Check Point Report

Vulnerable Application: BodgeIt

Team Name: AA Team

Kevin Wu 0808148w

Claudia Ortiz-Duron  2412650o

Laimonas Samalius 244831s

Sultan Altwijri 2312914a

Ali Rashed A Al Qarni 2286368a

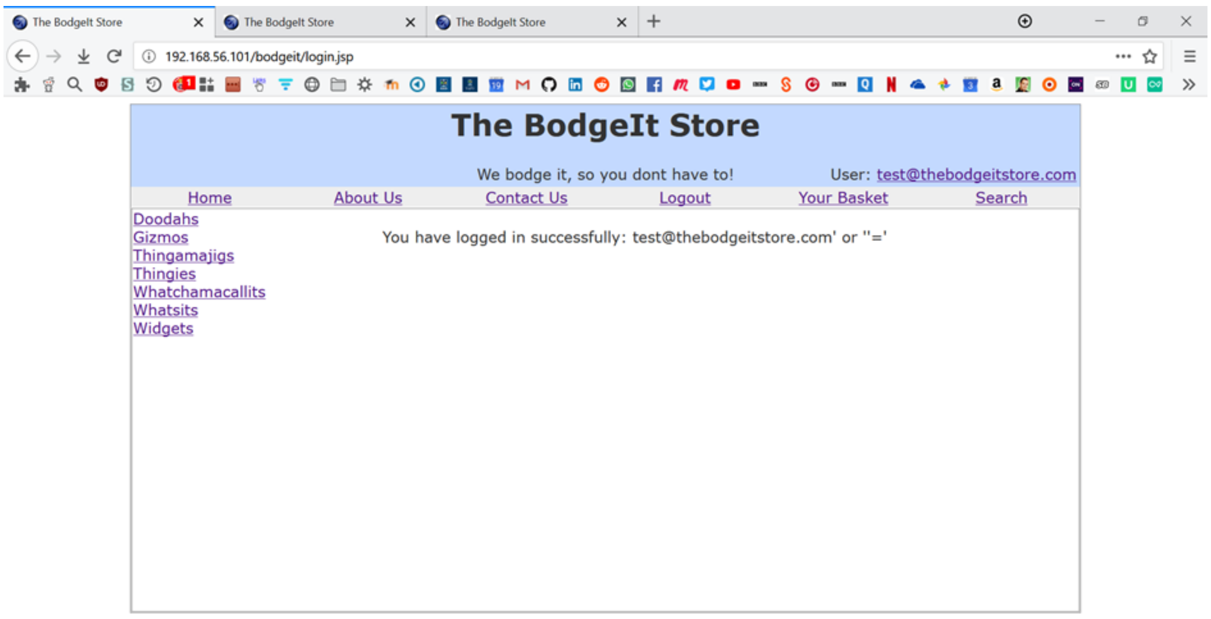
| Vulnerability | Type of Vulnerability | Details of the Attack | Screenshot |
|---|---|---|---|
| Login as test@thebodgeitstore.com | SQL Injection (Injection flaw) | Login using test@thebodgeitstore.com' or ''=' was entered in username field | Figure 1 |
| Login as user1@thebodgeitstore.com | SQL Injection (Injection flaw) | ' or ''=' was entered in both id and password to log on | Figure 2 |
| Login as admin@thebodgeitstore.com | SQL Injection (Injection flaw) | Login using admin@thebodgeitstore.com' or ''=' was entered in username field | Figure 3 |
| Find hidden content as a non admin user | Broken Access Control/Failure to restrict URL Access | Exploring URL links is noticeable that they have similar pattern: http://192.168.56.101/bodgeit/home.jsp;http://192.168.56.101/bodgeit/about.jsp;http://192.168.56.101/bodgeit/contact.jsp We try to check if Admin page uses the same address pattern. Entering http://192.168.56.3/bodgeit/admin.jsp lets us access unprotected Admin page with hidden information for non admin user. | Figure 4 |

| | | | |
|---|---|---|---|
| Find diagnostic data | Security Misconfiguration / Leftover Debug Code | Check on the web site all links by adding at the end of their URL addresses this code ?debug=true. If any debugging data was left by the developer, then the webpage will render it. In this case “DEBUG basketid = 2". | Figure 5 |
| Level 1: Display a popup using: <script>alert("XSS")</script> | Cross Site Scriptin | Go to Search page, enter following code into form field “<script>alert("XSS")</script>” and pop up appeared | Figure 6 |
| Level 2: Display a popup using: <script>alert("XSS")</script> | Cross-Site Scripting | Register a new account and entering aateam@legacy.com<script>alert(“XSS”)</script> in the username box | Figure 7 |
| Level 3: Display a popup using: <script>alert("XSS")</script> | Cross-Site Scripting | Login with aateam@legacy.com<script>alert’ or ‘’=’<script>(“XSS”)</script> in the username. | Figure 8 |
| Access someone else’s basket | Broken Authentication | Log in as an Admin and from Admin page check how basket ID’s are assigned. Then we can to try access someone else basket by manipulating cookies.  In this case we amended basked id value in the cookie “b_id:8”  to “b_id:1”. After pressing “Update basket” we have successfully, accessed another user’s basket. “b_id:1” | Figure 9 |
| Force someone to add an item to their basket when they visit your webpage. | Cross-Site Request Forgery | Notice that items are added to the basket by a post method. If the attacker views the network data, they can inspect the post request traffic. By | Figure 12 |

| | | | |
|---|---|---|---|
| | | clicking on the ‘edit and resent’ tab, the hacker can view the request body. This can then be added at the end of the link, e.g. http://192.168.56.101/bodgeit/basket.jsp?productid=8&price=3.7&quantity=1, which will send a query string to the server for this item to be added to the basket. An attacker might replace a normal link, such as the home link, with the query string link (by inspecting the link element and replacing the ahref attribute to this link). A victim can click the link unaware that they’ve been attacked | |
| Get the store to owe you money | Broken Access Control / Input validation. | Add purchase item to basket and update basket content. Next, explore the basket web page code trying to find the block for any relevant code related to the quantity of purchased items. After locating this, the value of number of items in basket can be changed to a negative number. Clicking update basket afterwards . The web application processes this as if it was trusted data, making the store owe money to the attacker | Figure 10 |
| Change your password via a GET request | Information exposure through query strings in URL | Click view page source, form submit is set to POST. Inspect one of the password | Figure 11 |

| | | | |
|---|---|---|---|
| | | field, replace FORM with GET – click change password. Notice new password is displayed in url bar | |
| Conquer AES encryption, and display a popup using: <script>alert("H@cked A3S")</script> | | | |
| Conquer AES encryption and append a list of table names to the normal results. | | | |

## Screendumps



192.168.56.101/bodgeit/login.jsp

The BodgeIt Store

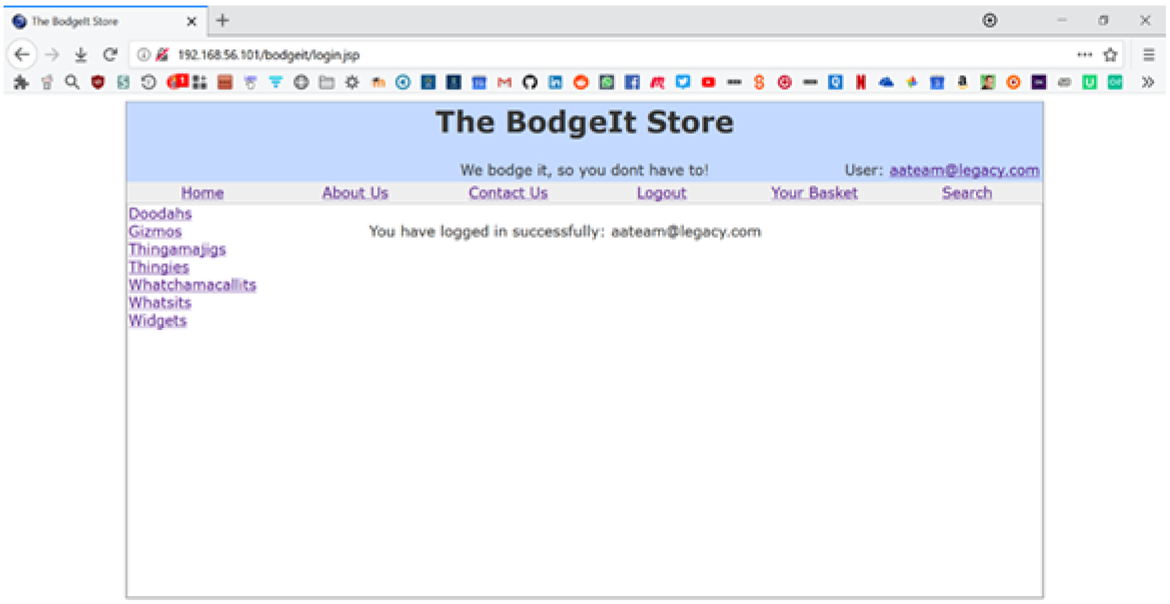
We bodge it, so you dont have to!

User: test@thebodgeitstore.com

Home | About Us | Contact Us | Logout | Your Basket | Search

Doodahs
Gizmos
Thingamajigs
Thingies
Whatchamacallits
Whatsits
Widgets

You have logged in successfully: test@thebodgeitstore.com' or ''='



192.168.56.101/bodgeit/login.jsp

The BodgeIt Store

We bodge it, so you dont have to!

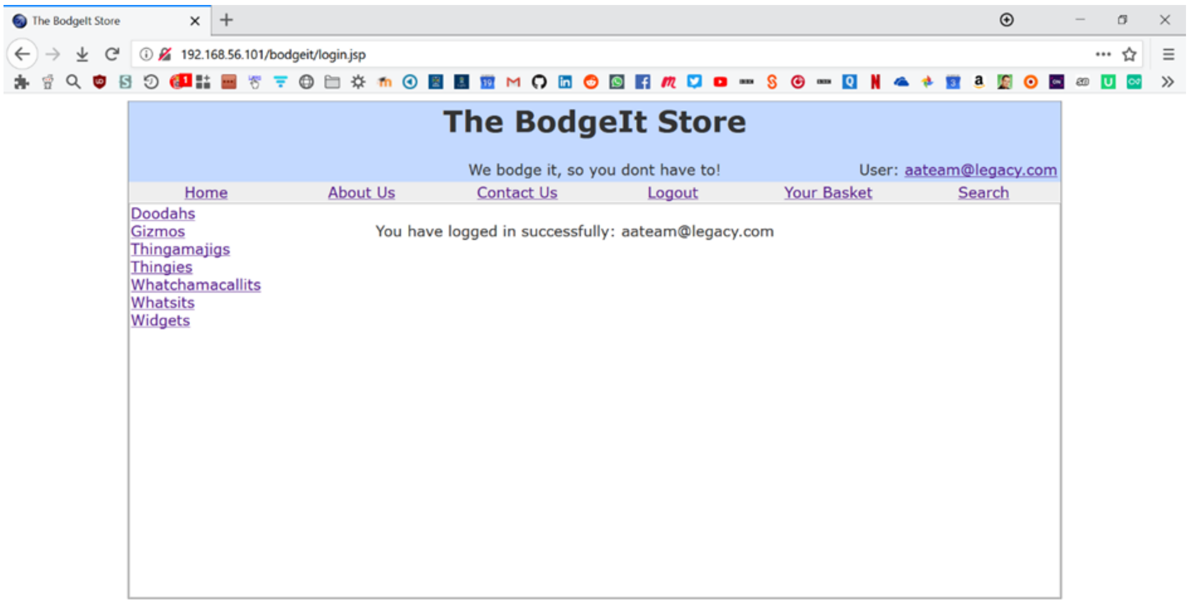
User: aateam@legacy.com

Home | About Us | Contact Us | Logout | Your Basket | Search

Doodahs
Gizmos
Thingamajigs
Thingies
Whatchamacallits
Whatsits
Widgets

You have logged in successfully: aateam@legacy.com

*Figure 1: Login as test@thebodgeitstore.com via a sql query*


The BodgeIt Store

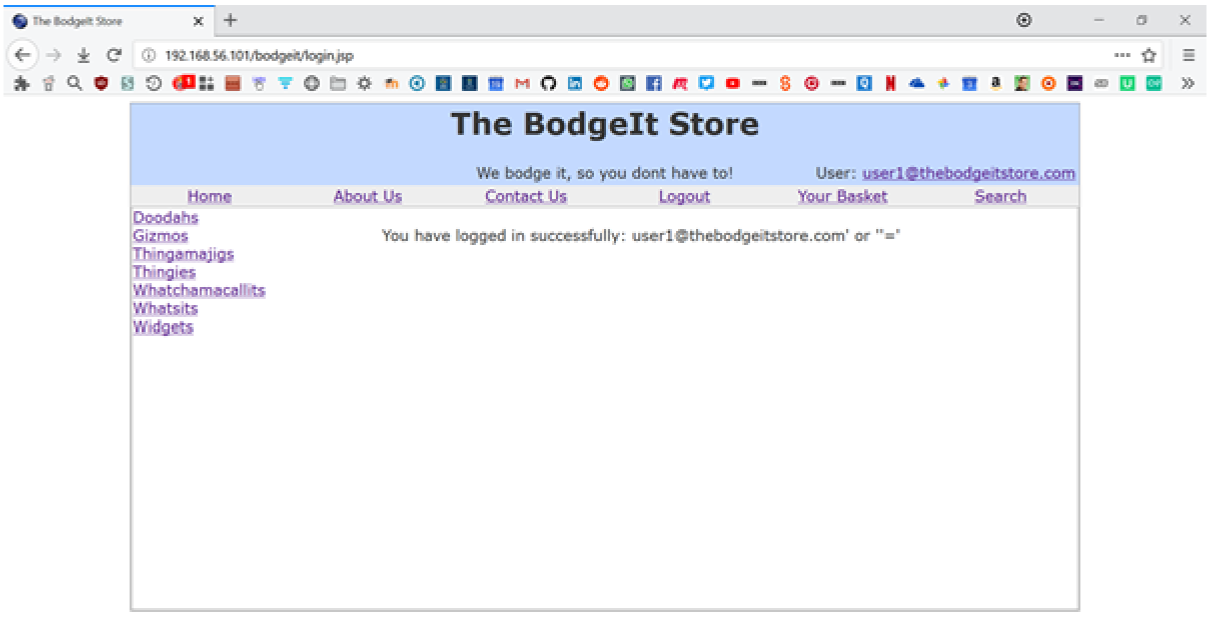
192.168.56.101/bodgeit/login.jsp

We bodge it, so you dont have to! User: aateam@legacy.com

Home About Us Contact Us Logout Your Basket Search

Doodahs
Gizmos
Thingamajigs
Thingies
Whatchamacallits
Whatsits
Widgets

You have logged in successfully: aateam@legacy.com


The BodgeIt Store

192.168.56.101/bodgeit/login.jsp

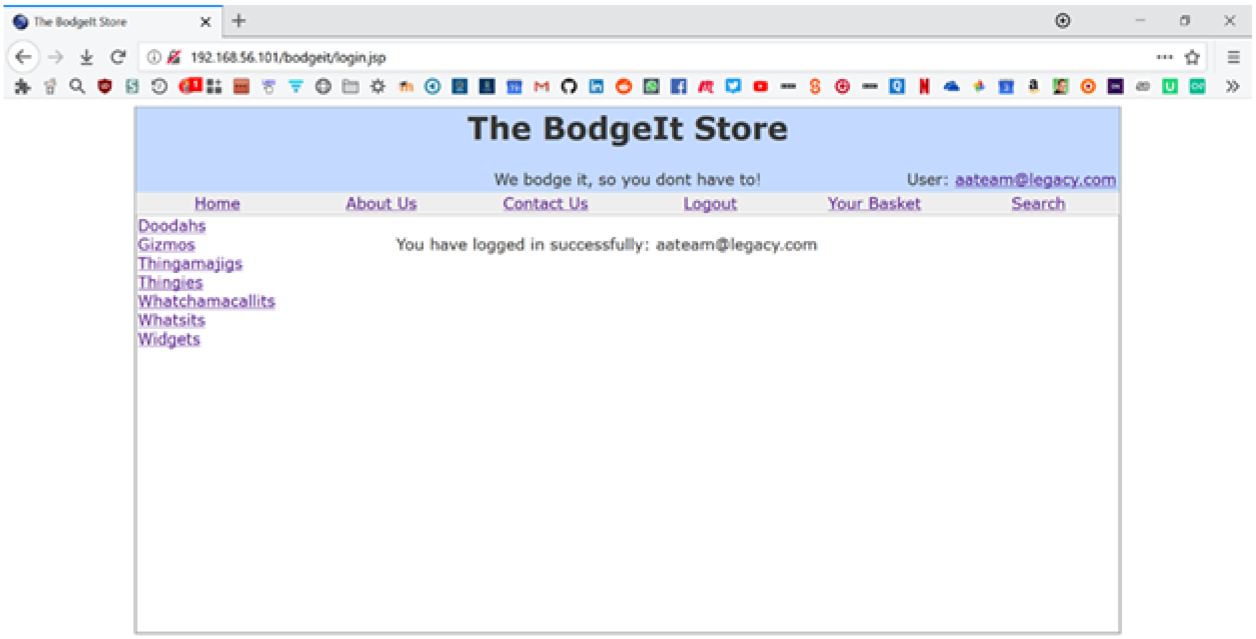
We bodge it, so you dont have to! User: user1@thebodgeitstore.com

Home About Us Contact Us Logout Your Basket Search

Doodahs
Gizmos
Thingamajigs
Thingies
Whatchamacallits
Whatsits
Widgets

You have logged in successfully: user1@thebodgeitstore.com' or ''='

*Figure 2: Login as user1@thebodgeitstore.com via SQL query*

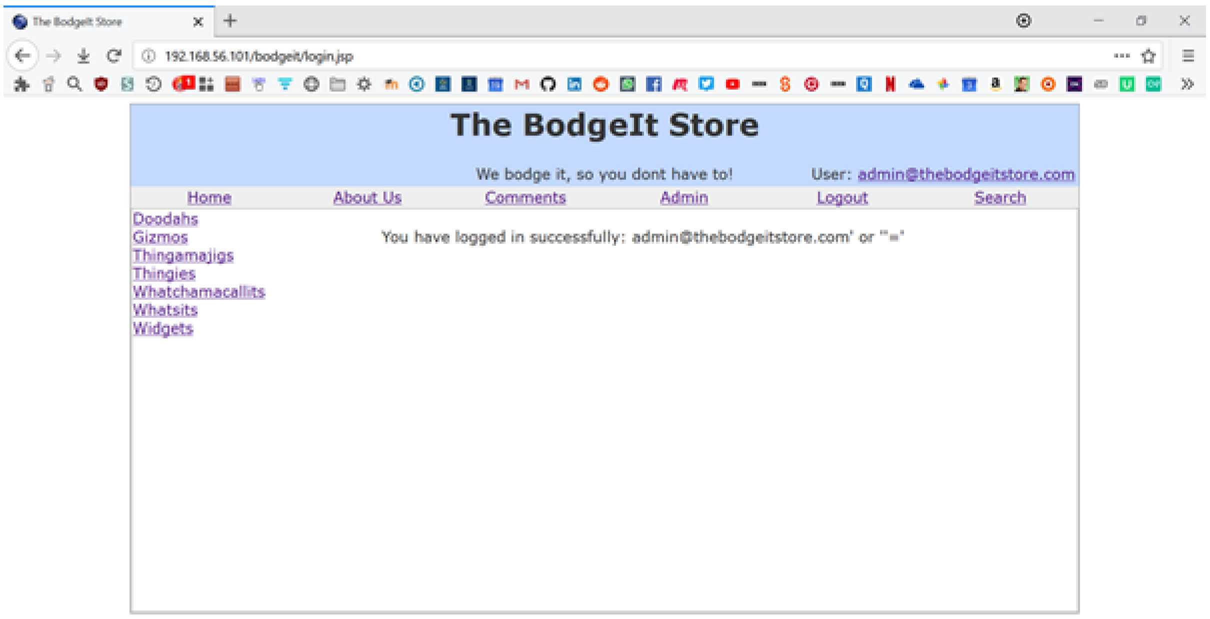


The BodgeIt Store

We bodge it, so you dont have to!

User: aateam@legacy.com

You have logged in successfully: aateam@legacy.com



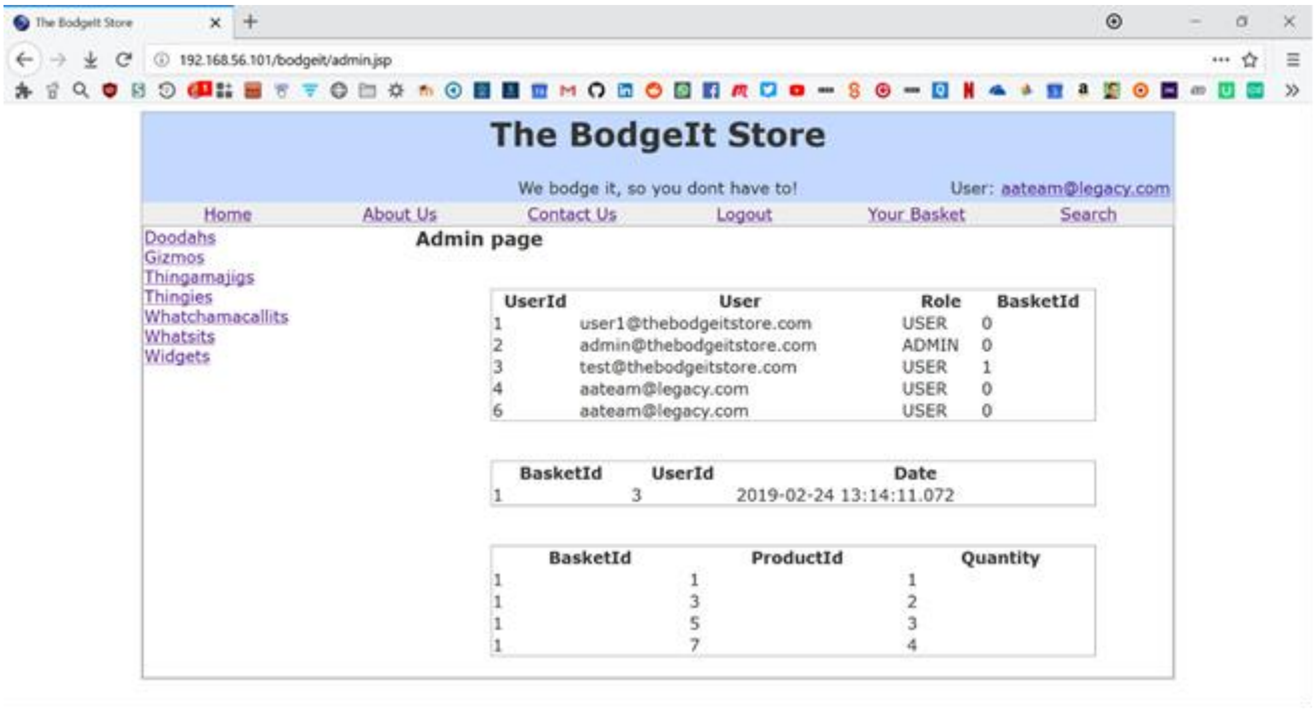
The BodgeIt Store

We bodge it, so you dont have to!

User: admin@thebodgeitstore.com

You have logged in successfully: admin@thebodgeitstore.com' or ''='

*Figure 3: Login as admin@thebodgeitstore.com via a sql injection*



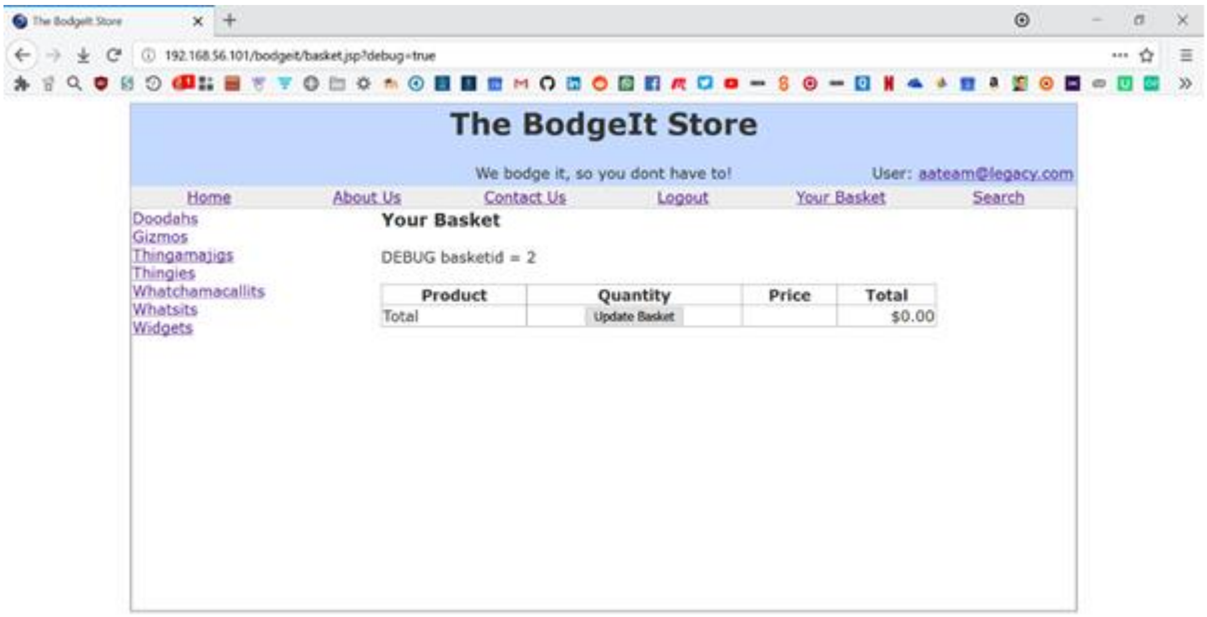
Admin page

| UserId | User | Role | BasketId |
|---|---|---|---|
| 1 | user1@thebodgeitstore.com | USER | 0 |
| 2 | admin@thebodgeitstore.com | ADMIN | 0 |
| 3 | test@thebodgeitstore.com | USER | 1 |
| 4 | aateam@legacy.com | USER | 0 |
| 6 | aateam@legacy.com | USER | 0 |

| BasketId | UserId | Date |
|---|---|---|
| 1 | 3 | 2019-02-24 13:14:11.072 |

| BasketId | ProductId | Quantity |
|---|---|---|
| 1 | 1 | 1 |
| 1 | 3 | 2 |
| 1 | 5 | 3 |
| 1 | 7 | 4 |

*Figure 4: Find hidden content as non-admin user via brute force*


The BodgeIt Store
192.168.56.101/bodgeit/basket.jsp?debug=true
The BodgeIt Store
We bodge it, so you dont have to!
User: aateam@legacy.com
Home About Us Contact Us Logout Your Basket Search
Doodahs
Gizmos
Thingamajigs
Thingies
Whatchamacallits
Whatsits
Widgets

Your Basket

DEBUG basketid = 2

| Product | Quantity | Price | Total |
|---|---|---|---|
| Total | Update Basket | | $0.00 |

*Figure 5: Find diagnostic data*

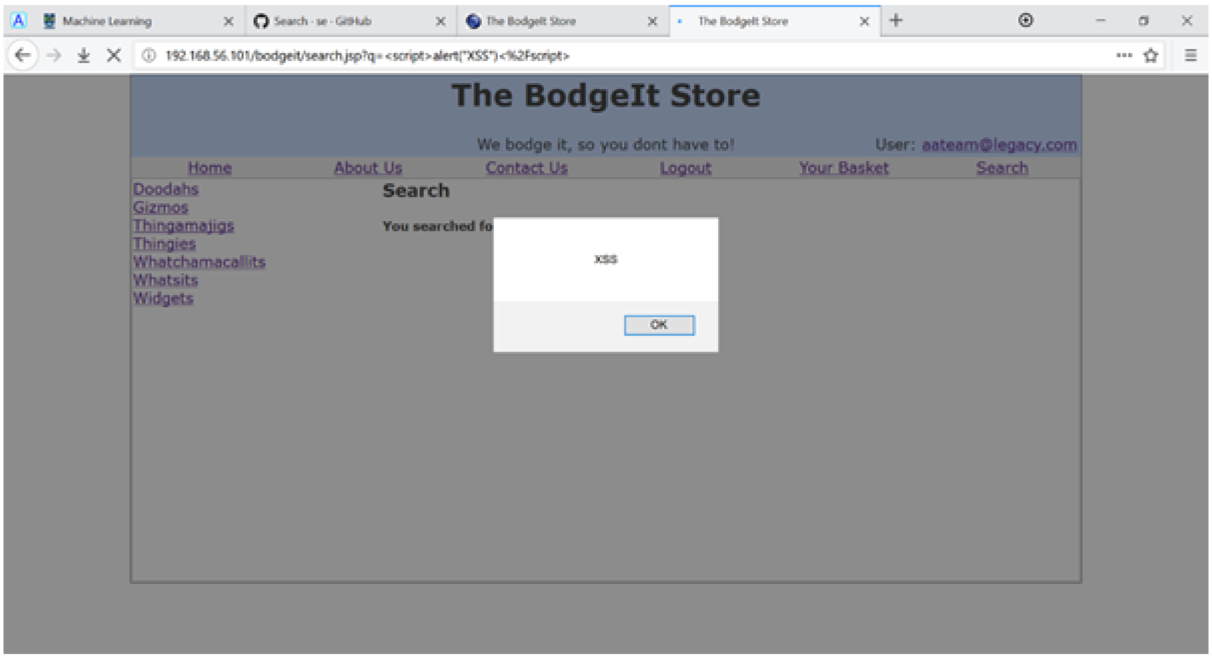


*Figure 6: Level 1: Display a popup using: <script>alert("XSS")</script> via SQL query in search box*

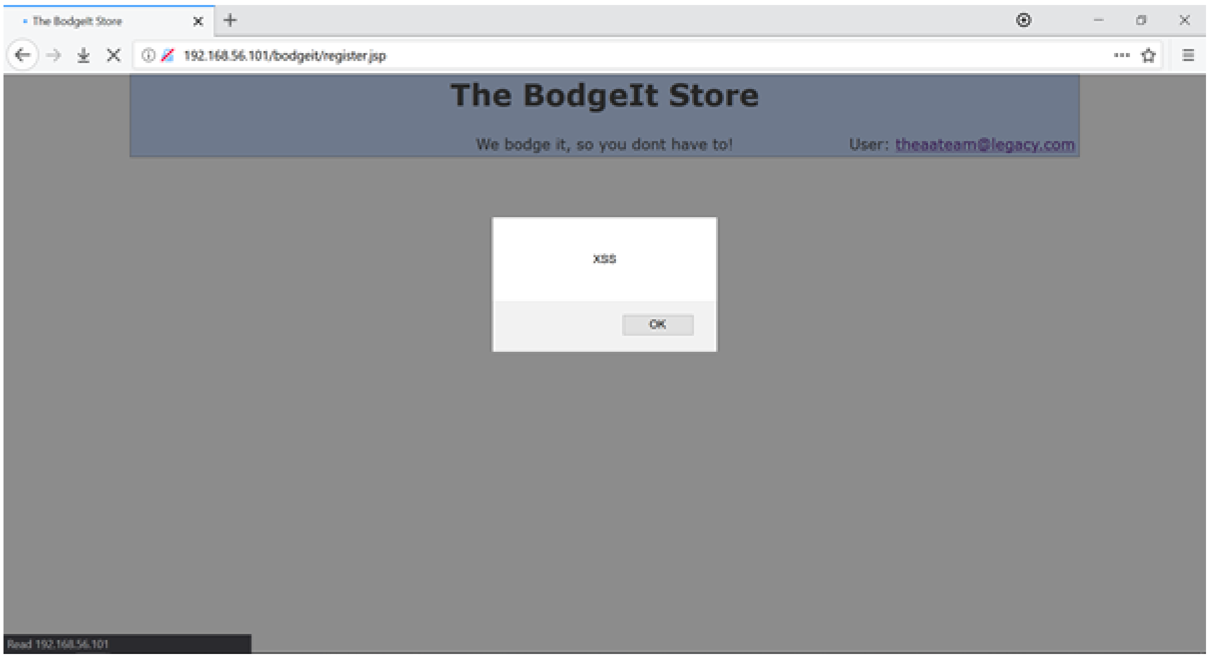
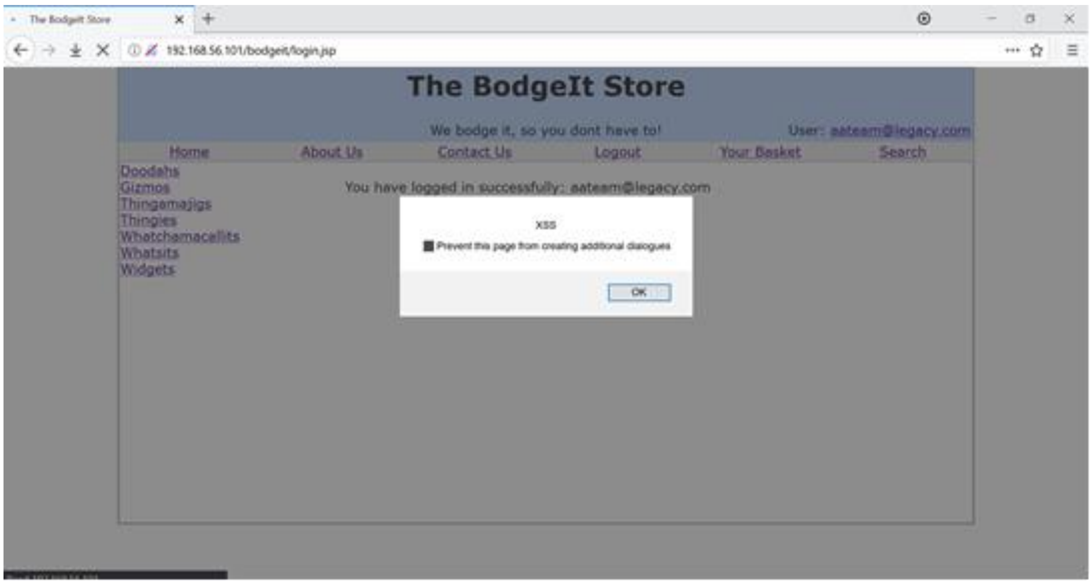

The BodgeIt Store
192.168.56.101/bodgeit/register.jsp
The BodgeIt Store
We bodge it, so you dont have to!
User: theaateam@legacy.com
XSS
OK
Read 192.168.56.101

*Figure 7: Level 2: Display a popup using: <script>alert("XSS")</script> using sql query via register page*


192.168.56.101/bodgeit/login.jsp

The BodgeIt Store

We bodge it, so you dont have to!

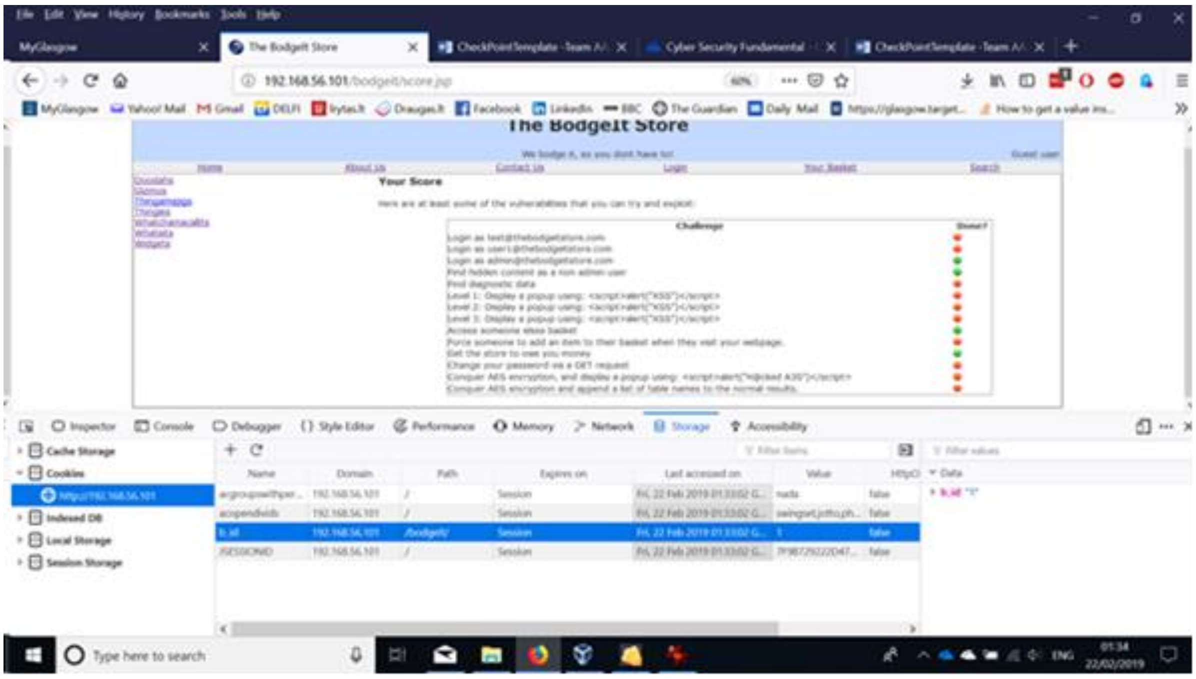
User: aateam@legacy.com

You have logged in successfully: aateam@legacy.com

XSS

Prevent this page from creating additional dialogues

*Figure 8 Level 3: Display a popup using: <script>alert("XSS")</script> Via the log in page*


192.168.56.101/bodgeit/score.jsp

The BodgeIt Store

We bodge it, so you dont have to!

Your Score

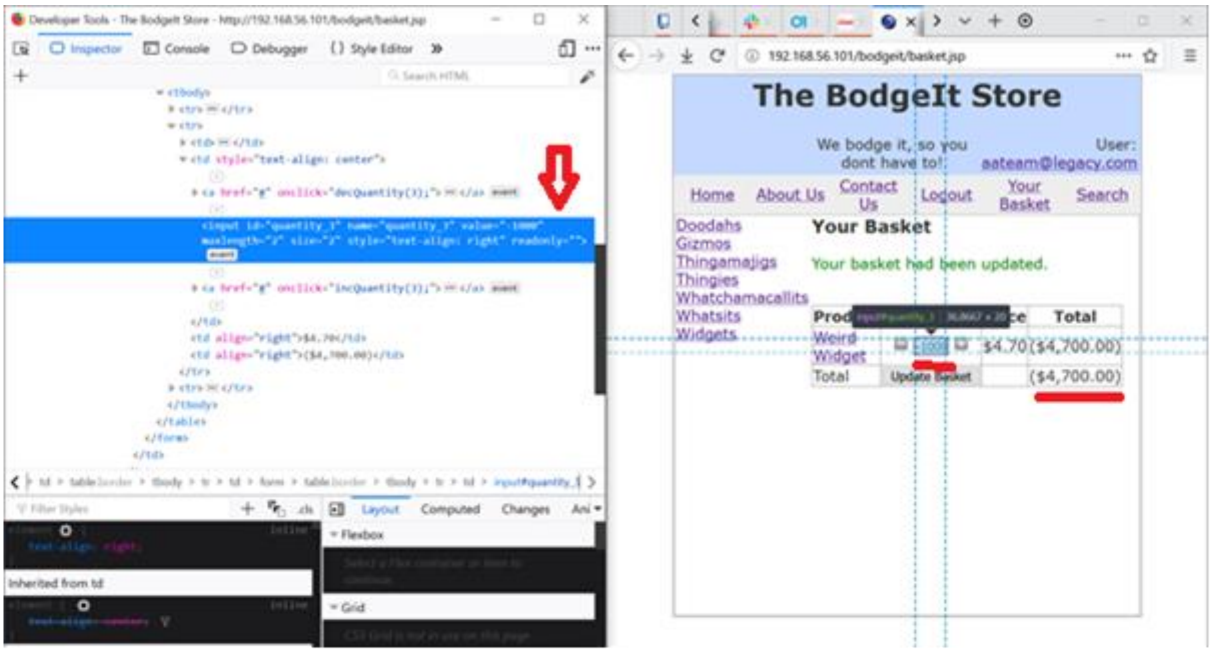
Here are at least some of the vulnerabilities that you can try and exploit:

| Challenge | Done? |
|---|---|
| Login as test@thebodgeitstore.com | 🟥 |
| Login as user1@thebodgeitstore.com | 🟥 |
| Login as admin@thebodgeitstore.com | 🟩 |
| Find hidden content as a non admin user | 🟩 |
| Find diagnostic data | 🟥 |
| Level 1: Display a popup using: <script>alert("XSS")</script> | 🟥 |
| Level 2: Display a popup using: <script>alert("XSS")</script> | 🟥 |
| Level 3: Display a popup using: <script>alert("XSS")</script> | 🟥 |
| Access someone elses basket | 🟩 |
| Force someone to add an item to their basket when they visit your webpage. | 🟥 |
| Get the store to owe you money | 🟩 |
| Change your password via a GET request | 🟥 |
| Conquer AES encryption, and display a popup using: <script>alert("H@cked A3S")</script> | 🟥 |
| Conquer AES encryption and append a list of table names to the normal results. | 🟥 |

| Name | Domain | Path | Expires on | Last accessed on | Value | HttpOnly |
|---|---|---|---|---|---|---|
| acgroupswithper... | 192.168.56.101 | / | Session | Fri, 22 Feb 2019 01:33:02 G... | nada | false |
| acopendivids | 192.168.56.101 | / | Session | Fri, 22 Feb 2019 01:33:02 G... | swingset,jotto,ph... | false |
| b_id | 192.168.56.101 | /bodgeit/ | Session | Fri, 22 Feb 2019 01:33:02 G... | 1 | false |
| JSESSIONID | 192.168.56.101 | / | Session | Fri, 22 Feb 2019 01:33:02 G... | 7F9877922D47... | false |

b_id: "1"

*Figure 9 Access someone else's basket by exploiting poor session management control*


Developer Tools - The BodgeIt Store - http://192.168.56.101/bodgeit/basket.jsp

```
▾ <tbody>
  ▸ <tr> ⋯ </tr>
  ▾ <tr>
    ▸ <td> ⋯ </td>
    ▾ <td style="text-align: center">
      ▸ <a href="#" onclick="decQuantity(3);"> ⋯ </a> event
        <input id="quantity_3" name="quantity_3" value="-1000"
        maxlength="2" size="2" style="text-align: right" readonly=""> event
      ▸ <a href="#" onclick="incQuantity(3);"> ⋯ </a> event
      </td>
      <td align="right">$4.70</td>
      <td align="right">($4,700.00)</td>
    </tr>
  ▸ <tr> ⋯ </tr>
  </tbody>
</table>
</form>
</td>
```

192.168.56.101/bodgeit/basket.jsp

The BodgeIt Store

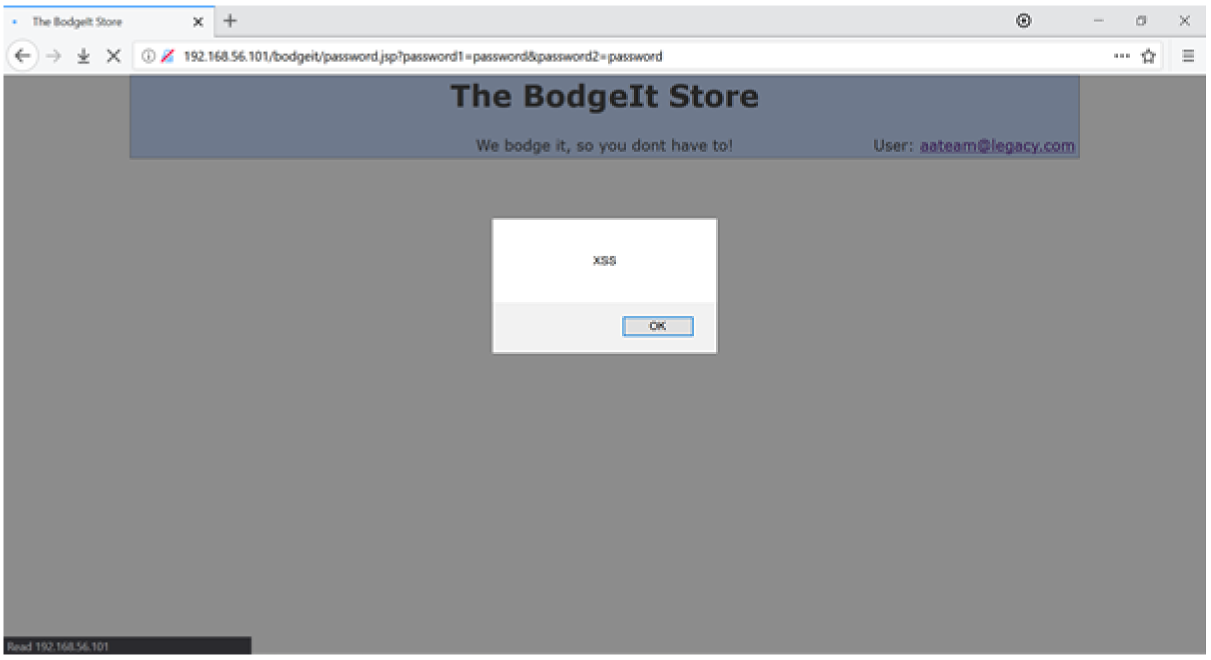
We bodge it, so you dont have to! User: aateam@legacy.com

Your Basket

Your basket had been updated.

| Product | Quantity | Price | Total |
|---|---|---|---|
| Weird Widget | -1000 | $4.70 | ($4,700.00) |
| Total | Update Basket | | ($4,700.00) |

*Figure 10 Get the store to owe you money by altering web page code*

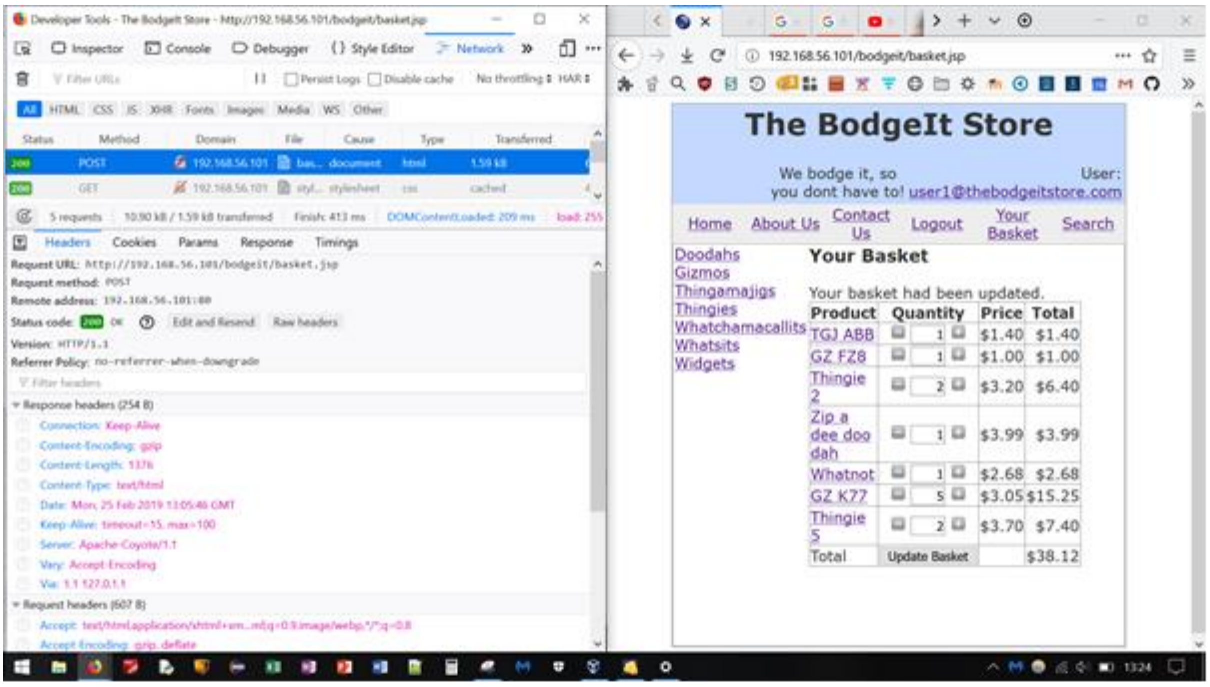

192.168.56.101/bodgeit/password.jsp?password1=password&password2=password

The BodgeIt Store

We bodge it, so you dont have to! User: aateam@legacy.com

XSS

*Figure 11 Changing your password via a GET request – new password ("password") is encoded in URL bar*



```
Developer Tools - The BodgeIt Store - http://192.168.56.101/bodgeit/basket.jsp

Status  Method  Domain          File  Cause     Type        Transferred
200     POST    192.168.56.101  bas…  document  html        1.59 kB
200     GET     192.168.56.101  styl… stylesheet css        cached

5 requests   10.90 kB / 1.59 kB transferred   Finish: 413 ms   DOMContentLoaded: 209 ms   load: 255

Request URL: http://192.168.56.101/bodgeit/basket.jsp
Request method: POST
Remote address: 192.168.56.101:80
Status code: 200 OK
Version: HTTP/1.1
Referrer Policy: no-referrer-when-downgrade

▾ Response headers (254 B)
  Connection: Keep-Alive
  Content-Encoding: gzip
  Content-Length: 1376
  Content-Type: text/html
  Date: Mon, 25 Feb 2019 13:05:46 GMT
  Keep-Alive: timeout=15, max=100
  Server: Apache-Coyote/1.1
  Vary: Accept-Encoding
  Via: 1.1 127.0.1.1
▾ Request headers (607 B)
  Accept: text/html,application/xhtml+xm…ml;q=0.9,image/webp,*/*;q=0.8
  Accept-Encoding: gzip, deflate
```

192.168.56.101/bodgeit/basket.jsp

The BodgeIt Store

We bodge it, so you dont have to! User: user1@thebodgeitstore.com

Home | About Us | Contact Us | Logout | Your Basket | Search

Doodahs
Gizmos
Thingamajigs
Thingies
Whatchamacallits
Whatsits
Widgets

Your Basket

Your basket had been updated.

| Product | Quantity | Price | Total |
|---|---|---|---|
| TGJ ABB | 1 | $1.40 | $1.40 |
| GZ FZ8 | 1 | $1.00 | $1.00 |
| Thingie 2 | 2 | $3.20 | $6.40 |
| Zip a dee doo dah | 1 | $3.99 | $3.99 |
| Whatnot | 1 | $2.68 | $2.68 |
| GZ K77 | 5 | $3.05 | $15.25 |
| Thingie 5 | 2 | $3.70 | $7.40 |
| Total | Update Basket | | $38.12 |

*Figure 12 Force someone to add an item to their basket when they visit your webpage.*