

EE6052 Web Application Design

Programming Project2

Group 14

Xiaolong Liang, UL student ID 15021793, M.Eng. Computer and Communications Systems

Benjamin Keil, UL student ID 13116371, B.Sc. Computer Systems

Abdul Halim, UL student ID 13029096, B.Sc. Computer Systems

Enda O'shea, UL student ID 13062344, B.Sc. Computer Systems

David Hammill, UL student ID 13069667, B.Sc. Computer Systems

University of Limerick

Limerick, Ireland

Project Description

The project is an online shop application using EJB, entity classes and servlets/JSF/HTML. Features implemented using servlets, JSF pages, and EJBs only. Use a stateful session bean for the shopping cart. Use a message-driven bean for the logging facility. This project is developed in NetBeans.

Project Requirements

- Access to the shop is limited via an authentication scheme.
 - Access rights are role-based, i.e. customer and administrator.
- Provide at least two accounts
 - Customer joe with password 1D10T?
 - Administrator toor with password 4uldo0!
- Functionality
 - Customer
 - Browse through all items
 - Search products by ID number and browse through the search results
 - Search products by name and browse through the search results
 - Add displayed items to shopping cart
 - Remove items from their shopping cart
 - Edit their profile – must contain at least name, Customer ID and a message to other users. Name and ID are taken from Customer table, message can be any text – allow at least for 500 characters
 - View profiles from other users – provide search by name and search by ID
 - Check out or cancel current order
 - Administrator
 - Add new products to the sale database
 - Remove products from the sale database
 - Increase/decrease available amount of any product
 - When customers check out, the quantity for your items in the database is adjusted correspondingly. Make sure the quantity of any product in the database cannot drop below 0.
 - When customers cancel their order, the database should remain unchanged.
- Logging facility
 - Every time a customer confirms an order or cancels an order, a corresponding entry is added to the log (use either log-file or table in database).
 - Every time an administrator adds or removes a product, a corresponding entry is added to the log.
- Security against specific OWASP Top 10 vulnerabilities
 - A1: Injection
 - A2: Broken Authentication & Session Management
 - A3: Cross-Site Scripting (XSS)
 - A4: Insecure Direct Object References
 - A7: Missing Function Level Access Control
 - A8: Cross-Site Request Forgery (CSRF)
 - A10: Invalidated Redirects and Forwards (your application must contain at least one user input-dependent redirect or forward)
 - Discuss what techniques were used to ensure the application is not vulnerable to the listed OWASP vulnerabilities.
 - Discuss how the application was tested to ensure the chosen defence is working correctly.

Fulfilment of Project Requirements: Access via Authentication Scheme

We are using form-based authentication using JDBC realm. Required Users, Groups are created by app on deployment but GlassFish server needs to be configured to allow this authentication mechanism properly. Please refer to “README_GlassFish_Config.txt” for Server configuration details.

- Access to the shop is limited via an authentication scheme.
 - Access rights are role-based, i.e. customer and administrator.
- Provide at least two accounts
 - Customer joe with password 1D10T?
 - Administrator toor with password 4uldo0!

Customer log in:

Bulletproof Systems

Please sign in

joe

.....

Sign in

Administrator log in:

Bulletproof Systems

Please sign in

toor

.....

Sign in

- *The customer and administer log in the system using the same login webpage.*
- *Only valid user name can log in the system.*

Bulletproof Systems

Invalid username or password.

Return to [Log in](#).

Fulfilment of Project Requirements: Customer Functions

- Browse through all items when Logged in as customer:

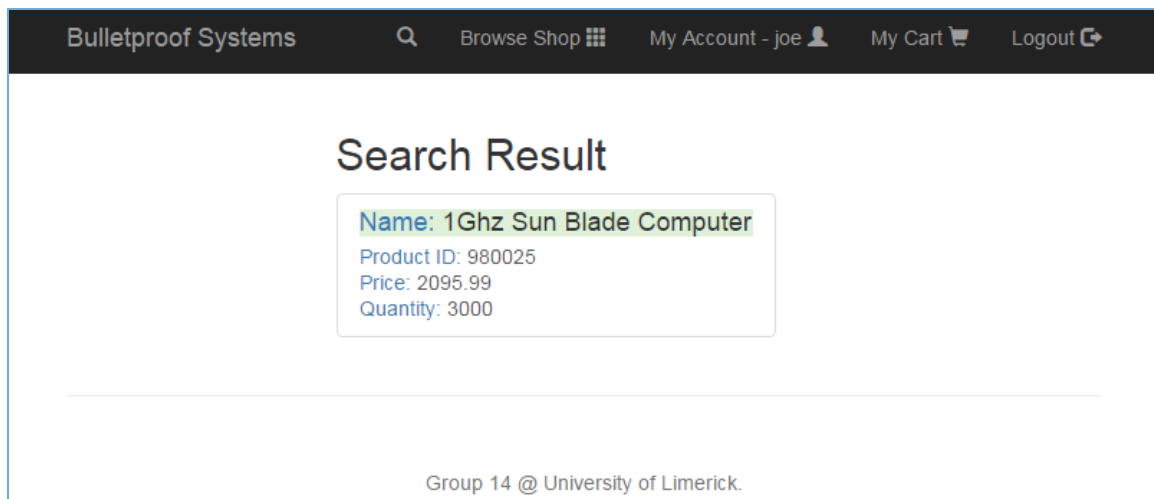
The screenshot shows the 'Product Catalog' page of the 'Bulletproof Systems' website. The header includes the site name, a search icon, and navigation links for 'Browse Shop', 'My Account - joe', 'My Cart', and 'Logout'. The main content area is divided into a 'Category' sidebar and a 'Product List' section. The sidebar lists categories: 'All Category', 'Software', 'Hardware', 'Firmware', 'Books', 'Cables', and 'Misc'. The 'Product List' section displays two products: 'Identity Server' and 'Accounting Application'. Each product entry includes its manufacturer ('Mfg: Happy End Searching' and 'Mfg: Smith Bird Watching'), price per unit (€1095.00 and €11500.99), and stock status ('In stock: 500' and 'In stock: 497'). An 'Add to cart' button is present for each product.

Category	Product Name	Manufacturer	Price per-unit	Stock
Identity Server	Identity Server	Mfg: Happy End Searching	€1095.00	In stock: 500
Accounting Application	Accounting Application	Mfg: Smith Bird Watching	€11500.99	In stock: 497

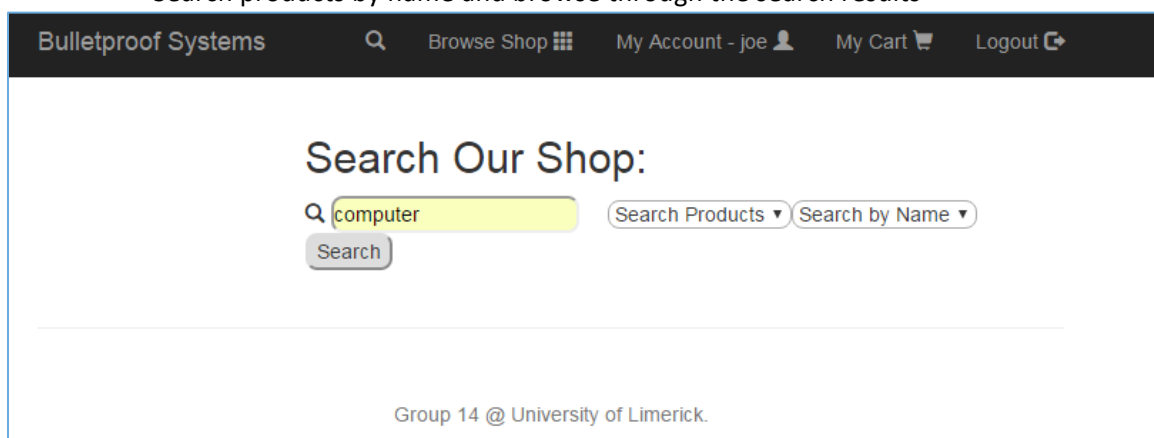
- Search products by ID number and browse through the search results

The screenshot shows the 'Search Our Shop:' page of the 'Bulletproof Systems' website. The header is identical to the previous screenshot. The main content area features a search bar with the text '980025' entered. Below the search bar is a 'Search' button. To the right of the search bar are two dropdown menus: 'Search Products' and 'Search by ID'. The footer of the page reads 'Group 14 @ University of Limerick.'

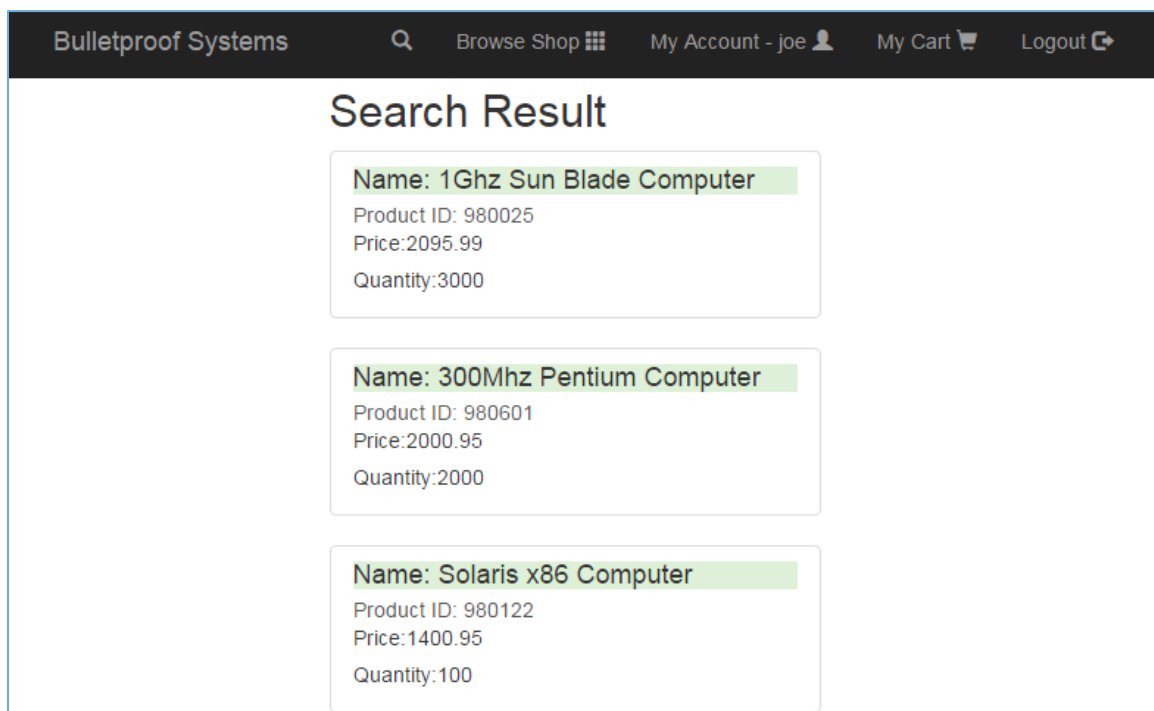
Search result



- Search products by name and browse through the search results



Search result



- Add displayed items to shopping cart

Add two products "Identity Server" and "Accounting Application" to cart:

Bulletproof Systems

Q

Browse Shop

My Account - joe

My Cart

Logout

Product Catalog

Product List

Category

All Category

Software

Hardware

Firmware

Books

Cables

Misc

Identity Server

Mfg: Happy End Searching

Price per-unit: €1095.00

Add to cart

In stock: 500

Accounting Application

Mfg: Smith Bird Watching

Price per-unit: €11500.99

Add to cart

In stock: 497

- Browse shopping cart (Update the quantity to 50 and 97 respectively)

Bulletproof Systems

Q

Browse Shop

My Account - joe

My Cart

Logout

Checkout

Continue shopping

Your Current Shopping Cart

Please select your required quantity for the items below.

Product Name	Price	Qty		Item total	
Identity Server	1095.00	50	Change Quantity: <input type="text" value="50"/> <button>Update</button>	54750.00	<button>Remove</button>
Accounting Application	11500.99	97	Change Quantity: <input type="text" value="97"/> <button>Update</button>	1115596.03	<button>Remove</button>

Total cost: 1170346.03

Checkout

- Checkout shopping cart

Bulletproof Systems

Q

Browse Shop

My Account - joe

My Cart

Logout

Checkout

Checkout List

Product Name	Price	Qty	Total Cost
Identity Server	1095.00	50	54750.00
Accounting Application	11500.99	97	1115596.03

Total Cost: 1170346.03

Cancel

Confirm

Confirm Checkout List

Bulletproof Systems

Browse Shop

My Account - joe

My Cart

Logout

Shop Name

Confirmation

Purchase Order

Product ID	Order Number	Customer ID	Quantity	Sales Date	Shipping Cost	Shipping Date	Courier
980001	30298011	1	50	Sat Apr 30 02:13:47 BST 2016	20	Sat May 14 02:13:47 BST 2016	DPD Couriers
980005	30298012	1	97	Sat Apr 30 02:13:47 BST 2016	20	Sat May 14 02:13:47 BST 2016	DPD Couriers

Total Cost : 1170346.03

Your order has been received.

Delivery is expected within two weeks.

When customers check out, the quantity for your items in the database is adjusted correspondingly.

Bulletproof Systems

Browse Shop

My Account - joe

My Cart

Logout

Product Catalog

Category

All Category

Software

Hardware

Firmware

Books

Cables

Misc

Product List

Identity Server

Mfg: Happy End Searching

Price per-unit: €1095.00

Add to cart

In stock: 450

Accounting Application

Mfg: Smith Bird Watching

Price per-unit: €11500.99

Add to cart

In stock: 400

When customers cancel their order, the database should remain unchanged

Bulletproof Systems

Browse Shop

My Account - joe

My Cart

Logout

Checkout

Checkout List

Product Name	Price	Qty	Total Cost
Identity Server	1095.00	1	1095.00
Accounting Application	11500.99	1	11500.99

Cancel

Confirm

Total Cost: 12595.99

Browser Shop again and the quantity didn't change.

Bulletproof Systems

Product Catalog

Category

- All Category
- Software
- Hardware
- Firmware
- Books
- Cables
- Misc

Product List

Identity Server	Mfg: Happy End Searching	Price per-unit: €1095.00	In stock: 450
Accounting Application	Mfg: Smith Bird Watching	Price per-unit: €11500.99	In stock: 400

- Edit user profile

Bulletproof Systems

Edit profile

Xiaolong Liang

Name: Xiaolong Liang

Address 1: Castletroy

Address 2: UL

City: Miami

State: FL

Phone: 0834831666

Email: 15021793@studentmail.ul.ie

Message: 15021793@studentmail.ul.ie

Update profile

Back to Start

Update profile.

You have successfully updated your profile information.

[View profile](#)

Group 14 @ University of Limerick.

- The quantity of a product in the database cannot drop below 0. If the customer buys 451 (database is 450) Identity Servers as shown below,

Bulletproof Systems
Browse Shop
My Account - joe
My Cart
Logout

Checkout

Checkout List

Product Name	Price	Qty	Total Cost
Identity Server	1095.00	451	493845.00

Total Cost: 493845.00

Cancel
Confirm

Confirm the Checkout List will lead to a message displaying on user's screen.

Bulletproof Systems
Browse Shop
My Account - joe
My Cart
Logout

Checkout

Continue shopping

Your Current Shopping Cart

That quantity is no longer available for Identity Server.Please select another quantity.

Product Name	Price	Qty		Item total	
Identity Server	1095.00	451	Change Quantity: <input type="text" value="451"/> Update	493845.00	Remove

Total cost: 493845.00

Checkout

The customer cannot checkout.

Bulletproof Systems
Browse Shop
My Account - joe
My Cart
Logout

Checkout

Checkout List

Product Name	Price	Qty	Total Cost
Identity Server	1095.00	451	493845.00

Total Cost: 493845.00

Cancel
Confirm

Now we logged in as toor

The confirmation and cancels of two orders we did before are logged as below.



Log File

Admin Options

Admin Options

[Add Item](#)[Delete Item](#)[Edit item](#)

Log Details

Date Sat Apr 30 01:43:48 BST 2016, AdminID:2, Added Item:Product ID =988766:Description = BirdersCables:Qty = 10

Date Sat Apr 30 01:49:39 BST 2016, AdminID:2, Removed Item: entity.Product[productId=988766]

PO:--OrderNo:30298012, CustID:entity.Customer[customerId=1], Carrier:DPD Couriers, ProdID:entity.Product[productId=980005], Qty:97, DateSold:Sat Apr 30 02:13:47 BST 2016, ShipDate:Sat May 14 02:13:47 BST 2016, ShipCost:20

PO:--OrderNo:30298011, CustID:entity.Customer[customerId=1], Carrier:DPD Couriers, ProdID:entity.Product[productId=980001], Qty:50, DateSold:Sat Apr 30 02:13:47 BST 2016, ShipDate:Sat May 14 02:13:47 BST 2016, ShipCost:20

Date:30 Apr 2016 01:17:06 GMT, ID: 13062344, Product ID:980001, Qty:1, Order Cancelled

Fulfilment of Project Requirements: Administrator Functions

Logged in as toor:

The screenshot shows the 'Product Catalog' page of the 'Bulletproof Systems' application. The user is logged in as 'toor'. The page features a sidebar with category links: All Category, Software, Hardware, Firmware, Books, Cables, and Misc. The main content area, titled 'Product List', displays two product entries. Each entry includes the product name, manufacturer information, price per unit, and stock status, along with an 'Add to cart' button.

Product Name	Manufacturer	Price per-unit	In stock
Identity Server	Mfg: Happy End Searching	€1095.00	500
Accounting Application	Mfg: Smith Bird Watching	€11500.99	497

Manage shop (Only logged in as toor can access the function “Manage Shop”)

The screenshot shows the 'Manage Shop' page of the 'Bulletproof Systems' application. The user is logged in as 'toor'. The page displays a 'Log File' path at the top. Below, the 'Product List' section shows three product entries. Each entry includes the product name, price, and stock status, along with a 'Remove Item' button. The sidebar on the left contains 'Admin Options' with links for 'Add item', 'Edit item', and 'Open Log'.

Product Name	Price	In stock
Identity Server	€1095.00	1000
Accounting Application	€11500.99	497
1Ghz Sun Blade Computer	€2095.99	3000

- Add new products to the sale database

Bulletproof Systems

Q

Browse Shop

Manage Shop

My Account - toor

My Cart

Logout

Shop Name

Category

Delete Item
Edit item
Open Log

Add New Item

Manufacturer	Birders United
Product Code	Cables
Purchase Cost	1234
Quantity	10
Markup	10.5
Product Code	False
Description	BirdersCables

Add Item

Item Added:

Bulletproof Systems

Q

Browse Shop

Manage Shop

My Account - toor

My Cart

Logout

Shop Name

Category

Delete Item
Edit item
Open Log

Add New Item

Manufacturer	Birders United
Product Code	Cables
Purchase Cost	1234
Quantity	10
Markup	10.5
Product Code	False
Description	BirdersCables

Add Item

Item Added

Item added successfully

Bulletproof Systems

Q

Browse Shop

Manage Shop

My Account - toor

My Cart

Logout

Firmware

Books

Cables

Misc

Network Cable

Mfg: Computer Support Center

Price per-unit: €25.95

Add to cart

In stock: 500

BirdersCables

Mfg: Birders United

Price per-unit: €1234

Add to cart

In stock: 10

- Remove products from the sale database
- Remove item BirdersCables we just added.

Bulletproof Systems		Q	Browse Shop	Manage Shop	My Account - toor	My Cart	Logout
Birders United	€36.95						
Remove Item	In stock: 50						
Flat screen Monitor							
Birders United	€199.95						
Remove Item	In stock: 25						
BirdersCables							
Birders United	€1234						
Remove Item	In stock: 10						

Item removed successfully

Bulletproof Systems

Q

Browse Shop

Manage Shop

My Account - toor

My Cart

Logout

Shop Name

Admin Options

Add Item

Edit Item

Open Log

Log File:C:\Program Files\glassfish-4.1.1\glassfish\domains\domain1\config\team8_logFile14.txt

Item Removed

Product List

Identity Server

€1095.00

Happy End Searching

Remove Item

In stock: 1000

Accounting Application

€11500.99

Smith Bird Watching

Remove Item

In stock: 497

- Increase/decrease available amount of any product

The quantity of Identity Server updated before is 1000

Bulletproof Systems

Browse Shop

Manage Shop

My Account - toor

My Cart

Logout

Product List

Category

All Category

Software

Hardware

Firmware

Books

Cables

Misc

Identity Server

Mfg: Happy End Searching

Price per-unit: €1095.00

Add to cart

In stock: 1000

Accounting Application

Mfg: Smith Bird Watching

Price per-unit: €11500.99

Update the item Identity Server to New Quantity of 500

Bulletproof Systems Q Browse Shop Manage Shop My Account - toor My Cart Logout

Shop Name

Admin Options

Add Item

Delete Item

Product List

Product	Identity Server
New Quantity	500

Update Quantity

Quantity has been updated

Bulletproof Systems Q Browse Shop Manage Shop My Account - toor My Cart Logout

Shop Name

Admin Options

Add Item

Delete Item

Open Log

Product List

Product	Identity Server
New Quantity	500

Update Quantity

Quantity has been updated

Quantity updated successfully

Bulletproof Systems Q Browse Shop Manage Shop My Account - toor My Cart Logout

Product Catalog

Category

All Category

Software

Hardware

Firmware

Books

Cables

Misc

Product List

Identity Server	
Mfg: Happy End Searching	Price per-unit: €1095.00
Add to cart	In stock: 500

Accounting Application	
Mfg: Smith Bird Watching	Price per-unit: €11500.99

▪ Every time an administrator adds/removes a product an entry is added to the log
Two entries of adding and removing an item above were added to the log.

Bulletproof Systems Q Browse Shop Manage Shop My Account - toor My Cart Logout

Admin Options

Add Item

Delete Item

Edit item

Log File

Log Details

Date Sat Apr 30 01:43:48 BST 2016, AdminID:2, Added Item:Product ID =988766:Description = BirdersCables:Qty = 10

Date Sat Apr 30 01:49:39 BST 2016, AdminID:2, Removed Item: entity.Product[productId=988766]

Fulfilment of Project Requirements: Detail how the techniques used that can ensure the application is not vulnerable

A1 – Injection:

These flaws occur when an application sends untrusted data to an interpreter. These types of flaws are found in SQL queries, LDAP queries, XPath queries, OS commands and other program arguments etc. These are easy to discover when examining code, but more hard via testing. In few cases, scanners and fuzzers can help attackers find these flaws.

Example in Shopping cart context:

In the context of shopping cart, we are using some commands in entity class like this:

```
"SELECT p FROM Product p WHERE p.productName=:pname OR plproductCode=:pid"
```

To prevent SQL injection.

A2 – Broken Authentication and Session Management:

These types of flaws are found in the context of building the account logging, secret questions, password management and few issues.

Example in Shopping cart context:

In this context, we are not passing the session ID's in the URL which prevents the attackers to manipulate the ID's and broke the authentication.

A3 – Cross-Site Scripting (XSS):

JSF is designed to have built-in XSS prevention. We can safely redisplay all user-controlled input including request headers, request parameters and request bodies by using any JSF component.

In the case of this project:

```
<h:outputText value="#{userProfileBean.customerDetails.name}" />
<h:outputText value="#{userProfileBean.customerMessage}" escape="true"/>
<h:inputText id="movie" value="#{item.product_quantity}"></h:inputText>
```

Etc...

Checking input in edit profile

```
<h:inputText id="name"
    styleClass="form-control"
    value="#{editProfileBean.name}"
    p:placeholder="Name"
    required="true"
    requiredMessage="Name is required"
    validatorMessage="Name contains invalid characters">
    <f:validateRegex pattern="^[^\\?\\%\\+\\$\\(\\)\\{\\}\\;\\'\\&\\&lt;\\&gt;]+$" />
</h:inputText>
```

Only valid input can be updated

Bulletproof Systems
Browse Shop
Manage Shop
My Account - toor
My Cart
Logout

Address 2
City
State
Phone
Email
Message
Update profile
Back to Start

Group 14 @ University of Limerick.

- State can be only alphabetic characters
- Message can be only alphabetic characters

Adding invalid new item

Bulletproof Systems
Browse Shop
Manage Shop
My Account - toor
My Cart

Shop Name
Add New Item
Category
Delete Item
Edit Item
Open Log

Manufacturer	Smith Bird Watching
Product Code	Software
Purchase Cost	1111
Quantity	1324
Markup	qequerq
Product Code	True
Description	Smith Bird

Add Item

Group 14 @ University of Limerick.

- j_idt12:markup: 'qequerq' must be a signed decimal number.
- Regex Pattern not matched

A4 – Insecure Direct Object References:

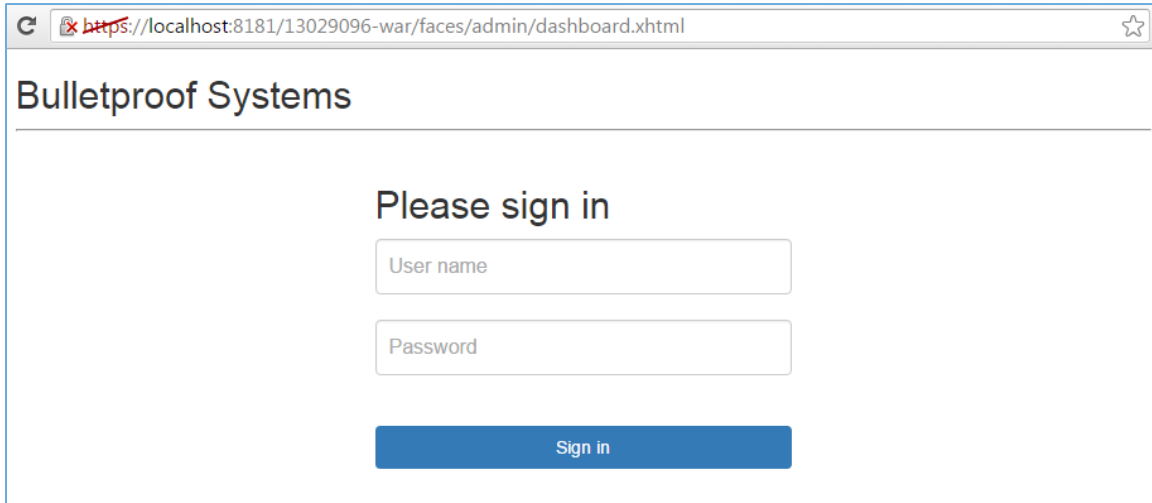
In many applications, the access is done by the actual name or key of the object. In such circumstances, these applications will not authorize the entry always, which results in insecure direct object access. This flaw can be easily noticed by manipulating some fields in the applications.

In the context of this project, we use per user or session indirect object references. Invalid users cannot directly target unauthorized resources. Alternatively, we are not passing the user's ID or username to the URL.

A7 – Missing Function Level Access Control:

Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.

In this project, only authorized user can login to the system and cannot access any webpage when not logging in.



This function is implemented in the web.xml file:

```
<security-constraint>
  <display-name>AuthorizedAccess</display-name>
  <web-resource-collection>
    <web-resource-name>shopping_catalog</web-resource-name>
    <description/>
    <url-pattern>/faces/shop/*</url-pattern>
  </web-resource-collection>
  <auth-constraint>
    <description/>
    <role-name>user</role-name>
  </auth-constraint>
</security-constraint>
```

Only logged in user role can access the url patterned /face/shop/*, user without login cannot access any url with pattern /face/shop/*

A8 – Cross Site Request Forgery (CSRF):

JSF 2.x has already built-in CSRF prevention, featured with javax.faces.viewstate hidden filed in the form when using server side state saving.

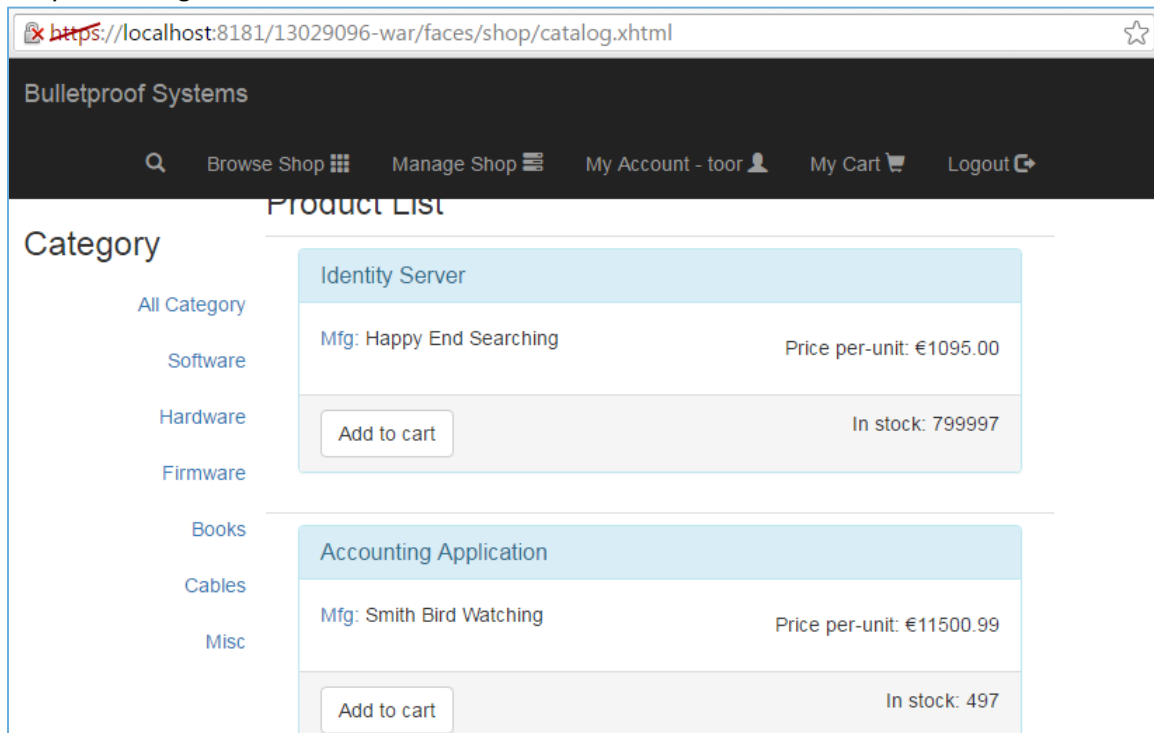
We'll have a CSRF attack hole only when using views as in <f:view transient="true">, or there's a XSS attack somewhere. In the context of this project, all transient is false.

A9 – Failure to Restrict URL Access:

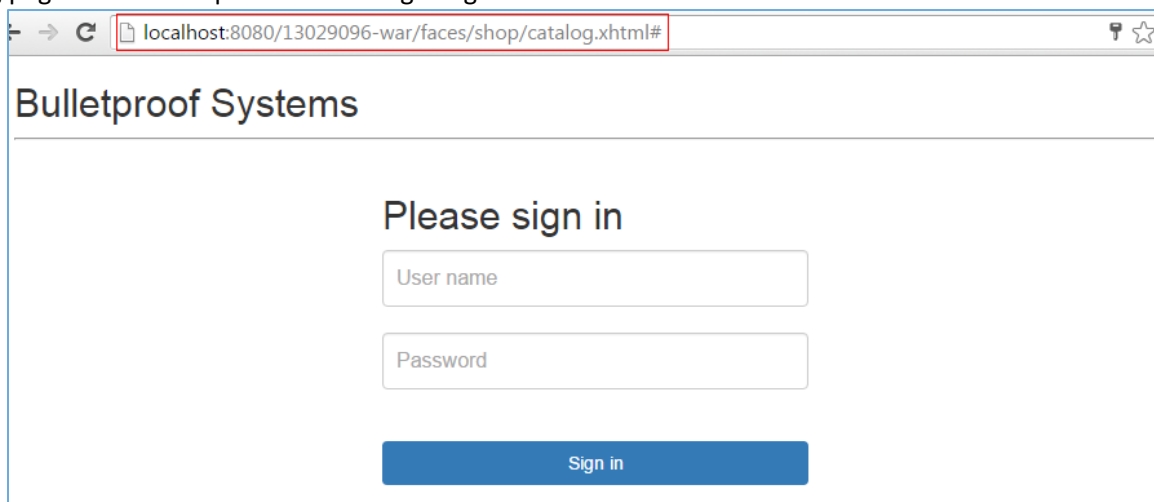
In many cases, some applications are not protecting the page requests properly. Sometimes, URL protection is managed via configuration and system is misconfigured. Hardest part is to detect the vulnerable pages.

Example in Shopping cart context:

Logging in the system using administrator username “toor”



After logging out the system and input the URL <http://localhost:8080/13029096-war/faces/shop/catalog.xhtml>, The catalog page cannot be opened unless log in again.



The implantation of avoiding this vulnerability:

➤ User that logged in the system as customer can access all the webpages.

```
<security-constraint>
  <display-name>AuthorizedAccess</display-name>
  <web-resource-collection>
    <web-resource-name>shopping_catalog</web-resource-name>
    <description/>
    <url-pattern>/faces/shop/*</url-pattern>
```

```

</web-resource-collection>
<auth-constraint>
  <description/>
  <role-name>user</role-name>
</auth-constraint>
</security-constraint>

```

- User that logged in the system as administrator can access all the webpages.

```

<security-constraint>
  <display-name>AdminAccess</display-name>
  <web-resource-collection>
    <web-resource-name>AllAdminOperations</web-resource-name>
    <description/>
    <url-pattern>/faces/admin/*</url-pattern>
  </web-resource-collection>
  <auth-constraint>
    <description>Admin Only Access</description>
    <role-name>admin</role-name>
  </auth-constraint>
  <user-data-constraint>
    <description>Secured Login</description>
    <transport-guarantee>CONFIDENTIAL</transport-guarantee>
  </user-data-constraint>
</security-constraint>

```

- Login authentication make sure only the valid user can log in the system

```

<login-config>
  <auth-method>FORM</auth-method>
  <realm-name>file</realm-name>
  <form-login-config>
    <form-login-page>/login.xhtml</form-login-page>
    <form-error-page>/error.xhtml</form-error-page>
  </form-login-config>
</login-config>

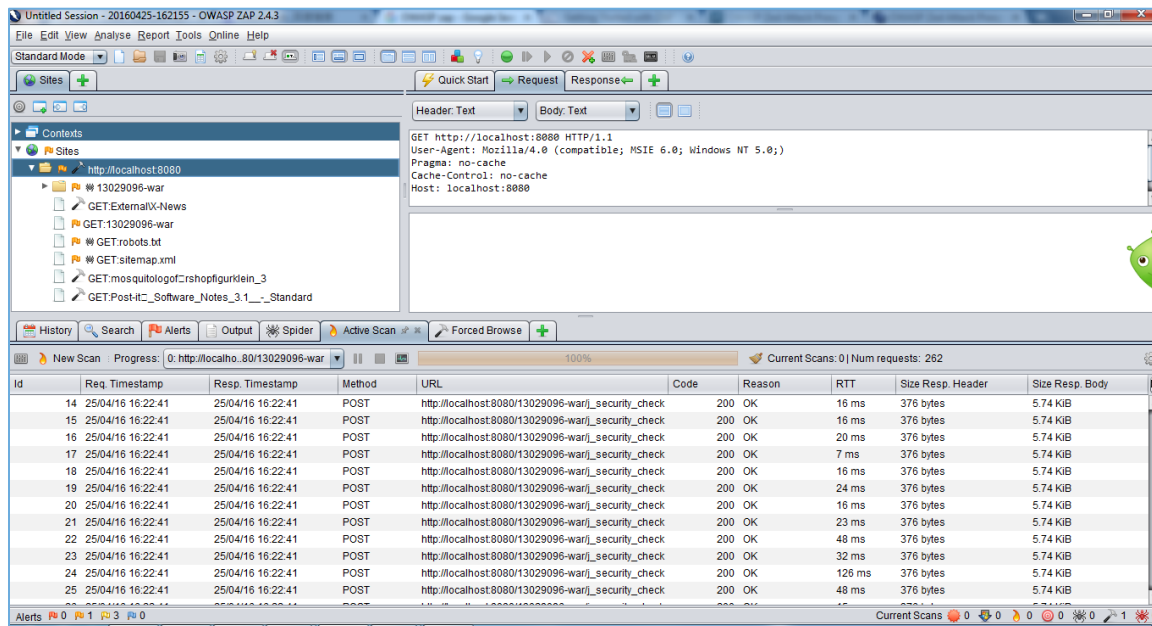
```

OWASP ZAP Description

- Security against specific OWASP Top 10 vulnerabilities
 - OWASP ZAP Tool was run to test the application for security flaws.
 - OWASP ZAP did not detect any security flaws.

OWASP Zed Attack Proxy (ZAP) is a common tool that used to find security vulnerabilities automatically in the web application while developing and testing the applications. This open-source tool was developed at the Open Web Application Security Project (OWASP). It is the Swiss army knife of web assessment tools. Its active scanner is integrated into many of the other functions of the application. Having a proxy and other tools built in is a huge plus. One of the unique features of ZAP is that its sensitivity and scan aggressiveness can be manually configured. There are three sensitivity settings---high, medium and low. ZAP allows a user to save sessions and persist sessions allowing you to take a break from your testing and come back to it. This is also a helpful feature when you need to confirm fixes and remediation.

Furthermore, ZAP is strong in consistency. Any difference between tests in ZAP is most likely caused by user. Before initiating the active scanner, it would be wise to spider the site multiple times. It has the ability to build on previous spider results until there are no new pages found.



Fulfilments of Project Requirements: Discuss how the application was tested to ensure the chosen defence is working correctly.

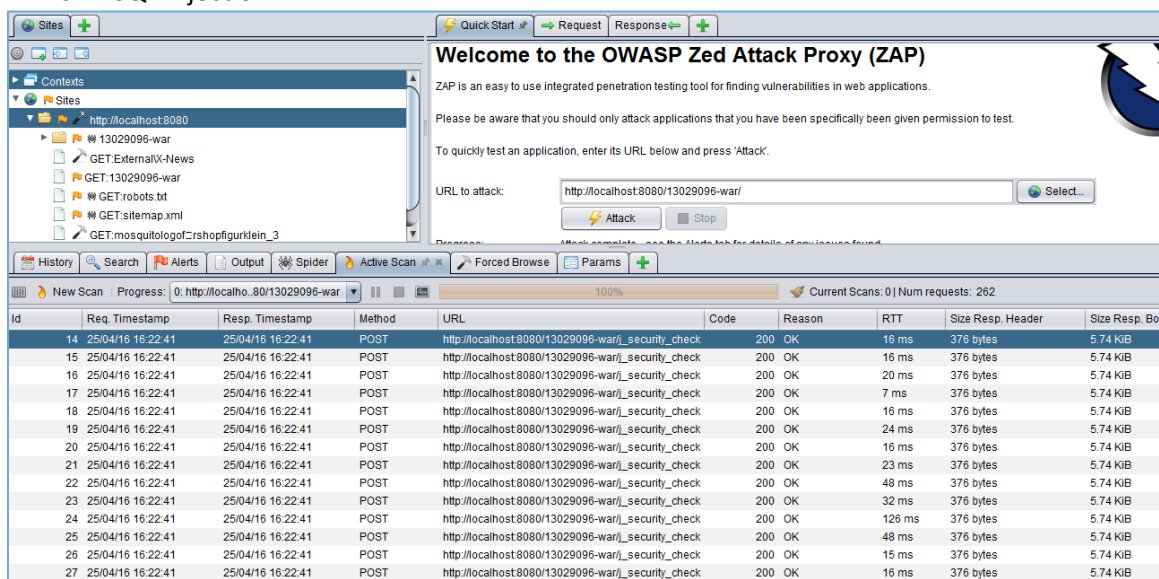
- OWASP ZAP was used to testing the following vulnerabilities:
 - A1 (injection)
 - A3 (cross-site scripting) (XSS)
 - A5 (security misconfiguration) (some instances)
 - A6 (sensitive data exposure) (some instances)
 - A8 (Cross site request forgery) (some instances)
 - A10 (invalidated redirects and forwards)

- The other vulnerabilities (as well as certain cases of some of those listed above) are hard or impossible to test for using automation and require manual testing. This usually involves surfing around with a browser proxied through OWASP ZAP, setting breakpoints, and then manually modifying requests before they are sent to the server.

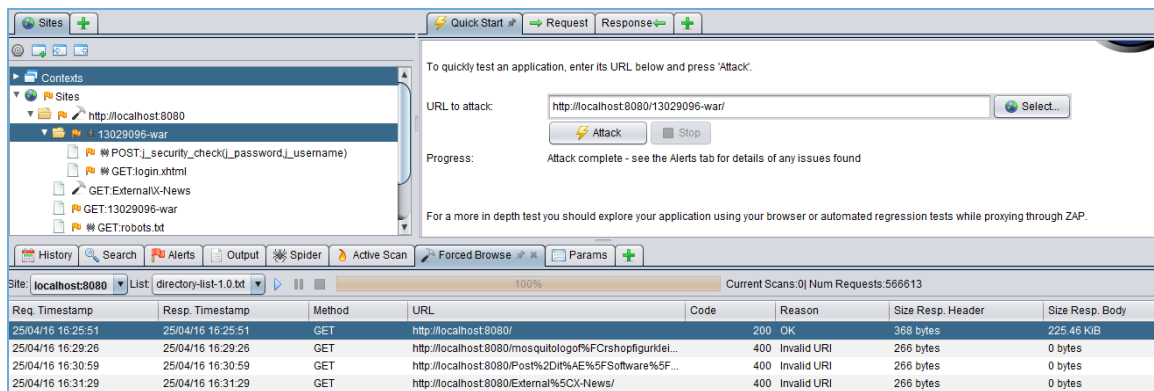
Quick Start is used to quickly test a web application with the active scanner.

The following release quality active scan rules are included in quick start.

- Buffer Overflow
- Code Injection
- Command Injection
- Client Browser Cache
- Cross Site Scripting (reflected)
- CRLF Injection
- Directory Browsing
- External Redirect
- Format String Error
- Parameter Tampering
- Path Traversal
- Remote File Include
- Server Side Include
- SQL Injection

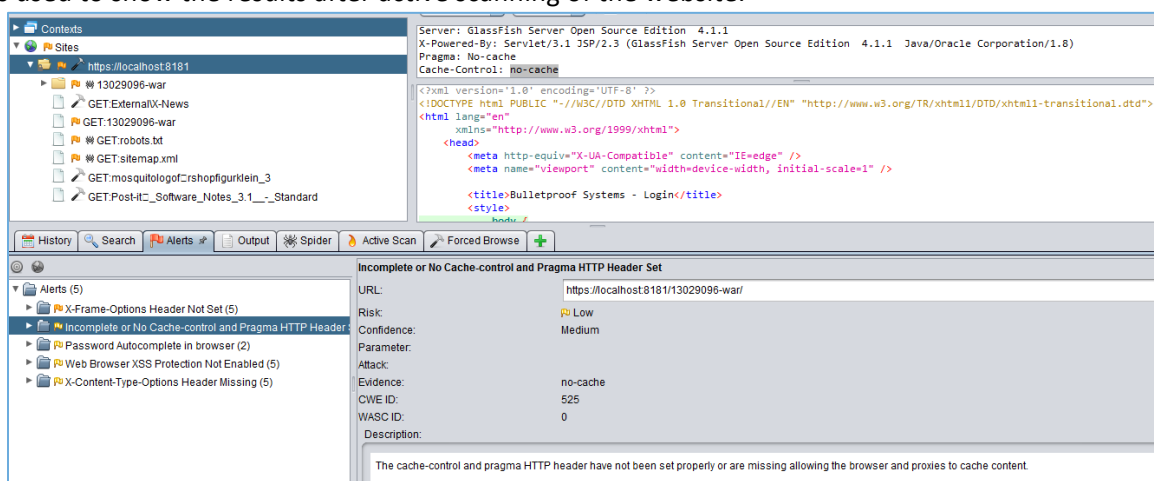


Forced Browse is used to try to discover directories and files using forced browsing. A set of files are provided which contain a large number of file and directory names. ZAP attempts to directly access all of the files and directories listed in the selected file directly rather than relying on finding links to them. It was used to test OWASP A7 Missing Function Level Access Control.

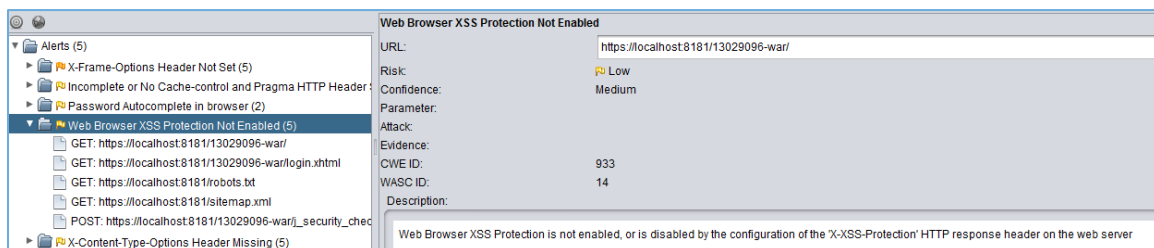


From the result above, we can see that only the URL of <http://localhost:8080/> can be opened, the rest of them are invalid URLs and cannot be opened without logging in.

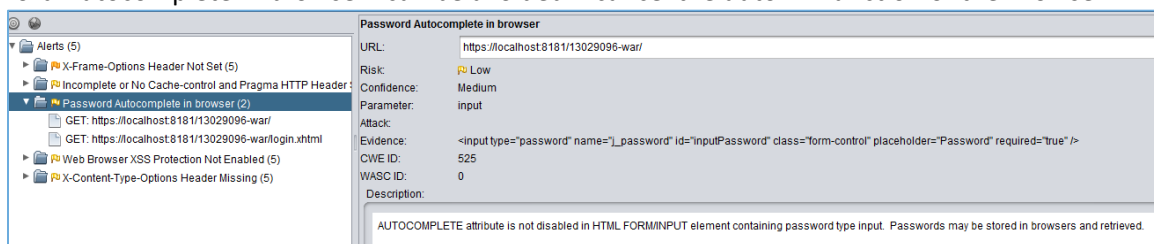
Alerts tab is used to show the results after active scanning of the website.



After the active scanning, we can see that there is a low risk of XSS --- web browser XSS Protection is not enabled, or is disabled by the configuration of the “X-XSS-Protection” HTTP response header on the web server, which is caused by the configuration of the Browser.



Alert “Password Autocomplete in browser” can be avoided if cancel the auto-fill function of the Browser.



Other than that, there are no vulnerabilities such as Injection, CSRF, Missing Function Level Access Control, Broken Authentication & Session Management, Failure to Restrict URL Access and Insecure Direct Object Reference.

Summary

After testing our application with OWASP ZAP tool, there are just a few medium standard alerts. Our application is not vulnerable to the required OWASP Top 10 vulnerabilities.