Appendix C
Inseure MusicStore Scan Results

	Name	MusicStore				
	URL	http://134.154.14.153:8080/yuliana/				
	User/ Password	test@test.com/falsepass				
	Pages	User:65				
	Vuln. user	55				
	Summary				Qualys	
				Found	32	
				Missed	23	
				False Positive/ Duplicate/May be	23	
	Status	Vulnerability Type	File	Parameter		
1	Verified	SQL	/validation/displayPasswordRecovery	emailAddress	Y	
2	Verified	SQL	/validation/displayPasswordRecovery	answer	Y	
3	Verified	SQL	/user/account/displayAccountDetails	country		
4	Verified	SQL	/user/account/displayAccountPassword	answer		
5	Verified	SQL	/user/review/displayReview	title		
6	Verified	SQL	/user/review/displayReview	message		
7	Verified	XSS	/registration/displayUserRegistration	firstName	Y	
8	Verified	XSS	/registration/displayUserRegistration	lastName	Y	
9	Verified	XSS	/registration/displayUserRegistration	emailAddress	Y	
10	Verified	XSS	/registration/displayUserRegistration	companyName	Y	
11	Verified	XSS	/registration/displayUserRegistration	address1	Y	
12	Verified	XSS	/registration/displayUserRegistration	address2	Y	
13	Verified	XSS	/registration/displayUserRegistration	city	Y	
14	Verified	XSS	/registration/displayUserRegistration	state	Y	
15	Verified	XSS	/registration/displayUserRegistration	zip	Y	
16	Verified	XSS	/registration/displayUserRegistration	country	Y	
17	Verified	XSS (stored)	/user/account/ displayAccountDetails	country	Y	
18	Verified	XSS (stored)	/user/review/displayReview	title	Y	
19	Verified	XSS (stored)	/user/review/displayReview	message	Y	
20	Verified	XSS (stored)	/user/account/displayAccountPassword	answer		
21	Verified	XSS (DOM)	/email/join_email_list.jsp?name=%3Cscript%3Ealert%28%22DOM%20XSS%22%29%3C/script%3E	name	Y	
22	Verified	XSS (AJAX)	/email/join_email_list.jsp?name=guest	firstName		
23	Verified	XSS (AJAX)	/email/join_email_list.jsp?name=guest	lastName		
24	Verified	XSS (AJAX)	/email/join_email_list.jsp?name=guest	emailAddress		
25	Verified	Broken Auth. (passw. guess)	/validation/displayPasswordRecovery	answer		
26	Verified	Broken Auth.	/user/validation/validateUser	j_password/	Y	

		(brute force)		j_username		
27	Verified	Insecure Direct Obj. Ref.	/partners	letter	Y	
28	Verified	CSRF	/user/order/displayInvoice			
29	Verified	CSRF	/user/order/displayUserCart			
30	Verified	CSRF	/user/order/completeOrder			
31	Verified	CSRF	/user/account/displayAccount			
32	Verified	CSRF	/user/account/displayAccountDetails		Y	
33	Verified	CSRF	/user/account/displayAccountPassword		Y	
34	Verified	CSRF	/user/account/updateUserPassword			
35	Verified	CSRF	/user/account/updateUserDetails			
36	Verified	CSRF	/user/review/displayReview		Y	
37	Verified	CSRF	/user/review/addReview			
38	Verified	CSRF	/cart/displayCart		Y	
39	Verified	Sec. Misconfig. (POST vs GET)	/user/account/updateUserPassword?password=falsepass&answer=black			
40	Verified	Sec. Misconfig. (slow HTTP headers DDoS attack)	/validation/displayPasswordRecovery		Y	
41	Verified	Sec. Misconfig. (slow HTTP POST DDoS attack)	/validation/displayPasswordRecovery		Y	
42	Verified	Sec. Misconfig. (POST vs GET)	/validation/passwordRecovery?emailAddress=test%40test.com&answer=black			
43	Verified	Sec. Misconfig. (Sec. data displayed)	/validation/displayPasswordRecovery	password		
44	Verified	Insec. Crypt. Storage	/user/account/displayAccountDetails	creditCardNumber	Y	
45	Verified	Insec. Crypt. Storage	/registration/displayUserRegistration	creditCardNumber	Y	
46	Verified	Insec. Crypt. Storage	/user/account/displayAccountPassword	password		
47	Verified	Insec. Crypt. Storage	/registration/displayUserRegistration	password		
48	Verified	Insec. Crypt. Storage	/validation/displayPasswordRecovery	answer		
49	Verified	Insec. Crypt. Storage	session cookie does not contain the 'secure' attribute		Y	
50	Verified	Insec. Crypt. Storage	session cookie does not contain the 'HTTPOnly' attribute		Y	
51	Verified	URL access	/userAccess.jsp			
52	Verified	Transport Layer	/user/validation/validateUser		Y	
53	Verified	Transport Layer	session cookie does not contain the 'secure' attribute		Y	
54	Verified	Transport Layer	session cookie does not contain the 'HTTPOnly' attribute		Y	
55	Verified	Redirect and Forward	/partners/displayParnerLetter	site	Y	
1	FP	CSRF	/partners		Y	
2	FP	CSRF	/catalog/**displayProduct?productCode=8601**		Y	
3	FP	CSRF	/validation/displayPasswordRecovery		Y	
4	FP	CSRF	**/cart/displayQuickOrder**		Y	
5	FP	XSS (stored)	/user/account/ displayAccountDetails	zip	Y	

1	Maybe	Clickjacking	/user/validation/validateUser		Y	
2	Maybe	Clickjacking	/catalog/displayProduct?productCode=pf02		Y	
3	Maybe	Clickjacking	/		Y	
4	Maybe	Clickjacking	**/cart**		Y	
1	Duplicate	XSS	/registration/displayUserRegistration	firstName	Y	
2	Duplicate	XSS	/registration/displayUserRegistration	lastName	Y	
3	Duplicate	XSS	/registration/displayUserRegistration	companyName	Y	
4	Duplicate	XSS	/registration/displayUserRegistration	address1	Y	
5	Duplicate	XSS	/registration/displayUserRegistration	address2	Y	
6	Duplicate	XSS	/registration/displayUserRegistration	city	Y	
7	Duplicate	XSS	/registration/displayUserRegistration	state	Y	
8	Duplicate	XSS	/registration/displayUserRegistration	zip	Y	
9	Duplicate	XSS	/registration/displayUserRegistration	country	Y	
10	Duplicate	XSS	/registration/displayUserRegistration	emailAddress		
11	Duplicate	XSS (stored)	/user/account/ displayAccountDetails	country	Y	
12	Duplicate	XSS (stored)	/user/account/ displayAccountDetails	country	Y	
13	Duplicate	Redirect and Forward	/partners/displayParnerLetter	site	Y	
14	Maybe/ Duplicate	Clickjacking	/cart/displayCart		Y	