups enable	ed on your browser or this won't wo	ork.) Alternatively, you can examine the
cookies directly using Firefox developer too	ls. Recall	that cookies are pairs <i>key=value</i> . V	Vhat is the key name of the session
cookie?			
You entered:			
Your Answer		Score	Explanation
	×	0.00	
Total		0.00 / 3.00	

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?

#### You entered:

Your Answer Score Explanation

	×	0.00
Total		0.00 / 3.00

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?

Your Answer	Score	Explanation
MD5 hash of password	<b>✓</b> 0.50	This is the second field
role	<b>×</b> 0.00	This is the fourth field
user ID	<b>×</b> 0.00	This is the third field
integer that counts the number of times ever logged in	<b>✓</b> 0.50	This is not part of the cookie
expiration timeout	<b>✓</b> 0.50	This is not part of the cookie
e-mail address	<b>✓</b> 0.50	This is the first field

https://class.coursera.org/softwaresec-001/quiz/feedback?subm...

the number of failed login attempts	✓ 0.50 This is not part of the second s	ne cookie
SHA1 hash of password	✓ 0.50 The password hash	uses MD5, not SHA1
Total	3.00 / 4.00	

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?

#### You entered:

3

Your Answer		Score	Explanation
3	<b>~</b>	3.00	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
Total		3.00 /	
		3.00	

https://class.coursera.org/softwaresec-001/quiz/feedback?subm...