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 evidence
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) ~~SQL Injection~~	' or "=' was entered in both id and password to log on	Figure 2
Login as admin@thebodgeitstore.com	SQL Injection (Injection flaw) ~~SQL Injection~~	Login using admin@thebodgeitstore.com' or "=' was entered in username field	Figure 3
Find hidden content as a non admin user	~~Security Misconfiguration~~ 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;	Figure 4

Formatted: Heading 2

Formatted: Font: (Default) Times New Roman, 12 pt, Spanish (Spain)

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Space After: 8 pt, Line spacing: Multiple 1.08 li

Formatted: Font: (Default) Times New Roman, 12 pt, Spanish (Spain)

Formatted: Space After: 8 pt, Line spacing: Multiple 1.08 li

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt, Spanish (Spain)

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt, Spanish (Spain)

Formatted: Justified, Space After: 8 pt, Line spacing: Multiple 1.08 li

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font color: Background 1

Formatted: Centered

Formatted Table

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) time, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) time, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt

		~~So 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. 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.~~	
Find diagnostic data	~~Security Misconfiguration~~Security Misconfiguration / Leftover Debug Code~~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.
		~~there debugged appear on page "Your Basket" which is "DEBUG basketid = 4" (ALI)~~	~~Figure 5.1~~
Level 1: Display a popup using: <script>alert("XSS") </script>	Cross-Site Scripting	~~Went~~ Go to Search page, ~~Copy and pasted~~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")	Cross-Site Scripting	Register a new account and entering aateam@legacy.com	Figure 7.

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt, Underline, Font color: Auto

Formatted: Font: (Default) Times New Roman, 12 pt, Font color: Auto

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt, Underline

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, Font color: Auto

Formatted: Font: (Default) Times New Roman, Font color: Auto

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted Table

Formatted: Font: (Default) Times New Roman, 12 pt

</script>		<script>alert(“XSS”) </script> in the username box~~Register a new account entering aateam@legacy.com <script>alert(“XSS”) </script> in the username.~~	
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	~~s~~ Broken Auth~~ee~~ntication	~~Log in as admin admin page check asd basket ID~~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~~d~~ by manipulating cookies. In this case we amended basked id value in the cookie “b_id~~“b_id~~:8” to “b_id:1”. After pressing “Update basket” we have successfully, accessed another user’s ~~can access~~ basket. “b_id:1” ~~content.~~	Figure 9
Force someone to add an item to their basket when they visit your webpage.	~~Looking for this one~~Cross-Site Request Forgery ~~Broken Access Control~~	~~Are you ok, Alexa. Dids you see Kevs link ? Ah?~~ ~~😲, the final report? Yes At the end of this table! yes, the final report yep~~ Notice that items are added to the basket	~~10~~Figure 12

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt

Field Code Changed

Formatted: Font: (Default) Times New Roman, 12 pt, Font color: Auto

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Space After: 10 pt, Line spacing: Multiple 1.15 li

Formatted: Font: (Default) Segoe UI Emoji, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt

		by a post method. If the attacker views the network data, they can inspect the post request traffic. By 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~~n~~ Access Control, ~~Security Misconfiguration~~/ I~~No i~~nput validation.	~~I've attached a screenshot at the end of this page.~~ Add purchase item to basket and update basket content. Next, explore the~~can explore~~ basket web page code trying to find the block for any relevant~~of~~ code related to the quantity of purchased items. After locating this, the value of number of items in basket can be	Figure 10~~1~~

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt, Not Bold, Font color: Auto,

Formatted: Heading 1

Formatted: Font: (Default) Times New Roman, 12 pt,

Formatted: Font: (Default) Times New Roman, 12 pt

		changed~~value we change it~~ to a negative number. C ~~and~~licking update basket afterwards . The web application processes this as if it was trusted data, making the ~~it makes~~ store~~-~~ owe money to the attacker	
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 field, replace FORM with GET – click change password. Notice new password is displayed in url bar	Figure 11
Conquer AES encryption, and display a popup using: <script>alert("H@cked A3S")</script>	~~We do not have to this exercise~~		
Conquer AES encryption and append a list of table names to the normal results.	~~We do not have to this exercise~~		

~~Helping liks:~~

- ~~https://www.synackfin.tech/documents/Final_Report_CS_Fundamentals.pdf~~
- https://www.synackfin.tech/documents/Final_Report_CS_Fundamentals.pdf

Screendumps

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Justified, Space After: 8 pt, Line spacing: Multiple 1.08 li

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt, Font color: Auto

Formatted Table

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: Font: (Default) Times New Roman, 12 pt, Font color: Auto

Formatted: Font: (Default) Times New Roman, 12 pt

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.63 cm + Indent at: 1.27 cm

Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0.63 cm + Indent at: 1.27 cm

Formatted: Font: Bold, Underline

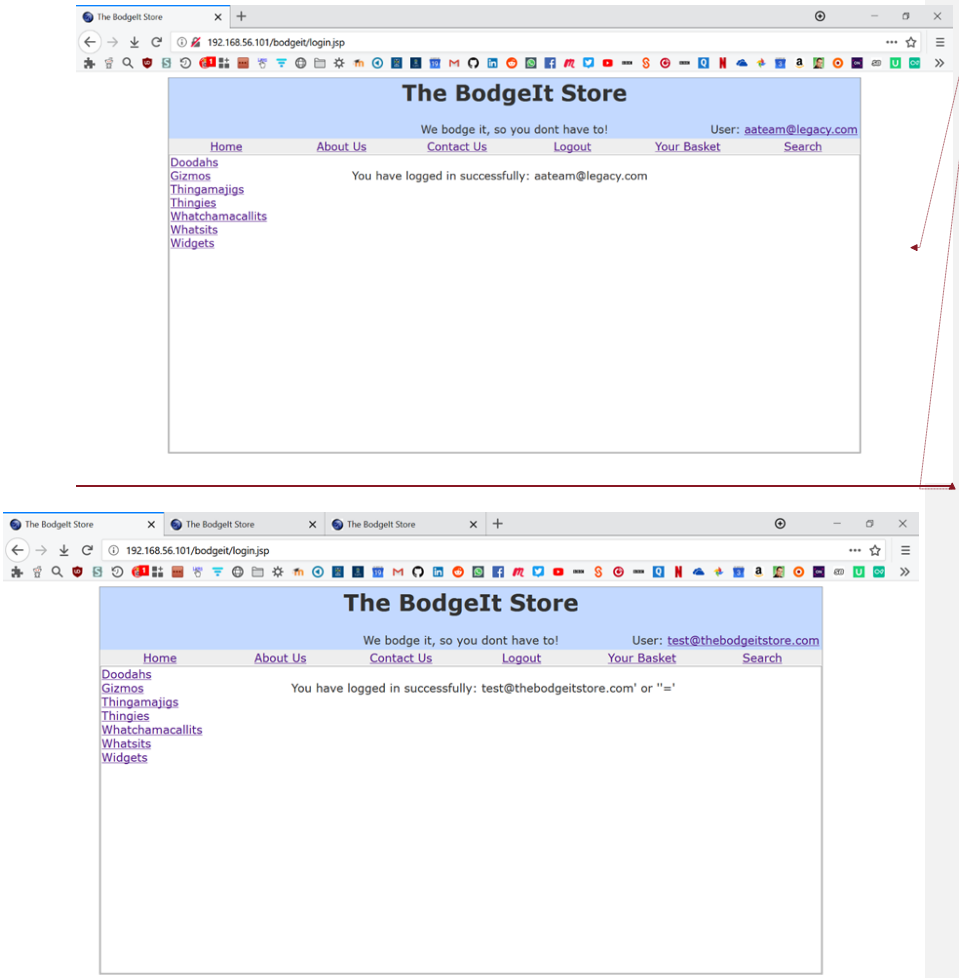


Figure 1: Login as test@thebodgeitstore.com

Formatted: List Paragraph

Formatted: Font: Bold, Underline

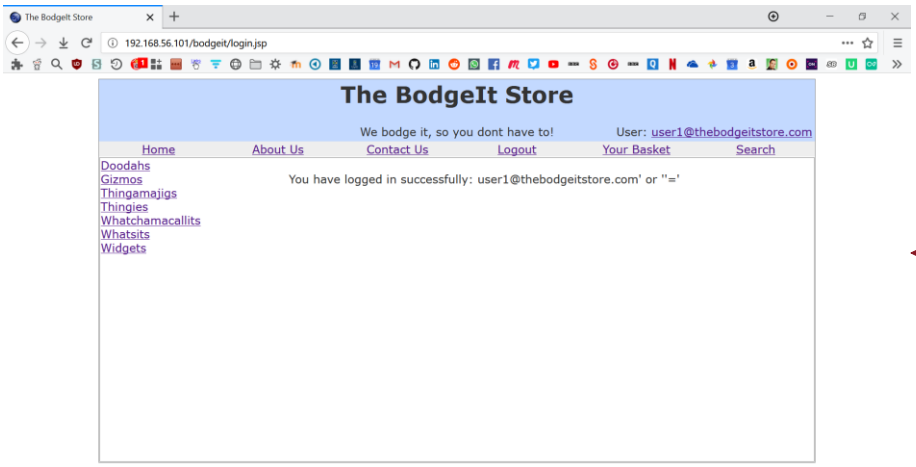
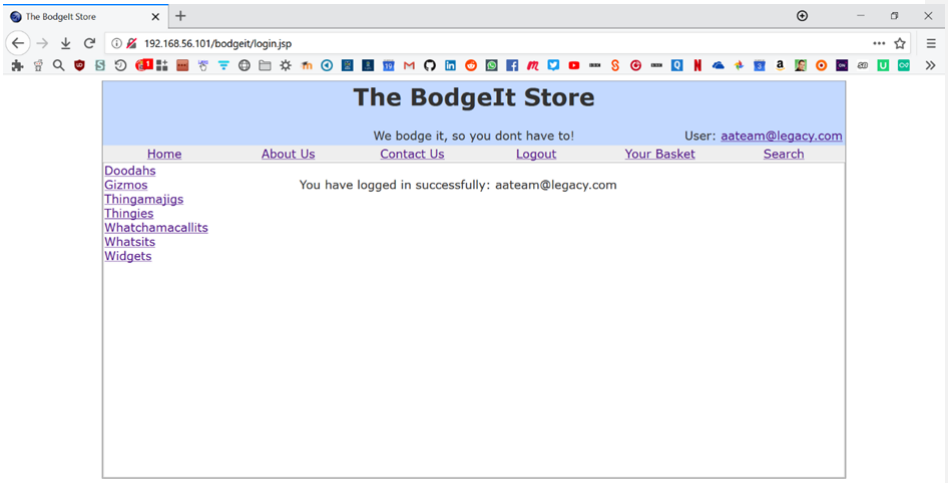


Figure 2 Login as user1@thebodgeitstore.com

Formatted: Keep with next



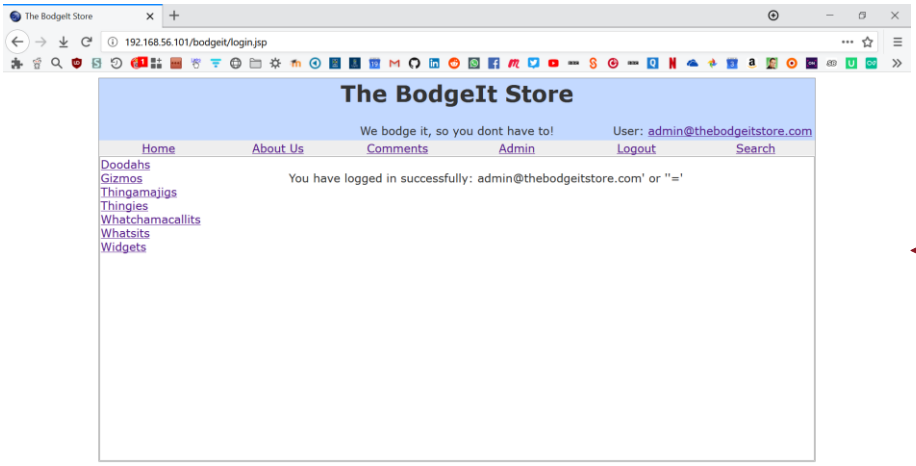


Figure 3 Login as admin@thebodgeitstore.com

Formatted: Keep with next

Formatted: Caption

Formatted: Font: Not Italic

Formatted: Underline

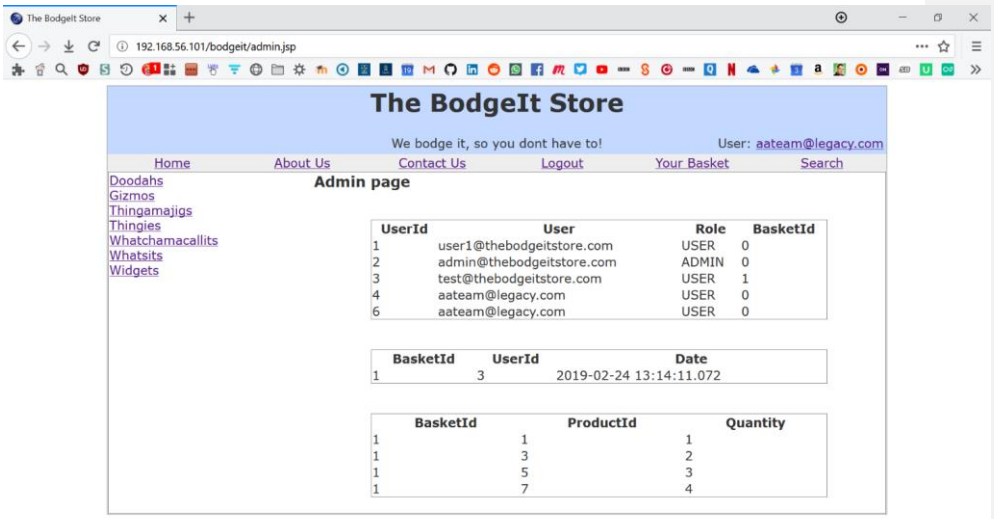


Figure 4 Find hidden content as a non- admin user

Formatted: Keep with next

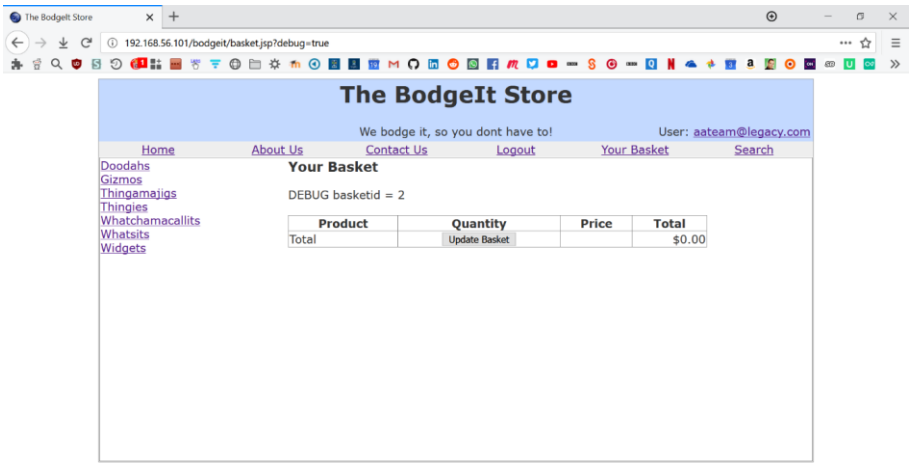


Figure 5 Find diagnostic data

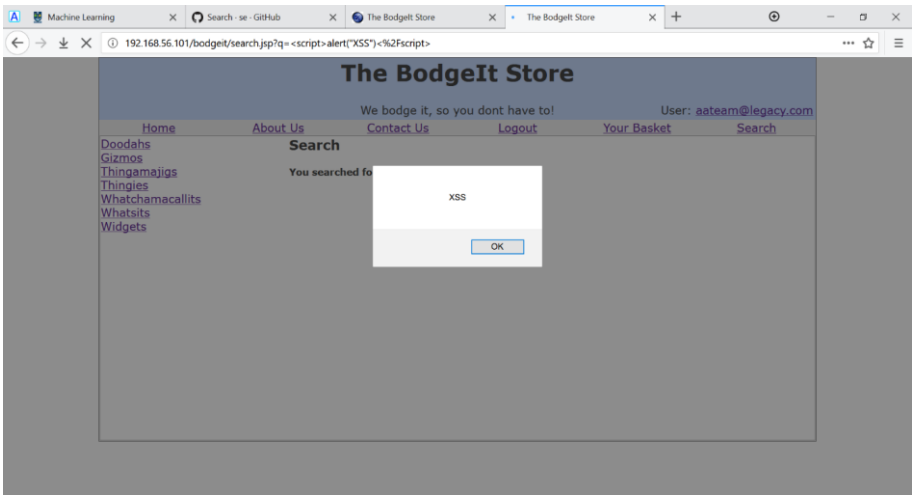


Figure 6 Level 1: Display a popup using: <script>alert("XSS")</script> via SQL query in search box

~~Figure 7~~

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

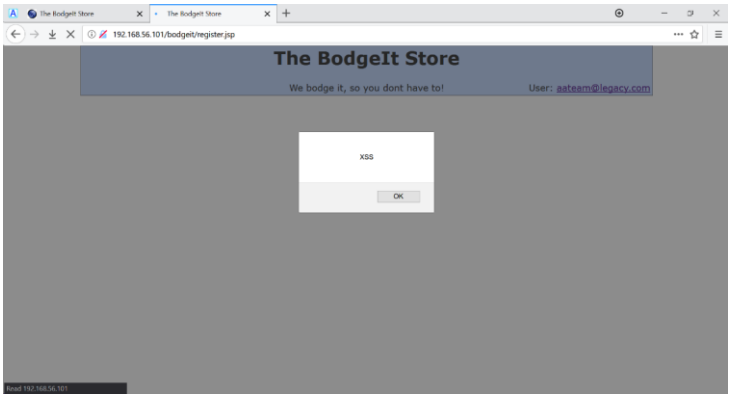


Figure 8 Level 3: Display a popup using: <script>alert("XSS")</script> Via the log in page

Formatted: Underline

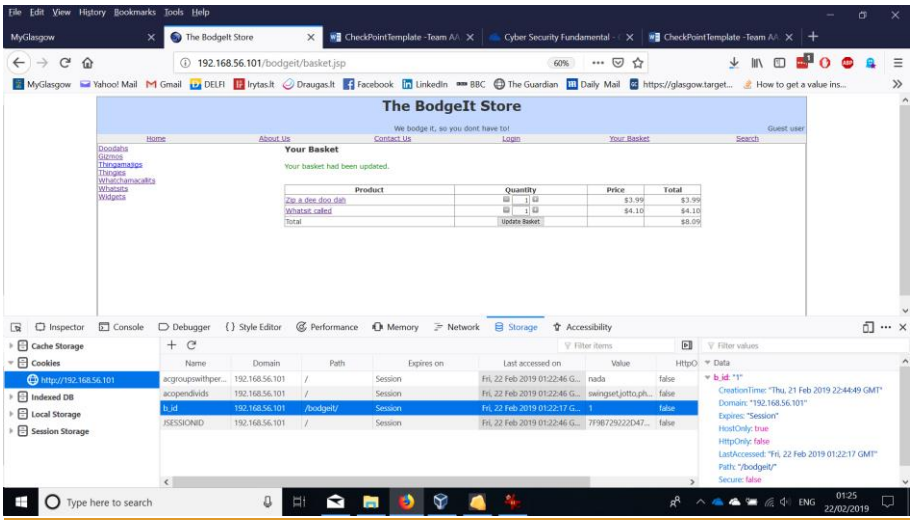
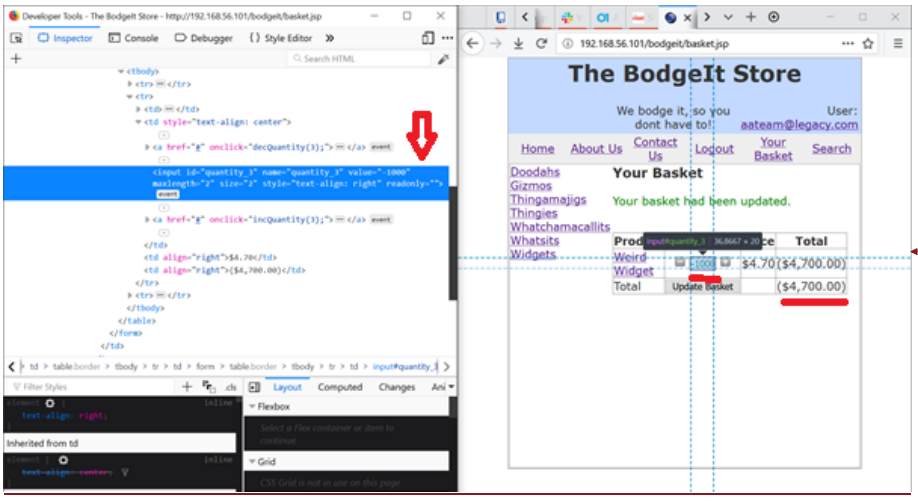
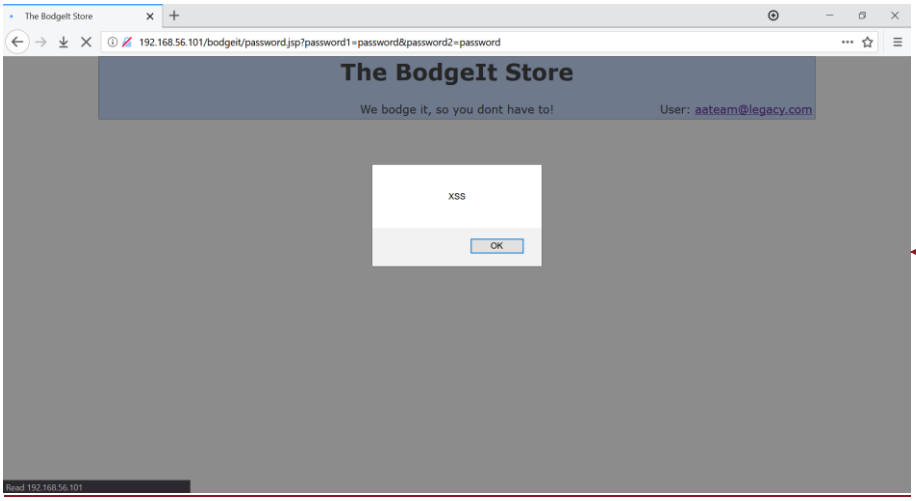


Figure 9: Access someone else's basket by exploiting poor session management control



Formatted: Keep with next



Formatted: Keep with next

Figure 10 Changing your password via a GET request – new password ("password") is encoded in URL bar

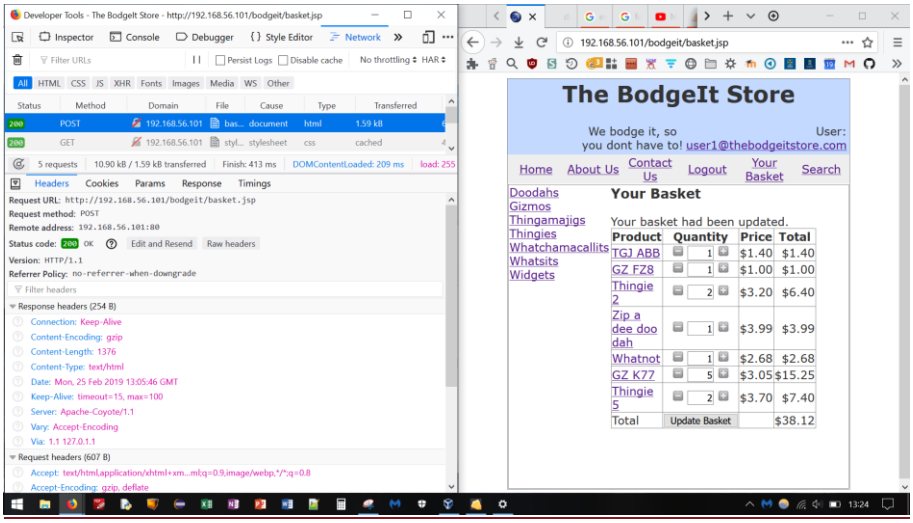


Figure 12: Force someone to add an item to their basket when they visit your webpage (using home link)

Formatted: Font: (Default) Times New Roman, 12 pt