iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** IX **Month of publication:** September 2020

DOI: https://doi.org/10.22214/ijraset.2020.31452

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IX Sep 2020- Available at www.ijraset.com

Where is the Coupon?

Arafat Badiuzzaman Khan[1], Abhijit Desai[2]
[1, 2]*Bharati Vidyapeeth' Institute of Management & information Technology, India*

Abstract: Coupon and promo codes have emerged in recent years as a way for shoppers to save lots of money at checkout on eCommerce platforms. Retailers can offer site wide discounts, alleviate shipping costs, and give access to special products by simply sharing a code with consumers. These promotional codes are often the defining reason customers move through the web checkout process.
It was an e-commerce store selling some stuff. I was checking it out and trying to understand the flow of the target. What I noticed was, there was no user account system. All you need is to choose the object you want to purchase, add to cart and give your bank card credentials. That's it. Very simple? Right.
The research mentioned in this paper is about finding the coupons and how it works.

I. INTRODUCTION

Loyalty discounts are some things given to loyal customers who made regular purchases thereupon particular store. As they're regular customers, they're given high discounts sometimes. But something which grabbed my attention was, how XYZ goes to understand that I even have made purchases with them previously or not as there's no user account ? Of Course they have an authentication system for it. You need to put your email, they will verify it. If you've made some regular previous purchases with them , they're going to directly apply the discount coupon. After verification, all you need is, pick an object, add to cart and give your credit card credentials. And you will see the 50% off in your final total at checkout. That's it.

II. RESEARCH METHODOLOGY

A. What is Research Methodology?

A Research Method represents the steps involved in performing the research. Details about the methods focus on characterizing and defining them, but also explaining your chosen techniques, and providing a full account on the procedures used for selecting, collecting and analyzing the data.

B. How data was collected?

While conducting the research I used a qualitative experimental study method for obtaining qualitative data. The aim of this method is to produce generalizable knowledge about the cause of a phenomenon. I studied the behavior of the system, analyzed its properties and its working and then experimented on it. This approach of finding data is flexible and subjective.

C. How analysis was done?

After collecting Data,I analysed it and tried to find faults in the system by testing the application. For this approach Intruder attack tool was used. Using this tool I was able to find the bug in the system.
Choosing the correct research methodology can determine the success and quality of your report. Hence it is essential to get the initial stage of your research right. The approach used for this research provided relevant information, necessary descriptions and explanations.

III. FINDING

Where have they kept the coupon after verifying the email address for previous purchases? Either they need to stay it in my session storage or either in cookies. But there is no account system in this store. Well, quite clear then, they keep that coupon within the cookies.
" I badly want that cookie ". I said to myself
But to urge that cookie, I want someone email who had previous purchases with XYZ store. Time for reconnaissance. I went to find their employee email. For sure they would have purchased those products (Free or paid; Not my headache) . LinkedIn was there to do the job. Spent an hour and finally found one (not of internee :p) . Put any random email and catch the request. The request is like this.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IX Sep 2020- Available at www.ijraset.com

```
POST /api/discount/email HTTP/1.1
Host: XYZ.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0)
Gecko/20100101 Firefox/60.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://XYZ.com/store
content-type: application/json
x-csrf-token:
WgT1jCcK9K39IWKBhD5Y5Kyi8RdvBNcJB33jYVpx
origin: https://XYZ.com
Content-Length: 29
Cookie: ....
Connection: close

{"email":"valid@XYZ.com"}
```

Send it to repeater and replace the random email with the one having previous purchases. Check out the 'set-cookie' in http response header and game over.

```
HTTP/1.1 200 OK
Date: Wed, 25 Mar 2020 12:05:50 GMT
Content-Type: application/json
Connection: close
Vary: Accept-Encoding
Set-Cookie: coupon=EXAMPLE; expires=Fri,
24-Apr-2020 12:05:50 GMT; Max-Age=2592000; path=/
Set-Cookie:
CouponObject= ....
expires=Fri, 24-Apr-2020 12:05:50 GMT;
Max-Age=2592000; path=/
Cache-Control: no-cache, private
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 59
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Referrer-Policy: no-referrer-when-downgrade
Strict-Transport-Security: max-age=15768000
Content-Length: 5939

{"ok":true}
```

Now because the cookie has been updated with the coupon, I selected an object, added to the cardboard and saw the five hundred off within the final total. And that's how can everybody get 50% off on their purchases without being a loyal customer. The coupon values are often checked from the storage portion of the inspect element.

Sometimes the target is as simple as this. All we need is an eye with a focus to see and observe what others can't.

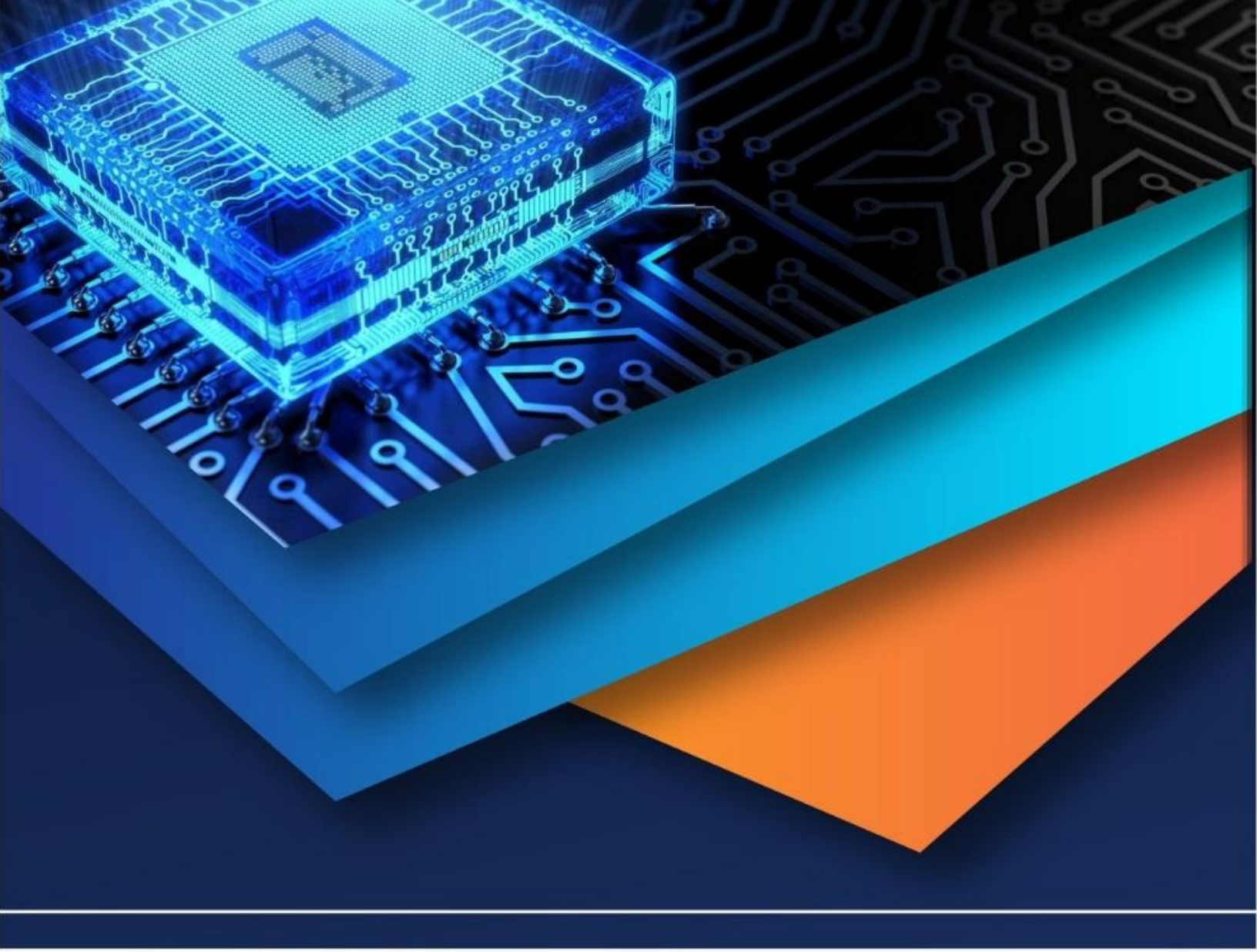
Because the store was having no user account system to store coupons in their session cookies, they might be gotten by anyone. Anyone could get that prime discount, without having previous purchases. I have found another security flaw using the same methodology but that was marked as duplicate to this as the source of flaw was the same.

©IJRASET: All Rights are Reserved

REFERENCES

[1] https://www.scribbr.com/category/research-paper/
[2] https://writing.wisc.edu/handbook/assignments/planresearchpaper/
[3] https://www.grammarly.com/blog/how-to-write-a-research-paper/
[4] https://ijarcce.com/upload/2015/january/IJARCCE2O.pdf
[5] https://portswigger.net/burp/documentation/desktop/tools/intruder/using

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)