

## TEAM 8 MEMBERS IDS:

› ZLI36, XDING3, FLUAN, TNNGUYE6

## › [A1 - 01 - Injection] [ Drop Table ]

DESIGNER : [Fuxing Luan] UPDATED ON : [09/09/2017]

› Name of module : [ Search ]

› Priority : [ high ]

### › Test Description

Injection attacks occur when unvalidated input is embedded in an instruction stream and cannot be distinguished from valid instructions. This test is to see whether using SQL key words in the search fields will affect the database.

### › \* Precondition

1. A local computer with administrator privilege
2. Java environment installed
3. OpenMRS Standalone Version 2.6.0 downloaded and unzipped
4. Latest Chrome browser

### › \* Assumption

1. OpenMRS with demo database runs normally

### › \* Test steps

1. Start local openMRS and log in with the username(nurse) and password(Nurse123)
2. Click "Find Patient Record" in the main page
3. Input a'; Drop Table Patients;" in the search field

## Find Patient Record

a'; Drop Table Patients;"

Identifier	Name	Gender	Age
No matching records found			

### › \* Expected results

1. No result will be shown
2. Existed patients will not be deleted

### › \* Actual results

No result showed Existing patients still there

# Find Patient Record

Search by ID or Name

Identifier	Name	Gender	Age
1003A5 <span>Recent</span>	Michael Jordan	M	17

Showing 1 to 1 of 1 entries

› Test status : [ Pass ]

## › [A1 - 02 - Injection] [ Tautology ]

DESIGNER : [Fuxing Luan] UPDATED ON : [09/09/2017]

› Name of module : [ Login ]

› Priority : [ High ]

### › Test Description

Injection attacks occur when unvalidated input is embedded in an instruction stream and cannot be distinguished from valid instructions. This test case is to test whether using tautology can bypass password authentication.

### › \* Precondition

- 1. A local computer with administrator privilege
- 2. Java environment installed
- 3. OpenMRS Standalone Version 2.6.0 downloaded and unzipped
- 4. Latest Chrome browser

### › \* Assumption

- 1. OpenMRS with demo database runs normally

### › \* Test Data

- 1. Username: ' OR '1' = '1 Password: ' OR '1' = '1

Username:

' OR '1' = '1

Password:

.....

Location for this session:

Inpatient Ward

Isolation Ward

Laboratory

Outpatient Clinic

Pharmacy

Registration Desk

› \* **Test steps**

1. Start local openMRS
2. Log in with the username and password

› \* **Expected results**

1. Fail to login

› \* **Actual results**

Login Failed

› **Test status : [ pass ]**

› **[A2 - 01 - BAC] [ Exposed Session IDs ]**

DESIGNER : [Fuxing Luan] UPDATED ON : [09/09/2017]

› **Name of module : [ Session ]**

› **Priority : [high]**

› **Test Description : Broken Access Control**

Access control, sometimes called authorization, is how a web application grants access to content and functions to some users and not others. These checks are performed after authentication, and govern what 'authorized' users are allowed to do. This test case focuses on whether the session IDs are exposed to the URLs.

› \* **Precondition**

1. A local computer with administrator privilege
2. Java environment installed
3. OpenMRS Standalone Version 2.6.0 downloaded and unzipped
4. Latest Chrome browser

› \* **Assumption**

1. OpenMRS with demo database runs normally

› \* **Test Data**

1. Username: nurse
2. Password: Nurse123

› \* **Test steps**

1. Start local openMRS and log in with the username and password
2. Click all links on the web page and see the URLs

› \* **Expected results**

1. No session information will be exposed in the URLs

› \* **Actual results**

No session information exposed

› **Test status : [ pass ]**

---

› **[A2 - 02 - BAC] [ Session Time Outs ]**

---

DESIGNER : [Fuxing Luan] UPDATED ON : [09/09/2017]

› **Name of module : [ Session ]**

› **Priority : [high]**

› **Test Description : Broken Access Control**

Access control, sometimes called authorization, is how a web application grants access to content and functions to some users and not others. These checks are performed after authentication, and govern what 'authorized' users are allowed to do. In this test, we will test whether the session is ended when the browser closes.

› \* **Precondition**

1. A local computer with administrator privilege
2. Java environment installed
3. OpenMRS Standalone Version 2.6.0 downloaded and unzipped
4. Latest Chrome browser

› \* **Assumption**

1. OpenMRS with demo database runs normally

› \* **Test Data**

1. Username: nurse
2. Password: Nurse123

› \* **Test steps**

1. Start local openMRS and log in with the username and account
2. Close browser
3. Reopen browser and visit the website again

› \* **Expected results**

1. Login will be required

› \* **Actual results**

Login is required

› **Test status : [ pass ]**

---

## › [A3 - 01 - XSS] [ Detecting Reflected XSS ]

DESIGNER : [Xiangqing Ding] UPDATED ON : [09/12/2017]

› Name of module : [ Search field in Find Patient Record ]

› Priority : [high]

### › Test Description

XSS attacks are essentially code injection attacks into the various interpreters in the browser. This test case is trying to detect if a script can be integrated in HTML and executed.

### › \* Precondition

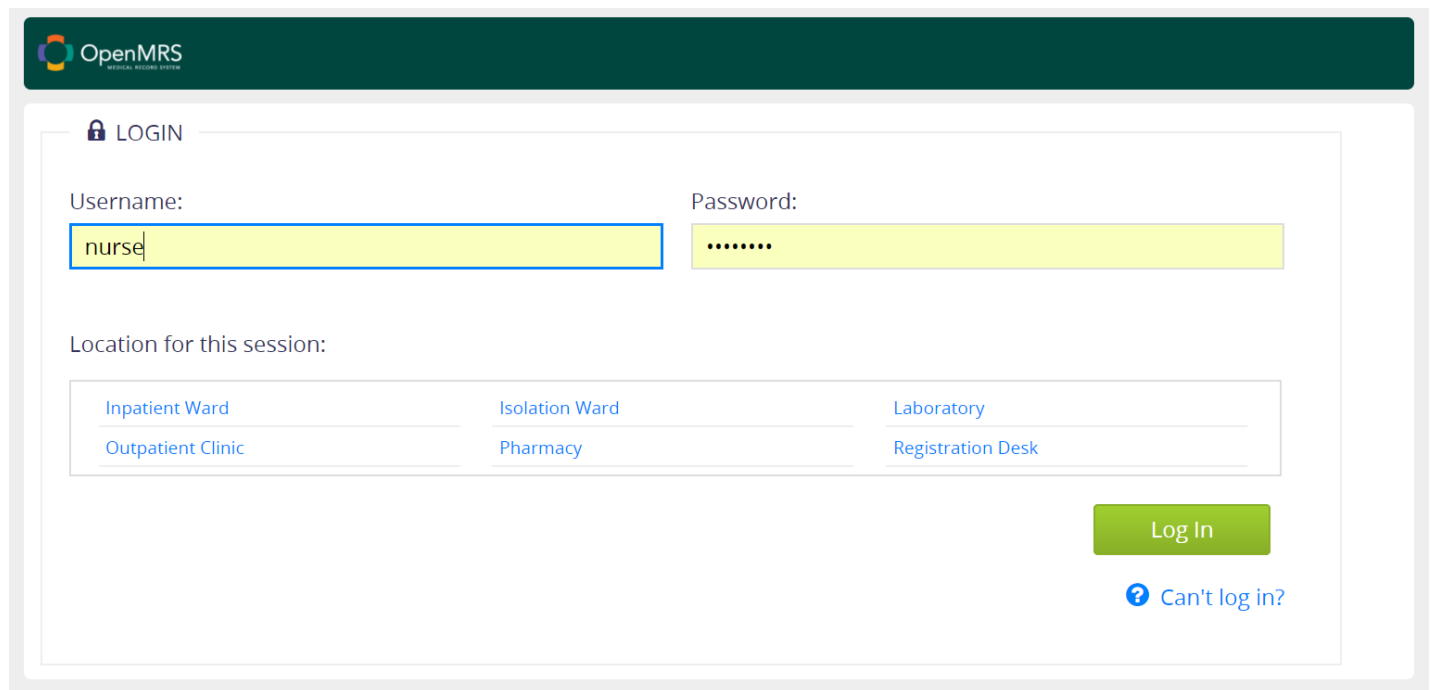
1. A local computer with administrator privilege
2. Java environment installed
3. OpenMRS Standalone Version 2.6.0 downloaded and unzipped
4. Latest Chrome browser

### › \* Assumption

1. OpenMRS with demo database runs normally

### › \* Test steps

1. Start local openMRS and log in with the username (nurse) and password (Nurse123)



OpenMRS  
MEDICAL RECORD SYSTEM

LOGIN

Username: nurse Password: .....


Location for this session:

Inpatient Ward	Isolation Ward	Laboratory
Outpatient Clinic	Pharmacy	Registration Desk

Log In


? Can't log in?


2. Click "Find Patient Record" in the main page


 nurse Isolation Ward Logout


Please tell us about your installation for the OpenMRS Atlas [Configure Atlas](#)

Logged in as Jane Smith (nurse) at Isolation Ward.


  
Find Patient Record

  
Active Visits

  
Capture Vitals

  
Appointment Scheduling

3. Input script (`<script>alert("Attacked")</script>`) in the search field and search

 nurse Isolation Ward Logout

[Home](#) > Find Patient Record


Find Patient Record

`<script>alert("Attacked")</script>`

Identifier	Name	Gender	Age	Birthdate
No matching records found				

[First](#) [Previous](#) [Next](#) [Last](#)

4. Input script (`%3cscript%3e alert("Attacked") %3cscript%3e`) in the search field and search

 nurse Isolation Ward Logout

[Home](#) > Find Patient Record

Find Patient Record

`%3cscript%3e alert("Attacked") %3cscript%3e`

Identifier	Name	Gender	Age	Birthdate
No matching records found				


[First](#) [Previous](#) [Next](#) [Last](#)

#### \* Expected results

- Scripts are not accepted
- Scripts are accepted but not executed

#### \* Actual results

Scripts are accepted but not executed.


 nurse Isolation Ward Logout

[Home](#) > Find Patient Record

Find Patient Record

Identifier	Name	Gender	Age	Birthdate
No matching records found				

[First](#) [Previous](#) [Next](#) [Last](#)

 nurse Isolation Ward Logout

[Home](#) > Find Patient Record

Find Patient Record

Identifier	Name	Gender	Age	Birthdate
No matching records found				

[First](#) [Previous](#) [Next](#) [Last](#)

Test status : [ Pass ]

## [ A3 - 02 - XSS ] [ Detecting Stored XSS ]

DESIGNER : [Xiangqing Ding] UPDATED ON : [09/09/2017]

Name of module : [ Allergy page ]

Priority : [high]

### Test Description

XSS attacks are essentially code injection attacks into the various interpreters in the browser. This test case is trying to see if script can be stored and executed in the allergy page.

### \* Precondition


1. A local computer with administrator privilege
2. Java environment installed
3. OpenMRS Standalone Version 2.6.0 downloaded and unzipped


### \* Assumption

1. OpenMRS with demo database runs normally

### \* Test steps

1. Start openMRS and log in with username(nurse) and password(Nurse123)

OpenMRS  
MEDICAL RECORD SYSTEM

 LOGIN

Username:

nurse

Password:

.....

Location for this session:

Inpatient Ward

Outpatient Clinic


Isolation Ward

Pharmacy


Laboratory


Registration Desk


Log In


 Can't log in?


2. Click "Find Patient Record" button in the main page

OpenMRS  
MEDICAL RECORD SYSTEM


 nurse ▾


 Isolation Ward ▾


Logout 


 Please tell us about your installation for the OpenMRS Atlas [Configure Atlas](#)

Logged in as Jane Smith (nurse) at Isolation Ward.

  
Find Patient Record

  
Active Visits

  
Capture Vitals

  
Appointment Scheduling

3. Search one of the patient (e.g. Christopher Allen) and go to the patient page by clicking the entry



nurse
Isolation Ward
Logout

Find Patient Record

### Find Patient Record

Identifier	Name	Gender	Age	Birthdate
10008D <span>Recent</span>	Melissa Miller	F	60	20.Sep.1956
1001W2 <span>Recent</span>	Christoper Allen	M	59	17.May.1958
1001U6 <span>Recent</span>	Jennifer Green	F	75	13.Nov.1941

Showing 1 to 3 of 3 entries
First Previous 1 Next Last

4. In the patient page, find ALLERGIES column and click the edit button

nurse
Isolation Ward
Logout

Christoper Allen

## Christoper Allen

Male 59 year(s) (17.May.1958)
Edit
Show Contact Info
Patient ID 1001W2

Active Visit - 06.Sep.2017, 02:36:08
Outpatient

### DIAGNOSES

- Hepatotoxicity
- Acute viral hepatitis, other
- Disease of bone and joint
- Fever
- HUMAN IMMUNODEFICIENCY VIRUS (HIV) DISEASE
- Superficial injury of abdomen, lower back or pelvis
- Hemorrhoids
- Itching

### RECENT VISITS

06.Sep.2017	Active - Outpatient
12.Jul.2016	Outpatient
18.Jan.2016	Outpatient
15.Jan.2016	Outpatient
21.Dec.2015 - 22.Dec.2015	Inpatient

### RECENT VISITS

06.Sep.2017

### FAMILY

None

### ALLERGIES

Unknown

### Current Visit Actions

- End Visit
- Admit to Inpatient
- Capture Vitals

### General Actions

- Add Past Visit
- Merge Visits
- Request Appointment
- Mark Patient Deceased

### VITALS

Last Vitals: 12.Jul.2016 12:49 PM

Height (cm) 51cm

Weight (kg) 86kg

(Calculated) BMI 330.6

Temperature 38.6

5. In the allergy page, click "Add New Allergy" button to add a new allergy

nurse
Isolation Ward
Logout

[Home](#) > [Allen, Christopher](#) > Allergies

**Christopher Allen**
Male 59 year(s) (17.May.1958)
[Edit](#)
[Show Contact Info](#)

Patient ID 1001W2

Active Visit - 06.Sep.2017, 02:36:08
Outpatient

### Allergies

Allergen	Reaction	Severity	Comment	Last Updated	Actions
Unknown					

Return
No Known Allergy
Add New Allergy

6. In the "comment" field, add the script (`<script>alert("Attacked")</script>`). Other field can be filled with own choice. After that, save the allergy.

nurse
Isolation Ward
Logout

[Home](#) > [Allen, Christopher](#) > [Allergies](#) > Add New Allergy

**Christopher Allen**
Male 59 year(s) (17.May.1958)
[Edit](#)
[Show Contact Info](#)

Patient ID 1001W2

Active Visit - 06.Sep.2017, 02:36:08
Outpatient

### Add New Allergy

DRUG
FOOD
OTHER

- ☐ ACE inhibitors
- ☐ ARBs (angiotensin II receptor blockers)
- ☐ Aspirin
- ☐ Cephalosporins
- ☐ Codeine
- ☒ Erythromycins
- ☐ Heparins
- ☐ Morphine
- ☐ NSAIDs
- ☐ Penicillins
- ☐ Statins
- ☐ Sulfonamides
- ☐ Other

Reactions: (check all that apply):

- ☐ Unknown
- ☐ Anaemia
- ☐ Anaphylaxis
- ☐ Angioedema
- ☐ Arrhythmia
- ☐ Bronchospasm
- ☐ Cough
- ☒ Diarrhea
- ☐ Dystonia
- ☒ Fever
- ☐ Flushing
- ☐ GI upset
- ☐ Headache
- ☐ Hepatotoxicity
- ☐ Hives
- ☐ Hypertension
- ☐ Itching
- ☐ Mental status change
- ☐ Musculoskeletal pain
- ☐ Myalgia
- ☐ Rash
- ☐ Other

Severity:
☐ Mild
☐ Moderate
☐ Severe
✕


Comment:

<script>alert("Attacked")</script>

Cancel
Save

7. Go to the allergy page again to see if there is a pop-up with message "Attacked"

8. Again add a new allergy and In the "comment" field, add the script(comment"><script>alert("Attacked")</script>). Other field can be filled with own choice. After that, save the allergy.

 OpenMRS  
MEDICAL RECORD SYSTEM

nurse ▾ Isolation Ward ▾ Logout ↗

Home > Allen, Christopher > Allergies > Add New Allergy

**Christopher Allen** Male 59 year(s) (17.May.1958) Edit Show Contact Info ▾  
Given Family Name

Patient ID 1001W2

Active Visit - 06.Sep.2017, 02:36:08 Outpatient

**Add New Allergy**

DRUG FOOD OTHER

☐ ACE inhibitors  
☐ ARBs (angiotensin II receptor blockers)  
☐ Aspirin  
☒ Cephalosporins  
☐ Codeine  
☐ Erythromycins  
☐ Heparins  
☐ Morphine  
☐ NSAIDs  
☐ Penicillins  
☐ Statins  
☐ Sulfonamides  
☐ Other

Severity: ☐ Mild ☐ Moderate ☐ Severe ✕

Comment:

Cancel Save

Reactions: (check all that apply):  

<input type="checkbox"/> Unknown	<input type="checkbox"/> Headache
<input type="checkbox"/> Anaemia	<input type="checkbox"/> Hepatotoxicity
<input type="checkbox"/> Anaphylaxis	<input type="checkbox"/> Hives
<input type="checkbox"/> Angioedema	<input type="checkbox"/> Hypertension
<input type="checkbox"/> Arrhythmia	<input type="checkbox"/> Itching
<input type="checkbox"/> Bronchospasm	<input type="checkbox"/> Mental status change
<input type="checkbox"/> Cough	<input type="checkbox"/> Musculoskeletal pain
<input type="checkbox"/> Diarrhea	<input checked="" type="checkbox"/> Myalgia
<input type="checkbox"/> Dystonia	<input type="checkbox"/> Rash
<input type="checkbox"/> Fever	<input type="checkbox"/> Other
<input type="checkbox"/> Flushing	<input type="text"/>
<input checked="" type="checkbox"/> GI upset	


9. Go to the allergy page again to see if there is a pop-up with message "Attacked"


#### \* Expected results


1. Scripts are not accepted. No pop-up.
2. Scripts are accepted but not executed. No pop-up.


#### \* Actual results


Scripts are accepted but not executed. No pop-up.

OpenMRS  
MEDICAL RECORD SYSTEM

nurse ▾

Isolation Ward ▾

Logout 

 > [Allen, Christopher](#) > Allergies

Christopher Allen

Male 59 year(s) (17.May.1958) [Edit](#) [Show Contact Info](#) ▾

Given





Family Name

Active Visit - 06.Sep.2017, 02:36:08

Outpatient

Patient ID 1001W2

Allergies

Allergen	Reaction	Severity	Comment	Last Updated	Actions
Cephalosporins	GI upset, Myalgia		comment"> <script>alert("Attac... </script>	Today 07:49 PM	 
Erythromycins	Diarrhea, Fever		<script>alert("Attac... </script>	Today 07:49 PM	 

Return

Add New Allergy

› Test status : [ Pass ]

## › [ A4 - 01 - BAC ] [ Non-admin account access to admin function ]

DESIGNER : [Xiangqing Ding] UPDATED ON : [09/09/2017]

› Name of module : [ System Administration ]

› Priority : [high]

### › Test Description

This test case is designed to test whether a non-admin user can access to admin functions

### › \* Precondition


1. A local computer with administrator privilege
2. Java environment installed
3. OpenMRS Standalone Version 2.6.0 downloaded and unzipped
4. Latest Chrome browser


### › \* Assumption

1. OpenMRS with demo database runs normally

### › \* Test steps

1. Start local openMRS and log in with username(nurse) and password(Nurse123)

OpenMRS  
MEDICAL RECORD SYSTEM

 LOGIN

Username:

Password:

Location for this session:

[Inpatient Ward](#)

[Isolation Ward](#)


[Laboratory](#)

[Outpatient Clinic](#)


[Pharmacy](#)

[Registration Desk](#)

Log In

 [Can't log in?](#)

2. Replace the `/referenceapplication/home.page` in the URL with `/coreapps/systemadministration/systemAdministration.page`

 `localhost:8081/openmrs-standalone/coreapps/systemadministration/systemAdministration.page`


3. Direct the URL to see if the user can access to the system administration page


#### › \* Expected results


User cannot access to system administration page while logging in as Nurse account (non-admin)


#### › \* Actual results


The Nurse account can access to the administration page


OpenMRS  
MEDICAL RECORD SYSTEM


 nurse ▾


 Isolation Ward ▾

Logout 

 > System Administration

 Please tell us about your installation for the OpenMRS Atlas [Configure Atlas](#)

Manage Global Properties

Manage Accounts

› Test status : [ Fail ]

› [ A4 - 02 - BAC ] [ Unauthorized access to system ]

DESIGNER : [Xiangqing Ding] UPDATED ON : [09/09/2017]

› **Name of module** : [ Main Page ]

› **Priority** : [high]

› **Test Description**

This test case is designed to test whether someone could access to the system without logging in

› \* **Precondition**

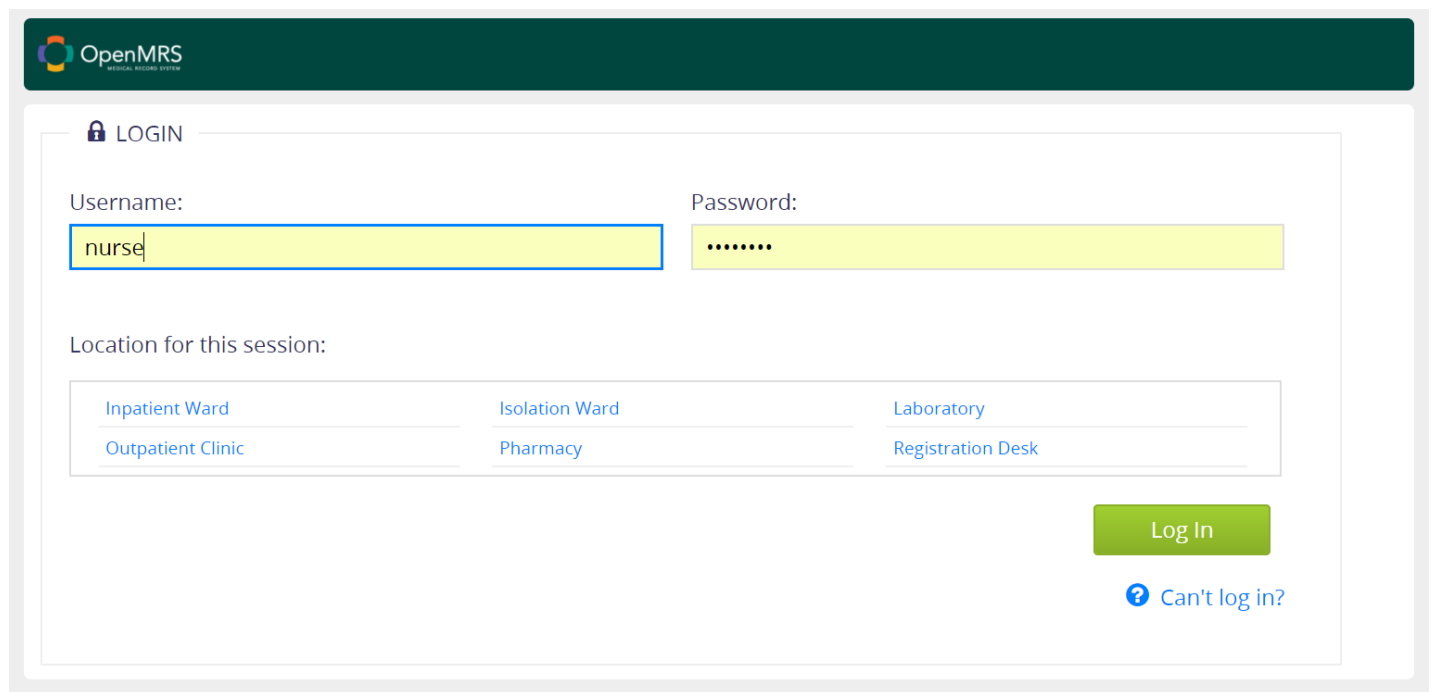
1. A local computer with administrator privilege
2. Java environment installed
3. OpenMRS Standalone Version 2.6.0 downloaded and unzipped
4. Latest Chrome browser

› \* **Assumption**

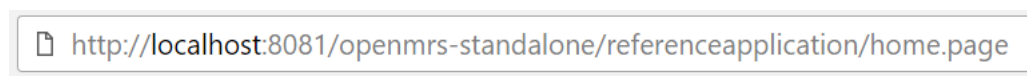
1. OpenMRS with demo database runs normally

› \* **Test steps**

1. Start local openMRS



2. Without logging in, put `http://localhost:8081/openmrs-standalone/referenceapplication/home.page` in the URL of browser.



3. Direct the URL to see if it can access to the system.

› \* **Expected results**

User cannot access to the main page without logging in

› \* **Actual results**

No response from the page. User cannot access to the main page without logging in

› Test status : [ pass ]

---

## › [A5 - 01 - Security Misconfiguration ] [ Default username and password]

---

› Test status : [ pass ]

DESIGNER : [ZHUO LI]  
UPDATED ON : [05SEP2017]

### › \* Description

This test verifies there is no default username and password which can be used by hackers.

### › \* Precondition

1. A local computer with administrator privilege
2. Java environment installed
3. OpenMRS Standalone Version 2.6.0 downloaded and unzipped
4. Latest Chrome browser

### › \* Assumption

1. OpenMRS with demo database runs normally

### › \* Test Data

Test username: admin

Test password: password

Test username: user

Test password: password

### › \* Test steps

1. Go to <http://localhost:8081/openmrs-standalone/login.htm>
2. Try to login with default user name and password (listed in Test Data section)


### › \* Expected results


There should be no default user name and password and tester should not be able to logon

### › \* Actual results

Log in failed with test username and password.

Invalid username/password. Please try again.

 OpenMRS  
Open Source Medical Record System

 LOGIN

Username:

Password:

Location for this session:

Inpatient Ward

Outpatient Clinic


Isolation Ward

Pharmacy

Laboratory

Registration Desk

Log In

 Can't log in?

## [A5 - 02 - Security Misconfiguration ] [ DirectoryListing]

› Test status : [ pass ]

DESIGNER : [ ZHUO LI ] UPDATED ON : [ 05SEP2017 ]

### › \* Description

This test verifies the application will not list any directory when we only change the link.

### › \* Precondition

1. A local computer with administrator privilege
2. Java environment installed
3. OpenMRS Standalone Version 2.6.0 downloaded and unzipped
4. Latest Chrome browser

### › \* Assumption

1. OpenMRS with demo database runs normally

### › \* Test Data

Test username: admin

Test password: Admin123

### › \* Test steps

1. Go to `http://localhost:8081/openmrs-standalone/login.htm` . Log in as admin (credentials in Test Data section)
2. Change the link to `directorylisting.(http://localhost:8081/openmrs-standalone/directorylisting)`

### › \* Expected results

The application should not list any directory.

### › \* Actual results

No directory was listed following the test steps.



## HTTP Status 404 - /openmrs-standalone/directorylisting

**Type** Status report

**Message** /openmrs-standalone/directorylisting

**Description** The requested resource is not available.

Apache Tomcat/7.0.50

## › [A6 - 01 - Sensitive Data Exposure ] [ Search History ]

### › Test status : [ Failed ]

DESIGNER : [ZHUO LI] UPDATED ON : [05SEP2017]

### › \* Description

This test verified the application will not list searching history when we exit the searching page.

### › \* Precondition

1. A local computer with administrator privilege
2. Java environment installed
3. OpenMRS Standalone Version 2.6.0 downloaded and unzipped
4. Latest Chrome browser

### › \* Assumption

1. OpenMRS with demo database runs normally

### › \* Test Data

Test username: admin

Test password: Admin123

### › \* Test steps

1. Go to <http://localhost:8081/openmrs-standalone/login.htm> . Log in as admin and register two patients named "Frank" and "Fred"
2. Back to home page.
3. Click on "search patient" and right click "Frank" to view the source code.
4. Redo step 2-3 and search "Fred".
5. Check whether the source code remember admin's behavior by searching "Frank".

### › \* Expected results

There should be no information about Frank.

### › \* Actual results

When we check the source code of webpage for patient Fred, the visit patient history part of code showed information of Frank, which is kind of sensitive exposure.

```

<script type="text/javascript">
  var listtableAttributeTypes = [];

  var lastViewedPatients = [];

  var patientObj = {
    uuid:"0415770a-fe72-4523-b2e0-56448ab0c2fa",
    name:"Fred Fred",
    gender:"M",
    // it.age is of type int (doesn't need sanitization)
    age:"16",
    birthdate:"01.Jan.2001",
    // it.birthdateEstimated is of type boolean (doesn't need sanitization)
    birthdateEstimated: false,
    identifier:"1003C3",
    widgetBirthdate:"2001-01-01"
  }

  lastViewedPatients.push(patientObj);

  var patientObj = {
    uuid:"e5bda5f-8159-4fe4-9e1f-ce3277fcf67b",
    name:"Frank Frank",
    gender:"M",
    // it.age is of type int (doesn't need sanitization)
    age:"16",
    birthdate:"01.Jan.2001",
    // it.birthdateEstimated is of type boolean (doesn't need sanitization)
    birthdateEstimated: false,
    identifier:"1003A5",
    widgetBirthdate:"2001-01-01"
  }

  lastViewedPatients.push(patientObj);

```

## › [A6 - 02 - Sensitive Data Exposure ] [ Web Certification ]

### › Test status : [ Failed ]

DESIGNER : [ZHUO LI]  
 UPDATED ON : [05SEP2017]

### › \* Description

This test verified the application need to certificate on every web page.

### › \* Precondition

1. A local computer with administrator privilege
2. Java environment installed
3. OpenMRS Standalone Version 2.6.0 downloaded and unzipped
4. Latest Chrome browser

### › \* Assumption

1. OpenMRS with demo database runs normally
2. Chrome or Firefox that can check security

### › \* Test Data

Test username: admin

Test password: Admin123

### › \* Test steps

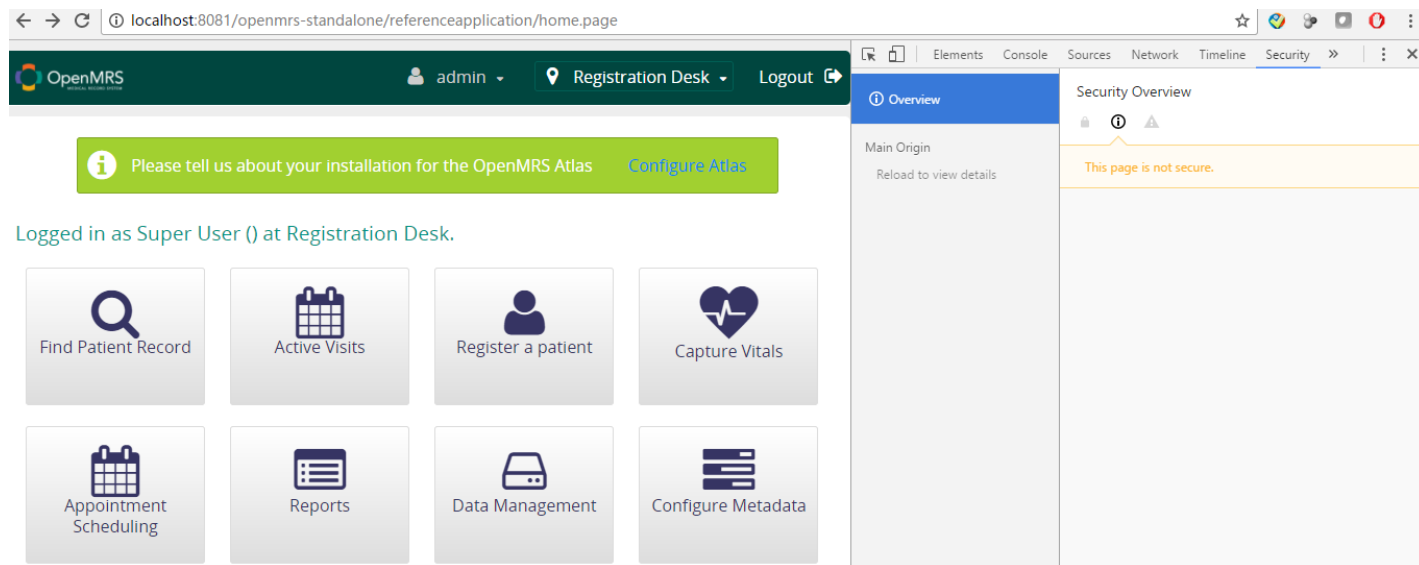
1. Log in as admin
2. Test the certificate via Google chrome

### › \* Expected results

The web application should have certification on each available website.

## › \* Actual results

The settings showed us that even the home page for this application is not secure.



## › [A7 - 01 - IAP ] [ DETECTING LEADING SPACE ATTACKS ]

› Priority : medium

› Test status : FAILED

DESIGNER : TAM N NGUYEN  
EXECUTED BY : TAM N NGUYEN  
UPDATED ON : 09SEP2017  
EXECUTED ON : 09SEP2017

## › \* Description

› Name of module : OpenMRS Login page

This test determines the level of OpenMRS protection against leading space attack attempts on the login page.

## › \* Precondition

1. A local computer with administrator privilege
2. Java JRE installed
3. OpenMRS Standalone Version 2.6.0 downloaded and unzipped
4. OWASP ZAP Version 2.6.0 downloaded and installed

## › \* Dependencies

1. OpenMRS with demo database was loaded and runs normally
2. OWASP ZAP runs normally

## › \* Test Data

- Pair 1 Username: 5 empty spaces Password: 5 empty spaces
- Pair 2 Username: admin Password: 100 empty spaces followed by "password"
- Pair 3 Username: 100 empty spaces followed by "admin" Password: 100 empty spaces followed by "password"

### › \* Test steps

1. Open up OpenMRS V. 2.6.0 Standalone. Make sure Tomcat Port is 8081 and MySQL port is 3316. A web page starting with localhost:8081 will be automatically opened upon successful start.
2. Open up browser and go to "<http://localhost:8081/openmrs-standalone/login.htm>" (without the brackets)
3. Put in the value of pair 1 and click "login" button. Observe the OpenMRS 2.6.0 Standalone window (the one with the "Start" and "Stop" button)
4. Put in the value of pair 2 and click "login" button. Observe the OpenMRS 2.6.0 Standalone window (the one with the "Start" and "Stop" button)
5. Put in the value of pair 3 and click "login" button. Observe the OpenMRS 2.6.0 Standalone window (the one with the "Start" and "Stop" button)

### › \* Expected results

1. For pair 1, there must be a log with "INFO" type in the service console, saying "Failed login attempt - Empty username and password"
2. For pair 2, there must be a log with "INFO" type in the service console, saying "Failed login attempt - Username = admin and Password = password"
3. For pair 3, there must be a log with "INFO" type in the service console, saying "Failed login attempt - Username = admin and Password = password"

### › \* Post-condition

Login page is still available to whoever was doing the attack.

### › \* Actual results

1. There was no log in the service console after logging in with pair 1
2. With pair 2, post login log in the service console is "Failed login attempt (login=admin) - Invalid usrxname and/or password : admin". This means the system was not able to record the malicious string after large enough leading spaces.
3. There was no log in the service console after logging in with pair 3. This means with large enough trailing spaces, injection attacks on both username and password will go undetected

### › \* NOTES:

Contact [tam.nguyen@ncsu.edu](mailto:tam.nguyen@ncsu.edu) if you have problems following instructions in this test case.

---

## › [ A7 - 02 - IAP ] [ PROTECTION AGAINST AUTOMATIC SCAN ]

---

### › Priority : medium

### › Test status : FAILED

DESIGNER : TAM N NGUYEN  
EXECUTED BY : TAM N NGUYEN  
UPDATED ON : 09SEP2017  
EXECUTED ON : 09SEP2017

### › \* Description

#### › Name of module : OpenMRS Login page

This test determines the level of OpenMRS protection against repeated, automatic attack attempts on the login page.

### › \* Precondition

1. A local computer with administrator privilege
2. Java JRE installed
3. OpenMRS Standalone Version 2.6.0 downloaded and unzipped
4. OWASP ZAP Version 2.6.0 downloaded and installed

### › \* Dependencies

1. OpenMRS with demo database was loaded and runs normally
2. OWASP ZAP runs normally

## › \* Test Data

Default rules that were pre-loaded in OWASP ZAP scanner

## › \* Test steps

1. Open up OpenMRS V. 2.6.0 Standalone. Make sure Tomcat Port is 8081 and MySQL port is 3316. A web page starting with localhost:8081 will be automatically opened upon successful start.
2. Open up OWASP ZAP 2.6.0
3. From OWASP ZAP menu, go to Tools > Spider. In tab "Scope" box "Starting point", type : "<http://localhost:8081/openmrs-standalone/login.htm>" (without the brackets) and then click "Start Scan".
4. After the spider is done, from the OWASP ZAP main screen, type "<http://localhost:8081/openmrs-standalone/login.htm>" (without the brackets) into the box "URL to attack" and then click "Attack".
5. OWASP ZAP may relaunch the spider. At the bottom section, you may found the current tab is the "Spider" tab. After the spider is done, the program will automatically switch to the "Active" tab.
6. Monitor the column "Code" in OWASP ZAP scanner, the "Active Scan" tab and the OpenMRS 2.6.0 Standalone service console (the one with the "Tomcat port" and the "MySQL port" boxes)

## › \* Expected results

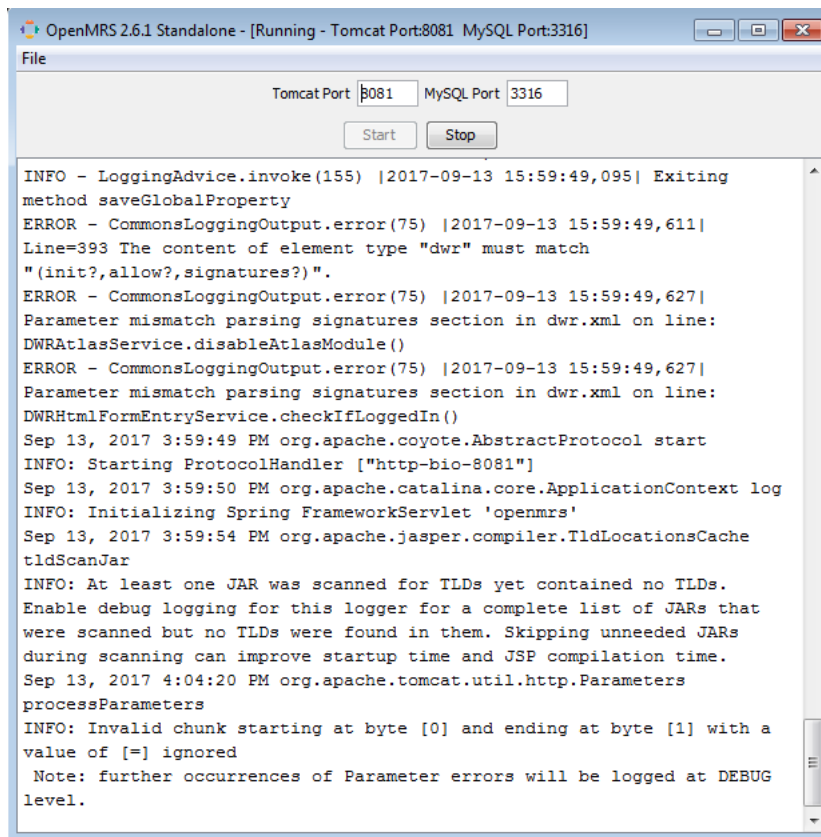
1. For each of OWASP ZAP's probe, the OpenMRS 2.6.0 Standalone console must give a description indicating a fail attempt at attacking the login page
2. After a certain number of attempts, server will throw a 4xx page (for example a "HTTP 400 - Bad Request" page). This expectation can be substituted with a page redirection code.

## › \* Post-condition

Login page is made unavailable to whoever was doing the attack.

## › \* Actual results

1. There was no alert in the OpenMRS 2.6.0 Standalone console while more than 100 of probing attempts were carried out on the login page



2. Login page's status codes returned to OWASP ZAP were all "200"

Untitled Session - 20170913-155744 - OWASP ZAP 2.6.0

File Edit View Analyse Report Tools Online Help

Standard Mode

Sites + Quick Start Request Response +

Contexts

- Default Context
- Sites
  - http://localhost:8081
    - openmrs-standalone
      - GET:login.htm
      - ms
      - POST:login.htm(password,redirectUrl,sessionLo
      - referenceapplication

Header: Text Body: Text

```

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=765A6CA495AF0F49DD8E2354BB48DE22; Path=/openmrs-standalone/; HttpOnly
Cache-Control: no-cache,no-store,must-revalidate
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html;charset=UTF-8
Content-Language: en-GB
Content-Length: 7872
Date: Wed, 13 Sep 2017 20:04:19 GMT
  
```

```

332776938"></script>
<script type="text/javascript" src=
"/openmrs-standalone/ms/uiframework/resource/uicommons/scripts/jquery.simplemodal.1.4.4.min.js?c
ache=1505332776938"></script>
<link rel="stylesheet" href=
"/openmrs-standalone/ms/uiframework/resource/uicommons/styles/styleguide/jquery-ui-1.9.2.custom.
min.css?cache=1505332776938" type="text/css"/>
<link rel="stylesheet" href=
"/openmrs-standalone/ms/uiframework/resource/uicommons/styles/styleguide/jquery.toastmessage.css
?cache=1505332776938" type="text/css"/>
<link rel="stylesheet" href=
"/openmrs-standalone/ms/uiframework/resource/referenceapplication/styles/login.css?cache=1505332
776938" type="text/css"/>
<link rel="stylesheet" href=
  
```

History Search Alerts Output Spider Active Scan +

New Scan Progress: 0: http://localhost:8081/openmrs-standalone/login.htm 100% Current Scans: 0 Num requests: 137

Id	Req. Timestamp	Resp. Timestamp	Method	URL	Co...	Re...	RTT	Siz...	Siz...
209	13/09/17 16:04:19	13/09/17 16:04:19	GET	http://localhost:8081/openmrs-standalone/login.htm?query=Set-cookie%3A+tamper%3...	200	OK	10...	371...	7,8...
210	13/09/17 16:04:19	13/09/17 16:04:19	GET	http://localhost:8081/openmrs-standalone/login.htm?query=any%0D%0ASet-cookie%3A...	200	OK	31...	371...	7,8...
211	13/09/17 16:04:19	13/09/17 16:04:19	GET	http://localhost:8081/openmrs-standalone/login.htm?query=any%3F%0D%0ASet-cookie...	200	OK	31...	371...	7,8...
212	13/09/17 16:04:19	13/09/17 16:04:19	GET	http://localhost:8081/openmrs-standalone/login.htm?query=any%0ASet-cookie%3A+Ta...	200	OK	47...	371...	7,8...
213	13/09/17 16:04:19	13/09/17 16:04:19	GET	http://localhost:8081/openmrs-standalone/login.htm?query=any%3F%0ASet-cookie%3A...	200	OK	47...	371...	7,8...
214	13/09/17 16:04:19	13/09/17 16:04:19	GET	http://localhost:8081/openmrs-standalone/login.htm?query=any%0D%0ASet-cookie%3A...	200	OK	31...	371...	7,8...
215	13/09/17 16:04:19	13/09/17 16:04:20	GET	http://localhost:8081/openmrs-standalone/login.htm?query=any%3F%0D%0ASet-cookie...	200	OK	12...	371...	7,8...
216	13/09/17 16:04:20	13/09/17 16:04:20	GET	http://localhost:8081/openmrs-standalone/login.htm	200	OK	59...	371...	7,8...
217	13/09/17 16:04:20	13/09/17 16:04:20	GET	http://localhost:8081/openmrs-standalone/login.htm?query=	200	OK	62...	371...	7,8...
218	13/09/17 16:04:20	13/09/17 16:04:20	GET	http://localhost:8081/openmrs-standalone/login.htm?query=	200	OK	47...	371...	7,8...
219	13/09/17 16:04:20	13/09/17 16:04:20	GET	http://localhost:8081/openmrs-standalone/login.htm?query=%40	200	OK	47...	371...	7,8...
220	13/09/17 16:04:20	13/09/17 16:04:21	GET	http://localhost:8081/openmrs-standalone/login.htm?query=%2B	200	OK	62...	371...	7,8...
221	13/09/17 16:04:21	13/09/17 16:04:21	GET	http://localhost:8081/openmrs-standalone/login.htm?query=%00	200	OK	78...	371...	7,8...
222	13/09/17 16:04:21	13/09/17 16:04:21	GET	http://localhost:8081/openmrs-standalone/login.htm?query=%7C	200	OK	31...	371...	7,8...
223	13/09/17 16:04:21	13/09/17 16:04:21	GET	http://localhost:8081/openmrs-standalone/login.htm?query=zApX0sS	200	OK	17...	371...	7,8...
224	13/09/17 16:04:21	13/09/17 16:04:21	GET	http://localhost:8081/openmrs-standalone/login.htm	200	OK	32...	371...	7,8...

Alerts 0 0 1 2 0 Current Scans 0 0 0 0 0 0 0 0 0

## \* NOTES:

Contact [tam.nguyen@ncsu.edu](mailto:tam.nguyen@ncsu.edu) if you have problems following instructions in this test case.

## [ A8 - 01 - CSRF ] [ CHANGE DEFAULT LANGAUGE ATTACK ]

Priority : HIGH

Test status : PASSED

DESIGNER : TAM N NGUYEN  
 EXECUTED BY : TAM N NGUYEN  
 UPDATED ON : 09SEP2017  
 EXECUTED ON : 09SEP2017

## \* Description

› Name of module : OpenMRS default setting page

› \* **Precondition**

1. A local computer with administrator privilege
2. Java JRE installed
3. OpenMRS Standalone Version 2.6.0 downloaded and unzipped
4. A connection to the internet

› \* **Dependencies**

1. OpenMRS with demo database was loaded and runs normally
2. Good connection to the internet

› \* **Test Data**

<http://localhost:8081/openmrs-standalone/adminui/myaccount/changeDefaults.page?defaultLocale=fr>

› \* **Test steps**

1. Open up OpenMRS V. 2.6.0 Standalone. Make sure Tomcat Port is 8081 and MySQL port is 3316. A web page starting with localhost:8081 will be automatically opened upon successful start. The default language should be English. Login to OpenMRS
2. Using Windows Edge browser, go to "[https://www.w3schools.com/tags/tryit.asp?filename=tryhtml\\_iframe](https://www.w3schools.com/tags/tryit.asp?filename=tryhtml_iframe)"
3. At the W3School page, replace the value of iframe src with "<http://localhost:8081/openmrs-standalone/adminui/myaccount/changeDefaults.page?defaultLocale=fr>" without the double quotes and click the "Run" button.
4. You may have to choose "Load all protected content" and repeat step 3. Go back to the homepage of OpenMRS and observe the language of the page

› \* **Expected results**

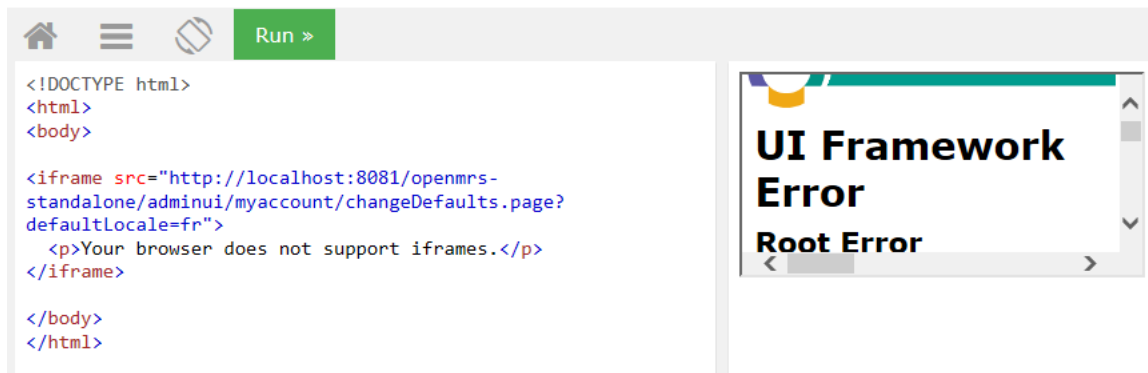
In the iframe, OpenMRS server will give an error message and the default language is still English.

› \* **Post-condition**

The OpenMRS service should still be able to run normally with the right language

› \* **Actual results**

In the iframe, OpenMRS server gave an error message and the default language is still English. "UI Framework Error - Root Error"



› \* **NOTES:**

Contact [tam.nguyen@ncsu.edu](mailto:tam.nguyen@ncsu.edu) if you have problems following instructions in this test case.

---

› **[ A8 - 02 - CSRF ] [ COMMAND EXECUTION ]**

---

› Priority : HIGH

Test status : PASSED

DESIGNER : TAM N NGUYEN  
EXECUTED BY : TAM N NGUYEN  
UPDATED ON : 09SEP2017  
EXECUTED ON : 09SEP2017

)\* **Description**

2) Name of module : OpenMRS help page

A different page will embed a link to OpenMRS. While the link appears to be normal (going to a known good site - the OpenMRS site), once the user clicks on it, it will launch an attack to the server under the logged in identity of the user.

- \* **Precondition**

1. A local computer with administrator privilege
2. Java JRE installed
3. OpenMRS Standalone Version 2.6.0 downloaded and unzipped
4. A connection to the internet

## \* Dependencies

1. OpenMRS with demo database was loaded and runs normally
2. Good connection to the internet

## )\* Test Data

[illegible]

## 2 \* Test steps

- [illegible]

### )\* Expected results

In the iframe, OpenMRS server will give an internal server error message HTTP Status 500 - Request processing failed; nested exception is java.lang.IllegalArgumentException ...

\*) **Post-condition**

The OpenMRS service should still be able to run normally

\*) Actual results

In the iframe, OpenMRS server gave an internal server error message HTTP Status 500 - Request processing failed; nested exception is java.lang.IllegalArgumentException ...





#### › \* NOTES:

Contact [tam.nguyen@ncsu.edu](mailto:tam.nguyen@ncsu.edu) if you have problems following instructions in this test case.

## › [A9 - UCKA] [ Finding Components with Known Vulnerabilities ]

DESIGNER : [Xiangqing Ding] UPDATED ON : [09/09/2017]

#### › Name of module : [ Third Party Libraries & Database ]

#### › Priority : [low]

#### › Description

This case is listing all the components with known vulnerabilities. And describe some related vulnerabilities.

#### › List of Components

1. Apache Tomcat: 7.0.50
2. MySQL: Latest
3. JQuery: 1.12.4
4. Spring framework: 3.x
5. Hibernate: N/A
6. Java: Java 6 is minimal
7. JDK: JDK 7
8. Liquibase: 2.0

#### › Vulnerabilities

Module: Tomcat

Vulnerability: A malicious web application running on Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 was able to bypass a configured SecurityManager via manipulation of the configuration parameters for the JSP Servlet

Link: <https://nvd.nist.gov/vuln/detail/CVE-2016-6796>

Module: Hibernate

Vulnerability: ReflectionHelper (org.hibernate.validator.util.ReflectionHelper) in Hibernate Validator 4.1.0 before 4.2.1, 4.3.x before 4.3.2, and 5.x before 5.1.2 allows attackers to bypass Java Security Manager (JSM) restrictions and execute restricted reflection calls via a crafted application.

Link: <https://nvd.nist.gov/vuln/detail/CVE-2014-3558>

## › [ A10 - 01 - API ] [ User object - Unvalidated Redirects and Forwards ]

› **Priority : medium**

› **Test status : PASSED**

DESIGNER : Fuxing Luan

› \* **Description**

› **Name of module : OpenMRS API - "User" object**

This test determines the level of OpenMRS API User object's protection against unauthorized access.

› \* **Precondition**

1. A local computer with administrator privilege
2. Java JRE installed
3. OpenMRS Standalone Version 2.6.0 downloaded and unzipped
4. OpenMRS Webservice API installed
5. Curl installed (optional)

› \* **Dependencies**

1. OpenMRS with demo database was loaded and runs normally
2. OpenMRS webservice API (<https://modules.openmrs.org/#/show/153/webservices-rest>)

› \* **Test Data**

<http://localhost:8081/openmrs-standalone/coreapps/activeVisits.page?app=www.google.com>

› \* **Test steps**

1. Open up OpenMRS V. 2.6.0 Standalone.
2. direct to the url in the test data

› \* **Expected results**

1. The page should be redirected to "[www.google.com](http://www.google.com)"

› \* **Actual results**

1. The page was redirected to "[www.google.com](http://www.google.com)"
- 

## › [ A10 - 02 - API] [ User object - TEST FOR AUTHENTICATION ]

---

› **Priority : medium**

› **Test status : PASSED**

DESIGNER : TAM N NGUYEN  
EXECUTED BY : TAM N NGUYEN  
UPDATED ON : 09SEP2017  
EXECUTED ON : 09SEP2017

› \* **Description**

› **Name of module : OpenMRS API - "User" object**

This test determines the level of OpenMRS API User object's protection against unauthorized access.

› \* **Precondition**

1. A local computer with administrator privilege

2. Java JRE installed
3. OpenMRS Standalone Version 2.6.0 downloaded and unzipped
4. OpenMRS Webservice API installed
5. Curl installed (optional)

#### › \* Dependencies

1. OpenMRS with demo database was loaded and runs normally
2. OpenMRS webservice API (<https://modules.openmrs.org/#/show/153/webservices-rest>)

#### › \* Test Data

<http://localhost:8081/openmrs-standalone/ws/rest/v1/user/> and/or curl -X GET --header 'Accept: application/json' '<http://localhost:8081/openmrs-standalone/ws/rest/v1/user/>' (optional)

#### › \* Test steps

1. Open up OpenMRS V. 2.6.0 Standalone. Make sure Tomcat Port is 8081 and MySQL port is 3316. A web page starting with localhost:8081 will be automatically opened upon successful start.
2. Open a web browser. Make sure no user was logged in, and paste this following url in : <http://localhost:8081/openmrs-standalone/ws/rest/v1/user/>
3. This step is optional. Open a command line, make sure Curl was installed, paste and run this command: curl -X GET --header 'Accept: application/json' '<http://localhost:8081/openmrs-standalone/ws/rest/v1/user/>'
4. In either case, observe to see if there is a prompt for inputting username/password. If there is a prompt, please put in wrong username/password and observe the result.

#### › \* Expected results

1. For test step 2, web browser should load an XML file. Around line 15, you will see "User is not logged in [Privileges required: Get Users]" and the rest of the file contains troubleshooting information regarding the api.
2. For test step 3, you should be able to see the similar message and/or a 401 message, saying "User not logged in"

#### › \* Post-condition

Webservice API is still up, available to serve further requests.

#### › \* Actual results

1. Used the browser test method and received and XML with "User is not logged in [Privileges required: Get Users]"

![User is not logged in [Privileges required: Get Users](#)

#### › \* NOTES:

- OpenMRS API documentation together with examples can be found at <http://localhost:8081/openmrs-standalone/module/webservices/rest/apiDocs.htm> (logged in as admin first) You can expand the objects and click "try it out" to get sample codes.
- You can install the OpenMRS webservice API by downloading it from <https://modules.openmrs.org/#/show/153/webservices-rest> and then move the downloaded file to [download folder]\referenceapplication-standalone-2.6.0\appdata\modules
- Contact [tam.nguyen@ncsu.edu](mailto:tam.nguyen@ncsu.edu) if you have problems following instructions in this test case.