Web Application Report

This report includes important security information about your Web Application.

Security Report

This report was created by IBM Rational AppScan 7.8.0.2

10/25/2009 12:21:45 PM

Report Information

Web Application Report

Scan Name: openmrs

Scanned Host(s)

Host	Operating System	Web Server	Application Server
192.168.1.104:8080		Apache	Apache AXIS

Content

This report contains the following sections:

- Executive Summary
- Detailed Security Issues

Executive Summary

Test Policy

- Default

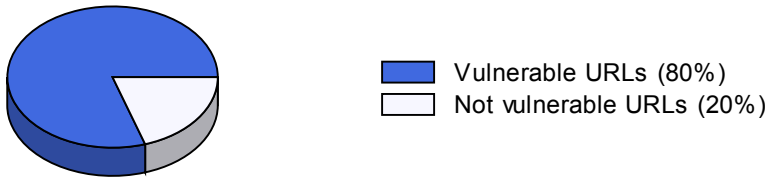
Security Risks

Following are the security risks that appeared most often in the application. To explore which issues included these risks, please refer to the 'Detailed Security Issues' section in this report.

- It is possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
- It is possible to gather sensitive debugging information
- It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
- It is possible to upload, modify or delete web pages, scripts and files on the web server
- It is possible to view, modify or delete database entries and tables

Vulnerable URLs

80% of the URLs had test results that included security issues.



Scanned URLs

631 URLs were scanned by AppScan.

Security Issue Possible Causes

Following are the most common causes for the security issues found in the application. The causes below are those that repeated in the maximal number of issues. To explore which issues included these causes, please refer to the 'Detailed Security Issues' section in this report.

- Sanitation of hazardous characters was not performed correctly on user input
- No validation was done in order to make sure that user input matches the data type expected
- Proper bounds checking were not performed on incoming parameter values
- The web server or application server are configured in an insecure way

- Sensitive input fields such as usernames, password and credit card numbers are passed unencrypted

URLs with the Most Security Issues (number issues)

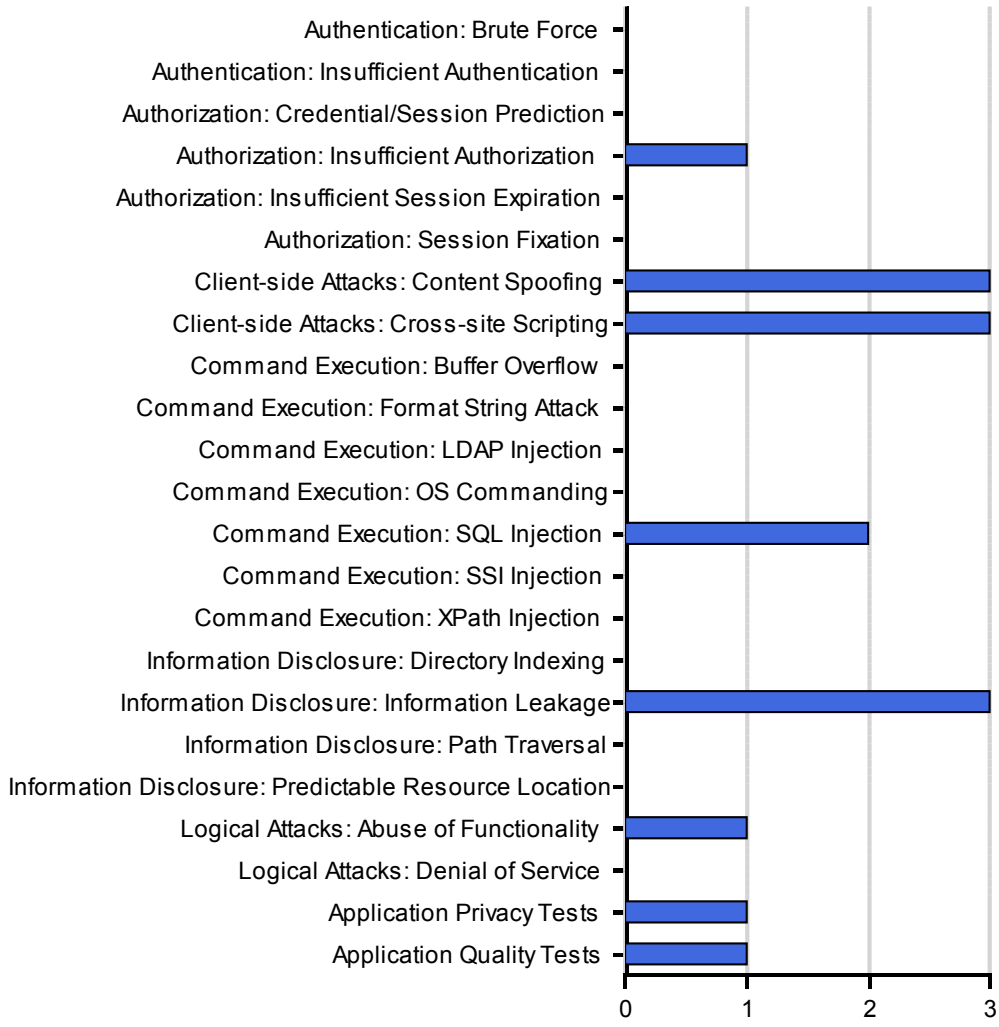
- http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (58)
- http://192.168.1.104:8080/openmrs/options.form (51)
- http://192.168.1.104:8080/openmrs/admin/maintenance/implementationid.form (17)
- http://192.168.1.104:8080/openmrs/admin/person/addPerson.htm (16)
- http://192.168.1.104:8080/openmrs/dictionary/ (14)

Security Issues per Host

Hosts	High	Medium	Low	Informational	Total
http://192.168.1.104:8080/	247	95	4	92	438
Total	**247**	**95**	**4**	**92**	**438**

Security Issue Distribution per Threat Class

The following is a list of the security issues, distributed by Threat Class.



Security Issue Cause Distribution

96% Application-related Security Issues (421 out of a total of 438 issues).
Application-related Security Issues can usually be fixed by application developers, as they result from defects in the application code.
4% Infrastructure and Platform Security Issues (17 out of a total 438 issues).
Infrastructure and Platform Security Issues can usually be fixed by system and network administrators as these security issues result from misconfiguration of, or defects in 3rd party products.

Detailed Security Issues

Vulnerable URL: http://192.168.1.104:8080/openmrs/auditServlet

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/auditServlet (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=49867]

The following changes were applied to the original request:
• Set path to '/openmrs/auditServlet/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/findPatient.htm

Total of 3 security issues in this URL

[1 of 3] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/findPatient.htm (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 6 [ID=7873]

The following changes were applied to the original request:
• Set path to '/openmrs/findPatient.htm/'

[2 of 3] Blind SQL Injection

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/findPatient.htm (Parameter = lang)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 1 [ID=21584]

The following changes were applied to the original request:
• Set parameter 'lang's value to 'en_GB'%20and%20'foobar'='foobar'%20--'

[3 of 3] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/findPatient.htm (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=21714]

The following changes were applied to the original request:
- Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/help.htm

Total of 3 security issues in this URL

[1 of 3] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/help.htm (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 6 [ID=7864]

The following changes were applied to the original request:
- Set path to '/openmrs/help.htm/'

[2 of 3] Blind SQL Injection

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/help.htm (Parameter = lang)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 1 [ID=13170]

The following changes were applied to the original request:
- Set parameter 'lang's value to '"%20+%20"'%20+%20'en_GB'

[3 of 3] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/help.htm (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=13298]

The following changes were applied to the original request:

• Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/index.htm

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/index.htm (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 7 [ID=196]

The following changes were applied to the original request:
• Cleared the value of parameter ''
• Injected '>"'><script>alert(4703)</script>' into parameter 'lang's value

[2 of 2] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/index.htm (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=10095]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/index.htm;jsessionid=1C64E3EA3F29D761AD259554F15C4492

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/index.htm;jsessionid=1C64E3EA3F29D761AD259554F15C4492 (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 4 [ID=7588]

The following changes were applied to the original request:
• Set path to '1C64E3EA3F29D761AD259554F15C4492/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/index.htm;jsessionid=39188CAF42540B3EC4FBDA8DBCECA143

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/index.htm;jsessionid=39188CAF42540B3EC4FBDA8DBCECA143 (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 10 [ID=10762]

The following changes were applied to the original request:
- Cleared the value of parameter ''
- Injected '>'"><script>alert(35531)</script>' into parameter 'lang's value

[2 of 2] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/index.htm;jsessionid=39188CAF42540B3EC4FBDA8DBCECA143 (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=13118]

The following changes were applied to the original request:
- Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/loginServlet

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/loginServlet (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 3 [ID=7680]

The following changes were applied to the original request:
- Set path to '/openmrs/loginServlet/'
- Set method to 'GET'

Vulnerable URL: http://192.168.1.104:8080/openmrs/openmrs.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/openmrs.js (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=7564]

The following changes were applied to the original request:
• Set path to '/openmrs/openmrs.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form

Total of 51 security issues in this URL

[1 of 51] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = newPassword)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 14 [ID=19371]

The following changes were applied to the original request:
• Set parameter 'newPassword's value to '>%22%27><img%20src%3d%22javascript:alert(65481)%22>'

[2 of 51] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = confirmPassword)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 14 [ID=19472]

The following changes were applied to the original request:
• Set parameter 'confirmPassword's value to '>%22%27><img%20src%3d%22javascript:alert(65683)%22>'

[3 of 51] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = oldPassword)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 16 [ID=19270]

The following changes were applied to the original request:
• Set parameter 'oldPassword's value to '>%22%27><img%20src%3d%22javascript:alert(65279)%22>'

[4 of 51] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = username)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 16 [ID=18862]

The following changes were applied to the original request:
• Set parameter 'username's value to '>%22%27><img%20src%3d%22javascript:alert(64463)%22>'

[5 of 51] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = secretQuestionPassword)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 16 [ID=19573]

The following changes were applied to the original request:
• Set parameter 'secretQuestionPassword's value to '>%22%27><img%20src%3d%22javascript:alert(65885)%22>'

[6 of 51] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = notificationAddress)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 12 [ID=20420]

The following changes were applied to the original request:
• Set parameter 'notificationAddress's value to '1234>%22%27><img%20src%3d%

22javascript:alert(67579)%22>'

[7 of 51] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 6 [ID=7772]

The following changes were applied to the original request:
• Set path to '/openmrs/options.form/'

[8 of 51] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = personName.givenName)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 14 [ID=18964]

The following changes were applied to the original request:
• Set parameter 'personName.givenName's value to '>%22%27><img%20src%3d%22javascript:alert(64667)%22>'

[9 of 51] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = secretAnswerConfirm)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 13 [ID=20056]

The following changes were applied to the original request:
• Set parameter 'secretAnswerConfirm's value to '1234>%22%27><img%20src%3d%22javascript:alert(66851)%22>'

[10 of 51] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = secretQuestionNew)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 14 [ID=19680]

The following changes were applied to the original request:
• Set parameter 'secretQuestionNew's value to '1234>%22%27><img%20src%3d%

22javascript:alert(66099)%22>'

[11 of 51] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = personName.middleName)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 14 [ID=19066]

The following changes were applied to the original request:
• Set parameter 'personName.middleName's value to '>%22%27><img%20src%3d%22javascript:alert(64871)%22>'

[12 of 51] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = secretAnswerNew)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 13 [ID=19869]

The following changes were applied to the original request:
• Set parameter 'secretAnswerNew's value to '1234>%22%27><img%20src%3d%22javascript:alert(66477)%22>'

[13 of 51] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = proficientLocales)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 14 [ID=18339]

The following changes were applied to the original request:
• Set parameter 'proficientLocales's value to '1234>%22%27><img%20src%3d%22javascript:alert(63417)%22>'

[14 of 51] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = defaultLocation)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 16 [ID=17976]

The following changes were applied to the original request:

• Set parameter 'defaultLocation's value to '1>%22%27><img%20src%3d%22javascript:alert(62691)%22>'

[15 of 51] Blind SQL Injection

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = secretAnswerNew)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=19864]

The following changes were applied to the original request:
• Set parameter 'secretAnswerNew's value to '1234%27+and+%27foobar%27%3D%27foobar'

[16 of 51] Cross-Site Request Forgery

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form

Remediation Tasks: Decline malicious requests

Variant 1 of 1 [ID=17579]

[17 of 51] Phishing Through Frames

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = newPassword)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=19427]

The following changes were applied to the original request:
• Set parameter 'newPassword's value to '%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%3E'

[18 of 51] Phishing Through Frames

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = confirmPassword)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=19528]

The following changes were applied to the original request:
• Set parameter 'confirmPassword's value to '%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%3E'

[19 of 51] Phishing Through Frames

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = oldPassword)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=19326]

The following changes were applied to the original request:
• Set parameter 'oldPassword's value to '%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%3E'

[20 of 51] Phishing Through Frames

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = username)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=18919]

The following changes were applied to the original request:
• Set parameter 'username's value to '%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%3E'

[21 of 51] Phishing Through Frames

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = secretQuestionPassword)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=19629]

The following changes were applied to the original request:
• Set parameter 'secretQuestionPassword's value to '%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%3E'

[22 of 51] Phishing Through Frames

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = notificationAddress)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=20558]

The following changes were applied to the original request:
• Set parameter 'notificationAddress's value to '1234%27%22%3E%3Ciframe+src%3Dhttp%3A%

2F%2Fdemo.testfire.net%3E'

[23 of 51] Phishing Through Frames

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = personName.givenName)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=19021]

The following changes were applied to the original request:
• Set parameter 'personName.givenName's value to '%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%3E'

[24 of 51] Phishing Through Frames

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = secretAnswerConfirm)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=20193]

The following changes were applied to the original request:
• Set parameter 'secretAnswerConfirm's value to '1234%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%3E'

[25 of 51] Phishing Through Frames

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = secretQuestionNew)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=19818]

The following changes were applied to the original request:
• Set parameter 'secretQuestionNew's value to '1234%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%3E'

[26 of 51] Phishing Through Frames

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = personName.middleName)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=19123]

The following changes were applied to the original request:

• Set parameter 'personName.middleName's value to '%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%3E'

[27 of 51] Phishing Through Frames

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = secretAnswerNew)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=20006]

The following changes were applied to the original request:
• Set parameter 'secretAnswerNew's value to '1234%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%3E'

[28 of 51] Phishing Through Frames

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = proficientLocales)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=18477]

The following changes were applied to the original request:
• Set parameter 'proficientLocales's value to '1234%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%3E'

[29 of 51] Phishing Through Frames

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = defaultLocation)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=18112]

The following changes were applied to the original request:
• Set parameter 'defaultLocation's value to '1%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%3E'

[30 of 51] Link Injection (facilitates Cross-Site Request Forgery)

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = newPassword)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=19440]

The following changes were applied to the original request:
• Set parameter 'newPassword's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[31 of 51] Link Injection (facilitates Cross-Site Request Forgery)

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = confirmPassword)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=19541]

The following changes were applied to the original request:
• Set parameter 'confirmPassword's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[32 of 51] Link Injection (facilitates Cross-Site Request Forgery)

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = oldPassword)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=19339]

The following changes were applied to the original request:
• Set parameter 'oldPassword's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[33 of 51] Link Injection (facilitates Cross-Site Request Forgery)

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = username)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=18932]

The following changes were applied to the original request:
• Set parameter 'username's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[34 of 51] Link Injection (facilitates Cross-Site Request Forgery)

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = secretQuestionPassword)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=19643]

The following changes were applied to the original request:
• Set parameter 'secretQuestionPassword's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[35 of 51] Link Injection (facilitates Cross-Site Request Forgery)

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/options.form (Parameter = notificationAddress)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 1 [ID=20571]

The following changes were applied to the original request:
• Set parameter 'notificationAddress's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[36 of 51] Link Injection (facilitates Cross-Site Request Forgery)

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/options.form (Parameter = personName.givenName)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 1 [ID=19034]

The following changes were applied to the original request:
• Set parameter 'personName.givenName's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[37 of 51] Link Injection (facilitates Cross-Site Request Forgery)

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/options.form (Parameter = secretAnswerConfirm)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 1 [ID=20206]

The following changes were applied to the original request:
• Set parameter 'secretAnswerConfirm's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[38 of 51] Link Injection (facilitates Cross-Site Request Forgery)

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = secretQuestionNew)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=19832]

The following changes were applied to the original request:
• Set parameter 'secretQuestionNew's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[39 of 51] Link Injection (facilitates Cross-Site Request Forgery)

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = personName.middleName)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=19136]

The following changes were applied to the original request:
• Set parameter 'personName.middleName's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[40 of 51] Link Injection (facilitates Cross-Site Request Forgery)

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = secretAnswerNew)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=20019]

The following changes were applied to the original request:
• Set parameter 'secretAnswerNew's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[41 of 51] Link Injection (facilitates Cross-Site Request Forgery)

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/options.form (Parameter = proficientLocales)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=18490]

The following changes were applied to the original request:
• Set parameter 'proficientLocales's value to '%22%27%3E%3CIMG+SRC%3D%22%

2FWF_XSRF.html%22%3E'

[42 of 51] Link Injection (facilitates Cross-Site Request Forgery)

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/options.form (Parameter = defaultLocation)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 1 [ID=18125]

The following changes were applied to the original request:
• Set parameter 'defaultLocation's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[43 of 51] Unencrypted Login Request

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/options.form
Remediation Tasks:	Always use the HTTP POST method when sending sensitive information

Variant 1 of 1 [ID=19425]

The following may require user attention:

```
POST /openmrs/options.form HTTP/1.0
Cookie: __openmrs_language=en_GB;
JSESSIONID=97605BBA26DE7D3A3E3E851092661D72
Content-Length: 364
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: 192.168.1.104:8080
Content-Type: application/x-www-form-urlencoded
Referer: http://192.168.1.104:8080/openmrs/options.form

defaultLocation=1&defaultLocale=en_GB&proficientLocales=1234&_showRetiredMessage
=true&_verbose=true&username=&personName.givenName=&personName.middleName=
&personName.familyName=&oldPassword=&newPassword=&confirmPassword=&secretQ
uestionPassword=&secretQuestionNew=1234&secretAnswerNew=1234&secretAnswerCon
firm=1234&notification=internalOnly&notificationAddress=1234
HTTP/1.1 200 OK
Content-Length: 12220
Server: Apache-Coyote/1.1
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache
Cache-Control: no-store
Content-Type: text/html;charset=UTF-8
Content-Language: en-GB
Date: Sun, 25 Oct 2009 00:37:34 GMT
```

Connection: close

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <script src="/openmrs/openmrs.js?v=1.5.0.35" type="text/javascript" ></script>
    <link href="/openmrs/openmrs.css?v=1.5.0.35" type="text/css" rel="stylesheet" />
    <link href="/openmrs/style.css?v=1.5.0.35" type="text/css" rel="stylesheet" />
    <script src="/openmrs/dwr/engine.js?v=1.5.0.35" type="text/javascript" ></script>
    <script src="/openmrs/dwr/interface/DWRAlertService.js?v=1.5.0.35"
type="text/javascript" ></script>

      <title>OpenMRS - User Options</title>

    <script type="text/javascript">
      /* variable used in js to know the context path */
      var openmrsContextPath = '/openmrs';
    </script>

  </head>

```
<body>
  <div id="pageBody">
    <div id="userBar">


          <span id="userLoggedInAs" class="firstChild">
            Currently logged in as Super  User
          </span>
          <span id="userLogout">
            <a href='/openmrs/logout'>Log out</a>
          </span>
          <span>
            <a href="/openmrs/options.form">My Profile</a>
          </span>



      <span id="userHelp">
        <a href='/openmrs/help.htm'>Help</a>
      </span>
    </div>

    <div id="banner">
      <a href="http://www.openmrs.org">
 <img src="/openmrs/images/openmrs_logo_short.gif" alt="OpenMRS Logo" border="0"/>
</a>
    </div>



      <div id="gutter">
        <ul id="navList">
  <li id="homeNavLink" class="firstChild">
    <a href="/openmrs/">Home</a>
  </li>

  <li id="findPatientNavLink">
    <a href="/openmrs/findPatient.htm">

        Find/Create Patient


    </a>
  </li>


    <li id="dictionaryNavLink">
      <a href="/openmrs/dictionary">Dictionary</a>
    </li>
```

```
      <li id="administrationNavLink">
        <a href="/openmrs/admin">Administration</a>
      </li>



</ul>
        </div>


      <div id="content">

        <script type="text/javascript">
          // prevents users getting popup alerts when viewing pages
          var handler = function(msg, ex) {
            var div = document.getElementById("openmrs_dwr_error");
            div.style.display = ""; // show the error div
            var msgDiv = document.getElementById("openmrs_dwr_error_msg");
            msgDiv.innerHTML = 'A javascript error has occurred:' + " <b>" + msg + "</b>";

          };
          dwr.engine.setErrorHandler(handler);
          dwr.engine.setWarningHandler(handler);
        </script>




        <div id="openmrs_dwr_error" style="display:none" class="error">
          <div id="openmrs_dwr_error_msg"></div>
          <div id="openmrs_dwr_error_close" class="smallMessage">
            <i>The full stacktrace for this error can usually be found in your server's error
logs.</i>  
            <a href="#" onclick="this.parentNode.parentNode.style.display='none'">Hide
error</a>
          </div>
        </div>



<script type="text/javascript">

window.onload = init;

function init() {
  var sections = new Array();
  var optform = document.getElementById("optionsForm");
```

```
var seci = 0;
for(i=0;i<children.length;i++) {
  if(children[i].nodeName.toLowerCase().indexOf('fieldset') != -1) {
    children[i].id = 'optsection-' + seci;
    children[i].className = 'optsection';
    legends = children[i].getElementsByTagName('legend');
    sections[seci] = new Object();
    if(legends[0] && legends[0].firstChild.nodeValue)
      sections[seci].text = legends[0].firstChild.nodeValue;
    else
      sections[seci].text = '# ' + seci;
    sections[seci].secid = children[i].id;
    sections[seci].error = containsError(children[i]);
    seci++;
    if(sections.length != 1)
      children[i].style.display = 'none';
    else
      var selectedid = children[i].id;
  }
}

var toc = document.createElement('ul');
toc.id = 'optionsTOC';
toc.selectedid = selec...
```

[44 of 51] Unencrypted Login Request

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/options.form
Remediation Tasks:	Always use the HTTP POST method when sending sensitive information

Variant 1 of 1 [ID=19526]

The following may require user attention:

```
POST /openmrs/options.form HTTP/1.0
Cookie: __openmrs_language=en_GB;
JSESSIONID=97605BBA26DE7D3A3E3E851092661D72
Content-Length: 364
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: 192.168.1.104:8080
Content-Type: application/x-www-form-urlencoded
Referer: http://192.168.1.104:8080/openmrs/options.form

defaultLocation=1&defaultLocale=en_GB&proficientLocales=1234&_showRetiredMessage
=true&_verbose=true&username=&personName.givenName=&personName.middleName=
&personName.familyName=&oldPassword=&newPassword=&confirmPassword=&secretQ
uestionPassword=&secretQuestionNew=1234&secretAnswerNew=1234&secretAnswerCon
```

firm=1234&notification=internalOnly&notificationAddress=1234
HTTP/1.1 200 OK
Content-Length: 12220
Server: Apache-Coyote/1.1
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache
Cache-Control: no-store
Content-Type: text/html;charset=UTF-8
Content-Language: en-GB
Date: Sun, 25 Oct 2009 00:37:34 GMT
Connection: close

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <script src="/openmrs/openmrs.js?v=1.5.0.35" type="text/javascript" ></script>
    <link href="/openmrs/openmrs.css?v=1.5.0.35" type="text/css" rel="stylesheet" />
    <link href="/openmrs/style.css?v=1.5.0.35" type="text/css" rel="stylesheet" />
    <script src="/openmrs/dwr/engine.js?v=1.5.0.35" type="text/javascript" ></script>
    <script src="/openmrs/dwr/interface/DWRAlertService.js?v=1.5.0.35"
type="text/javascript" ></script>

        <title>OpenMRS - User Options</title>

```
      <script type="text/javascript">
         /* variable used in js to know the context path */
         var openmrsContextPath = '/openmrs';
      </script>



   </head>

<body>
   <div id="pageBody">
      <div id="userBar">


               <span id="userLoggedInAs" class="firstChild">
                  Currently logged in as Super  User
               </span>
               <span id="userLogout">
                  <a href='/openmrs/logout'>Log out</a>
               </span>
               <span>
                  <a href="/openmrs/options.form">My Profile</a>
               </span>




         <span id="userHelp">
            <a href='/openmrs/help.htm'>Help</a>
         </span>
      </div>

      <div id="banner">
         <a href="http://www.openmrs.org">
  <img src="/openmrs/images/openmrs_logo_short.gif" alt="OpenMRS Logo" border="0"/>
</a>
      </div>




         <div id="gutter">
            <ul id="navList">
   <li id="homeNavLink" class="firstChild">
      <a href="/openmrs/">Home</a>
   </li>

   <li id="findPatientNavLink">
      <a href="/openmrs/findPatient.htm">
```

```
            Find/Create Patient


        </a>
      </li>


        <li id="dictionaryNavLink">
          <a href="/openmrs/dictionary">Dictionary</a>
        </li>




        <li id="administrationNavLink">
          <a href="/openmrs/admin">Administration</a>
        </li>



</ul>
        </div>


        <div id="content">

          <script type="text/javascript">
            // prevents users getting popup alerts when viewing pages
            var handler = function(msg, ex) {
              var div = document.getElementById("openmrs_dwr_error");
              div.style.display = ""; // show the error div
              var msgDiv = document.getElementById("openmrs_dwr_error_msg");
              msgDiv.innerHTML = 'A javascript error has occurred:' + " <b>" + msg + "</b>";

            };
            dwr.engine.setErrorHandler(handler);
            dwr.engine.setWarningHandler(handler);
          </script>




          <div id="openmrs_dwr_error" style="display:none" class="error">
            <div id="openmrs_dwr_error_msg"></div>
            <div id="openmrs_dwr_error_close" class="smallMessage">
              <i>The full stacktrace for this error can usually be found in your server's error
logs.</i>  
              <a href="#" onclick="this.parentNode.parentNode.style.display='none'">Hide
error</a>
            </div>
          </div>
```

```
<script type="text/javascript">

window.onload = init;

function init() {
   var sections = new Array();
   var optform = document.getElementById("optionsForm");
   children = optform.childNodes;
   var seci = 0;
   for(i=0;i<children.length;i++) {
      if(children[i].nodeName.toLowerCase().indexOf('fieldset') != -1) {
         children[i].id = 'optsection-' + seci;
         children[i].className = 'optsection';
         legends = children[i].getElementsByTagName('legend');
         sections[seci] = new Object();
         if(legends[0] && legends[0].firstChild.nodeValue)
            sections[seci].text = legends[0].firstChild.nodeValue;
         else
            sections[seci].text = '# ' + seci;
         sections[seci].secid = children[i].id;
         sections[seci].error = containsError(children[i]);
         seci++;
         if(sections.length != 1)
            children[i].style.display = 'none';
         else
            var selectedid = children[i].id;
      }
   }

   var toc = document.createElement('ul');
   toc.id = 'optionsTOC';
   toc.selectedid = selec...
```

[45 of 51] Unencrypted Login Request

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/options.form
Remediation Tasks:	Always use the HTTP POST method when sending sensitive information

Variant 1 of 1 [ID=19324]

The following may require user attention:

```
POST /openmrs/options.form HTTP/1.0
Cookie: __openmrs_language=en_GB;
JSESSIONID=97605BBA26DE7D3A3E3E851092661D72
Content-Length: 364
```

Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: 192.168.1.104:8080
Content-Type: application/x-www-form-urlencoded
Referer: http://192.168.1.104:8080/openmrs/options.form

defaultLocation=1&defaultLocale=en_GB&proficientLocales=1234&_showRetiredMessage=true&_verbose=true&username=&personName.givenName=&personName.middleName=&personName.familyName=&oldPassword=&newPassword=&confirmPassword=&secretQuestionPassword=&secretQuestionNew=1234&secretAnswerNew=1234&secretAnswerConfirm=1234&notification=internalOnly&notificationAddress=1234
HTTP/1.1 200 OK
Content-Length: 12220
Server: Apache-Coyote/1.1
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache
Cache-Control: no-store
Content-Type: text/html;charset=UTF-8
Content-Language: en-GB
Date: Sun, 25 Oct 2009 00:37:34 GMT
Connection: close

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <script src="/openmrs/openmrs.js?v=1.5.0.35" type="text/javascript" ></script>

```
      <link href="/openmrs/openmrs.css?v=1.5.0.35" type="text/css" rel="stylesheet" />
      <link href="/openmrs/style.css?v=1.5.0.35" type="text/css" rel="stylesheet" />
      <script src="/openmrs/dwr/engine.js?v=1.5.0.35" type="text/javascript" ></script>
      <script src="/openmrs/dwr/interface/DWRAlertService.js?v=1.5.0.35"
type="text/javascript" ></script>



            <title>OpenMRS - User Options</title>




      <script type="text/javascript">
         /* variable used in js to know the context path */
         var openmrsContextPath = '/openmrs';
      </script>



   </head>

<body>
   <div id="pageBody">
      <div id="userBar">


            <span id="userLoggedInAs" class="firstChild">
               Currently logged in as Super  User
            </span>
            <span id="userLogout">
               <a href='/openmrs/logout'>Log out</a>
            </span>
            <span>
               <a href="/openmrs/options.form">My Profile</a>
            </span>




         <span id="userHelp">
            <a href='/openmrs/help.htm'>Help</a>
         </span>
      </div>

      <div id="banner">
         <a href="http://www.openmrs.org">
  <img src="/openmrs/images/openmrs_logo_short.gif" alt="OpenMRS Logo" border="0"/>
</a>
      </div>
```

```
        <div id="gutter">
          <ul id="navList">
    <li id="homeNavLink" class="firstChild">
      <a href="/openmrs/">Home</a>
    </li>

    <li id="findPatientNavLink">
      <a href="/openmrs/findPatient.htm">

          Find/Create Patient


      </a>
    </li>


      <li id="dictionaryNavLink">
        <a href="/openmrs/dictionary">Dictionary</a>
      </li>




      <li id="administrationNavLink">
        <a href="/openmrs/admin">Administration</a>
      </li>



</ul>
        </div>


      <div id="content">

        <script type="text/javascript">
          // prevents users getting popup alerts when viewing pages
          var handler = function(msg, ex) {
            var div = document.getElementById("openmrs_dwr_error");
            div.style.display = ""; // show the error div
            var msgDiv = document.getElementById("openmrs_dwr_error_msg");
            msgDiv.innerHTML = 'A javascript error has occurred:' + " <b>" + msg + "</b>";

          };
          dwr.engine.setErrorHandler(handler);
          dwr.engine.setWarningHandler(handler);
        </script>
```

```
        <div id="openmrs_dwr_error" style="display:none" class="error">
          <div id="openmrs_dwr_error_msg"></div>
          <div id="openmrs_dwr_error_close" class="smallMessage">
            <i>The full stacktrace for this error can usually be found in your server's error
logs.</i>  
            <a href="#" onclick="this.parentNode.parentNode.style.display='none'">Hide
error</a>
          </div>
        </div>



<script type="text/javascript">

window.onload = init;

function init() {
  var sections = new Array();
  var optform = document.getElementById("optionsForm");
  children = optform.childNodes;
  var seci = 0;
  for(i=0;i<children.length;i++) {
    if(children[i].nodeName.toLowerCase().indexOf('fieldset') != -1) {
      children[i].id = 'optsection-' + seci;
      children[i].className = 'optsection';
      legends = children[i].getElementsByTagName('legend');
      sections[seci] = new Object();
      if(legends[0] && legends[0].firstChild.nodeValue)
        sections[seci].text = legends[0].firstChild.nodeValue;
      else
        sections[seci].text = '# ' + seci;
      sections[seci].secid = children[i].id;
      sections[seci].error = containsError(children[i]);
      seci++;
      if(sections.length != 1)
        children[i].style.display = 'none';
      else
        var selectedid = children[i].id;
    }
  }

  var toc = document.createElement('ul');
  toc.id = 'optionsTOC';
  toc.selectedid = selec...
```

[46 of 51] Unencrypted Login Request

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/options.form
Remediation Tasks:	Always use the HTTP POST method when sending sensitive information

Variant 1 of 1 [ID=19627]

The following may require user attention:

```
POST /openmrs/options.form HTTP/1.0
Cookie: __openmrs_language=en_GB;
JSESSIONID=97605BBA26DE7D3A3E3E851092661D72
Content-Length: 364
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: 192.168.1.104:8080
Content-Type: application/x-www-form-urlencoded
Referer: http://192.168.1.104:8080/openmrs/options.form

defaultLocation=1&defaultLocale=en_GB&proficientLocales=1234&_showRetiredMessage
=true&_verbose=true&username=&personName.givenName=&personName.middleName=
&personName.familyName=&oldPassword=&newPassword=&confirmPassword=&secretQ
uestionPassword=&secretQuestionNew=1234&secretAnswerNew=1234&secretAnswerCon
firm=1234&notification=internalOnly&notificationAddress=1234
HTTP/1.1 200 OK
Content-Length: 12220
Server: Apache-Coyote/1.1
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache
Cache-Control: no-store
Content-Type: text/html;charset=UTF-8
Content-Language: en-GB
Date: Sun, 25 Oct 2009 00:37:34 GMT
Connection: close
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">



<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <script src="/openmrs/openmrs.js?v=1.5.0.35" type="text/javascript" ></script>
    <link href="/openmrs/openmrs.css?v=1.5.0.35" type="text/css" rel="stylesheet" />
    <link href="/openmrs/style.css?v=1.5.0.35" type="text/css" rel="stylesheet" />
    <script src="/openmrs/dwr/engine.js?v=1.5.0.35" type="text/javascript" ></script>
    <script src="/openmrs/dwr/interface/DWRAlertService.js?v=1.5.0.35"
type="text/javascript" ></script>



        <title>OpenMRS - User Options</title>




    <script type="text/javascript">
      /* variable used in js to know the context path */
      var openmrsContextPath = '/openmrs';
    </script>



  </head>

<body>
  <div id="pageBody">
    <div id="userBar">


          <span id="userLoggedInAs" class="firstChild">
            Currently logged in as Super  User
          </span>
          <span id="userLogout">
            <a href='/openmrs/logout'>Log out</a>
          </span>
          <span>
            <a href="/openmrs/options.form">My Profile</a>
          </span>
```

```
        <span id="userHelp">
          <a href='/openmrs/help.htm'>Help</a>
        </span>
      </div>

      <div id="banner">
        <a href="http://www.openmrs.org">
  <img src="/openmrs/images/openmrs_logo_short.gif" alt="OpenMRS Logo" border="0"/>
</a>
      </div>




        <div id="gutter">
          <ul id="navList">
   <li id="homeNavLink" class="firstChild">
     <a href="/openmrs/">Home</a>
   </li>

   <li id="findPatientNavLink">
     <a href="/openmrs/findPatient.htm">

         Find/Create Patient


     </a>
   </li>


      <li id="dictionaryNavLink">
        <a href="/openmrs/dictionary">Dictionary</a>
      </li>




      <li id="administrationNavLink">
        <a href="/openmrs/admin">Administration</a>
      </li>



</ul>
        </div>


      <div id="content">
```

```
        <script type="text/javascript">
          // prevents users getting popup alerts when viewing pages
          var handler = function(msg, ex) {
            var div = document.getElementById("openmrs_dwr_error");
            div.style.display = ""; // show the error div
            var msgDiv = document.getElementById("openmrs_dwr_error_msg");
            msgDiv.innerHTML = 'A javascript error has occurred:' + " <b>" + msg + "</b>";

          };
          dwr.engine.setErrorHandler(handler);
          dwr.engine.setWarningHandler(handler);
        </script>




        <div id="openmrs_dwr_error" style="display:none" class="error">
          <div id="openmrs_dwr_error_msg"></div>
          <div id="openmrs_dwr_error_close" class="smallMessage">
            <i>The full stacktrace for this error can usually be found in your server's error
logs.</i>  
            <a href="#" onclick="this.parentNode.parentNode.style.display='none'">Hide
error</a>
          </div>
        </div>



<script type="text/javascript">

window.onload = init;

function init() {
  var sections = new Array();
  var optform = document.getElementById("optionsForm");
  children = optform.childNodes;
  var seci = 0;
  for(i=0;i<children.length;i++) {
    if(children[i].nodeName.toLowerCase().indexOf('fieldset') != -1) {
      children[i].id = 'optsection-' + seci;
      children[i].className = 'optsection';
      legends = children[i].getElementsByTagName('legend');
      sections[seci] = new Object();
      if(legends[0] && legends[0].firstChild.nodeValue)
        sections[seci].text = legends[0].firstChild.nodeValue;
      else
        sections[seci].text = '# ' + seci;
      sections[seci].secid = children[i].id;
      sections[seci].error = containsError(children[i]);
      seci++;
```

```
            children[i].style.display = 'none';
        else
            var selectedid = children[i].id;
    }
}

var toc = document.createElement('ul');
toc.id = 'optionsTOC';
toc.selectedid = selec...
```

[47 of 51] Unencrypted Login Request

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/options.form
Remediation Tasks:	Always use the HTTP POST method when sending sensitive information

Variant 1 of 1 [ID=20191]

The following may require user attention:

```
POST /openmrs/options.form HTTP/1.0
Cookie: __openmrs_language=en_GB;
JSESSIONID=97605BBA26DE7D3A3E3E851092661D72
Content-Length: 364
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: 192.168.1.104:8080
Content-Type: application/x-www-form-urlencoded
Referer: http://192.168.1.104:8080/openmrs/options.form

defaultLocation=1&defaultLocale=en_GB&proficientLocales=1234&_showRetiredMessage
=true&_verbose=true&username=&personName.givenName=&personName.middleName=
&personName.familyName=&oldPassword=&newPassword=&confirmPassword=&secretQ
uestionPassword=&secretQuestionNew=1234&secretAnswerNew=1234&secretAnswerCon
firm=1234&notification=internalOnly&notificationAddress=1234
HTTP/1.1 200 OK
Content-Length: 12220
Server: Apache-Coyote/1.1
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache
Cache-Control: no-store
Content-Type: text/html;charset=UTF-8
Content-Language: en-GB
Date: Sun, 25 Oct 2009 00:37:34 GMT
Connection: close
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">



<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <script src="/openmrs/openmrs.js?v=1.5.0.35" type="text/javascript" ></script>
    <link href="/openmrs/openmrs.css?v=1.5.0.35" type="text/css" rel="stylesheet" />
    <link href="/openmrs/style.css?v=1.5.0.35" type="text/css" rel="stylesheet" />
    <script src="/openmrs/dwr/engine.js?v=1.5.0.35" type="text/javascript" ></script>
    <script src="/openmrs/dwr/interface/DWRAlertService.js?v=1.5.0.35"
type="text/javascript" ></script>



        <title>OpenMRS - User Options</title>




    <script type="text/javascript">
      /* variable used in js to know the context path */
      var openmrsContextPath = '/openmrs';
    </script>



  </head>

<body>
  <div id="pageBody">
    <div id="userBar">
```

```
                <span id="userLoggedInAs" class="firstChild">
                   Currently logged in as Super  User
                </span>
                <span id="userLogout">
                   <a href='/openmrs/logout'>Log out</a>
                </span>
                <span>
                   <a href="/openmrs/options.form">My Profile</a>
                </span>




          <span id="userHelp">
             <a href='/openmrs/help.htm'>Help</a>
          </span>
       </div>

       <div id="banner">
          <a href="http://www.openmrs.org">
  <img src="/openmrs/images/openmrs_logo_short.gif" alt="OpenMRS Logo" border="0"/>
</a>
       </div>




          <div id="gutter">
             <ul id="navList">
   <li id="homeNavLink" class="firstChild">
      <a href="/openmrs/">Home</a>
   </li>

   <li id="findPatientNavLink">
      <a href="/openmrs/findPatient.htm">

            Find/Create Patient


      </a>
   </li>


      <li id="dictionaryNavLink">
         <a href="/openmrs/dictionary">Dictionary</a>
      </li>
```

```
      <li id="administrationNavLink">
        <a href="/openmrs/admin">Administration</a>
      </li>



</ul>
        </div>


      <div id="content">

        <script type="text/javascript">
          // prevents users getting popup alerts when viewing pages
          var handler = function(msg, ex) {
            var div = document.getElementById("openmrs_dwr_error");
            div.style.display = ""; // show the error div
            var msgDiv = document.getElementById("openmrs_dwr_error_msg");
            msgDiv.innerHTML = 'A javascript error has occurred:' + " <b>" + msg + "</b>";

          };
          dwr.engine.setErrorHandler(handler);
          dwr.engine.setWarningHandler(handler);
        </script>




        <div id="openmrs_dwr_error" style="display:none" class="error">
          <div id="openmrs_dwr_error_msg"></div>
          <div id="openmrs_dwr_error_close" class="smallMessage">
            <i>The full stacktrace for this error can usually be found in your server's error
logs.</i>  
            <a href="#" onclick="this.parentNode.parentNode.style.display='none'">Hide
error</a>
          </div>
        </div>



<script type="text/javascript">

window.onload = init;

function init() {
  var sections = new Array();
  var optform = document.getElementById("optionsForm");
  children = optform.childNodes;
  var seci = 0;
  for(i=0;i<children.length;i++) {
    if(children[i].nodeName.toLowerCase().indexOf('fieldset') != -1) {
```

```
        children[i].className = 'optsection';
        legends = children[i].getElementsByTagName('legend');
        sections[seci] = new Object();
        if(legends[0] && legends[0].firstChild.nodeValue)
          sections[seci].text = legends[0].firstChild.nodeValue;
        else
          sections[seci].text = '# ' + seci;
        sections[seci].secid = children[i].id;
        sections[seci].error = containsError(children[i]);
        seci++;
        if(sections.length != 1)
          children[i].style.display = 'none';
        else
          var selectedid = children[i].id;
      }
    }

    var toc = document.createElement('ul');
    toc.id = 'optionsTOC';
    toc.selectedid = selec...
```

[48 of 51] Unencrypted Login Request

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/options.form
Remediation Tasks:	Always use the HTTP POST method when sending sensitive information

Variant 1 of 1 [ID=20004]

The following may require user attention:

```
POST /openmrs/options.form HTTP/1.0
Cookie: __openmrs_language=en_GB;
JSESSIONID=97605BBA26DE7D3A3E3E851092661D72
Content-Length: 364
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: 192.168.1.104:8080
Content-Type: application/x-www-form-urlencoded
Referer: http://192.168.1.104:8080/openmrs/options.form

defaultLocation=1&defaultLocale=en_GB&proficientLocales=1234&_showRetiredMessage
=true&_verbose=true&username=&personName.givenName=&personName.middleName=
&personName.familyName=&oldPassword=&newPassword=&confirmPassword=&secretQ
uestionPassword=&secretQuestionNew=1234&secretAnswerNew=1234&secretAnswerCon
firm=1234&notification=internalOnly&notificationAddress=1234
HTTP/1.1 200 OK
Content-Length: 12220
Server: Apache-Coyote/1.1
```

Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache
Cache-Control: no-store
Content-Type: text/html;charset=UTF-8
Content-Language: en-GB
Date: Sun, 25 Oct 2009 00:37:34 GMT
Connection: close

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <script src="/openmrs/openmrs.js?v=1.5.0.35" type="text/javascript" ></script>
    <link href="/openmrs/openmrs.css?v=1.5.0.35" type="text/css" rel="stylesheet" />
    <link href="/openmrs/style.css?v=1.5.0.35" type="text/css" rel="stylesheet" />
    <script src="/openmrs/dwr/engine.js?v=1.5.0.35" type="text/javascript" ></script>
    <script src="/openmrs/dwr/interface/DWRAlertService.js?v=1.5.0.35"
type="text/javascript" ></script>

      <title>OpenMRS - User Options</title>

    <script type="text/javascript">

```
        /* variable used in js to know the context path */
        var openmrsContextPath = '/openmrs';
      </script>



  </head>

<body>
  <div id="pageBody">
    <div id="userBar">


          <span id="userLoggedInAs" class="firstChild">
            Currently logged in as Super  User
          </span>
          <span id="userLogout">
            <a href='/openmrs/logout'>Log out</a>
          </span>
          <span>
            <a href="/openmrs/options.form">My Profile</a>
          </span>




      <span id="userHelp">
        <a href='/openmrs/help.htm'>Help</a>
      </span>
    </div>

    <div id="banner">
      <a href="http://www.openmrs.org">
 <img src="/openmrs/images/openmrs_logo_short.gif" alt="OpenMRS Logo" border="0"/>
</a>
    </div>




      <div id="gutter">
        <ul id="navList">
  <li id="homeNavLink" class="firstChild">
    <a href="/openmrs/">Home</a>
  </li>

  <li id="findPatientNavLink">
    <a href="/openmrs/findPatient.htm">

        Find/Create Patient


    </a>
```

```
    </li>


    <li id="dictionaryNavLink">
      <a href="/openmrs/dictionary">Dictionary</a>
    </li>




    <li id="administrationNavLink">
      <a href="/openmrs/admin">Administration</a>
    </li>



</ul>
    </div>


    <div id="content">

      <script type="text/javascript">
        // prevents users getting popup alerts when viewing pages
        var handler = function(msg, ex) {
          var div = document.getElementById("openmrs_dwr_error");
          div.style.display = ""; // show the error div
          var msgDiv = document.getElementById("openmrs_dwr_error_msg");
          msgDiv.innerHTML = 'A javascript error has occurred:' + " <b>" + msg + "</b>";

        };
        dwr.engine.setErrorHandler(handler);
        dwr.engine.setWarningHandler(handler);
      </script>




      <div id="openmrs_dwr_error" style="display:none" class="error">
        <div id="openmrs_dwr_error_msg"></div>
        <div id="openmrs_dwr_error_close" class="smallMessage">
          <i>The full stacktrace for this error can usually be found in your server's error
logs.</i>  
          <a href="#" onclick="this.parentNode.parentNode.style.display='none'">Hide
error</a>
        </div>
      </div>
```

```
window.onload = init;

function init() {
  var sections = new Array();
  var optform = document.getElementById("optionsForm");
  children = optform.childNodes;
  var seci = 0;
  for(i=0;i<children.length;i++) {
    if(children[i].nodeName.toLowerCase().indexOf('fieldset') != -1) {
      children[i].id = 'optsection-' + seci;
      children[i].className = 'optsection';
      legends = children[i].getElementsByTagName('legend');
      sections[seci] = new Object();
      if(legends[0] && legends[0].firstChild.nodeValue)
        sections[seci].text = legends[0].firstChild.nodeValue;
      else
        sections[seci].text = '# ' + seci;
      sections[seci].secid = children[i].id;
      sections[seci].error = containsError(children[i]);
      seci++;
      if(sections.length != 1)
        children[i].style.display = 'none';
      else
        var selectedid = children[i].id;
    }
  }

  var toc = document.createElement('ul');
  toc.id = 'optionsTOC';
  toc.selectedid = selec...
```

[49 of 51] HTML Comments Sensitive Information Disclosure

Severity:	Low
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/options.form
Remediation Tasks:	Remove sensitive information from HTML comments

Variant 1 of 1 [ID=22389]

The following may require user attention:

```
POST /openmrs/options.form HTTP/1.0
Cookie: __openmrs_language=en_GB;
JSESSIONID=97605BBA26DE7D3A3E3E851092661D72
Content-Length: 364
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: 192.168.1.104:8080
```

Content-Type: application/x-www-form-urlencoded
Referer: http://192.168.1.104:8080/openmrs/options.form

defaultLocation=1&defaultLocale=en_GB&proficientLocales=1234&_showRetiredMessage=true&_verbose=true&username=&personName.givenName=&personName.middleName=&personName.familyName=&oldPassword=&newPassword=&confirmPassword=&secretQuestionPassword=&secretQuestionNew=1234&secretAnswerNew=1234&secretAnswerConfirm=1234&notification=internalOnly&notificationAddress=1234
HTTP/1.1 200 OK
Content-Length: 12220
Server: Apache-Coyote/1.1
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache
Cache-Control: no-store
Content-Type: text/html;charset=UTF-8
Content-Language: en-GB
Date: Sun, 25 Oct 2009 00:37:34 GMT
Connection: close

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <script src="/openmrs/openmrs.js?v=1.5.0.35" type="text/javascript" ></script>
    <link href="/openmrs/openmrs.css?v=1.5.0.35" type="text/css" rel="stylesheet" />
    <link href="/openmrs/style.css?v=1.5.0.35" type="text/css" rel="stylesheet" />
    <script src="/openmrs/dwr/engine.js?v=1.5.0.35" type="text/javascript" ></script>
    <script src="/openmrs/dwr/interface/DWRAlertService.js?v=1.5.0.35"

```
></script>

        <title>OpenMRS - User Options</title>

    <script type="text/javascript">
      /* variable used in js to know the context path */
      var openmrsContextPath = '/openmrs';
    </script>

  </head>

<body>
  <div id="pageBody">
    <div id="userBar">

        <span id="userLoggedInAs" class="firstChild">
          Currently logged in as Super  User
        </span>
        <span id="userLogout">
          <a href='/openmrs/logout'>Log out</a>
        </span>
        <span>
          <a href="/openmrs/options.form">My Profile</a>
        </span>

      <span id="userHelp">
        <a href='/openmrs/help.htm'>Help</a>
      </span>
    </div>

    <div id="banner">
      <a href="http://www.openmrs.org">
  <img src="/openmrs/images/openmrs_logo_short.gif" alt="OpenMRS Logo" border="0"/>
</a>
    </div>

      <div id="gutter">
        <ul id="navList">
```

```
    <li id="homeNavLink" class="firstChild">
      <a href="/openmrs/">Home</a>
    </li>

    <li id="findPatientNavLink">
      <a href="/openmrs/findPatient.htm">

            Find/Create Patient


      </a>
    </li>


      <li id="dictionaryNavLink">
        <a href="/openmrs/dictionary">Dictionary</a>
      </li>




      <li id="administrationNavLink">
        <a href="/openmrs/admin">Administration</a>
      </li>



  </ul>
        </div>


      <div id="content">

        <script type="text/javascript">
          // prevents users getting popup alerts when viewing pages
          var handler = function(msg, ex) {
            var div = document.getElementById("openmrs_dwr_error");
            div.style.display = ""; // show the error div
            var msgDiv = document.getElementById("openmrs_dwr_error_msg");
            msgDiv.innerHTML = 'A javascript error has occurred:' + " <b>" + msg + "</b>";

          };
          dwr.engine.setErrorHandler(handler);
          dwr.engine.setWarningHandler(handler);
        </script>




        <div id="openmrs_dwr_error" style="display:none" class="error">
          <div id="openmrs_dwr_error_msg"></div>
```

```
            <div id="openmrs_dwr_error_close" class="smallMessage">
              <i>The full stacktrace for this error can usually be found in your server's error
logs.</i>  
              <a href="#" onclick="this.parentNode.parentNode.style.display='none'">Hide
error</a>
            </div>
          </div>



<script type="text/javascript">

window.onload = init;

function init() {
  var sections = new Array();
  var optform = document.getElementById("optionsForm");
  children = optform.childNodes;
  var seci = 0;
  for(i=0;i<children.length;i++) {
    if(children[i].nodeName.toLowerCase().indexOf('fieldset') != -1) {
      children[i].id = 'optsection-' + seci;
      children[i].className = 'optsection';
      legends = children[i].getElementsByTagName('legend');
      sections[seci] = new Object();
      if(legends[0] && legends[0].firstChild.nodeValue)
        sections[seci].text = legends[0].firstChild.nodeValue;
      else
        sections[seci].text = '# ' + seci;
      sections[seci].secid = children[i].id;
      sections[seci].error = containsError(children[i]);
      seci++;
      if(sections.length != 1)
        children[i].style.display = 'none';
      else
        var selectedid = children[i].id;
    }
  }

  var toc = document.createElement('ul');
  toc.id = 'optionsTOC';
  toc.selectedid = selec...
```

[50 of 51] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/options.form (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=17920]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

[51 of 51] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/options.form (Parameter = defaultLocation)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 8 [ID=18018]

The following changes were applied to the original request:
• Set parameter 'defaultLocation's value to '1XYZ'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/index.htm

Total of 3 security issues in this URL

[1 of 3] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/index.htm (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 6 [ID=8065]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/index.htm/'

[2 of 3] HTML Comments Sensitive Information Disclosure

Severity:	Low
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/index.htm
Remediation Tasks:	Remove sensitive information from HTML comments

Variant 1 of 1 [ID=10648]

The following may require user attention:

```
GET /openmrs/admin/index.htm HTTP/1.0
Cookie: JSESSIONID=39188CAF42540B3EC4FBDA8DBCECA143
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: 192.168.1.104:8080
Referer: http://192.168.1.104:8080/openmrs/admin/
```

HTTP/1.1 200 OK
Content-Length: 11622
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Content-Language: en-US
Date: Sun, 25 Oct 2009 00:36:46 GMT
Connection: close

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <script src="/openmrs/openmrs.js?v=1.5.0.35" type="text/javascript" ></script>
    <link href="/openmrs/openmrs.css?v=1.5.0.35" type="text/css" rel="stylesheet" />
    <link href="/openmrs/style.css?v=1.5.0.35" type="text/css" rel="stylesheet" />
    <script src="/openmrs/dwr/engine.js?v=1.5.0.35" type="text/javascript" ></script>
    <script src="/openmrs/dwr/interface/DWRAlertService.js?v=1.5.0.35"
type="text/javascript" ></script>

        <title>OpenMRS - Home</title>

    <script type="text/javascript">

```
        /* variable used in js to know the context path */
        var openmrsContextPath = '/openmrs';
      </script>



  </head>

<body>
  <div id="pageBody">
    <div id="userBar">


          <span id="userLoggedInAs" class="firstChild">
            Currently logged in as Super  User
          </span>
          <span id="userLogout">
            <a href='/openmrs/logout'>Log out</a>
          </span>
          <span>
            <a href="/openmrs/options.form">My Profile</a>
          </span>




      <span id="userHelp">
        <a href='/openmrs/help.htm'>Help</a>
      </span>
    </div>

    <div id="banner">
      <a href="http://www.openmrs.org">
 <img src="/openmrs/images/openmrs_logo_short.gif" alt="OpenMRS Logo" border="0"/>
</a>
    </div>




      <div id="gutter">
        <ul id="navList">
  <li id="homeNavLink" class="firstChild">
    <a href="/openmrs/">Home</a>
  </li>

  <li id="findPatientNavLink">
    <a href="/openmrs/findPatient.htm">

        Find/Create Patient


    </a>
```

```
    </li>


    <li id="dictionaryNavLink">
      <a href="/openmrs/dictionary">Dictionary</a>
    </li>




    <li id="administrationNavLink">
      <a href="/openmrs/admin">Administration</a>
    </li>



</ul>
    </div>


    <div id="content">

      <script type="text/javascript">
        // prevents users getting popup alerts when viewing pages
        var handler = function(msg, ex) {
          var div = document.getElementById("openmrs_dwr_error");
          div.style.display = ""; // show the error div
          var msgDiv = document.getElementById("openmrs_dwr_error_msg");
          msgDiv.innerHTML = 'A javascript error has occurred:' + " <b>" + msg + "</b>";

        };
        dwr.engine.setErrorHandler(handler);
        dwr.engine.setWarningHandler(handler);
      </script>




      <div id="openmrs_dwr_error" style="display:none" class="error">
        <div id="openmrs_dwr_error_msg"></div>
        <div id="openmrs_dwr_error_close" class="smallMessage">
          <i>The full stacktrace for this error can usually be found in your server's error
logs.</i>  
          <a href="#" onclick="this.parentNode.parentNode.style.display='none'">Hide
error</a>
        </div>
      </div>
```

```
   .adminMenuList #menu li {
      display: list-item;
      border-left-width: 0px;

   }
   .adminMenuList #menu li.first {
      display: none;
   }
   .adminMenuList #menu {
      list-style: none;
      margin-left: 10px;
      margin-top: 0;
   }
   h4 {
      margin-bottom: 0;
   }
</style>

<h2>Administration</h2>

<table border="0" width="93%">
   <tbody>
   <tr>

      <td valign="top" width="30%">


            <div class="adminMenuList">
               <h4>Users</h4>
                  <ul id="menu">
   <li class="first">
      <a href="/openmrs/admin">Admin</a>
   </li>

      <li >
         <a href="/openmrs/admin/users/user.list">
            Manage Users
         </a>
      </li>


      <li >
         <a href="/openmrs/admin/users/role.list">
            Manage Roles
         </a>
      </li>


      <li >
         <a href="/openmrs/admin/users/privilege.list">
            Manage Privileges
         </a>
      </li>
```

```
        <li >
          <a href="/openmrs/admin/users/alert.list">
            Manage Alerts
          </a>
        </li>


</ul>
            </div>



            <div class="adminMenuList">
               <h4>Patients</h4>
                  <ul id="menu">
    <li class="first">
      <a href="/openmrs/admin">Admin</a>
    </li>

        <li >
          <a href="/openmrs/admin/patients/">
            Manage Patients
          </a>
        </li>




          <li >
            <a href="/openmrs/admin/patients/tribe.list">
              Manage Tribes
            </a>
          </li>



        <li >
          <a href="/openmrs/admin/patients/findDuplicatePatients.htm">
            Find Patients to Merge
          </a>
        </li>


        <li >
          <a href="/openmrs/admin/patients/patientIdentifierType.list">
            Manage Identifier ...
```

[3 of 3] Application Error

Severity: Informational

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/index.htm (Parameter = lang)

Remediation Tasks: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=17505]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/dictionary/

Total of 14 security issues in this URL

[1 of 14] Blind SQL Injection

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/dictionary/ (Parameter = [x].source)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=66733]

The following changes were applied to the original request:
• Set parameter '[x].source's value to '%2F**%2Fand%2F**%2F7659%3D7659'

[2 of 14] Blind SQL Injection

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/dictionary/ (Parameter = concept.conceptSets)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=64403]

The following changes were applied to the original request:
• Set parameter 'concept.conceptSets's value to '%27+and+%27foobar%27%3D%27foobar%27+--'

[3 of 14] Blind SQL Injection

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/dictionary/ (Parameter = concept.version)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=66842]

The following changes were applied to the original request:
• Set parameter 'concept.version's value to '%27+%2B+%27%27+%2B+%271234'

[4 of 14] Blind SQL Injection

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/dictionary/ (Parameter = concept.conceptClass)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 1 [ID=63945]

The following changes were applied to the original request:
• Set parameter 'concept.conceptClass's value to '15%27+and+%27foobar%27%3D%27foobar%27+--'

[5 of 14] Blind SQL Injection

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/dictionary/ (Parameter = lowCritical)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 1 [ID=65537]

The following changes were applied to the original request:
• Set parameter 'lowCritical's value to '%27+%7C%7C+%27%27+%7C%7C+%271234'

[6 of 14] Blind SQL Injection

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/dictionary/ (Parameter = shortNamesByLocale[en].name)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 1 [ID=63548]

The following changes were applied to the original request:
• Set parameter 'shortNamesByLocale[en].name's value to '%27+%7C%7C+%27%27+%7C%7C+%27'

[7 of 14] Blind SQL Injection

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/dictionary/ (Parameter = lowNormal)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 1 [ID=65342]

The following changes were applied to the original request:

• Set parameter 'lowNormal's value to '0%2B0%2B0%2B1234'

[8 of 14] Blind SQL Injection

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/dictionary/ (Parameter = namesByLocale[en].name)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=63436]

The following changes were applied to the original request:
• Set parameter 'namesByLocale[en].name's value to '+and+7659%3D7659'

[9 of 14] Blind SQL Injection

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/dictionary/ (Parameter = [x].sourceCode)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=66544]

The following changes were applied to the original request:
• Set parameter '[x].sourceCode's value to '0%2B0%2B0%2B1234'

[10 of 14] Blind SQL Injection

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/dictionary/ (Parameter = [x].name)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=63836]

The following changes were applied to the original request:
• Set parameter '[x].name's value to '%2F**%2Fand%2F**%2F7659%3D7659'

[11 of 14] Blind SQL Injection

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/dictionary/ (Parameter = concept.answers)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=64684]

The following changes were applied to the original request:
• Set parameter 'concept.answers's value to '%27+and+%27foobar%27%3D%27foobar'

[12 of 14] Blind SQL Injection

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/dictionary/ (Parameter = units)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 1 [ID=65910]

The following changes were applied to the original request:
• Set parameter 'units's value to '1234%27+and+%27foobar%27%3D%27foobar%27+--'

[13 of 14] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/dictionary/ (Parameter = lowCritical)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=65667]

[14 of 14] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/dictionary/ (Parameter = concept.datatype)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=64629]

The following changes were applied to the original request:
• Set parameter 'concept.datatype's value to ';'

Vulnerable URL: http://192.168.1.104:8080/openmrs/dictionary/concept.form

Total of 4 security issues in this URL

[1 of 4] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/dictionary/concept.form (Parameter = lang)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 1 [ID=67693]

The following changes were applied to the original request:
• Set parameter 'lang's value to 'en_US";alert(242793);//'

[2 of 4] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/dictionary/concept.form (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 6 [ID=22582]

The following changes were applied to the original request:
• Set path to '/openmrs/dictionary/concept.form/'

[3 of 4] Stored Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/dictionary/concept.form (= lang)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 1 [ID=141119]

The following changes were applied to the original request:
• Set parameter 'lang's value to 'en_US'%20and%20'foobar'='foobar'

[4 of 4] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/dictionary/concept.form (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=67784]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/dictionary/concept.htm

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/dictionary/concept.htm (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=54774]

The following changes were applied to the original request:
• Set path to '/openmrs/dictionary/concept.htm/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/dictionary/conceptForm.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/dictionary/conceptForm.js (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=22682]

The following changes were applied to the original request:
• Set path to '/openmrs/dictionary/conceptForm.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/dictionary/index.htm

Total of 5 security issues in this URL

[1 of 5] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/dictionary/index.htm (Parameter = phrase)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 28 [ID=63070]

The following changes were applied to the original request:
• Set parameter 'phrase's value to '1234>%22%27><img%20src%3d%22javascript:alert(231253)%22>'

[2 of 5] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/dictionary/index.htm (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 6 [ID=8074]

The following changes were applied to the original request:
• Set path to '/openmrs/dictionary/index.htm/'

[3 of 5] Phishing Through Frames

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/dictionary/index.htm (Parameter = phrase)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=63208]

The following changes were applied to the original request:
• Set parameter 'phrase's value to '1234'"><iframe%20src=http://demo.testfire.net>'

[4 of 5] Link Injection (facilitates Cross-Site Request Forgery)

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/dictionary/index.htm (Parameter = phrase)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=63221]

The following changes were applied to the original request:
• Set parameter 'phrase's value to ""><IMG%20SRC="/WF_XSRF.html">'

[5 of 5] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/dictionary/index.htm (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=23830]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/

Total of 1 security issues in this URL

[1 of 1] Insecure HTTP Methods Enabled

Severity:	Medium
Test Type:	Infrastructure
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/
Remediation Tasks:	Disable WebDAV, or disallow unneeded HTTP methods

Variant 1 of 1 [ID=6039]

The following changes were applied to the original request:

• Set path to '/openmrs/scripts/'
• Set method to 'OPTIONS'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojoConfig.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojoConfig.js (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=8083]

The following changes were applied to the original request:
• Set path to '/openmrs/scripts/dojoConfig.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojoUserSearchIncludes.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojoUserSearchIncludes.js (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=33329]

The following changes were applied to the original request:
• Set path to '/openmrs/scripts/dojoUserSearchIncludes.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/obs.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/obs.js (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=12950]

The following changes were applied to the original request:
• Set path to '/openmrs/scripts/obs.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/validation.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/validation.js (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=30322]

The following changes were applied to the original request:
• Set path to '/openmrs/scripts/validation.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/concepts/conceptClass.form

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/concepts/conceptClass.form (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 4 [ID=39890]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/concepts/conceptClass.form/'

[2 of 2] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/concepts/conceptClass.form (Parameter = conceptClassId)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 10 [ID=40953]

The following changes were applied to the original request:
• Set parameter 'conceptClassId's value to '1XYZ'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/concepts/conceptClass.list

Total of 3 security issues in this URL

[1 of 3] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/concepts/conceptClass.list (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 5 [ID=15941]

The following changes were applied to the original request:
- Set path to '/openmrs/admin/concepts/conceptClass.list/'

[2 of 3] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/concepts/conceptClass.list (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=41218]

The following changes were applied to the original request:
- Set parameter 'lang's value to '%00'

[3 of 3] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/concepts/conceptClass.list (Parameter = conceptClassId)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 12 [ID=40590]

The following changes were applied to the original request:
- Set parameter 'conceptClassId's value to '1XYZ'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/concepts/conceptDatatype.form

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/concepts/conceptDatatype.form (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 3 [ID=43000]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/concepts/conceptDatatype.form/'

[2 of 2] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/concepts/conceptDatatype.form (Parameter = conceptDatatypeId)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 10 [ID=43608]

The following changes were applied to the original request:
• Set parameter 'conceptDatatypeId's value to '1XYZ'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/concepts/conceptDatatype.list

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/concepts/conceptDatatype.list (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 5 [ID=16033]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/concepts/conceptDatatype.list/'

[2 of 2] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/concepts/conceptDatatype.list (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=43873]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/concepts/conceptDrug.form

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/concepts/conceptDrug.form (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 3 [ID=44940]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/concepts/conceptDrug.form/'

[2 of 2] Application Error

Severity: Informational

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/concepts/conceptDrug.form (Parameter = drugId)

Remediation Tasks: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 10 [ID=45483]

The following changes were applied to the original request:
• Set parameter 'drugId's value to '2XYZ'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/concepts/conceptDrug.list

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/concepts/conceptDrug.list (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 5 [ID=15573]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/concepts/conceptDrug.list/'

[2 of 2] Application Error

Severity: Informational

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/concepts/conceptDrug.list (Parameter = lang)

Remediation Tasks: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 2 [ID=45742]

The following changes were applied to the original request:
• Set parameter 'lang's value to '\"

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/concepts/conceptProposal.list

Total of 5 security issues in this URL

[1 of 5] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/concepts/conceptProposal.list (Parameter = includeCompleted)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 5 [ID=41628]

The following changes were applied to the original request:
• Injected 'false>"><script>alert(157407)</script>' into parameter 'includeCompleted's value

[2 of 5] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/concepts/conceptProposal.list (Parameter = sortOn)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 5 [ID=41982]

The following changes were applied to the original request:
• Injected 'occurences>"><script>alert(158115)</script>' into parameter 'sortOn's value

[3 of 5] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/concepts/conceptProposal.list (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 6 [ID=15665]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/concepts/conceptProposal.list/'

[4 of 5] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/concepts/conceptProposal.list (Parameter = sortOrder)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 5 [ID=41805]

The following changes were applied to the original request:
• Injected 'desc>"><script>alert(157761)</script>' into parameter 'sortOrder's value

[5 of 5] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/concepts/conceptProposal.list (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 2 [ID=41565]

The following changes were applied to the original request:
• Set parameter 'lang's value to '"

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/concepts/conceptSetDerived.form

Total of 3 security issues in this URL

[1 of 3] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/concepts/conceptSetDerived.form (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 5 [ID=15849]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/concepts/conceptSetDerived.form/'

[2 of 3] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/concepts/conceptSetDerived.form (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=38751]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

[3 of 3] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/concepts/conceptSetDerived.form (Parameter = conceptId)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 7 [ID=38565]

The following changes were applied to the original request:
• Set parameter 'conceptId's value to '%27'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/concepts/conceptSource.form

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/concepts/conceptSource.form (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 3 [ID=45032]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/concepts/conceptSource.form/'

[2 of 2] Database Error Pattern Found

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/concepts/conceptSource.form (=)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 1 [ID=141116]

The following changes were applied to the original request:
• Set method to 'POST'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/concepts/conceptSource.list

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/concepts/conceptSource.list (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 5 [ID=16125]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/concepts/conceptSource.list/'

[2 of 2] Application Error

Severity: Informational

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/concepts/conceptSource.list (Parameter = lang)

Remediation Tasks: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=45925]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/concepts/conceptWord.form

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/concepts/conceptWord.form (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 5 [ID=15757]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/concepts/conceptWord.form/'

[2 of 2] Application Error

Severity: Informational

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/concepts/conceptWord.form (Parameter = lang)

Remediation Tasks: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=37919]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/concepts/proposeConcept.form

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/concepts/proposeConcept.form (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 3 [ID=39982]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/concepts/proposeConcept.form/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/encounters/encounter.form

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/encounters/encounter.form (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 4 [ID=36393]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/encounters/encounter.form/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/encounters/encounterType.form

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/encounters/encounterType.form (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 4 [ID=32961]

The following changes were applied to the original request:

• Set path to '/openmrs/admin/encounters/encounterType.form/'

[2 of 2] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/encounters/encounterType.form (Parameter = encounterTypeId)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 10 [ID=34310]

The following changes were applied to the original request:
• Set parameter 'encounterTypeId's value to '1XYZ'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/encounters/encounterType.list

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/encounters/encounterType.list (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 5 [ID=12749]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/encounters/encounterType.list/'

[2 of 2] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/encounters/encounterType.list (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=34575]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/encounters/index.htm

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/encounters/index.htm (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 4 [ID=12648]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/encounters/index.htm/'

[2 of 2] Application Error

Severity: Informational

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/encounters/index.htm (Parameter = lang)

Remediation Tasks: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=37636]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/encounters/location.form

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/encounters/location.form (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 4 [ID=32869]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/encounters/location.form/'

[2 of 2] Application Error

Severity: Informational

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/encounters/location.form (Parameter = locationId)

Remediation Tasks: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 10 [ID=33770]

The following changes were applied to the original request:
• Set parameter 'locationId's value to '1XYZ'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/encounters/location.list

Total of 3 security issues in this URL

[1 of 3] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/encounters/location.list (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 5 [ID=12657]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/encounters/location.list/'

[2 of 3] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/encounters/location.list (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=34035]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

[3 of 3] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/encounters/location.list (Parameter = locationId)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 12 [ID=33407]

The following changes were applied to the original request:
• Set parameter 'locationId's value to '1XYZ'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/forms/field.form

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/forms/field.form (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 3 [ID=49959]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/forms/field.form/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/forms/field.list

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/forms/field.list (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 5 [ID=16309]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/forms/field.list/'

[2 of 2] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/forms/field.list (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=52912]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/forms/fieldType.form

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/forms/fieldType.form (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 4 [ID=43092]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/forms/fieldType.form/'

[2 of 2] Application Error

Severity: Informational

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/forms/fieldType.form (Parameter = fieldTypeId)

Remediation Tasks: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 10 [ID=44148]

The following changes were applied to the original request:
• Set parameter 'fieldTypeId's value to '1XYZ'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/forms/fieldType.list

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/forms/fieldType.list (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 5 [ID=16401]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/forms/fieldType.list/'

[2 of 2] Application Error

Severity: Informational

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/forms/fieldType.list (Parameter = lang)

Remediation Tasks: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=45385]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/forms/form.list

Total of 3 security issues in this URL

[1 of 3] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/forms/form.list (Parameter = duplicateFormId)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 10 [ID=46163]

The following changes were applied to the original request:
• Injected '1>"><script>alert(184439)</script>' into parameter 'duplicateFormId's value

[2 of 3] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/forms/form.list (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 5 [ID=16217]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/forms/form.list/'

[3 of 3] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/forms/form.list (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=47291]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/forms/formEdit.form

Total of 3 security issues in this URL

[1 of 3] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/forms/formEdit.form (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 5 [ID=44780]

The following changes were applied to the original request:
• Injected '>"'><script>alert(181673)</script>' into parameter 'duplicate's value
• Injected '>"'><script>alert(181673)</script>' into parameter 'formId's value

[2 of 3] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/forms/formEdit.form (Parameter = formId)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 17 [ID=46707]

The following changes were applied to the original request:
• Set parameter 'formId's value to '1>%22%27><img%20src%3d%22javascript:alert(185527)%22>'

[3 of 3] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/forms/formEdit.form (Parameter = duplicate)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 5 [ID=46893]

The following changes were applied to the original request:
• Injected 'true>"><script>alert(185899)</script>' into parameter 'duplicate's value

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/forms/formSchemaDesign.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/forms/formSchemaDesign.js (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=45216]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/forms/formSchemaDesign.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/hl7/

Total of 1 security issues in this URL

[1 of 1] Insecure HTTP Methods Enabled

Severity:	Medium
Test Type:	Infrastructure
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/hl7/
Remediation Tasks:	Disable WebDAV, or disallow unneeded HTTP methods

Variant 1 of 1 [ID=14832]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/hl7/'
• Set method to 'OPTIONS'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/hl7/hl7InError.list

Total of 3 security issues in this URL

[1 of 3] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/hl7/hl7InError.list (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 5 [ID=16585]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/hl7/hl7InError.list/'

[2 of 3] Blind SQL Injection

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/hl7/hl7InError.list (Parameter = lang)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 1 [ID=45975]

The following changes were applied to the original request:
• Set parameter 'lang's value to '"%20||%20"%20||%20'en_US'

[3 of 3] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/hl7/hl7InError.list (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=46102]

The following changes were applied to the original request:
- Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/hl7/hl7InQueue.list

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/hl7/hl7InQueue.list (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 5 [ID=16493]

The following changes were applied to the original request:
- Set path to '/openmrs/admin/hl7/hl7InQueue.list/'

[2 of 2] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/hl7/hl7InQueue.list (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=44050]

The following changes were applied to the original request:
- Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/

Total of 1 security issues in this URL

[1 of 1] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/maintenance/ (Parameter = passphrase)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=48637]

The following changes were applied to the original request:
• Set parameter 'passphrase's value to ""

Vulnerable URL:
http://192.168.1.104:8080/openmrs/admin/maintenance/auditPatientIdentifiers.htm

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/maintenance/auditPatientIdentifiers.htm (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 4 [ID=16778]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/maintenance/auditPatientIdentifiers.htm/'

[2 of 2] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/maintenance/auditPatientIdentifiers.htm (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=50765]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

Vulnerable URL:
http://192.168.1.104:8080/openmrs/admin/maintenance/databaseChangesInfo.list

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/databaseChangesInfo.list (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 5 [ID=16988]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/maintenance/databaseChangesInfo.list/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/globalProps.form

Total of 10 security issues in this URL

[1 of 10] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/globalProps.form (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 6 [ID=16796]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/maintenance/globalProps.form/'

[2 of 10] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/globalProps.form (Parameter = property)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 7 [ID=53140]

The following changes were applied to the original request:
• Set parameter 'property's value to '1234>%22%27><img%20src%3d%22javascript:alert(205161)%22>'

[3 of 10] Blind SQL Injection

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/globalProps.form (Parameter = description)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=54034]

The following changes were applied to the original request:
• Set parameter 'description's value to 'Concept%2Bid%2Bof%2Bthe%2Bconcept%2Bdefining%2Bthe%2BCAUSE%2BOF%2BDEATH%2Bconcept%27+and+%27foobar%27%3D%27foobar'

[4 of 10] Stored Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/globalProps.form (= property)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=141117]

The following changes were applied to the original request:
• Set parameter 'property's value to '%27+%7C%7C+%27%27+%7C%7C+%271234'

[5 of 10] Link Injection (facilitates Cross-Site Request Forgery)

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/globalProps.form (Parameter = property)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=53287]

The following changes were applied to the original request:
• Set parameter 'property's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[6 of 10] Application Error

Severity: Informational

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/globalProps.form (Parameter = lang)

Remediation Tasks: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 2 [ID=53986]

The following changes were applied to the original request:
• Set parameter 'lang's value to ')'

[7 of 10] Application Error

Severity: Informational

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/globalProps.form (Parameter = property)

Remediation Tasks: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=53265]

[8 of 10] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/maintenance/globalProps.form (Parameter = description)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 2 [ID=53631]

[9 of 10] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/maintenance/globalProps.form (Parameter = value)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=53444]

[10 of 10] Email Address Pattern Found

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/maintenance/globalProps.form
Remediation Tasks:	Remove email addresses from the website

Variant 1 of 1 [ID=17532]

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/implementationid.form

Total of 17 security issues in this URL

[1 of 17] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/maintenance/implementationid.form (Parameter = implementationId)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 13 [ID=47981]

The following changes were applied to the original request:
• Set parameter 'implementationId's value to '>%22%27><img%20src%3d%22javascript:alert(188075)%22>'

[2 of 17] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/implementationid.form (Parameter = passphrase)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 12 [ID=48087]

The following changes were applied to the original request:
• Set parameter 'passphrase's value to '>%22%27><img%20src%3d%22javascript:alert(188287)%22>'

[3 of 17] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/implementationid.form (Parameter = name)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 14 [ID=47875]

The following changes were applied to the original request:
• Set parameter 'name's value to '>%22%27><img%20src%3d%22javascript:alert(187863)%22>'

[4 of 17] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/implementationid.form (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 7 [ID=16677]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/maintenance/implementationid.form/'

[5 of 17] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/implementationid.form (Parameter = description)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 4 [ID=48209]

The following changes were applied to the original request:
• Injected '1234</TextArea><script>alert(188531)</script>' into parameter 'description's value

[6 of 17] Blind SQL Injection

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/implementationid.form (Parameter = implementationId)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 3 [ID=47974]

The following changes were applied to the original request:
• Set parameter 'implementationId's value to '+and+7659%3D7659'

[7 of 17] Blind SQL Injection

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/implementationid.form (Parameter = passphrase)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=48081]

The following changes were applied to the original request:
• Set parameter 'passphrase's value to '%2F**%2Fand%2F**%2F7659%3D7659'

[8 of 17] Stored Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/implementationid.form (=)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=141115]

[9 of 17] DOM Based Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/implementationid.form

Remediation Tasks: Analyze client side code and sanitize its input sources

Variant 1 of 1 [ID=48224]

The following changes were applied to the original request:
• Set parameter 'description's value to '%3Cscript%3Ewindow.open%28%27http%3A%2F%2FDOMXSSSucceeded%2F%27%29%3C%2Fscript%3E'

[10 of 17] Cross-Site Request Forgery

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/implementationid.form

Remediation Tasks: Decline malicious requests

Variant 1 of 3 [ID=44875]

[11 of 17] Phishing Through Frames

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/implementationid.form (Parameter = implementationId)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=48038]

The following changes were applied to the original request:
• Set parameter 'implementationId's value to '%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%3E'

[12 of 17] Phishing Through Frames

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/implementationid.form (Parameter = passphrase)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=48144]

The following changes were applied to the original request:
• Set parameter 'passphrase's value to '%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%3E'

[13 of 17] Phishing Through Frames

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/implementationid.form (Parameter = name)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=47932]

The following changes were applied to the original request:
• Set parameter 'name's value to '%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%3E'

[14 of 17] Link Injection (facilitates Cross-Site Request Forgery)

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/implementationid.form (Parameter = implementationId)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=48051]

The following changes were applied to the original request:
• Set parameter 'implementationId's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[15 of 17] Link Injection (facilitates Cross-Site Request Forgery)

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/implementationid.form (Parameter = passphrase)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=48157]

The following changes were applied to the original request:
• Set parameter 'passphrase's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[16 of 17] Link Injection (facilitates Cross-Site Request Forgery)

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/implementationid.form (Parameter = name)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=47945]

The following changes were applied to the original request:
• Set parameter 'name's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[17 of 17] Application Error

Severity: Informational

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/implementationid.form (Parameter = lang)

Remediation Tasks: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=49007]

The following changes were applied to the original request:

• Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/patientsWhoAreUsers.list

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/maintenance/patientsWhoAreUsers.list (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 5 [ID=17080]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/maintenance/patientsWhoAreUsers.list/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/quickReport.htm

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/maintenance/quickReport.htm (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 4 [ID=16787]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/maintenance/quickReport.htm/'

[2 of 2] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/maintenance/quickReport.htm (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=47645]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/serverLog.form

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/maintenance/serverLog.form (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 5 [ID=16896]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/maintenance/serverLog.form/'

[2 of 2] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/maintenance/serverLog.form (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=50942]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/maintenance/systemInfo.htm

Total of 3 security issues in this URL

[1 of 3] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/maintenance/systemInfo.htm (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 4 [ID=16769]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/maintenance/systemInfo.htm/'

[2 of 3] Internal IP Disclosure Pattern Found

Severity:	Low
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/maintenance/systemInfo.htm
Remediation Tasks:	Remove internal IP addresses from your website

Variant 1 of 2 [ID=17531]

[3 of 3] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/maintenance/systemInfo.htm (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=47468]

The following changes were applied to the original request:
- Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/modules/

Total of 1 security issues in this URL

[1 of 1] Insecure HTTP Methods Enabled

Severity:	Medium
Test Type:	Infrastructure
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/modules/
Remediation Tasks:	Disable WebDAV, or disallow unneeded HTTP methods

Variant 1 of 1 [ID=15039]

The following changes were applied to the original request:
- Set path to '/openmrs/admin/modules/'
- Set method to 'OPTIONS'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/modules/module.list

Total of 4 security issues in this URL

[1 of 4] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/modules/module.list (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 5 [ID=17172]

The following changes were applied to the original request:
- Set path to '/openmrs/admin/modules/module.list/'

[2 of 4] Blind SQL Injection

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/modules/module.list (Parameter = moduleFile)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 1 [ID=52045]

The following changes were applied to the original request:
• Set parameter 'moduleFile's value to '1234+and+7659%3D7659'

[3 of 4] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/modules/module.list (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=52566]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

[4 of 4] Potential File Upload

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/modules/module.list (Parameter = moduleFile)
Remediation Tasks:	Restrict user capabilities and permissions during the file upload process

Variant 1 of 1 [ID=52236]

The following may require user attention:

```
POST /openmrs/admin/modules/module.list HTTP/1.0
Cookie: __openmrs_language=en_US;
JSESSIONID=7561E09B61226638A3D50A2AF89CC20B
Content-Length: 253
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: 192.168.1.104:8080
Content-Type: multipart/form-data; boundary=AppScan_boundary_KOMJI
Referer: http://192.168.1.104:8080/openmrs/admin/modules/module.list

--AppScan_boundary_KOMJI
Content-Disposition: form-data; name="moduleFile"; filename="1234"
Content-Type: application/octet-stream
```

1234
--AppScan_boundary_KOMJI
Content-Disposition: form-data; name="action"

upload
--AppScan_boundary_KOMJI--

HTTP/1.1 302 Moved Temporarily
Content-Length: 0
Server: Apache-Coyote/1.1
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache
Cache-Control: no-store
Location: http://192.168.1.104:8080/openmrs/admin/modules/module.list
Content-Language: en-US
Date: Sun, 25 Oct 2009 00:39:58 GMT
Connection: close

GET /openmrs/admin/modules/module.list HTTP/1.0
Cookie: __openmrs_language=en_GB;
JSESSIONID=97605BBA26DE7D3A3E3E851092661D72
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: 192.168.1.104:8080
Referer: http://192.168.1.104:8080/openmrs/admin/index.htm

HTTP/1.1 200 OK
Content-Length: 4995
Server: Apache-Coyote/1.1
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache
Cache-Control: no-store
Content-Type: text/html;charset=UTF-8
Content-Language: en-GB
Date: Sun, 25 Oct 2009 00:37:21 GMT
Connection: close

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">



<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <script src="/openmrs/openmrs.js?v=1.5.0.35" type="text/javascript" ></script>
    <link href="/openmrs/openmrs.css?v=1.5.0.35" type="text/css" rel="stylesheet" />
    <link href="/openmrs/style.css?v=1.5.0.35" type="text/css" rel="stylesheet" />
    <script src="/openmrs/dwr/engine.js?v=1.5.0.35" type="text/javascript" ></script>
    <script src="/openmrs/dwr/interface/DWRAlertService.js?v=1.5.0.35"
type="text/javascript" ></script>



        <title>OpenMRS </title>



    <script type="text/javascript">
      /* variable used in js to know the context path */
      var openmrsContextPath = '/openmrs';
    </script>



  </head>

<body>
  <div id="pageBody">
    <div id="userBar">


          <span id="userLoggedInAs" class="firstChild">
            Currently logged in as Super  User
          </span>
          <span id="userLogout">
            <a href='/openmrs/logout'>Log out</a>
          </span>
```

```
                <span>
                   <a href="/openmrs/options.form">My Profile</a>
                </span>



            <span id="userHelp">
               <a href='/openmrs/help.htm'>Help</a>
            </span>
         </div>

         <div id="banner">
            <a href="http://www.openmrs.org">
  <img src="/openmrs/images/openmrs_logo_short.gif" alt="OpenMRS Logo" border="0"/>
</a>
         </div>



            <div id="gutter">
               <ul id="navList">
   <li id="homeNavLink" class="firstChild">
      <a href="/openmrs/">Home</a>
   </li>

   <li id="findPatientNavLink">
      <a href="/openmrs/findPatient.htm">

            Find/Create Patient


      </a>
   </li>


      <li id="dictionaryNavLink">
         <a href="/openmrs/dictionary">Dictionary</a>
      </li>




      <li id="administrationNavLink">
         <a href="/openmrs/admin">Administration</a>
      </li>



</ul>
            </div>
```

```
      <div id="content">

        <script type="text/javascript">
          // prevents users getting popup alerts when viewing pages
          var handler = function(msg, ex) {
            var div = document.getElementById("openmrs_dwr_error");
            div.style.display = ""; // show the error div
            var msgDiv = document.getElementById("openmrs_dwr_error_msg");
            msgDiv.innerHTML = 'A javascript error has occurred:' + " <b>" + msg + "</b>";

          };
          dwr.engine.setErrorHandler(handler);
          dwr.engine.setWarningHandler(handler);
        </script>




        <div id="openmrs_dwr_error" style="display:none" class="error">
          <div id="openmrs_dwr_error_msg"></div>
          <div id="openmrs_dwr_error_close" class="smallMessage">
            <i>The full stacktrace for this error can usually be found in your server's error
logs.</i>  
            <a href="#" onclick="this.parentNode.parentNode.style.display='none'">Hide
error</a>
          </div>
        </div>



<ul id="menu">
  <li class="first">
    <a href="/openmrs/admin">Admin</a>
  </li>

    <li class="active">
      <a href="/openmrs/admin/modules/module.list">
        Manage Modules
      </a>
    </li>


    <li >
      <a href="/openmrs/admin/modules/moduleProperties.form">
        Module Properties
      </a>
    </li>


</ul>
```

<h2>Modules</h2>

<p>NOTE: Adding, removing, or starting modules will restart OpenMRS, me...

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/modules/moduleProperties.form

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/modules/moduleProperties.form (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 5 [ID=17264]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/modules/moduleProperties.form/'

[2 of 2] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/modules/moduleProperties.form (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=51296]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/observations/index.htm

Total of 3 security issues in this URL

[1 of 3] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/observations/index.htm (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 4 [ID=12933]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/observations/index.htm/'

[2 of 3] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/observations/index.htm (Parameter = selectSearchStyle)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 10 [ID=36966]

The following changes were applied to the original request:
• Injected 'byPatientAndConcept>"><script>alert(140944)</script>' into parameter 'selectSearchStyle's value

[3 of 3] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/observations/index.htm (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=37459]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/observations/obs.form

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/observations/obs.form (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 4 [ID=36301]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/observations/obs.form/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/orders/order.form

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/orders/order.form (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 4 [ID=33237]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/orders/order.form/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/orders/order.list

Total of 3 security issues in this URL

[1 of 3] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/orders/order.list (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 5 [ID=12841]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/orders/order.list/'

[2 of 3] Blind SQL Injection

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/orders/order.list (Parameter = lang)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 1 [ID=36779]

The following changes were applied to the original request:
• Set parameter 'lang's value to 'en_GB'%20and%20'foobar'='foobar'

[3 of 3] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/orders/order.list (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=36910]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/orders/orderDrug.form

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/orders/orderDrug.form (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 4 [ID=36213]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/orders/orderDrug.form/'
• Set method to 'POST'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/orders/orderDrug.list

Total of 3 security issues in this URL

[1 of 3] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/orders/orderDrug.list (Parameter = showAll)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 10 [ID=51528]

The following changes were applied to the original request:
• Injected 'true>"><script>alert(201937)</script>' into parameter 'showAll's value

[2 of 3] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/orders/orderDrug.list (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 5 [ID=15113]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/orders/orderDrug.list/'

[3 of 3] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/orders/orderDrug.list (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=51996]

The following changes were applied to the original request:
- Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/orders/orderType.form

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/orders/orderType.form (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 4 [ID=36669]

The following changes were applied to the original request:
- Set path to '/openmrs/admin/orders/orderType.form/'

[2 of 2] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/orders/orderType.form (Parameter = orderTypeId)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 10 [ID=39212]

The following changes were applied to the original request:
- Set parameter 'orderTypeId's value to '1XYZ'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/orders/orderType.list

Total of 4 security issues in this URL

[1 of 4] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/orders/orderType.list (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 5 [ID=15205]

The following changes were applied to the original request:
- Set path to '/openmrs/admin/orders/orderType.list/'

[2 of 4] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/orders/orderType.list (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=40315]

The following changes were applied to the original request:
- Set parameter 'lang's value to '%00'

[3 of 4] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/orders/orderType.list (Parameter = action)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 9 [ID=39106]

The following changes were applied to the original request:
- Cleared the value of parameter 'action'

[4 of 4] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/orders/orderType.list (Parameter = orderTypeId)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 12 [ID=38849]

The following changes were applied to the original request:
- Set parameter 'orderTypeId's value to '1XYZ'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/findDuplicatePatients.htm

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/patients/findDuplicatePatients.htm (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 4 [ID=12355]

The following changes were applied to the original request:
- Set path to '/openmrs/admin/patients/findDuplicatePatients.htm/'

[2 of 2] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/patients/findDuplicatePatients.htm (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=35383]

The following changes were applied to the original request:
- Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/index.htm

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/patients/index.htm (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 4 [ID=12254]

The following changes were applied to the original request:
- Set path to '/openmrs/admin/patients/index.htm/'

[2 of 2] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/patients/index.htm (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=32057]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/mergePatients.form

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/patients/mergePatients.form (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 3 [ID=33145]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/patients/mergePatients.form/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form

Total of 58 security issues in this URL

[1 of 58] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = identifier)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 13 [ID=55140]

The following changes were applied to the original request:
• Set parameter 'identifier's value to '>%22%27><img%20src%3d%22javascript:alert(215393)%22>'

[2 of 58] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = birthdateEstimated)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 32 [ID=56075]

The following changes were applied to the original request:
• Set parameter 'birthdateEstimated's value to 'true>%22%27><img%20src%3d%22javascript:alert(217263)%22>'

[3 of 58] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = addAge)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 10 [ID=22064]

The following changes were applied to the original request:
• Set parameter 'addAge's value to '25"></STYLE><STYLE>@import"javascript:alert(70867)";</STYLE>'

[4 of 58] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = deathDate)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 28 [ID=57962]

The following changes were applied to the original request:
• Set parameter 'deathDate's value to '1234>%22%27><img%20src%3d%22javascript:alert(221037)%22>'

[5 of 58] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = dead)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 16 [ID=57780]

The following changes were applied to the original request:
• Set parameter 'dead's value to 'on>%22%27><img%20src%3d%22javascript:alert(220673)%

22>'

[6 of 58] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = address.address2)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 26 [ID=56431]

The following changes were applied to the original request:
• Set parameter 'address.address2's value to '753+Main+Street>%22%27><img%20src%3d%22javascript:alert(217975)%22>'

[7 of 58] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = birthdate)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 25 [ID=55801]

The following changes were applied to the original request:
• Injected '1234>"><script>alert(216715)</script>' into parameter 'birthdate's value

[8 of 58] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = address.cityVillage)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 28 [ID=56610]

The following changes were applied to the original request:
• Set parameter 'address.cityVillage's value to '753+Main+Street>%22%27><img%20src%3d%22javascript:alert(218333)%22>'

[9 of 58] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = addBirthdate)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 10 [ID=21875]

The following changes were applied to the original request:
• Injected '1234>"><script>alert(70489)</script>' into parameter 'addBirthdate's value

[10 of 58] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 12 [ID=17608]

The following changes were applied to the original request:
- Injected '>"'><script>alert(61955)</script>' into parameter 'addName's value
- Injected '>"'><script>alert(61955)</script>' into parameter 'addBirthdate's value
- Injected '>"'><script>alert(61955)</script>' into parameter 'addAge's value
- Injected '>"'><script>alert(61955)</script>' into parameter 'addGender's value

[11 of 58] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = addName)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 13 [ID=21770]

The following changes were applied to the original request:
- Injected '>"><script>alert(70279)</script>' into parameter 'addName's value

[12 of 58] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = address.address1)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 25 [ID=56252]

The following changes were applied to the original request:
- Set parameter 'address.address1's value to '753+Main+Street>%22%27><img%20src%3d%22javascript:alert(217617)%22>'

[13 of 58] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = address.stateProvince)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 28 [ID=56789]

The following changes were applied to the original request:

• Set parameter 'address.stateProvince's value to '753+Main+Street>%22%27><img%20src%3d%22javascript:alert(218691)%22>'

[14 of 58] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = name.middleName)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 27 [ID=54928]

The following changes were applied to the original request:
• Set parameter 'name.middleName's value to '>%22%27><img%20src%3d%22javascript:alert(214969)%22>'

[15 of 58] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = name.givenName)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 28 [ID=54822]

The following changes were applied to the original request:
• Set parameter 'name.givenName's value to '>%22%27><img%20src%3d%22javascript:alert(214757)%22>'

[16 of 58] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = addGender)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 10 [ID=22242]

The following changes were applied to the original request:
• Injected 'M>"><script>alert(71223)</script>' into parameter 'addGender's value

[17 of 58] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = address.postalCode)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 28 [ID=57147]

The following changes were applied to the original request:

• Set parameter 'address.postalCode's value to '753+Main+Street>%22%27><img%20src%3d%22javascript:alert(219407)%22>'

[18 of 58] Blind SQL Injection

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = identifier)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=55134]

The following changes were applied to the original request:
• Set parameter 'identifier's value to '%2F**%2Fand%2F**%2F7659%3D7659'

[19 of 58] Blind SQL Injection

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = identifierType)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=59934]

The following changes were applied to the original request:
• Set parameter 'identifierType's value to '1%27+and+%27foobar%27%3D%27foobar%27+--'

[20 of 58] Blind SQL Injection

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = _birthdateEstimated)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=55979]

The following changes were applied to the original request:
• Set parameter '_birthdateEstimated's value to '%27+and+%27foobar%27%3D%27foobar%27+--'

[21 of 58] Blind SQL Injection

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = deathDate)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=57958]

The following changes were applied to the original request:
• Set parameter 'deathDate's value to '1234%27+and+%27foobar%27%3D%27foobar%27+--'

[22 of 58] Blind SQL Injection

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = gender)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=58415]

The following changes were applied to the original request:
• Set parameter 'gender's value to 'M%27+and+%27foobar%27%3D%27foobar%27%29+--'

[23 of 58] Blind SQL Injection

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = address.country)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=56965]

The following changes were applied to the original request:
• Set parameter 'address.country's value to '753+Main+Street%27+and+%27foobar%27%3D%27foobar%27%29+--'

[24 of 58] Blind SQL Injection

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = birthdate)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=55792]

The following changes were applied to the original request:
• Set parameter 'birthdate's value to '1234%27+and+%27foobar%27%3D%27foobar%27+--'

[25 of 58] Blind SQL Injection

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = address.address1)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=61027]

The following changes were applied to the original request:
• Set parameter 'address.address1's value to '0%2B0%2B0%2B1234'

[26 of 58] Blind SQL Injection

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = address.stateProvince)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=56786]

The following changes were applied to the original request:
• Set parameter 'address.stateProvince's value to '753+Main+Street%27+and+%27foobar%27%3D%27foobar%27%29+--'

[27 of 58] Blind SQL Injection

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = name.middleName)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=54925]

The following changes were applied to the original request:
• Set parameter 'name.middleName's value to '%27+and+%27foobar%27%3D%27foobar%27%29+--'

[28 of 58] Blind SQL Injection

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = address.postalCode)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=61953]

The following changes were applied to the original request:
• Set parameter 'address.postalCode's value to '1234%27+and+%27foobar%27%3D%27foobar%27+--'

[29 of 58] Stored Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (= identifier)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=141118]

The following changes were applied to the original request:
• Set parameter 'identifier's value to '%27+and+%27foobar%27%3D%27foobar%27%29+--'

[30 of 58] Cross-Site Request Forgery

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form

Remediation Tasks: Decline malicious requests

Variant 1 of 3 [ID=54599]

[31 of 58] Phishing Through Frames

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = birthdateEstimated)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=56207]

The following changes were applied to the original request:
• Set parameter 'birthdateEstimated's value to 'true%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%3E'

[32 of 58] Phishing Through Frames

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = deathDate)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=58100]

The following changes were applied to the original request:
• Set parameter 'deathDate's value to '1234%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%3E'

[33 of 58] Phishing Through Frames

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = dead)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=57912]

The following changes were applied to the original request:
• Set parameter 'dead's value to 'on%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%3E'

[34 of 58] Phishing Through Frames

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = address.address2)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=56565]

The following changes were applied to the original request:
• Set parameter 'address.address2's value to '753+Main+Street%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%3E'

[35 of 58] Phishing Through Frames

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = birthdate)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=55934]

The following changes were applied to the original request:
• Set parameter 'birthdate's value to '1234%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%3E'

[36 of 58] Phishing Through Frames

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = address.cityVillage)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=56744]

The following changes were applied to the original request:
• Set parameter 'address.cityVillage's value to '753+Main+Street%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%3E'

[37 of 58] Phishing Through Frames

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = address.address1)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=61173]

The following changes were applied to the original request:
• Set parameter 'address.address1's value to '1234%27%22%3E%3Ciframe+src%3Dhttp%3A%

2F%2Fdemo.testfire.net%3E'

[38 of 58] Phishing Through Frames

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = address.stateProvince)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=56923]

The following changes were applied to the original request:
• Set parameter 'address.stateProvince's value to '753+Main+Street%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%3E'

[39 of 58] Phishing Through Frames

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = name.middleName)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=54985]

The following changes were applied to the original request:
• Set parameter 'name.middleName's value to '%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%3E'

[40 of 58] Phishing Through Frames

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = name.givenName)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=54879]

The following changes were applied to the original request:
• Set parameter 'name.givenName's value to '%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%3E'

[41 of 58] Phishing Through Frames

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = address.postalCode)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=57281]

The following changes were applied to the original request:

• Set parameter 'address.postalCode's value to '753+Main+Street%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%3E'

[42 of 58] Link Injection (facilitates Cross-Site Request Forgery)

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = birthdateEstimated)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=56220]

The following changes were applied to the original request:
• Set parameter 'birthdateEstimated's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[43 of 58] Link Injection (facilitates Cross-Site Request Forgery)

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = deathDate)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=58113]

The following changes were applied to the original request:
• Set parameter 'deathDate's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[44 of 58] Link Injection (facilitates Cross-Site Request Forgery)

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = dead)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=57925]

The following changes were applied to the original request:
• Set parameter 'dead's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[45 of 58] Link Injection (facilitates Cross-Site Request Forgery)

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = address.address2)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=56578]

The following changes were applied to the original request:
• Set parameter 'address.address2's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[46 of 58] Link Injection (facilitates Cross-Site Request Forgery)

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = birthdate)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=55947]

The following changes were applied to the original request:
• Set parameter 'birthdate's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[47 of 58] Link Injection (facilitates Cross-Site Request Forgery)

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = address.cityVillage)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=56757]

The following changes were applied to the original request:
• Set parameter 'address.cityVillage's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[48 of 58] Link Injection (facilitates Cross-Site Request Forgery)

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = address.address1)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=56399]

The following changes were applied to the original request:
• Set parameter 'address.address1's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[49 of 58] Link Injection (facilitates Cross-Site Request Forgery)

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = address.stateProvince)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=56936]

The following changes were applied to the original request:
• Set parameter 'address.stateProvince's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[50 of 58] Link Injection (facilitates Cross-Site Request Forgery)

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = name.middleName)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=54998]

The following changes were applied to the original request:
• Set parameter 'name.middleName's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[51 of 58] Link Injection (facilitates Cross-Site Request Forgery)

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = name.givenName)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=54892]

The following changes were applied to the original request:
• Set parameter 'name.givenName's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[52 of 58] Link Injection (facilitates Cross-Site Request Forgery)

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = address.postalCode)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=57294]

The following changes were applied to the original request:
• Set parameter 'address.postalCode's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[53 of 58] HTML Comments Sensitive Information Disclosure

Severity:	Low
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form
Remediation Tasks:	Remove sensitive information from HTML comments

Variant 1 of 1 [ID=67452]

The following may require user attention:

```
POST /openmrs/admin/patients/newPatient.form HTTP/1.0
Cookie: __openmrs_language=en_US;
JSESSIONID=21F3C6144479E14CEFA882FF8DCAA3DE
Content-Length: 515
Accept: */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: 192.168.1.104:8080
Content-Type: application/x-www-form-urlencoded
Referer: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form?
addName=&addBirthdate=1234&addAge=25&addGender=M

name.givenName=&name.middleName=&name.familyName=&identifier=&identifierType=1
&location=1&closeButton=Remove&birthdate=1234&_birthdateEstimated=&birthdateEstima
ted=true&address.address1=753+Main+Street&address.address2=753+Main+Street&addr
ess.cityVillage=753+Main+Street&address.stateProvince=753+Main+Street&address.count
ry=753+Main+Street&address.postalCode=753+Main+Street&address.latitude=753+Main+
Street&address.longitude=753+Main+Street&_dead=&dead=on&deathDate=1234&patientI
d=&action=Save&gender=M&preferred=
HTTP/1.1 200 OK
Content-Length: 21324
Server: Apache-Coyote/1.1
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache
Cache-Control: no-store
Content-Type: text/html;charset=UTF-8
Content-Language: en-US
Date: Sun, 25 Oct 2009 00:40:22 GMT
Connection: close
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">



<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <script src="/openmrs/openmrs.js?v=1.5.0.35" type="text/javascript" ></script>
    <link href="/openmrs/openmrs.css?v=1.5.0.35" type="text/css" rel="stylesheet" />
    <link href="/openmrs/style.css?v=1.5.0.35" type="text/css" rel="stylesheet" />
    <script src="/openmrs/dwr/engine.js?v=1.5.0.35" type="text/javascript" ></script>
    <script src="/openmrs/dwr/interface/DWRAlertService.js?v=1.5.0.35"
type="text/javascript" ></script>



        <title>OpenMRS </title>



    <script type="text/javascript">
      /* variable used in js to know the context path */
      var openmrsContextPath = '/openmrs';
    </script>



  </head>

<body>
  <div id="pageBody">
    <div id="userBar">


          <span id="userLoggedInAs" class="firstChild">
            Currently logged in as Super  User
          </span>
          <span id="userLogout">
            <a href='/openmrs/logout'>Log out</a>
          </span>
          <span>
```

```
                <a href="/openmrs/options.form">My Profile</a>
              </span>



          <span id="userHelp">
            <a href='/openmrs/help.htm'>Help</a>
          </span>
        </div>

        <div id="banner">
          <a href="http://www.openmrs.org">
  <img src="/openmrs/images/openmrs_logo_short.gif" alt="OpenMRS Logo" border="0"/>
</a>
        </div>



          <div id="gutter">
            <ul id="navList">
    <li id="homeNavLink" class="firstChild">
      <a href="/openmrs/">Home</a>
    </li>

    <li id="findPatientNavLink">
      <a href="/openmrs/findPatient.htm">

            Find/Create Patient


      </a>
    </li>


        <li id="dictionaryNavLink">
          <a href="/openmrs/dictionary">Dictionary</a>
        </li>




        <li id="administrationNavLink">
          <a href="/openmrs/admin">Administration</a>
        </li>



</ul>
          </div>
```

```
      <div id="content">

        <script type="text/javascript">
          // prevents users getting popup alerts when viewing pages
          var handler = function(msg, ex) {
            var div = document.getElementById("openmrs_dwr_error");
            div.style.display = ""; // show the error div
            var msgDiv = document.getElementById("openmrs_dwr_error_msg");
            msgDiv.innerHTML = 'A javascript error has occurred:' + " <b>" + msg + "</b>";

          };
          dwr.engine.setErrorHandler(handler);
          dwr.engine.setWarningHandler(handler);
        </script>




        <div id="openmrs_dwr_error" style="display:none" class="error">
          <div id="openmrs_dwr_error_msg"></div>
          <div id="openmrs_dwr_error_close" class="smallMessage">
            <i>The full stacktrace for this error can usually be found in your server's error
logs.</i>  
            <a href="#" onclick="this.parentNode.parentNode.style.display='none'">Hide
error</a>
          </div>
        </div>



<script src="/openmrs/scripts/calendar/calendar.js?v=1.5.0.35" type="text/javascript"
></script>

<script type="text/javascript">
  function addIdentifier(id, type, location, pref, oldIdentifier) {
    var tbody = document.getElementById('identifiersTbody');
    var row = document.getElementById('identifierRow');
    var newrow = row.cloneNode(true);
    newrow.style.display = "";
    newrow.id = tbody.childNodes.length;
    tbody.appendChild(newrow);
    var inputs = newrow.getElementsByTagName("input");
    var selects = newrow.getElementsByTagName("select");
    if (id) {
      for (var i in inputs) {
        if (inputs[i] && inputs[i].name == "identifier") {
          inputs[i].value = id;
          if (oldIdentifier && 1 == 0) {
            inputs[i].parentNode.appendChild(docume...
```

[54 of 58] Application Error

Severity: Informational

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = patientId)

Remediation Tasks: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 14 [ID=58183]

The following changes were applied to the original request:
- Set parameter 'patientId's value to '%27'

[55 of 58] Application Error

Severity: Informational

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = lang)

Remediation Tasks: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=59474]

The following changes were applied to the original request:
- Set parameter 'lang's value to '%00'

[56 of 58] Application Error

Severity: Informational

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = addAge)

Remediation Tasks: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=22183]

The following changes were applied to the original request:
- Set parameter 'addAge's value to '\"'

[57 of 58] Application Error

Severity: Informational

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = dead)

Remediation Tasks: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 2 [ID=57898]

The following changes were applied to the original request:

• Cleared the value of parameter 'dead'

[58 of 58] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/patients/newPatient.form (Parameter = addBirthdate)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 14 [ID=21993]

The following changes were applied to the original request:
• Set parameter 'addBirthdate's value to '"

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/patient.form

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/patients/patient.form (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 3 [ID=30230]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/patients/patient.form/'

[2 of 2] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/patients/patient.form (Parameter = patientId)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 8 [ID=31306]

The following changes were applied to the original request:
• Set parameter 'patientId's value to '"

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/patientIdentifierType.form

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/patientIdentifierType.form (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 4 [ID=30138]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/patients/patientIdentifierType.form/'

[2 of 2] Application Error

Severity: Informational

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/patientIdentifierType.form (Parameter = patientIdentifierTypeId)

Remediation Tasks: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 10 [ID=30771]

The following changes were applied to the original request:
• Set parameter 'patientIdentifierTypeId's value to '2XYZ'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/patientIdentifierType.list

Total of 3 security issues in this URL

[1 of 3] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/patientIdentifierType.list (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 5 [ID=12364]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/patients/patientIdentifierType.list/'

[2 of 3] Application Error

Severity: Informational

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/patientIdentifierType.list (Parameter = lang)

Remediation Tasks: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=31036]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

[3 of 3] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/patients/patientIdentifierType.list (Parameter = patientIdentifierTypeId)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 12 [ID=30408]

The following changes were applied to the original request:
• Set parameter 'patientIdentifierTypeId's value to '2XYZ'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/patients/tribe.list

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/patients/tribe.list (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 7 [ID=12263]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/patients/tribe.list/'

[2 of 2] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/patients/tribe.list (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=25419]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/

Total of 1 security issues in this URL

[1 of 1] Insecure HTTP Methods Enabled

Severity: Medium

Test Type: Infrastructure

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/

Remediation Tasks: Disable WebDAV, or disallow unneeded HTTP methods

Variant 1 of 1 [ID=11409]

The following changes were applied to the original request:
- Set path to '/openmrs/admin/person/'
- Set method to 'OPTIONS'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/addPerson.htm

Total of 16 security issues in this URL

[1 of 16] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/addPerson.htm (Parameter = postURL)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 5 [ID=31369]

The following changes were applied to the original request:
- Injected 'patient.form>"><script>alert(114248)</script>' into parameter 'postURL's value

[2 of 16] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/addPerson.htm (Parameter = personType)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 38 [ID=31577]

The following changes were applied to the original request:
- Set parameter 'personType's value to 'patient>%22%27><img%20src%3d%22javascript:alert(114664)%22>'

[3 of 16] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/addPerson.htm (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 4 [ID=17670]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/person/addPerson.htm/'

[4 of 16] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/person/addPerson.htm (Parameter = addName)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 13 [ID=20612]

The following changes were applied to the original request:
• Injected '>"><script>alert(67963)</script>' into parameter 'addName's value

[5 of 16] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/person/addPerson.htm (Parameter = viewType)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 45 [ID=21246]

The following changes were applied to the original request:
• Set parameter 'viewType's value to 'shortEdit>%22%27><img%20src%3d%22javascript:alert(69231)%22>'

[6 of 16] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/person/addPerson.htm (Parameter = addGender)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 11 [ID=21418]

The following changes were applied to the original request:
• Injected 'M>"><script>alert(69575)</script>' into parameter 'addGender's value

[7 of 16] DOM Based Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/person/addPerson.htm
Remediation Tasks:	Analyze client side code and sanitize its input sources

Variant 1 of 2 [ID=31608]

The following changes were applied to the original request:

• Injected '<script>window.open('http://DOMXSSSucceeded/')</script>' into parameter 'personType's value

[8 of 16] DOM Based Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/person/addPerson.htm
Remediation Tasks:	Analyze client side code and sanitize its input sources

Variant 1 of 2 [ID=32739]

[9 of 16] Phishing Through Frames

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/person/addPerson.htm (Parameter = personType)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=31709]

The following changes were applied to the original request:
• Set parameter 'personType's value to 'patient'"><iframe%20src=http://demo.testfire.net>'

[10 of 16] Phishing Through Frames

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/person/addPerson.htm (Parameter = viewType)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 3 [ID=21368]

The following changes were applied to the original request:
• Set parameter 'viewType's value to 'shortEdit'"><iframe%20src=http://demo.testfire.net>'

[11 of 16] Link Injection (facilitates Cross-Site Request Forgery)

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/person/addPerson.htm (Parameter = personType)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=31722]

The following changes were applied to the original request:
• Set parameter 'personType's value to ""><IMG%20SRC="/WF_XSRF.html">'

[12 of 16] Link Injection (facilitates Cross-Site Request Forgery)

Severity:	Medium
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/person/addPerson.htm (Parameter = viewType)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 3 [ID=21381]

The following changes were applied to the original request:
- Set parameter 'viewType's value to '"><IMG%20SRC="/WF_XSRF.html">'

[13 of 16] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/person/addPerson.htm (Parameter = addAge)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 16 [ID=20938]

The following changes were applied to the original request:
- Set parameter 'addAge's value to '25XYZ'

[14 of 16] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/person/addPerson.htm (Parameter = personType)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 14 [ID=21188]

The following changes were applied to the original request:
- Set parameter 'personType's value to '"

[15 of 16] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/person/addPerson.htm (Parameter = addBirthdate)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 14 [ID=20833]

The following changes were applied to the original request:
- Set parameter 'addBirthdate's value to '"

[16 of 16] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/person/addPerson.htm (Parameter = viewType)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 18 [ID=21354]

The following changes were applied to the original request:
- Cleared the value of parameter 'viewType'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/personAttributeType.form

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/person/personAttributeType.form (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 4 [ID=27817]

The following changes were applied to the original request:
- Set path to '/openmrs/admin/person/personAttributeType.form/'

[2 of 2] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/person/personAttributeType.form (Parameter = personAttributeTypeId)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 10 [ID=28511]

The following changes were applied to the original request:
- Set parameter 'personAttributeTypeId's value to '3XYZ'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/personAttributeType.list

Total of 12 security issues in this URL

[1 of 12] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/personAttributeType.list (Parameter = patient.headerAttributeTypes)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 7 [ID=29031]

The following changes were applied to the original request:
• Set parameter 'patient.headerAttributeTypes's value to '1234>%22%27><img%20src%3d%22javascript:alert(105443)%22>'

[2 of 12] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/personAttributeType.list (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 5 [ID=12548]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/person/personAttributeType.list/'

[3 of 12] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/personAttributeType.list (Parameter = patient.listingAttributeTypes)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 3 [ID=28660]

The following changes were applied to the original request:
• Injected '1234>"><script>alert(104701)</script>' into parameter 'patient.listingAttributeTypes's value

[4 of 12] Blind SQL Injection

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/personAttributeType.list (Parameter = patient.viewingAttributeTypes)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=28840]

The following changes were applied to the original request:
• Set parameter 'patient.viewingAttributeTypes's value to '1234%27+and+%27foobar%27%3D%27foobar%27%29+--'

[5 of 12] Blind SQL Injection

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/personAttributeType.list (Parameter = action)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=28290]

The following changes were applied to the original request:
• Set parameter 'action's value to 'delete%27+and+%27foobar%27%3D%27foobar'

[6 of 12] Blind SQL Injection

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/personAttributeType.list (Parameter = personAttributeTypeId)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=28107]

The following changes were applied to the original request:
• Set parameter 'personAttributeTypeId's value to '3+and+7659%3D7659'

[7 of 12] Blind SQL Injection

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/personAttributeType.list (Parameter = patient.listingAttributeTypes)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=28647]

The following changes were applied to the original request:
• Set parameter 'patient.listingAttributeTypes's value to '0%2B0%2B0%2B1234'

[8 of 12] Stored Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/personAttributeType.list (= patient.headerAttributeTypes)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=141114]

The following changes were applied to the original request:
• Set parameter 'patient.headerAttributeTypes's value to '1234%2F**%2Fand%2F**%2F7659%3D7659'

[9 of 12] Stored Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/personAttributeType.list (= patient.listingAttributeTypes)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=141113]

The following changes were applied to the original request:
• Set parameter 'patient.listingAttributeTypes's value to '1234%27+and+%27foobar%27%3D%27foobar'

[10 of 12] Phishing Through Frames

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/personAttributeType.list (Parameter = patient.listingAttributeTypes)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=28792]

The following changes were applied to the original request:
• Set parameter 'patient.listingAttributeTypes's value to '1234%27%22%3E%3Cframe+name%3DAppScan+src%3Dhttp%3A%2F%2Fdemo.testfire.net%3E'

[11 of 12] Link Injection (facilitates Cross-Site Request Forgery)

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/personAttributeType.list (Parameter = patient.headerAttributeTypes)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=29182]

The following changes were applied to the original request:
• Set parameter 'patient.headerAttributeTypes's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[12 of 12] Application Error

Severity: Informational

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/personAttributeType.list (Parameter = lang)

Remediation Tasks: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=29721]

The following changes were applied to the original request:

• Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/relationshipType.form

Total of 14 security issues in this URL

[1 of 14] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/relationshipType.form (Parameter = aIsToB)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 9 [ID=69871]

The following changes were applied to the original request:
• Set parameter 'aIsToB's value to '1234>%22%27><img%20src%3d%22javascript:alert(250416)%22>'

[2 of 14] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/relationshipType.form (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 10 [ID=25685]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/person/relationshipType.form/'

[3 of 14] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/relationshipType.form (Parameter = description)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 12 [ID=70255]

The following changes were applied to the original request:
• Injected '1234"></IFRAME><script>alert(251184)</script>' into parameter 'description's value

[4 of 14] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/relationshipType.form (Parameter = bIsToA)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 4 [ID=70068]

The following changes were applied to the original request:
• Injected '1234"></IFRAME><script>alert(250810)</script>' into parameter 'bIsToA's value

[5 of 14] Stored Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/person/relationshipType.form (= aIsToB)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 1 [ID=141125]

The following changes were applied to the original request:
• Set parameter 'aIsToB's value to '1234WFXSSProbe'

[6 of 14] Stored Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/person/relationshipType.form (=)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 4 [ID=141120]

The following changes were applied to the original request:
• Set HTTP header to '%2527'

[7 of 14] Stored Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/person/relationshipType.form (= description)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=141129]

The following changes were applied to the original request:
• Set parameter 'description's value to '1234WFXSSProbe'

[8 of 14] Stored Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/person/relationshipType.form (= bIsToA)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 1 [ID=141127]

The following changes were applied to the original request:
• Set parameter 'bIsToA's value to '1234WFXSSProbe%27%22%29%2F%3E'

[9 of 14] Database Error Pattern Found

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/relationshipType.form (= aIsToB)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=141126]

The following changes were applied to the original request:
• Set parameter 'aIsToB's value to '1234>'"><img%20src%3D%26%23x6a;%26%23x61;%26%23x76;%26%23x61;%26%23x73;%26%23x63;%26%23x72;%26%23x69;%26%23x70;%26%23x74;%26%23x3a;alert(250418)>'

[10 of 14] Database Error Pattern Found

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/relationshipType.form (= bIsToA)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=141128]

The following changes were applied to the original request:
• Set parameter 'bIsToA's value to '1234>'"><img%20src%3D%26%23x6a;%26%23x61;%26%23x76;%26%23x61;%26%23x73;%26%23x63;%26%23x72;%26%23x69;%26%23x70;%26%23x74;%26%23x3a;alert(250794)>'

[11 of 14] Link Injection (facilitates Cross-Site Request Forgery)

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/relationshipType.form (Parameter = description)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 4 [ID=70397]

The following changes were applied to the original request:
• Set parameter 'description's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[12 of 14] Application Error

Severity: Informational

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/relationshipType.form (Parameter = lang)

Remediation Tasks: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 2 [ID=70929]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

[13 of 14] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/person/relationshipType.form (Parameter = description)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 2 [ID=70375]

[14 of 14] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/person/relationshipType.form (Parameter = relationshipTypeId)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 20 [ID=26390]

The following changes were applied to the original request:
• Set parameter 'relationshipTypeId's value to '2XYZ'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/relationshipType.list

Total of 9 security issues in this URL

[1 of 9] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/person/relationshipType.list (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 5 [ID=12456]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/person/relationshipType.list/'

[2 of 9] Stored Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/relationshipType.list (= lang)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=141131]

The following changes were applied to the original request:
• Set parameter 'lang's value to 'en_GBWFXSSProbe'")/>'

[3 of 9] Stored Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/relationshipType.list (= action)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=141132]

The following changes were applied to the original request:
• Set parameter 'action's value to 'Delete%2BSelected%2BRelationship%2BTypesWFXSSProbe'

[4 of 9] Stored Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/relationshipType.list (=)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 1 [ID=141124]

[5 of 9] Link Injection (facilitates Cross-Site Request Forgery)

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/relationshipType.list (Parameter = lang)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=71125]

The following changes were applied to the original request:
• Set parameter 'lang's value to '"><IMG%20SRC="/WF_XSRF.html">'

[6 of 9] Link Injection (facilitates Cross-Site Request Forgery)

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/relationshipType.list (Parameter = action)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=71302]

The following changes were applied to the original request:
• Set parameter 'action's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[7 of 9] Application Error

Severity: Informational

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/relationshipType.list (Parameter = lang)

Remediation Tasks: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 2 [ID=26655]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

[8 of 9] Application Error

Severity: Informational

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/relationshipType.list (Parameter = action)

Remediation Tasks: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 9 [ID=26284]

The following changes were applied to the original request:
• Cleared the value of parameter 'action'

[9 of 9] Application Error

Severity: Informational

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/relationshipType.list (Parameter = relationshipTypeId)

Remediation Tasks: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 12 [ID=26029]

The following changes were applied to the original request:

• Set parameter 'relationshipTypeId's value to '2XYZ'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/person/relationshipTypeViews.form

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/person/relationshipTypeViews.form (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 3 [ID=25777]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/person/relationshipTypeViews.form/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/programs/

Total of 1 security issues in this URL

[1 of 1] Insecure HTTP Methods Enabled

Severity:	Medium
Test Type:	Infrastructure
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/programs/
Remediation Tasks:	Disable WebDAV, or disallow unneeded HTTP methods

Variant 1 of 1 [ID=14523]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/programs/'
• Set method to 'OPTIONS'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/programs/conversion.form

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/programs/conversion.form (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 4 [ID=50051]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/programs/conversion.form/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/programs/conversion.list

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/programs/conversion.list (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 5 [ID=15481]

The following changes were applied to the original request:
- Set path to '/openmrs/admin/programs/conversion.list/'

[2 of 2] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/programs/conversion.list (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=53089]

The following changes were applied to the original request:
- Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/programs/program.form

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/programs/program.form (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 4 [ID=36485]

The following changes were applied to the original request:
- Set path to '/openmrs/admin/programs/program.form/'

[2 of 2] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/programs/program.form (Parameter = programId)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 10 [ID=38017]

The following changes were applied to the original request:
- Set parameter 'programId's value to '1XYZ'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/programs/program.list

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/programs/program.list (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 5 [ID=15389]

The following changes were applied to the original request:
- Set path to '/openmrs/admin/programs/program.list/'

[2 of 2] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/programs/program.list (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=38468]

The following changes were applied to the original request:
- Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/programs/workflow.form

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/programs/workflow.form (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=36577]

The following changes were applied to the original request:
- Set path to '/openmrs/admin/programs/workflow.form/'

[2 of 2] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/programs/workflow.form (Parameter = programWorkflowId)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 13 [ID=38203]

The following changes were applied to the original request:
- Set parameter 'programWorkflowId's value to '1XYZ'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/scheduler/

Total of 1 security issues in this URL

[1 of 1] Insecure HTTP Methods Enabled

Severity:	Medium
Test Type:	Infrastructure
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/scheduler/
Remediation Tasks:	Disable WebDAV, or disallow unneeded HTTP methods

Variant 1 of 1 [ID=14420]

The following changes were applied to the original request:
- Set path to '/openmrs/admin/scheduler/'
- Set method to 'OPTIONS'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/scheduler/scheduler.form

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/scheduler/scheduler.form (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 3 [ID=40074]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/scheduler/scheduler.form/'

[2 of 2] Application Error

Severity: Informational

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/scheduler/scheduler.form (Parameter = taskId)

Remediation Tasks: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 12 [ID=42201]

The following changes were applied to the original request:
• Set parameter 'taskId's value to '1XYZ'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/scheduler/scheduler.list

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/scheduler/scheduler.list (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 5 [ID=15297]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/scheduler/scheduler.list/'

[2 of 2] Application Error

Severity: Informational

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/scheduler/scheduler.list (Parameter = lang)

Remediation Tasks: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=43333]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/users/alert.form

Total of 12 security issues in this URL

[1 of 12] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/users/alert.form (Parameter = userIds)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 24 [ID=68240]

The following changes were applied to the original request:
• Injected '--><script>alert(247154)</script>' into parameter 'userIds's value

[2 of 12] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/users/alert.form (Parameter = satisfiedByAny)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 3 [ID=68598]

The following changes were applied to the original request:
• Injected 'on--><script>alert(247870)</script>' into parameter 'satisfiedByAny's value

[3 of 12] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/users/alert.form (Parameter = text)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 4 [ID=68067]

The following changes were applied to the original request:
• Injected '1234</TextArea><script>alert(246808)</script>' into parameter 'text's value

[4 of 12] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/users/alert.form (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 8 [ID=24470]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/users/alert.form/'

[5 of 12] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/users/alert.form (Parameter = dateToExpire)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 32 [ID=68777]

The following changes were applied to the original request:
• Set parameter 'dateToExpire's value to '1234>%22%27><img%20src%3d%22javascript:alert(248228)%22>'

[6 of 12] Blind SQL Injection

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/users/alert.form (Parameter = dateToExpire)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=68769]

The following changes were applied to the original request:
• Set parameter 'dateToExpire's value to '0%2B0%2B0%2B1234'

[7 of 12] DOM Based Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/users/alert.form

Remediation Tasks: Analyze client side code and sanitize its input sources

Variant 1 of 2 [ID=68264]

The following changes were applied to the original request:
• Set parameter 'userIds's value to '%3Cscript%3Ewindow.open%28%27http%3A%2F%2FDOMXSSSucceeded%2F%27%29%3C%2Fscript%3E'

[8 of 12] DOM Based Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/users/alert.form

Remediation Tasks: Analyze client side code and sanitize its input sources

Variant 1 of 2 [ID=68082]

The following changes were applied to the original request:
• Set parameter 'text's value to '%3Cscript%3Ewindow.open%28%27http%3A%2F%2FDOMXSSSucceeded%2F%27%29%3C%2Fscript%3E'

[9 of 12] Cross-Site Request Forgery

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/users/alert.form

Remediation Tasks: Decline malicious requests

Variant 1 of 2 [ID=67823]

[10 of 12] Phishing Through Frames

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/users/alert.form (Parameter = dateToExpire)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=68915]

The following changes were applied to the original request:
• Set parameter 'dateToExpire's value to '1234%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fdemo.testfire.net%3E'

[11 of 12] Link Injection (facilitates Cross-Site Request Forgery)

Severity: Medium

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/users/alert.form (Parameter = dateToExpire)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=68928]

The following changes were applied to the original request:
• Set parameter 'dateToExpire's value to '%22%27%3E%3CIMG+SRC%3D%22%2FWF_XSRF.html%22%3E'

[12 of 12] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/users/alert.form (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=69086]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/users/alert.list

Total of 3 security issues in this URL

[1 of 3] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/users/alert.list (Parameter = includeExpired)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 5 [ID=24944]

The following changes were applied to the original request:
• Injected 'true>"><script>alert(84404)</script>' into parameter 'includeExpired's value

[2 of 3] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/users/alert.list (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 5 [ID=12162]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/users/alert.list/'

[3 of 3] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/users/alert.list (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=25242]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/users/privilege.form

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/users/privilege.form (Parameter = privilege)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 5 [ID=27348]

The following changes were applied to the original request:
• Injected 'Add%20Cohorts>"><script>alert(96990)</script>' into parameter 'privilege's value

[2 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/users/privilege.form (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 4 [ID=25869]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/users/privilege.form/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/users/privilege.list

Total of 3 security issues in this URL

[1 of 3] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/users/privilege.list (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 5 [ID=12070]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/users/privilege.list/'

[2 of 3] Application Error

Severity: Informational

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/users/privilege.list (Parameter = privilegeId)

Remediation Tasks: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 12 [ID=27204]

The following changes were applied to the original request:
• Set parameter 'privilegeId's value to 'Manage+FormEntry+XSNXYZ'

[3 of 3] Application Error

Severity: Informational

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/users/privilege.list (Parameter = lang)

Remediation Tasks: Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=28058]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/users/role.form

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/users/role.form (Parameter = roleName)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 5 [ID=24590]

The following changes were applied to the original request:
• Injected 'Anonymous>"><script>alert(83696)</script>' into parameter 'roleName's value

[2 of 2] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/users/role.form (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 3 [ID=24378]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/users/role.form/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/users/role.list

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/users/role.list (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 7 [ID=11978]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/users/role.list/'

[2 of 2] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/users/role.list (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=24888]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/users/user.form

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/users/user.form (Parameter = userId)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 5 [ID=34985]

The following changes were applied to the original request:
• Injected '>"><script>alert(127429)</script>' into parameter 'userId's value

[2 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/users/user.form (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 4 [ID=33053]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/users/user.form/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/admin/users/user.list

Total of 2 security issues in this URL

[1 of 2] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/users/user.list (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 5 [ID=11886]

The following changes were applied to the original request:
• Set path to '/openmrs/admin/users/user.list/'

[2 of 2] Application Error

Severity:	Informational
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/admin/users/user.list (Parameter = lang)
Remediation Tasks:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Variant 1 of 1 [ID=35206]

The following changes were applied to the original request:
• Set parameter 'lang's value to '%00'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/calendar/

Total of 1 security issues in this URL

[1 of 1] Insecure HTTP Methods Enabled

Severity: Medium

Test Type: Infrastructure

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/calendar/

Remediation Tasks: Disable WebDAV, or disallow unneeded HTTP methods

Variant 1 of 1 [ID=7390]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/calendar/'
- Set method to 'OPTIONS'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/calendar/calendar.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/calendar/calendar.js (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=8315]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/calendar/calendar.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/calendar/ipopeng.html

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/calendar/ipopeng.html (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=22574]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/calendar/ipopeng.html/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/calendar/plugins.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/calendar/plugins.js (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=22674]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/calendar/plugins.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/

Total of 1 security issues in this URL

[1 of 1] Insecure HTTP Methods Enabled

Severity:	Medium
Test Type:	Infrastructure
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/
Remediation Tasks:	Disable WebDAV, or disallow unneeded HTTP methods

Variant 1 of 1 [ID=6257]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/dojo/'
- Set method to 'OPTIONS'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/dojo.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/dojo.js (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=8091]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/dojo/dojo.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/

Total of 1 security issues in this URL

[1 of 1] Insecure HTTP Methods Enabled

Severity: Medium

Test Type: Infrastructure

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/

Remediation Tasks: Disable WebDAV, or disallow unneeded HTTP methods

Variant 1 of 1 [ID=6360]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/dojo/src/'
- Set method to 'OPTIONS'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/html.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/html.js (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=8251]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/dojo/src/html.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/io.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/io.js (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=8099]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/dojo/src/io.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/style.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/style.js (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=8259]

The following changes were applied to the original request:
• Set path to '/openmrs/scripts/dojo/src/style.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/event/

Total of 1 security issues in this URL

[1 of 1] Insecure HTTP Methods Enabled

Severity: Medium

Test Type: Infrastructure

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/event/

Remediation Tasks: Disable WebDAV, or disallow unneeded HTTP methods

Variant 1 of 1 [ID=6875]

The following changes were applied to the original request:
• Set path to '/openmrs/scripts/dojo/src/event/'
• Set method to 'OPTIONS'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/event/__package__.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/event/__package__.js (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=8187]

The following changes were applied to the original request:
• Set path to '/openmrs/scripts/dojo/src/event/__package__.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/event/browser.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/src/event/browser.js (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=8203]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/dojo/src/event/browser.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/event/topic.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/src/event/topic.js (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=8195]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/dojo/src/event/topic.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/graphics/

Total of 1 security issues in this URL

[1 of 1] Insecure HTTP Methods Enabled

Severity:	Medium
Test Type:	Infrastructure
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/src/graphics/
Remediation Tasks:	Disable WebDAV, or disallow unneeded HTTP methods

Variant 1 of 1 [ID=7081]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/dojo/src/graphics/'
- Set method to 'OPTIONS'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/graphics/color.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/src/graphics/color.js (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=8267]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/dojo/src/graphics/color.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/html/

Total of 1 security issues in this URL

[1 of 1] Insecure HTTP Methods Enabled

Severity:	Medium
Test Type:	Infrastructure
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/src/html/
Remediation Tasks:	Disable WebDAV, or disallow unneeded HTTP methods

Variant 1 of 1 [ID=7184]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/dojo/src/html/'
- Set method to 'OPTIONS'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/html/extras.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/src/html/extras.js (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=8275]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/dojo/src/html/extras.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/lang/

Total of 1 security issues in this URL

[1 of 1] Insecure HTTP Methods Enabled

Severity:	Medium
Test Type:	Infrastructure
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/src/lang/
Remediation Tasks:	Disable WebDAV, or disallow unneeded HTTP methods

Variant 1 of 1 [ID=6463]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/dojo/src/lang/'
- Set method to 'OPTIONS'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/lang/declare.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/src/lang/declare.js (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=8171]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/dojo/src/lang/declare.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/lang/extras.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/src/lang/extras.js (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=8107]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/dojo/src/lang/extras.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/lfx/

Total of 1 security issues in this URL

[1 of 1] Insecure HTTP Methods Enabled

Severity:	Medium
Test Type:	Infrastructure
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/src/lfx/
Remediation Tasks:	Disable WebDAV, or disallow unneeded HTTP methods

Variant 1 of 1 [ID=7287]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/dojo/src/lfx/'
- Set method to 'OPTIONS'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/lfx/Animation.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/src/lfx/Animation.js (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=8307]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/dojo/src/lfx/Animation.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/lfx/__package__.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/src/lfx/__package__.js (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=8291]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/dojo/src/lfx/__package__.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/lfx/html.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/src/lfx/html.js (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=8299]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/dojo/src/lfx/html.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/lfx/toggle.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/src/lfx/toggle.js (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=8283]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/dojo/src/lfx/toggle.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/uri/

Total of 1 security issues in this URL

[1 of 1] Insecure HTTP Methods Enabled

Severity:	Medium
Test Type:	Infrastructure
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/src/uri/
Remediation Tasks:	Disable WebDAV, or disallow unneeded HTTP methods

Variant 1 of 1 [ID=6978]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/dojo/src/uri/'
- Set method to 'OPTIONS'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/uri/Uri.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/uri/Uri.js (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=8235]

The following changes were applied to the original request:
• Set path to '/openmrs/scripts/dojo/src/uri/Uri.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/uri/__package__.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/uri/__package__.js (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=8227]

The following changes were applied to the original request:
• Set path to '/openmrs/scripts/dojo/src/uri/__package__.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/DomWidget.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/DomWidget.js (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=8219]

The following changes were applied to the original request:
• Set path to '/openmrs/scripts/dojo/src/widget/DomWidget.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/HtmlWidget.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/HtmlWidget.js (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=8243]

The following changes were applied to the original request:
• Set path to '/openmrs/scripts/dojo/src/widget/HtmlWidget.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/Manager.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/Manager.js (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=8179]

The following changes were applied to the original request:
• Set path to '/openmrs/scripts/dojo/src/widget/Manager.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/Parse.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/Parse.js (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=8211]

The following changes were applied to the original request:
• Set path to '/openmrs/scripts/dojo/src/widget/Parse.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/Widget.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/Widget.js (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=8155]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/dojo/src/widget/Widget.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/__package__.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/__package__.js (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=8139]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/dojo/src/widget/__package__.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/xml/

Total of 1 security issues in this URL

[1 of 1] Insecure HTTP Methods Enabled

Severity:	Medium
Test Type:	Infrastructure
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/src/xml/
Remediation Tasks:	Disable WebDAV, or disallow unneeded HTTP methods

Variant 1 of 1 [ID=6772]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/dojo/src/xml/'
- Set method to 'OPTIONS'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/xml/Parse.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/xml/Parse.js (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=8147]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/dojo/src/xml/Parse.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/openmrs/

Total of 1 security issues in this URL

[1 of 1] Insecure HTTP Methods Enabled

Severity: Medium

Test Type: Infrastructure

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/openmrs/

Remediation Tasks: Disable WebDAV, or disallow unneeded HTTP methods

Variant 1 of 1 [ID=6669]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/dojo/src/widget/openmrs/'
- Set method to 'OPTIONS'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/openmrs/ConceptSearch.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity: High

Test Type: Application

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/openmrs/ConceptSearch.js (Parameter =)

Remediation Tasks: Filter out hazardous characters from user input

Variant 1 of 2 [ID=8115]

The following changes were applied to the original request:
- Set path to '/openmrs/scripts/dojo/src/widget/openmrs/ConceptSearch.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/openmrs/EncounterSearch.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/openmrs/EncounterSearch.js (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=12942]

The following changes were applied to the original request:
• Set path to '/openmrs/scripts/dojo/src/widget/openmrs/EncounterSearch.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/openmrs/FieldSearch.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/openmrs/FieldSearch.js (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=16888]

The following changes were applied to the original request:
• Set path to '/openmrs/scripts/dojo/src/widget/openmrs/FieldSearch.js/'

Vulnerable URL: http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/openmrs/OpenmrsPopup.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/openmrs/OpenmrsPopup.js (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=30330]

The following changes were applied to the original request:
• Set path to '/openmrs/scripts/dojo/src/widget/openmrs/OpenmrsPopup.js/'

Vulnerable URL:
http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/openmrs/OpenmrsSearch.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/openmrs/OpenmrsSearch.js (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=8123]

The following changes were applied to the original request:
• Set path to '/openmrs/scripts/dojo/src/widget/openmrs/OpenmrsSearch.js/'

Vulnerable URL:
http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/openmrs/PatientSearch.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/openmrs/PatientSearch.js (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=8131]

The following changes were applied to the original request:
• Set path to '/openmrs/scripts/dojo/src/widget/openmrs/PatientSearch.js/'

Vulnerable URL:
http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/openmrs/PersonSearch.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/openmrs/PersonSearch.js (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=8163]

The following changes were applied to the original request:
• Set path to '/openmrs/scripts/dojo/src/widget/openmrs/PersonSearch.js/'

Vulnerable URL:
http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/openmrs/UserSearch.js

Total of 1 security issues in this URL

[1 of 1] Cross-Site Scripting

Severity:	High
Test Type:	Application
Vulnerable URL:	http://192.168.1.104:8080/openmrs/scripts/dojo/src/widget/openmrs/UserSearch.js (Parameter =)
Remediation Tasks:	Filter out hazardous characters from user input

Variant 1 of 2 [ID=12640]

The following changes were applied to the original request:
• Set path to '/openmrs/scripts/dojo/src/widget/openmrs/UserSearch.js/'