

Check Point Report

Vulnerable Application: Bodgeit

Team Name: Group X

Team Members: X, X, X

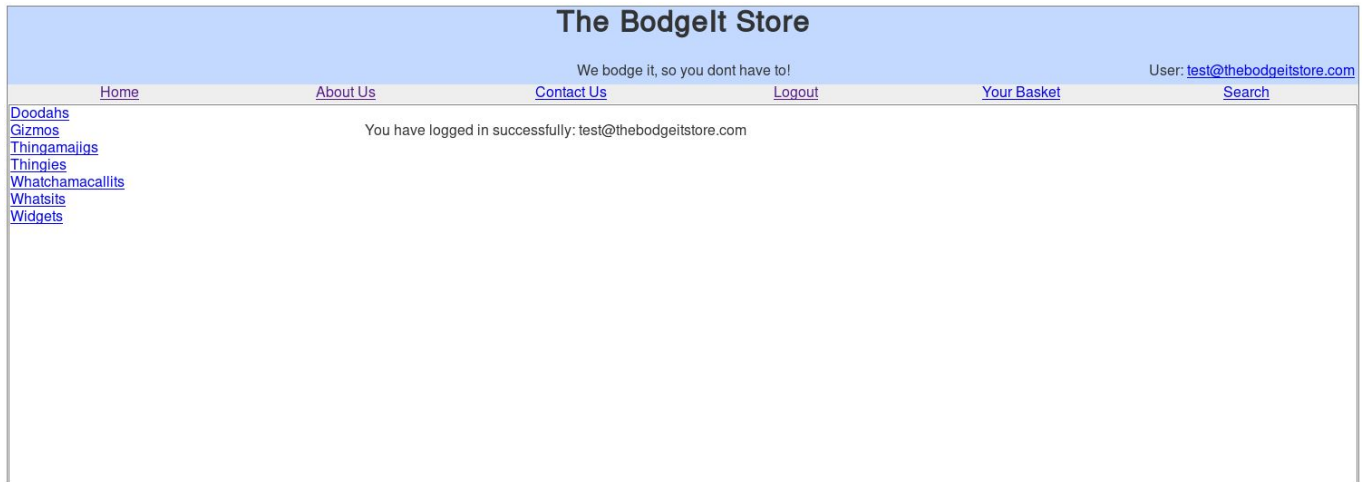
Vulnerability	Details of the Attack	Screenshot evidence
(C1) Broken Authentication since "password" is one of the most commonly used passwords	Attack: Brute force dictionary attack 1. Navigate to <i>/bodgeit/login.jsp</i> and input the username "test@thebodgeitstore.com" 2. Input the password "password" and click the "Login" button.	* included below table
(C2) SQL Injection	Attack: SQL injection 1) Navigate to <i>/bodgeit/login.jsp</i> 2) Enter user1@thebodgeitstore.com into the username field and enter ' or '1'='1 into the password field and press the <i>Login</i> button.	<<a screenshot showing the result of the attack>> * included below table
(C3) SQL Injection	Attack: SQL Injection 1) Navigate to <i>/bodgeit/login.jsp</i> 2) Enter admin@thebodgeitstore.com ' or '1'='1 into the username field and press the <i>Login</i> button.	* included below table
(C4) Insecure Direct Object References since an attacker can change a parameter value that directly	Attack: Insecure direct object reference attack 1) Inspect source code of <i>/bodgeit/login.jsp</i> to look for clues	* included below table

refers to a system object - in this case the admin page.	<ol style="list-style-type: none"> 2) Upon finding the line: <code><!-- td align="center" width="16%">Admin</td--></code> Navigate to <code>/bodgeit/admin.jsp</code> 3) You have now found an insecure admin page for the Bodgeit Store Website 	
(C5) Missing Function Level Access Control since the user can change the URL to enable access the debug function	Attack: Forced browsing attack <ol style="list-style-type: none"> 1) Navigate to <code>/bodgeit/basket.jsp</code>. Append <code>?debug=true</code> to the url to create <code>/bodgeit/basket.jsp?debug=true</code> 2) Create an exception by using Firebug (or any browser add-on to tamper data) to change the value of the <code>"quantity"</code> parameter from a numerical value to an alphabetic value such as <code>"a"</code>. 3) Upon updating the basket, the response will include diagnostic data for the exception that was created. 	* included below table
(C6) Cross-Site Scripting (XSS)	Attack: XSS attack <ol style="list-style-type: none"> 1) Navigate to <code>/bodgeit/search.jsp</code> 2) Inject <code><script>alert("XSS")</script></code> into the textbox and press the "search" button 3) A popup will be generated with the text "XSS" 	* included below table
(C7) Cross-Site Scripting (XSS)	Attack: XSS attack <ol style="list-style-type: none"> 1) Navigate to <code>/bodgeit/register.jsp</code> and enter <code>john@doe.com<script>alert("XSS")</script></code> into the form. Press <code>submit</code>. 2) Since the email is displayed at the top-right corner of the page once you are logged in, the XSS script will also be run and so a popup with the text "XSS" appears 	* included below table

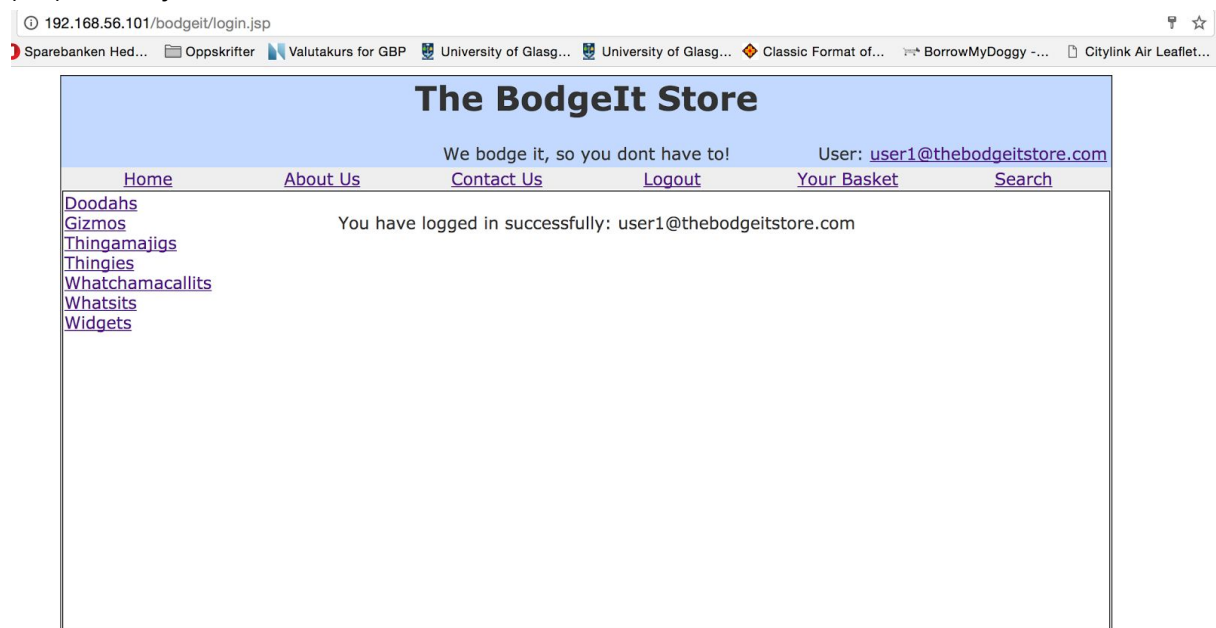
(C9) Broken Authentication	<p>Attack: Cookie manipulation</p> <ol style="list-style-type: none"> 1) As a guest user, add an item to your basket in order to generate the <i>b_id</i> cookie. 2) Upon viewing the admin.jsp panel, you can see the <i>b_id</i>'s of other users. Edit your new <i>b_id</i> cookie and change the value from the current value to 1. 3) Go to your basket and update the basket then refresh the page. You will now be viewing the test user's basket 	* included below table
(C12) Injection	<p>Attack: URL string injection</p> <ol style="list-style-type: none"> 1) Login as any user. I used user: <i>test@thebodgeitstore.com</i> and pass: <i>password</i> 2) Navigate to the password-changing page by clicking on the user's email at the top-right corner of the page. Enter a password. 3) Inspect the form element and find the following line: <i><form method="POST"></i> 4) Change "POST" to "GET" and click the "Submit" button 	* included below table
Cross Site Request Forgery	<ol style="list-style-type: none"> 1) Grab the GET request for password, e.g <i>http://0.0.0.0/bodgeit/password.jsp?password1=qwerty&password2=qwerty</i> 2) Execute CSRF by submitting the following as feedback in the contact form: <i></i> 3) When the Admin checks the comments in the contact.jsp, the "src" parameter value sends a request to change the admin password 	* included below table* included below table

Screenshots:

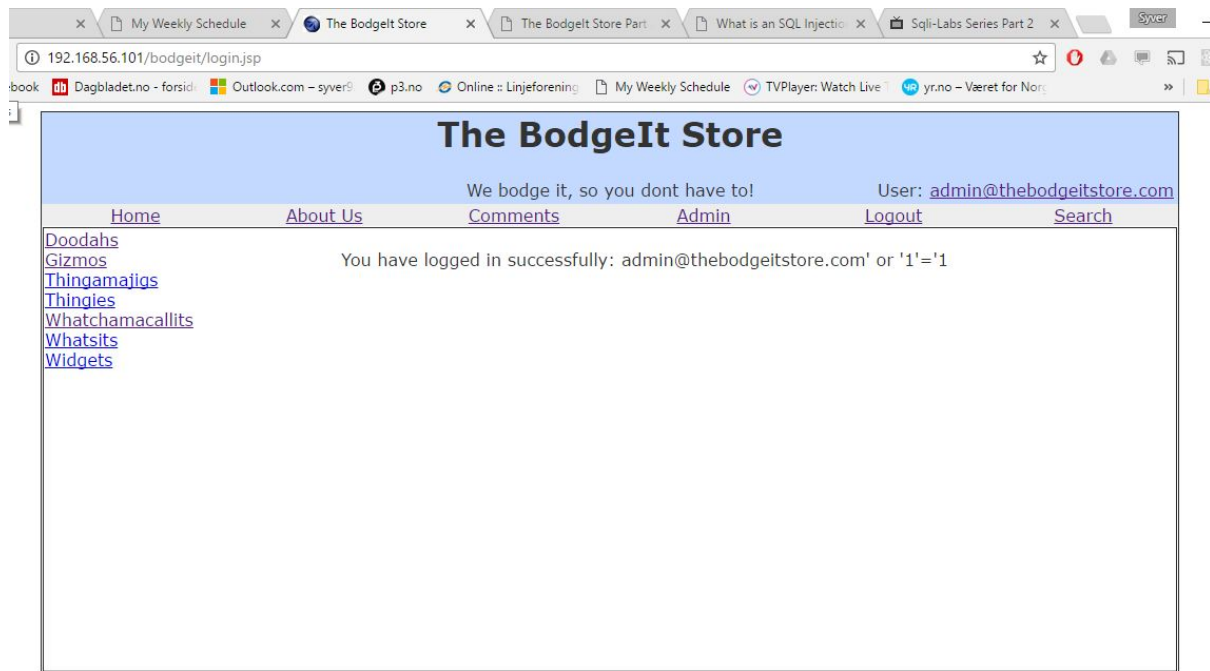
(C1) Insecure authentication



(C2) SQL Injection



(C3) SQL Injection



(C4) Insecure Direct Object References

```

view-source:http://192.168.171.129/bodgeit/
9
10
11 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2//EN">
12 <html>
13 <head>
14 <title>The BodgeIt Store</title>
15 <link href="style.css" rel="stylesheet" type="text/css" />
16 <script type="text/javascript" src="./js/util.js"></script>
17 </head>
18 <body>
19
20 <center>
21 <table width="80%" class="border">
22 <tr BGCOLOR=#C3D9FF>
23 <td align="center" colspan="6">
24 <h1>The BodgeIt Store</h1>
25 <table width="100%" class="noborder">
26 <tr BGCOLOR=#C3D9FF>
27 <td align="center" width="30%">&nbsp;</td>
28 <td align="center" width="40%">We bodge it, so you dont have to!</td>
29 <td align="center" width="30%" style="text-align: right" >
30 Guest user
31
32 </tr>
33 </table>
34 </td>
35 </tr>
36 <tr>
37 <td align="center" width="16%" BGCOLOR=#EEEEEE><a href="home.jsp">Home</a></td>
38 <td align="center" width="16%" BGCOLOR=#EEEEEE><a href="about.jsp">About Us</a></td>
39
40 <td align="center" width="16%" BGCOLOR=#EEEEEE><a href="contact.jsp">Contact Us</a></td>
41 <!-- td align="center" width="16%"><a href="admin.jsp">Admin</a></td-->
42
43 <td align="center" width="16%" BGCOLOR=#EEEEEE>
44
45 <a href="login.jsp">Login</a>
46
47 </td>
48
49 <td align="center" width="16%" BGCOLOR=#EEEEEE><a href="basket.jsp">Your Basket</a></td>
50
51 <td align="center" width="16%" BGCOLOR=#EEEEEE><a href="search.jsp">Search</a></td>
52 </tr>

```

http://192.168.171.129/bodgeit/admin.jsp

The Bodgeit Store

We bodge it, so you dont have to!

Guest user

Home
About Us
Contact Us
Login
Your Basket
Search

Admin page

[Doodahs](#)

[Glzmos](#)

[Thingamajigs](#)

[Thingies](#)

[Whatchamacallits](#)

[Whatsits](#)

[Widgets](#)

Userid	User	Role	Basketid
1	user1@thebodgeitstore.com	USER	0
2	admin@thebodgeitstore.com	ADMIN	0
3	test@thebodgeitstore.com	USER	1

Basketid	Userid	Date
1	3	2017-02-08 23:54:58.774

Basketid	Productid	Quantity
1	1	1
1	3	2
1	5	3
1	7	4

(C5) Missing Function Level Access Control

192.168.56.101/bodgeit/basket.jsp?debug=true

Apps Facebook Dagbladet.no - forsid Outlook.com - syver9 p3.no My Weekly Schedule Online ::

HTTP Status 500 -

type Exception report

message

description The server encountered an internal error () that prevented it from fulfilling this request.

exception

```
org.apache.jasper.JasperException: java.lang.NumberFormatException: For input string: "a"
    org.apache.jasper.servlet.JspServletWrapper.handleJspException(JspServletWrapper.java:491)
    org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:419)
    org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:313)
    org.apache.jasper.servlet.JspServlet.service(JspServlet.java:260)
    javax.servlet.http.HttpServlet.service(HttpServlet.java:717)
```

root cause

```
java.lang.NumberFormatException: For input string: "a"
    java.lang.NumberFormatException.forInputString(NumberFormatException.java:65)
    java.lang.Integer.parseInt(Integer.java:481)
    java.lang.Integer.parseInt(Integer.java:514)
    org.apache.jsp.basket_jsp._jspService(basket_jsp.java:321)
    org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
    javax.servlet.http.HttpServlet.service(HttpServlet.java:717)
    org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:377)
    org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:313)
    org.apache.jasper.servlet.JspServlet.service(JspServlet.java:260)
    javax.servlet.http.HttpServlet.service(HttpServlet.java:717)
```

note The full stack trace of the root cause is available in the Apache Tomcat/6.0.24 logs.

Apache Tomcat/6.0.24

(C6) Cross-Site Scripting (XSS)

Search

Search for >alert("XSS")</script>

[Advanced Search](#)

Search

You searched for:

XSS

(C7) Cross-Site Scripting (XSS)

The BodgeIt Store

We bodge it, so you dont have to!

[About Us](#)

[Contact Us](#)

[Login](#)

[Your Basket](#)

Register

A user with this name already exists.

Please enter the following details to register with us:

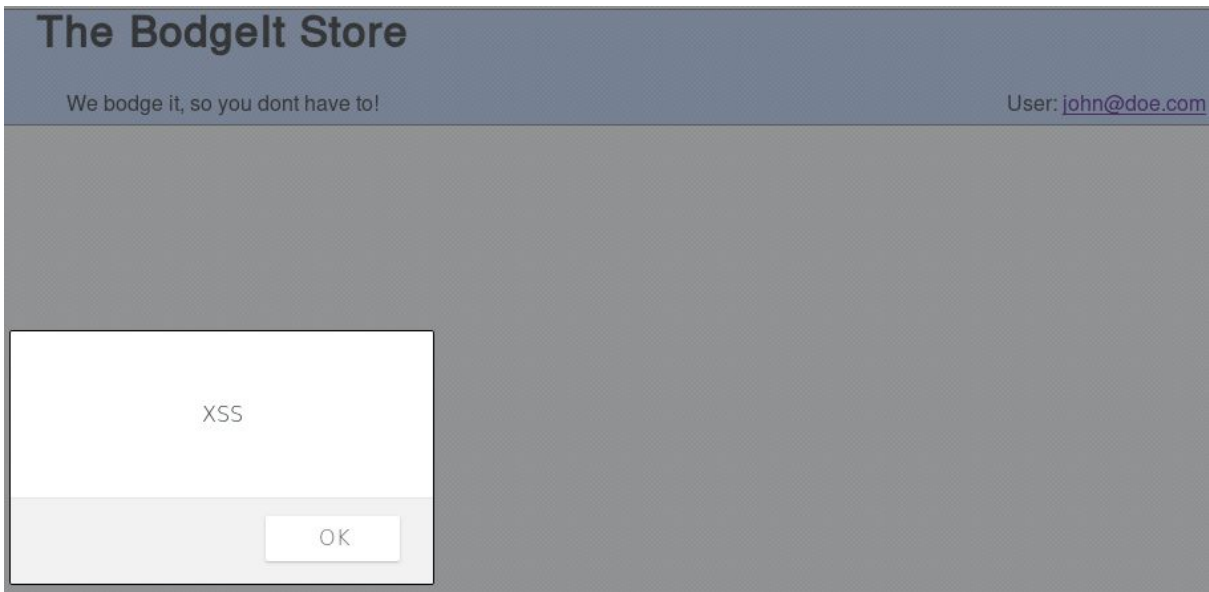
Username (your email address): john@doe.com<script>a

Password:

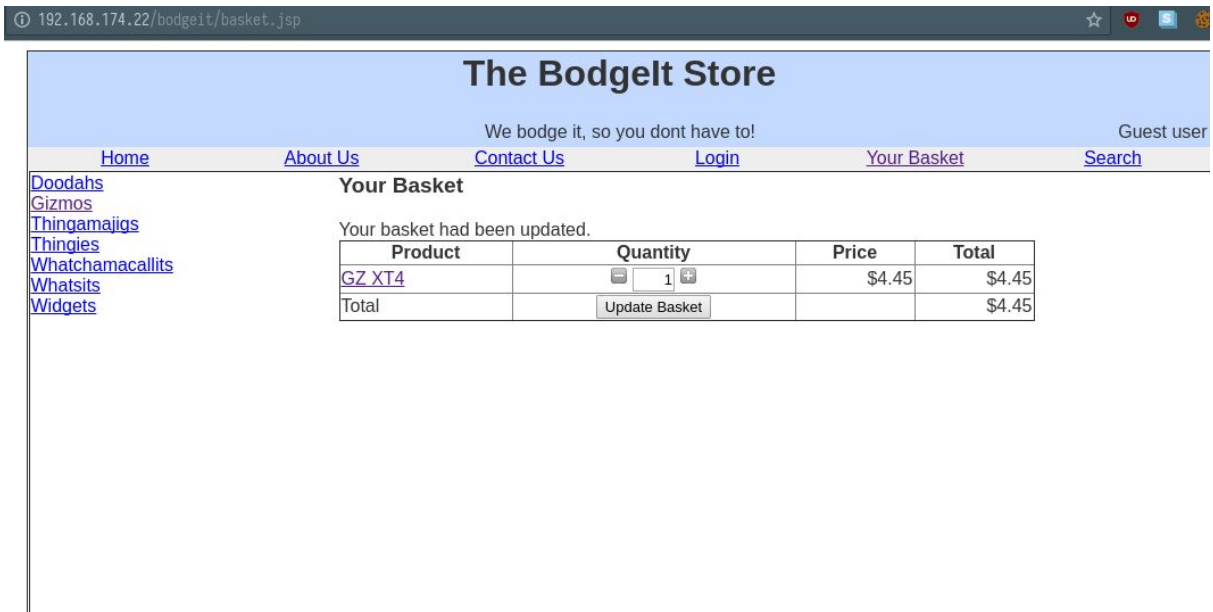
••••••••

Confirm Password:

••••••••



(C9) Broken Authentication



[Doodahs](#)
[Gizmos](#)
[Thingamajigs](#)
[Thingies](#)
[Whatchamacallits](#)
[Whatsits](#)
[Widgets](#)

Your Basket

Your basket had been updated.

Product	Quantity	Price	Total
Basic Widget	<input type="text" value="1"/>	\$1.10	\$1.10
Weird Widget	<input type="text" value="2"/>	\$2.10	\$4.20
Thingie 2	<input type="text" value="3"/>	\$1.50	\$4.50
Thingie 4	<input type="text" value="4"/>	\$0.95	\$3.80
Total	<input type="button" value="Update Basket"/>		\$13.60

(C12) Injection

```
Inspect... Console Debugger {} Style
+
<table class="border" width="100%">
  <tbody>
    <tr>
      <td width="25%" valign="top" align="center">
        <td width="70%" valign="top">
          <h3>Your profile</h3>
          Change your password:
          <br>
          <br>
          <form method="GET">
            <center></center>
          </form>
        </td>
```

192.168.56.101/bodgeit/password.jsp?password1=hi123&password2=hi123

Cross Site Request Forgery

We bodge it, so you dont have to!				Gu
Us	Contact Us	Login	Your Basket	Search

Contact Us

Please send us your feedback:

Submit

We bodge it, so you dont have to!		User: admin@thebodgeitstore	
Comments	Admin	Logout	Search

User	Comment
null	window.alert(Playyy);
null	alert(XSS)
test@thebodgeitstore.com	alert(XSS)
null	
null	