Abstract: Since 2021 the world has been facing the problem of website login. The OTP bypass attack is taken because the real-time there are a lot of many people who get attacked by someone. They lost valuable credentials the Facebook accounts are most hacked in recent years. So this is the process the attackers attacked to our account through burp suite by using the OTP bypass method and another method is brute-force attack like this there are different types of attacks. To solve the problem for this there is a lot many ways before but they are the 60-79% accuracy this can give 85% accurate result. The old version models have some drawbacks like they are not efficient and another one is almost all models are dummy it has no use. This can give the best result this also has a limitation it gives only 85% accurate results but in most cases, it cannot give the result. It can be overridden in the future by our team. This can be given the knowledge of how the hackers enter our accounts without any details by using the mobile number. This can help how to prevent hackers. In this first have to open the burp suite tools that which has the licensed version then enter into the proxy then turn on intruder then open any website which you want to enter then enter the mobile number and continue then wait for OTP then you have to enter the dummy OTP in the website after going the burp suite tool then forward it you will find the dummy OTP which you have entered then remove all the dollars then add the dollar to the dummy OTP only then go to the payloads tool then enter the how many digits thus the OTP is and get the step as one by one then start the attack. It will give all the combinations of OTP from 0000-9999 and then check the response in it. It will be whether the OTP is a success or valid if not it will give the invalid OTP please enter the correct OTP.so you will get the OTP which you can enter into the account which you want. then you will log in to the website with their number. To overcome this type of attack from the general people to know awareness of how the process should be done and how others can easily enter the account. To prevent this must use two-step verification and use a 30-sec time-limited site and a strong password (it must contain Caps letters, small letters, numbers, specials symbols, especially the space between the name in the password) then it has very less amount of change to get hacked.

Keywords: Websites, Burp-suite, Credentials, Brute-force, Hackers, Attackers, Time-limit, Onetime Password, Verification, Response, Proxy, Combinations, Dummy, License, Versions, Bypass-attack, Accuracy, Awareness, Victims, Overcomes.

1. Introduction

The term cyber security means the protection of digital data. Cyber means digital data. Security means protection. Digital data like computer data, network data, internet data, mobile data, wi-fi data, website data, IoT data, and Cloud data. For these all kinds of data if we provide the security it seems to be cyber security.

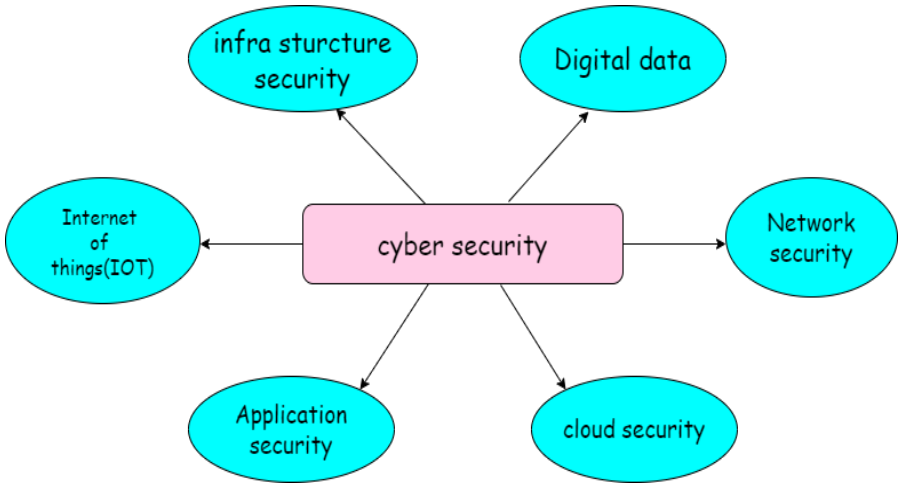

Figure A: Types of cyber security

Figure A represents the types of cyber security. Infrastructure security, Internet of things, Application security, cloud security, Network security. A cyber attack is an attack performed on digital data. There are a few common attacks. Malware attacks, Crypto-jacking, Steganography, OTP bypass, Ransomeware, SQL injection attacks, etc.. are performed to attack the personal information of a user on the internet.

Infrastructure security is a practice of protecting the system from cyber and physical attacks including software and hardware assets such as networking systems, data center resources,end-user devices, and cloud resources.

Digital data security is used to secure our digital data such as online websites, and social media and digital security protect your online presence(data, identity, assets). At the same time, it provides security for the entire network and other digital components.

Network security helps to keep the user network safe and protect the system from cyber attacks, through the network many cyber attacks will be done on the system to prevent those attacks network security helps. and there are 3 types of components of network security: hardware, software, and cloud services.

Cloud security is a discipline of cyber security provided to secure the cloud computing system and it provides both private and public data.

Application security is the process of testing security features within the applications to protect the system from cyber attacks and to prevent security vulnerabilities against threats such as unauthorized access and modification.

Internet of things(IoT) refers to the way devices connect from one device to another within a network environment such as cloud, internet communication, etc.

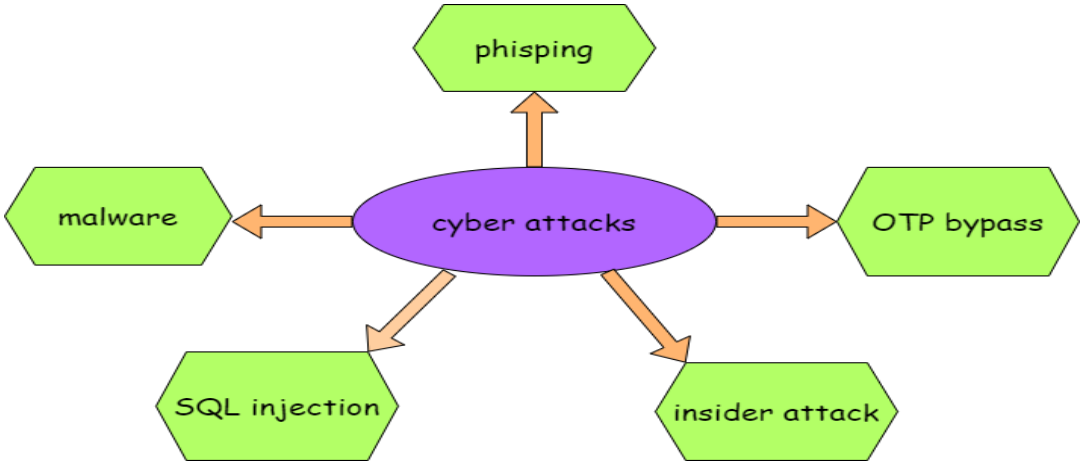

Figure B: Few types of cyber attacks

Figure B represents different cyberattacks in daily life. It shows a few attacks they are:

phishing attacks are the practices of sending fraudulent communications from a particular reputable source. It is usually done through email. The main goal is to steal the personal information of a user and install the malware on the victim's machine.

Malware---It is malicious software and is used as a single term to refer to viruses, spyware, worm, etc. It is used to gain unauthorized access to a computer.

SQL injection---It is a web security vulnerability that allows the attacker to interface with all the queries which are used to retrieve the information from the database. Through this attack, they steal information or data. The attackers retrieve information that they can not retrieve normally.

Insider attack---It is the security risk that comes in particular organizations. The attack acts as an employee for a particular organization, he also deals with the very sensitive information of a company. He misuses the access which is given by the company.

OTP Bypass—It is also like an attack that is used to grab the OTP of a particular user of a particular website. We generally use the tool called burp suite which creates a wonderful platform for finding the OTP through various methods.

We also mainly perform this OTP Bypass attack. To find the OTP of a particular User for a website. For the complete project, we will be using the Burp suite tool for performing this attack.

2. Literature Survey

Table Number:1 Tools used for the OTP bypass attack

S.No	Author	Tools	Merits	Demerits	Accuracy
1.	**Siddhesh Deepak Patil**	**Guard**	It will help with the three-step verification of a computer.	It is easily crackable and everyone can easily enter the system.	**87%**
2.	**Jurusan Teknik Elektro**	**OTP berbasiskan algoritma matematika**	For high security issue to the websites.	Its for their college only	**86%**
3.	**Prof. Antonio Lioy**	**Securing Vulnerable Web Applications**	To keep the more secure from penetration testing.	There are a lot many bugs.	**79%**

In [1], Siddhesh Deepak Patil has several different authentication methods which are very much useful to cyber attackers. They can find your vulnerability and then collect all your information of yours. So the system must be protected and the user has to enter a strong password that they cannot easily crackable. In [1.1] So they will try different ways and different tools to know the vulnerability of the system and then will start the attack. So they will get all the information about your system. There are three layers of protection to the system. In [1.2] They are 1. Layer one, 2. Layer two, 3. Layer three, 4. System Security, 5. Virus solutions, 6. User account management. These are the layers of security to the system. Let me explain in detail. In [1.3] Layer one: In the first layer of your computer, the user has to enter their user-id and password which they had used during the time of registration, it is the same as the original method but with various approaches, as this computer has their original password matching algorithm which is unique in its different way, and we can enter the password in many different ways with certain keyword (i.e.., password), the user has only three chances to enter their password if they fail to do the application will terminate itself. In [1.4] Layer two: The second layer consists of a One-Time password which will be sent to the mobile number of the user, which will be consists of 4 to 6-digit content which are randomly generated by the systems algorithm itself. To send the one-time password we are making use of an API called Text Local API services, it is an SMS service provider which will be sent the One-Time password to the user, the user should enter that OTP in the computer to pass the second layer. In [1.5] Layer Three: - The final layer of this system will make use of email-id image verification which means one image will be sent to the user's registered email-id they have to see that particular image and match it from six sets of images shown on the screen, it is one type of OTP system but here its make use of pictures and the user has only three chances to pass this verification if they fail then the application will close and will capture the image of the user. For example (I am not a robot popup in the browser).

In [2] Jurusan Teknik Elektro was worked as the assocaiated professor in SSO University. They work under the tools of HTML and PHP and CSS for designing a website for their college. They work for the management to build a strong website that they have ty to prevent attackers so they implemented it most securely by using the algorithm of OTP berbasiskan algoritma matematika. By using this algorithm they build a perfect website the most secure. And also they used cryptography techniques so they can make every text encrypted to the server. If even an attacker can hack their credentials but can not understand the encrypted data so they can't know our credentials of ours. They had used the inbuilt VPN in it so the attackers can not find the location of their college so they made the users more comfortable. the crypto card is the thing that card is very high in advanced so the hackers have no chance to get entry to the entrance but they hav3e as the way its nothing than network high jacking so it is not at all tough to get the logging to the website through background. So there is a chance so to protect they have just such tools to overcome it they made their website more [proteceted so they cannot the beginner-level hacker can not enter to the website so they can not modify.CRYPTOCard generates a new OTP each time the button is pressed. The computer system will receive some return values if the key is pressed more than once by mistake or if the client fails to authenticate**.** OTP based on mathematical algorithm This type of OTP is another type of OTP that uses complex mathematical algorithms such as **a** cryptographic hash function to generate a password new based on the previous password and starting from **a** shared secret key. Examples of mathematical algorithms used in this OTP are an open algorithm standardized OATH source and other patented algorithms. Multiple products Applications that use this authentication are **crypto card, Verisign, E-Token Aladdin Knowledge System NG-OTP.** These are the methods in it.

In[3] Securing Vulnerable Web Applications is the process of finding vulnerabilities in the website. To prevent the website from attackers so they can not enter the website because it has a lot much venerability. Prof. Antonio Lioy is the man who builds the security for the website from the pen-testers so that they cannot enter the website so most of the hackers use different types of software. So in this, there is a way how to prevent some types of attacks so that normal people will get the basic knowledge from it how to protect their sites so that they will try to protect. In this, there is another topic using the burp suite they will how to attack you. So that you will understand the how to know from the attacker side view that you will know how to attackers attack you in the website there is a lot of many tools in the burp suite that will help not only in the web hacking it also helps us in different types of attacks like pen-testing, brute-force attack, password cracking, et all, these are the attacks that can be done by using the burp suite room. They build their website by using HTML, CSS, and PHP programming languages so that they can build their website more securely. In this Prof. Antonio Lioy has tested all the security of the languages at whether the program is secured or not.

3. PROPOSED METHODOLOGY

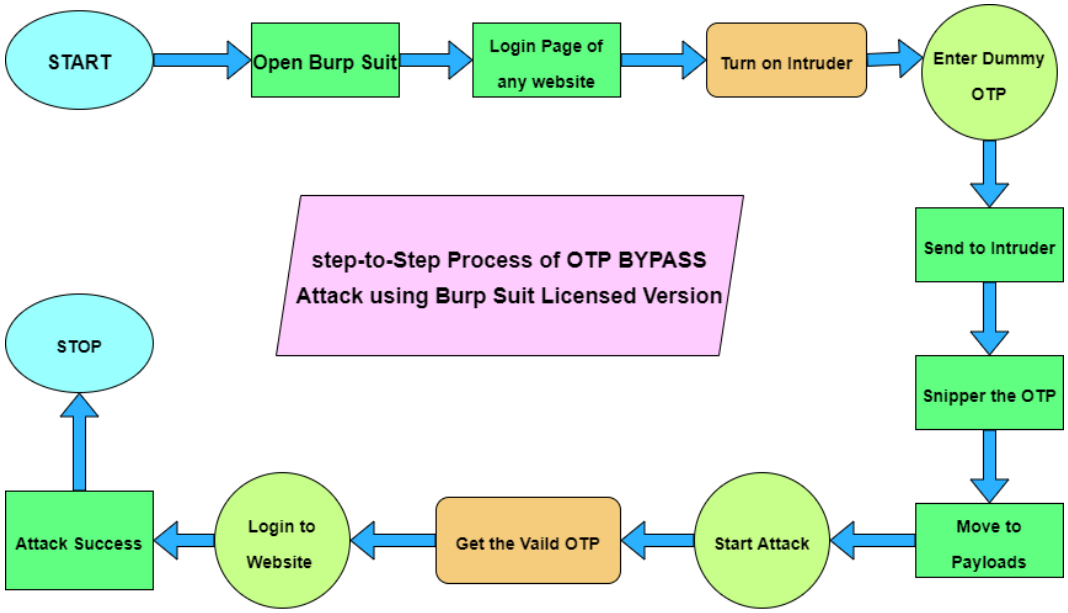

Figure: A

3.1. START:

Click on the start button in the windows. Check the burp suite licensed version and click it to start the process.

3.2. Open Burp suit:

So, to perform the OTP Bypass we need to start the Burp suit first. The Loading of a burp suit professional tool only works no other third-party tools are not allowed to work properly. After that, we face an interface popup that is like a path of the burp suite files for storing purposes then click next. It directly takes to the main dashboard where every tool is present as their go-to proxy and then clicks open browser which is used to connect the browser with burp suit from this we can enter to the website or any applications which you want to attack. And try to log in with your mobile number and get the OTP using the burp suit.

3.3. Login page of any website:

Through the open browser that means the burp suite browser clicks any website in which there is a chance of signing up or logging in through the mobile number and also needs to be logged in through the OTP, only such website needs to be selected. Enter your mobile number and click continue.

3.4. Turn on intruder:

Here it means we need to be given a dummy OTP and on the intercept which is present on the proxy tool page.

3.5. Enter dummy OTP:

We just need to enter the dummy OTP for getting the correct OTP through this Bypass attack. And intercept is must turn on.

3.6. Send to the intruder:

In the proxy tool page, we first need to clear all $ and need to add the $ before and after the dummy OTP. The dummy OTP is sent to the intruder.

3.7. Snipper the OTP:

In the intruder tool page, we have positions click on that where it consists of the attack type we need to set into the snipper to work the attack.

3.8. Move to the payloads:

After setting the snipper type we need to go to the payloads here are the payload type and payload options where the range of the OTP(4(or)6-digits) for this 0000-9999 This is the limit of the payload type. And we will get the ranges of the OTP.

3.9. Start Attack:

Just click on Start attack.

3.9.1. Get the valid OTP:

We will get a valid OTP on the intruder attack page. where the abnormal change in length seems to be our required OTP.

3.9.2. Login to the website:

With that OTP we just logged into the website and we can enter the website.

3.9.3. Attack Success:

The attack is finally a success.

3.9.4. Stop:

Need to end the process with this we completed the OTP Bypass attack.

4. Results and Discussion

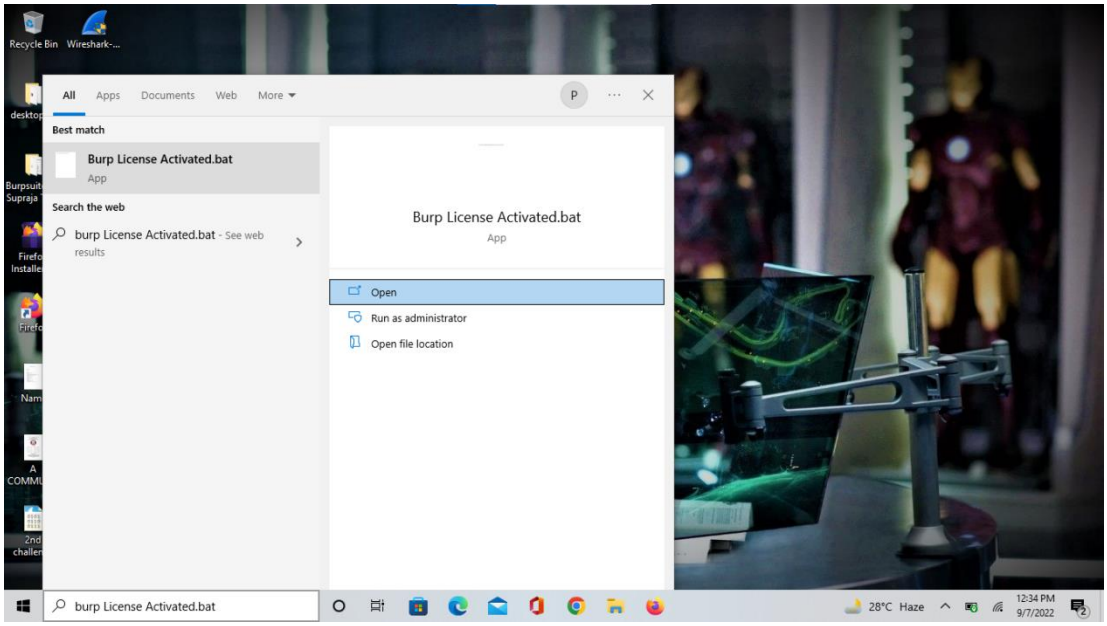

Figure 1: The find and open a licensed burp suit.

The opening of a burp suit from the system by searching at the search box of the system which is given in the windows operating system. It must be a license version only.

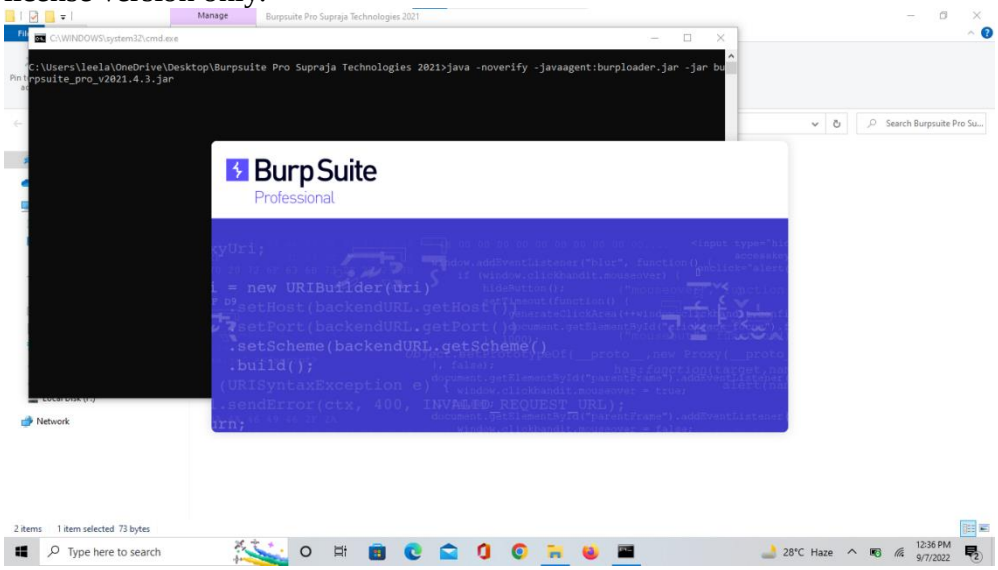

Figure 2: launching burp suit.

Loading of a burp suit professional tool only works other third-party tools are not allowed to do this.

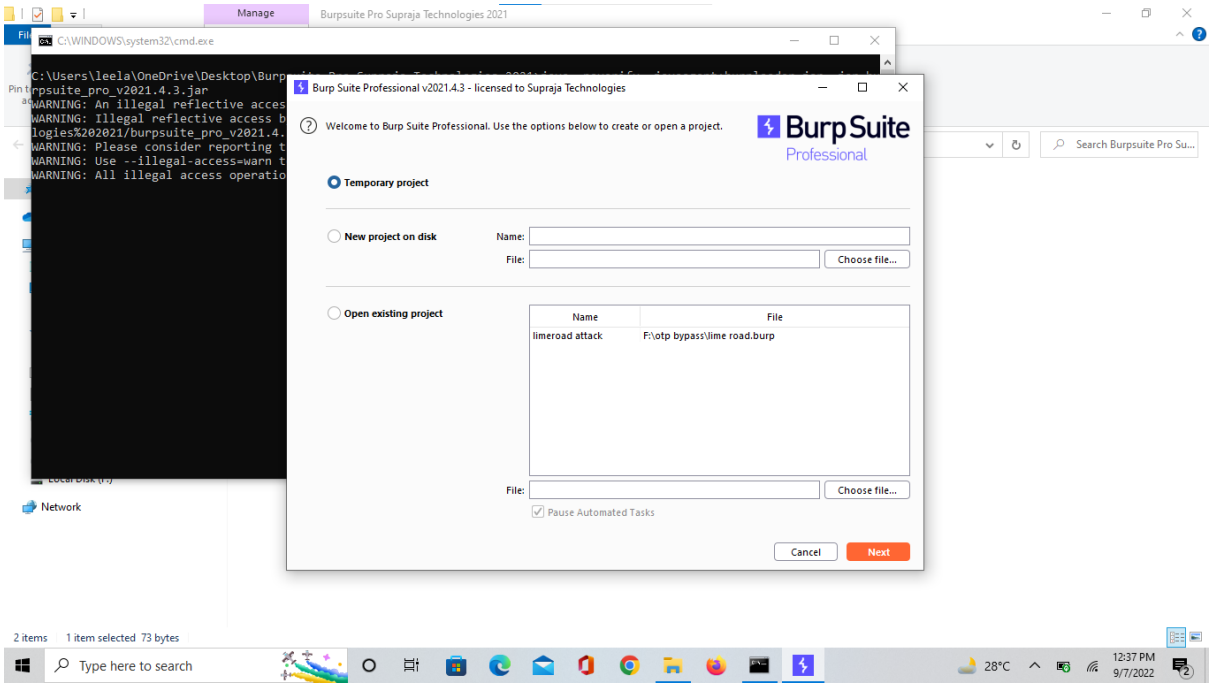

Figure 3: File saving popup of a burp suit.

Placing a path that the project has to store the file in the file explorer of the system. So it can make sure that has to stores them in file explorer and keep on saving.

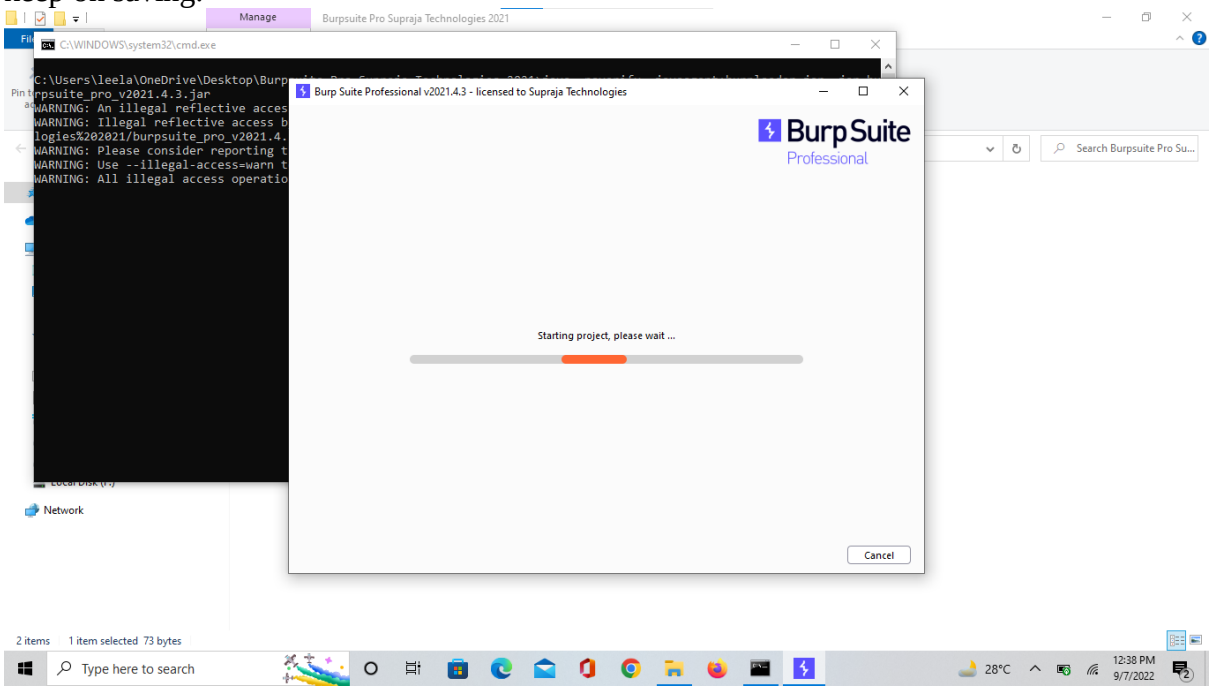

Figure 4: starting project.

The loading of the new project loading screen.

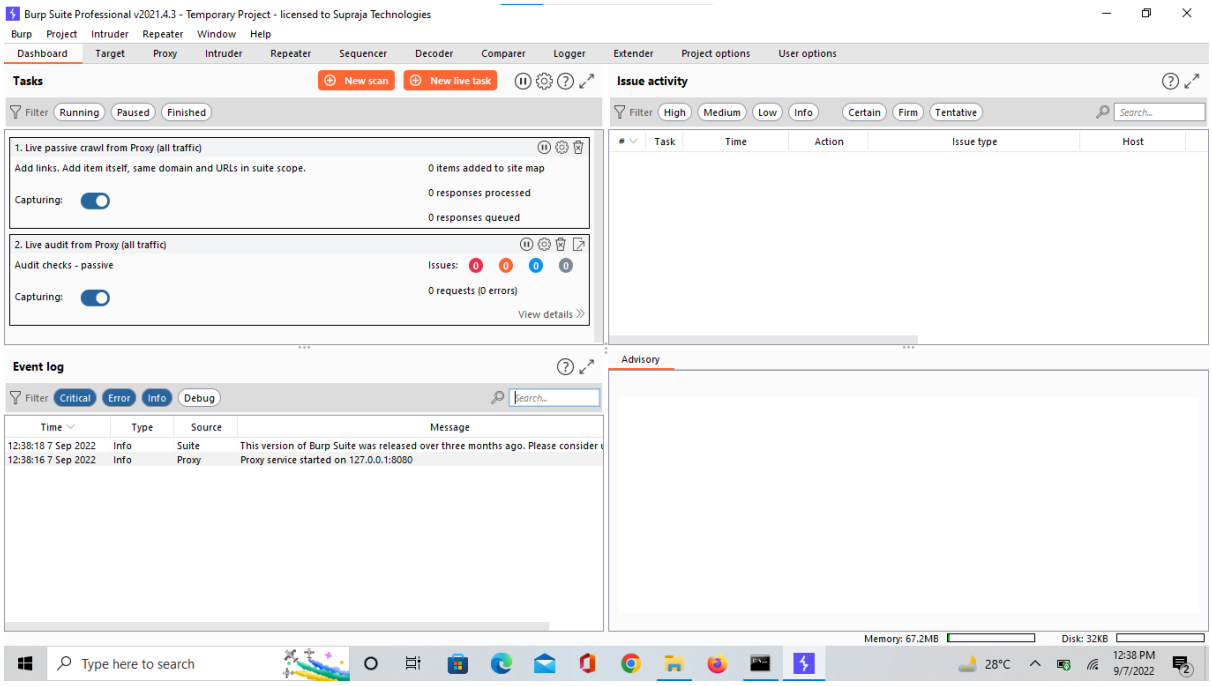

Figure 5: The main interface of a burp suit.

The main interface of the burp suite looks like the above figure then we have to select the proxy and do the changes in it.

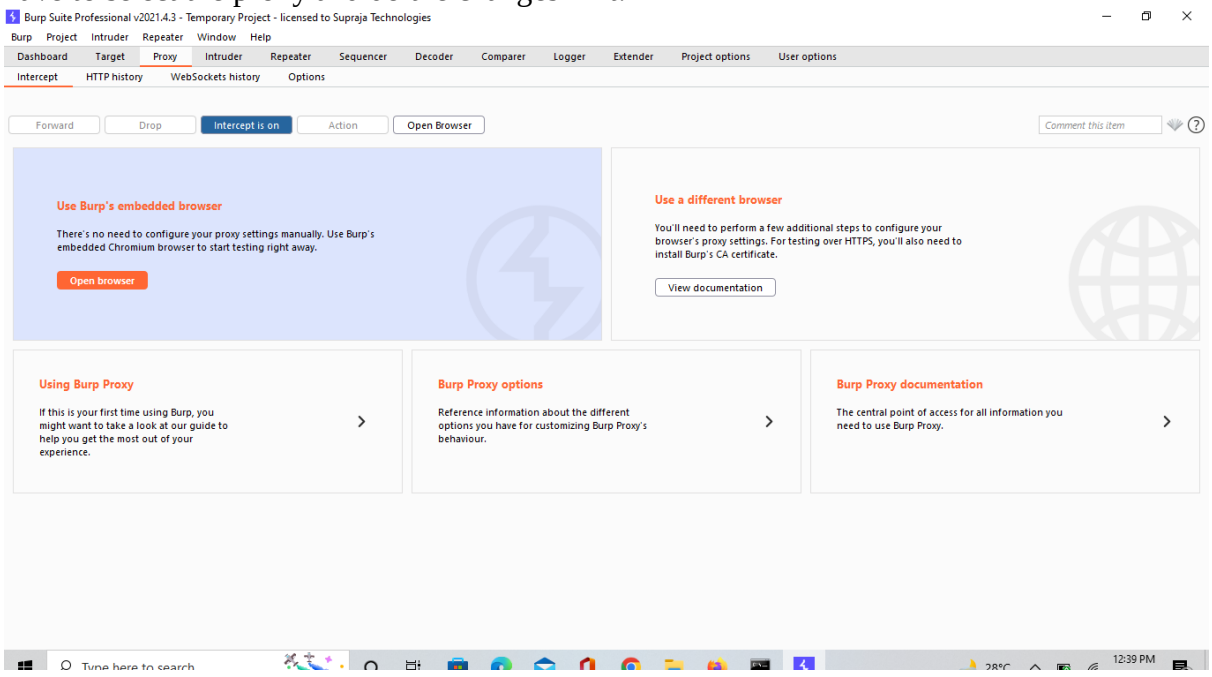

Figure 6: opening a proxy in a burp suit.

we have to turn on the interface proxy and select the intercept in it which will help you to open the browser.

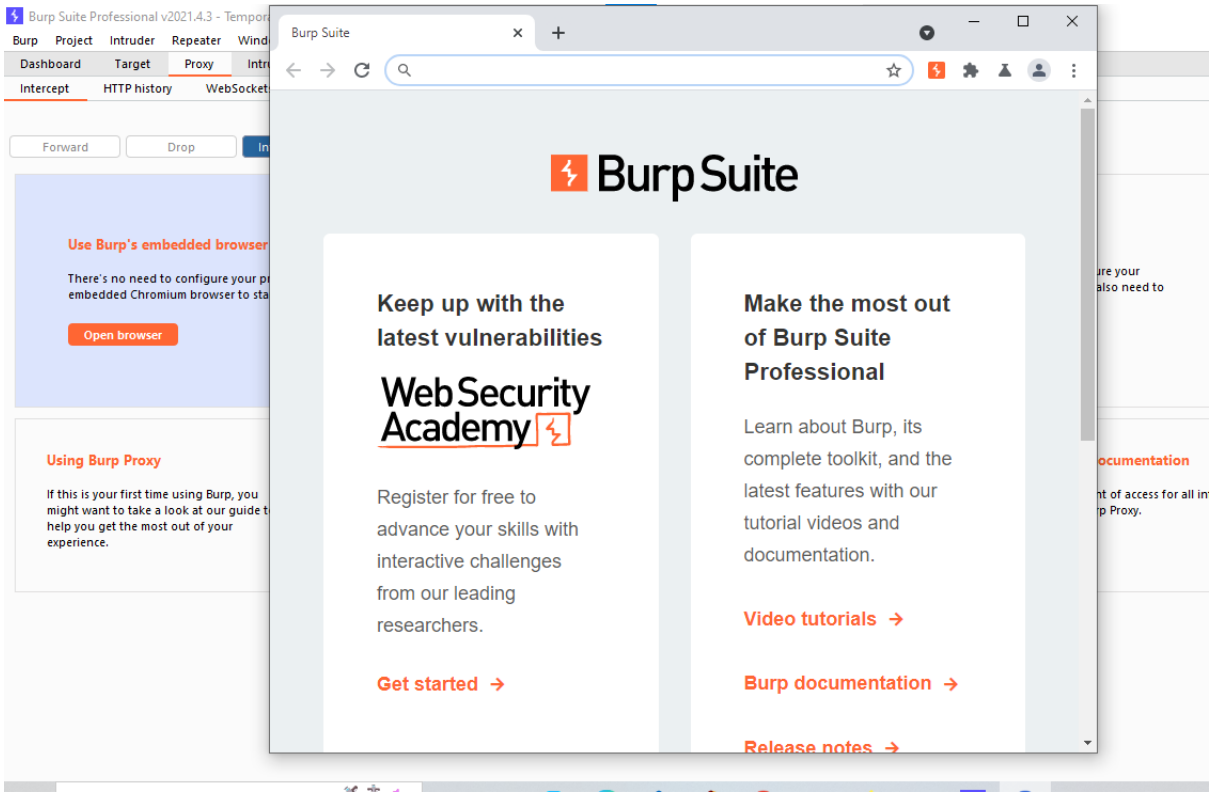

Figure 7: opening chrome from burp suit.

This browser which is opened by the burp suit will help to search the sites which we have to work on it.

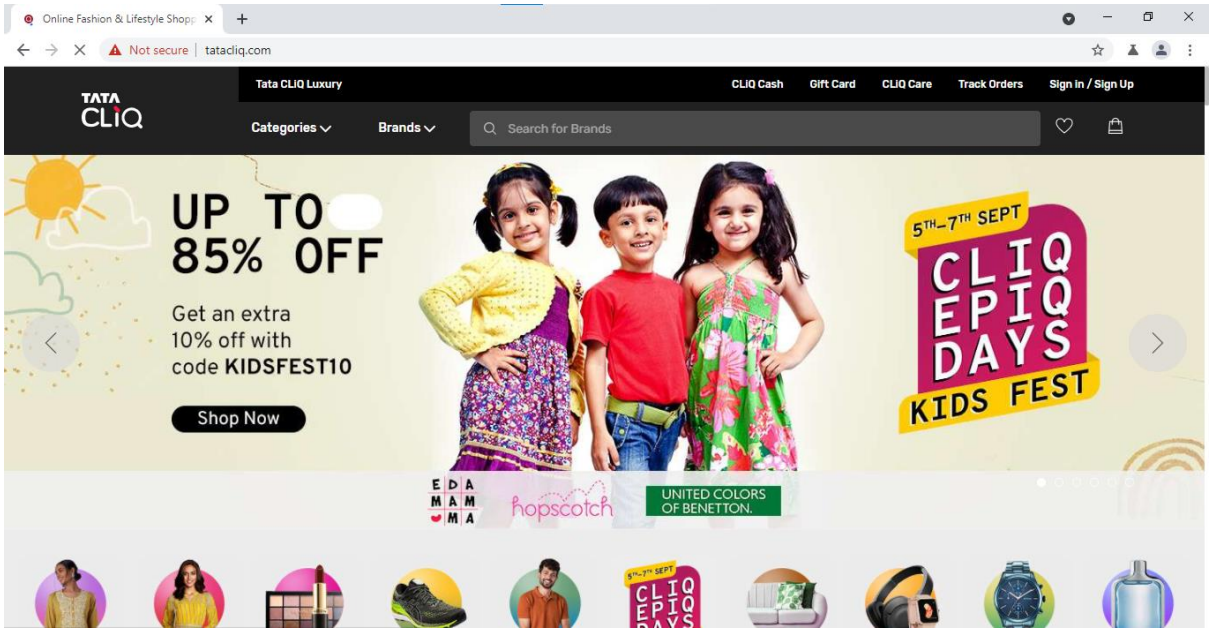

Figure 8: searching the website.

This is the site that I have to attack an OTP bypass attack on it.

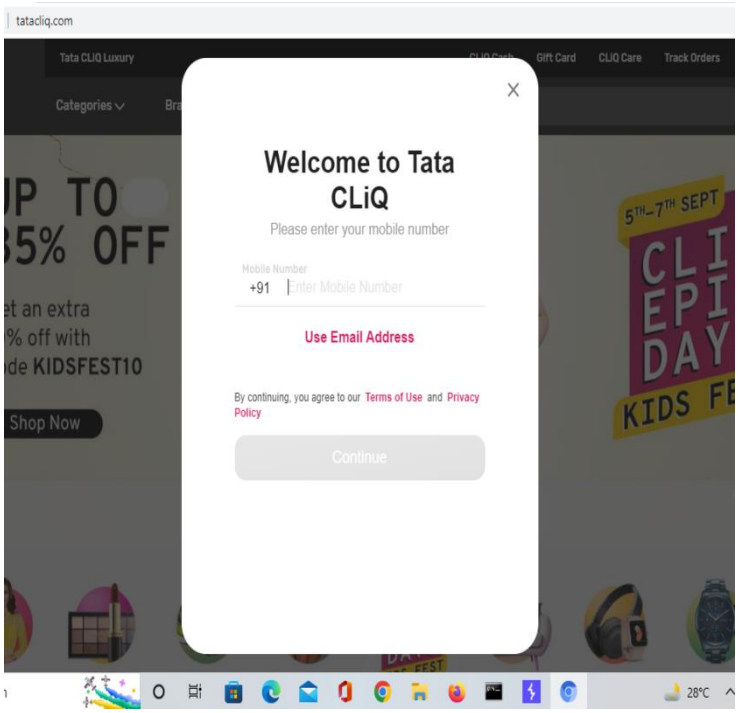

Figure 9: login page of the website

We have to log in to the site by entering the mobile number of your credentials. Click on continue.

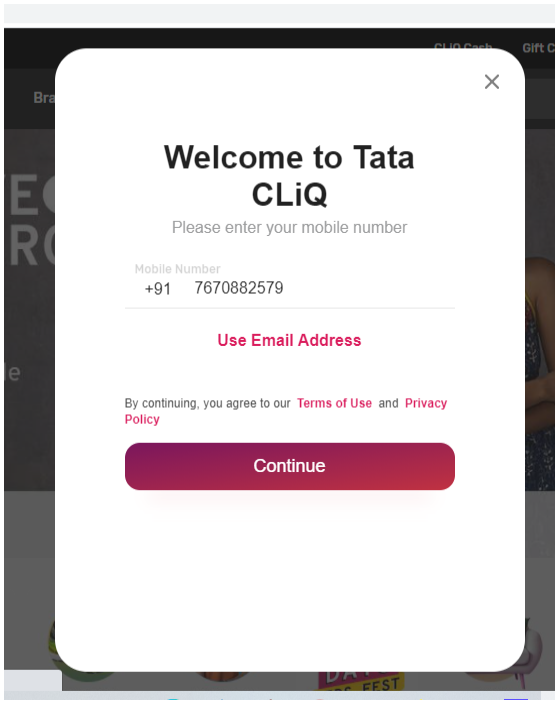

Figure 10: entered credentials on the login page.

Here above figure 10 represents the entry of mobile numbers into the website.

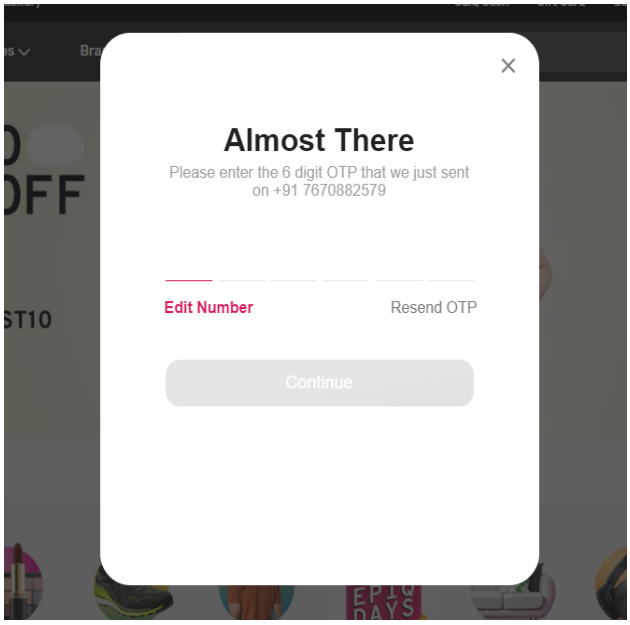

Figure 11: 6-digit OTP popup.

Here we have to enter the OTP for entry into the website. The OTP is a 6-digit number.

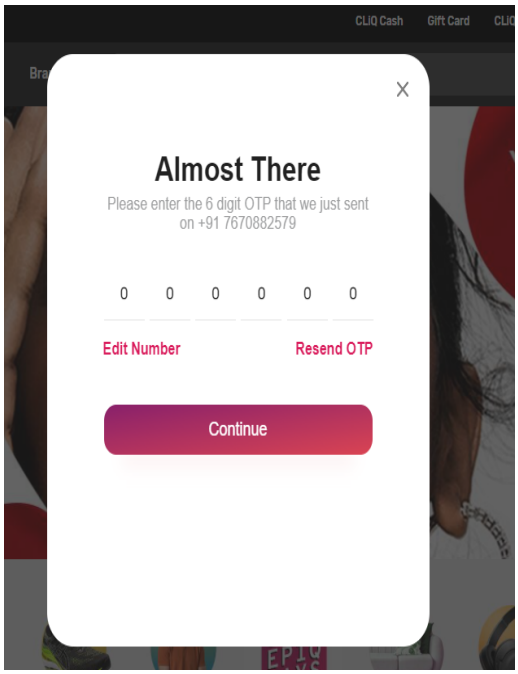

Figure 12: OTP popup

Where this figure 12 represents the dummy OTP entered in this site for traping the original OTP by using a burp suit.

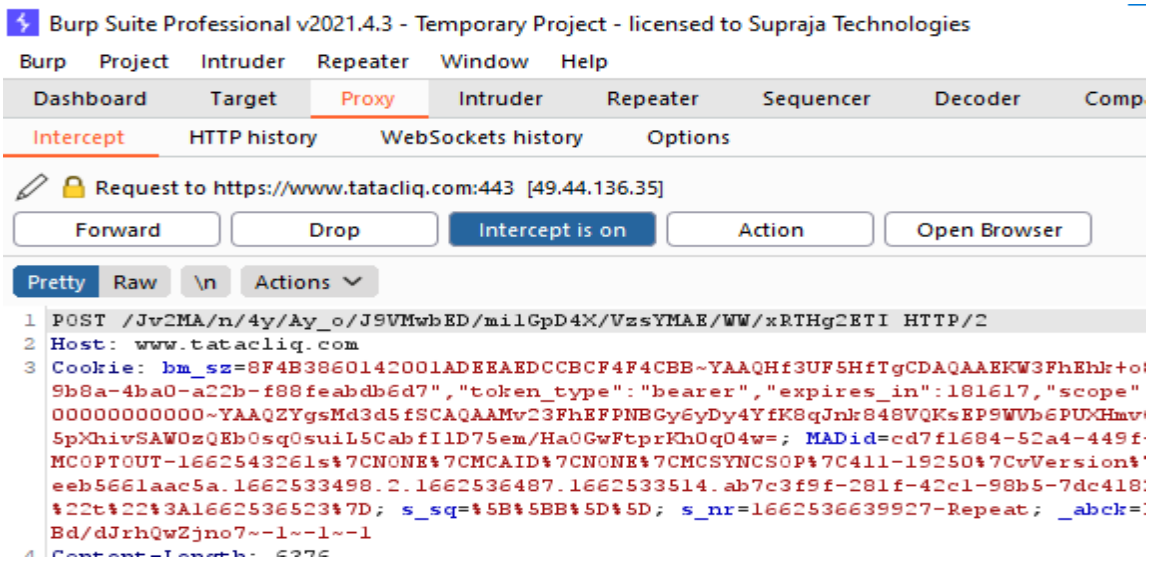

Figure 13: burp suit proxy tool

Figure 13 represents the burp suite tool called proxy which contains
.Pretty
.Raw
.Actions

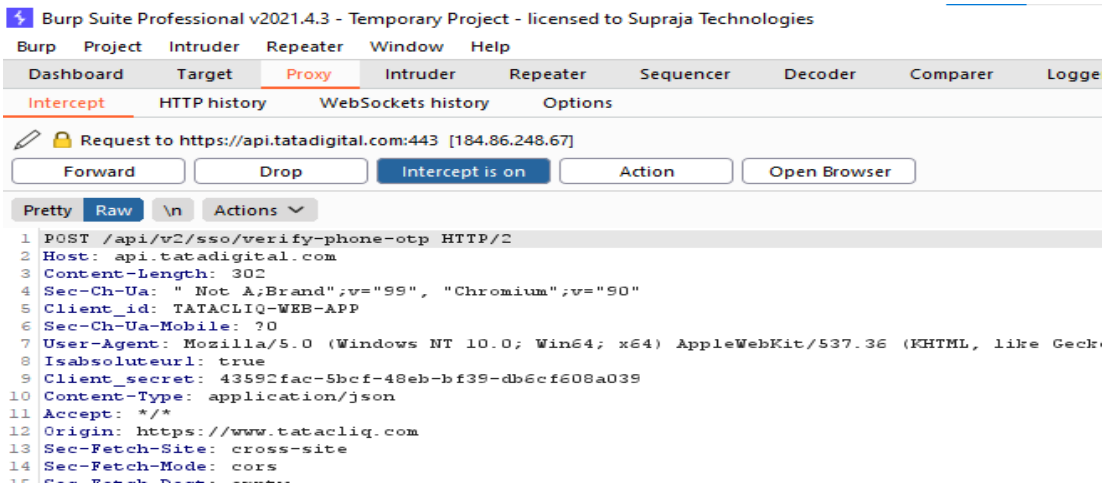

Figure 14: burp suit proxy tool

Figure 14 represents the conversion of the pretty to Raw tool for performing correct operations.

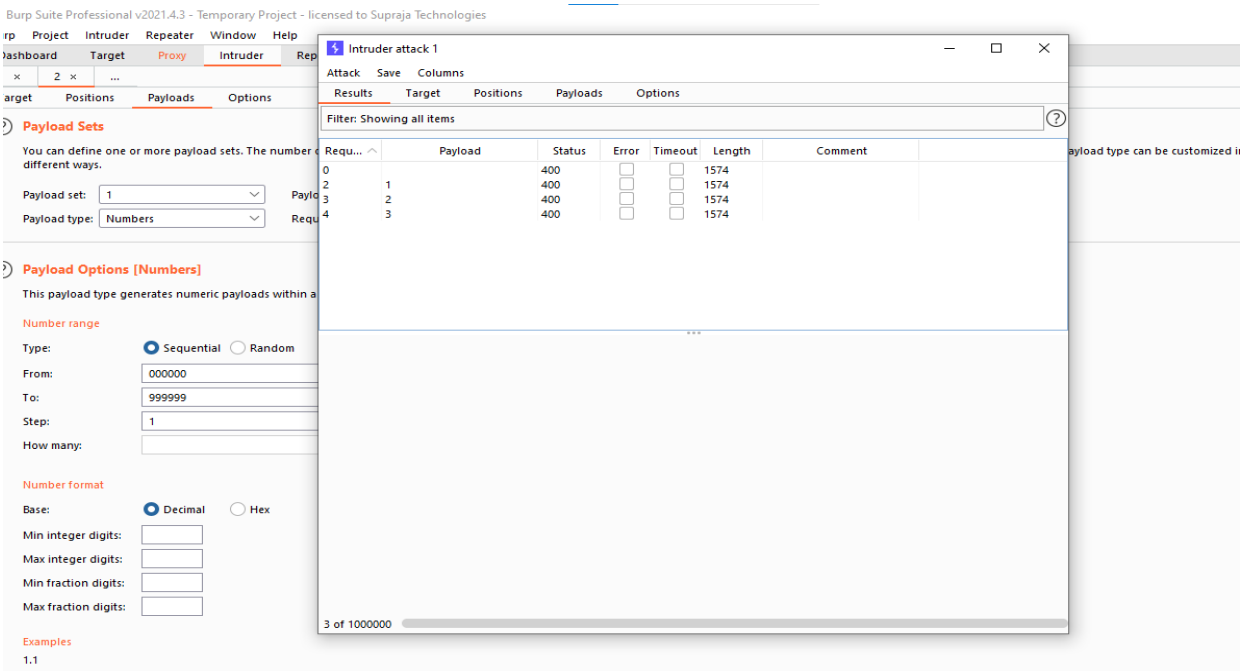

Figure 15: burp suit intruder tool

Figure 15 represents the intruder tool in the burp suit and which performs the scanning operations of all the OTP s

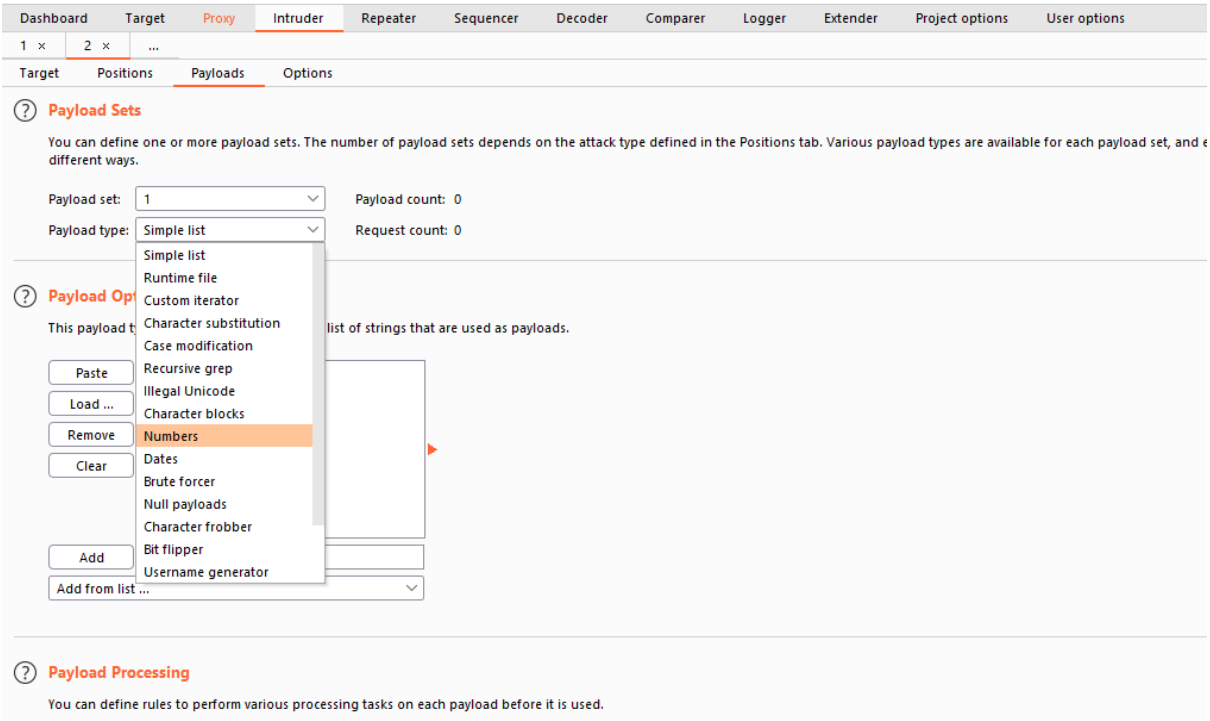

Figure 16: burp suit intruder tool page

Figure 16 represents the intruder tool which contains the options like target, positions, payloads, and options. We just click the payloads page for the type of OTP and OTPs range.

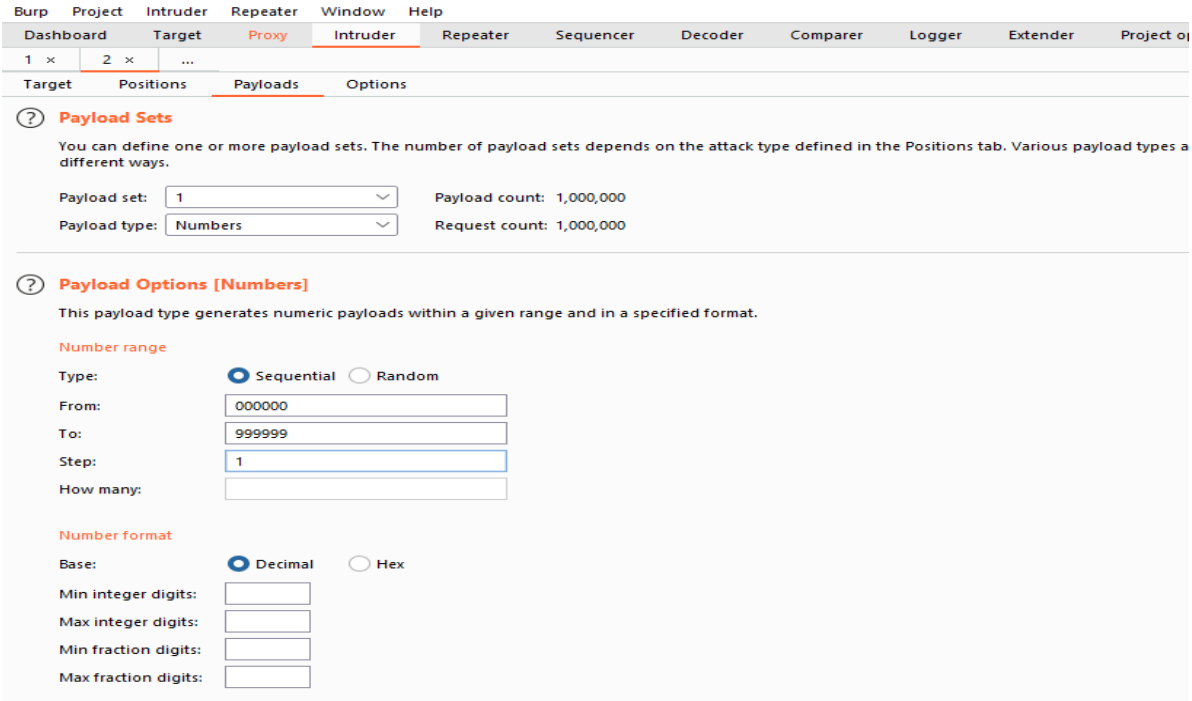

Figure 17: burp suit intruder tool page

Figure 17 represents the selection of payload type and selecting the range of payload.

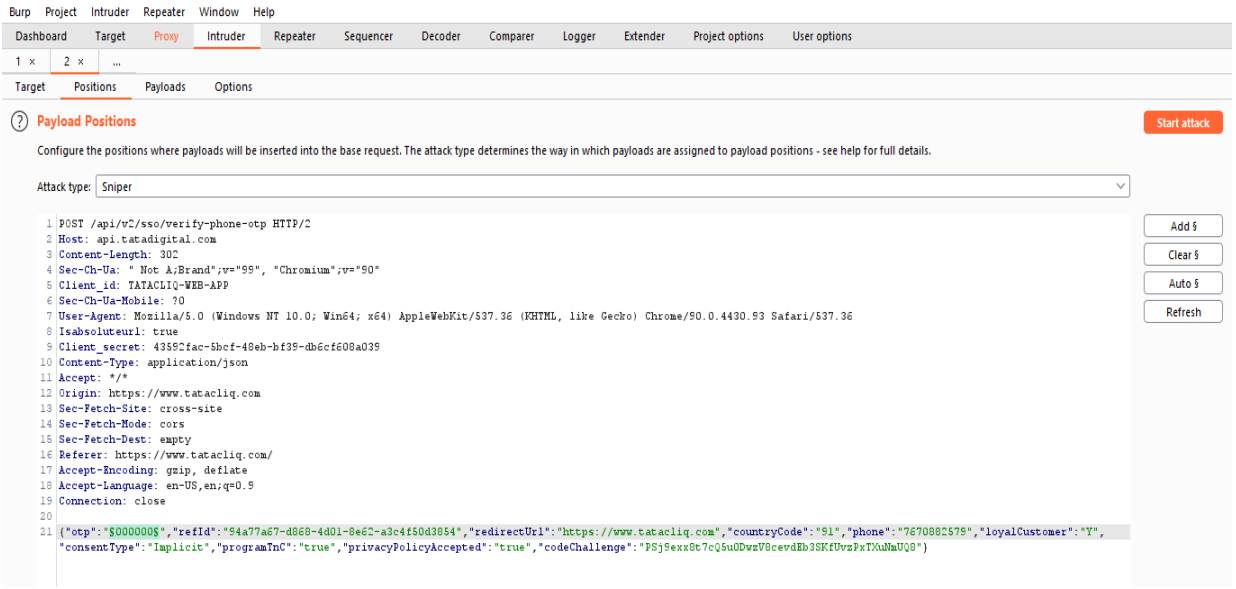

Figure 18: burp suit intruder tool page

Figure 17 represents the positions in the intruder tool that it can use to select the type of attack. We selected the type of attack as a sniper. Here we clear all the $ in the last line of the interface.

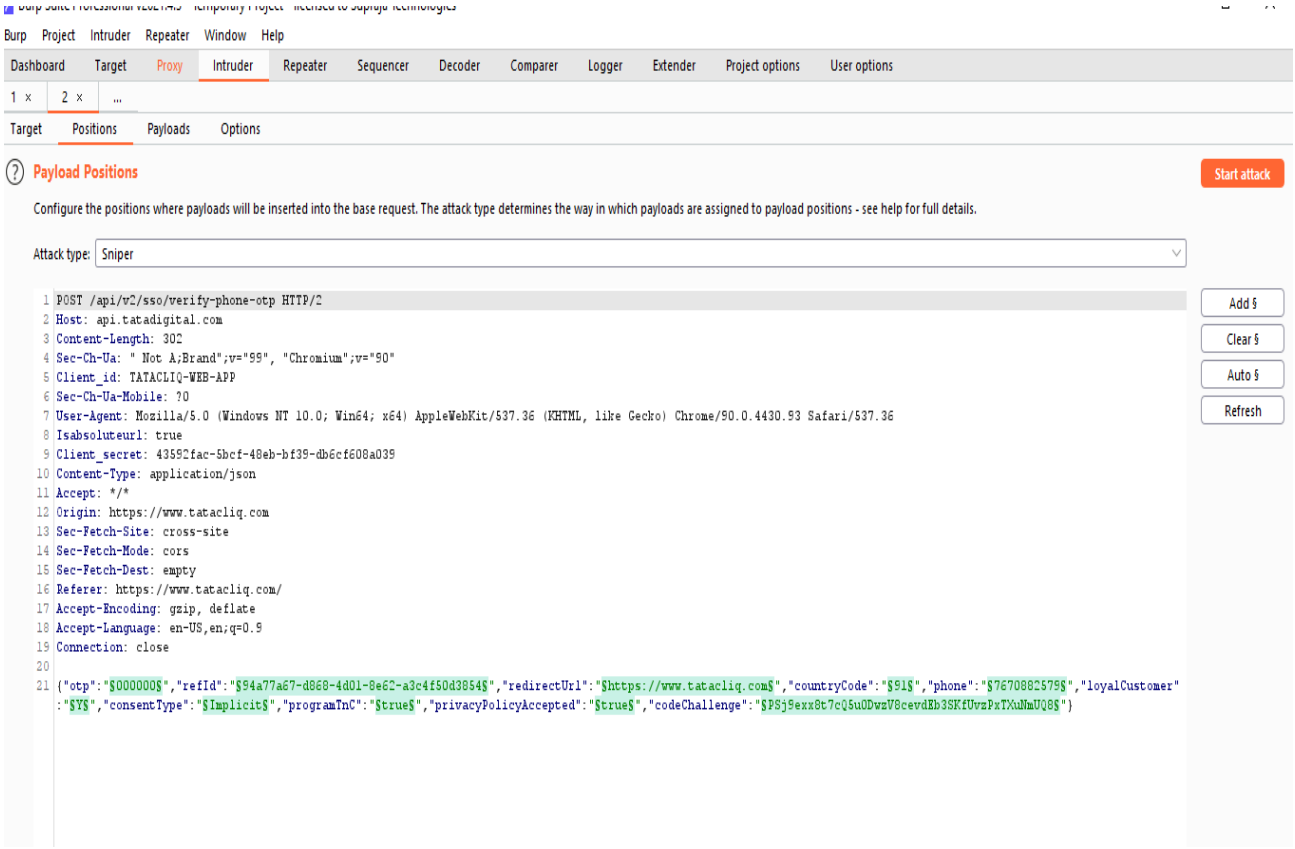

Figure 19: burp suit intruder tool page

Figure 18 represents the removed $ symbols and we need to add the $ here for the assumed OTP.

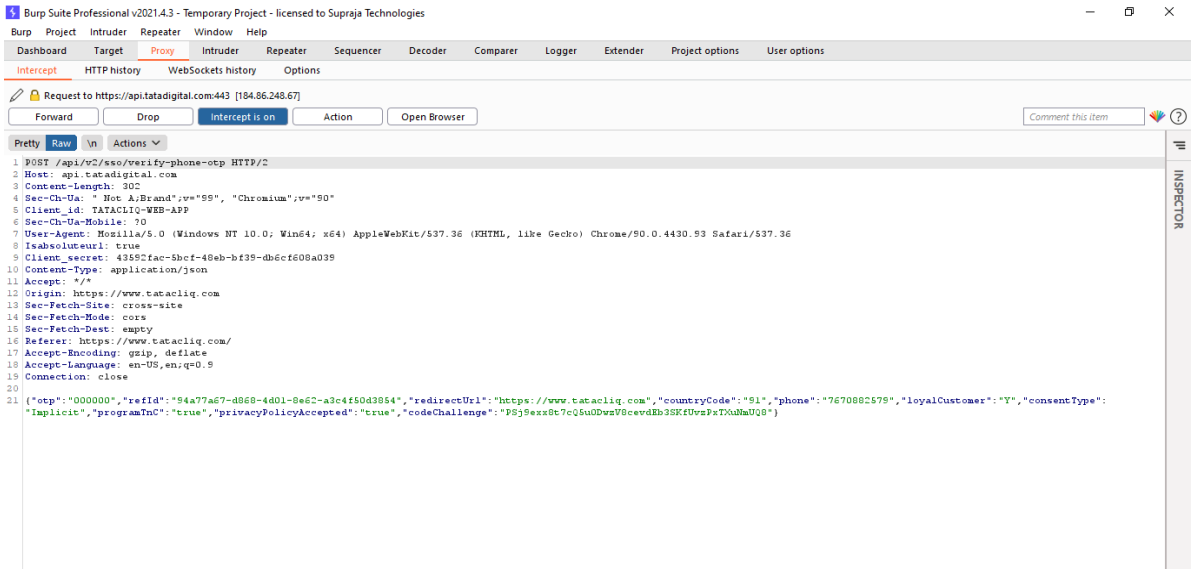

Figure 20: burp suit proxy tool page

Figure 19 represents the proxy tool page where the intercept is on-ed. Intercept is used to pause the current working website at the burp suite browser.

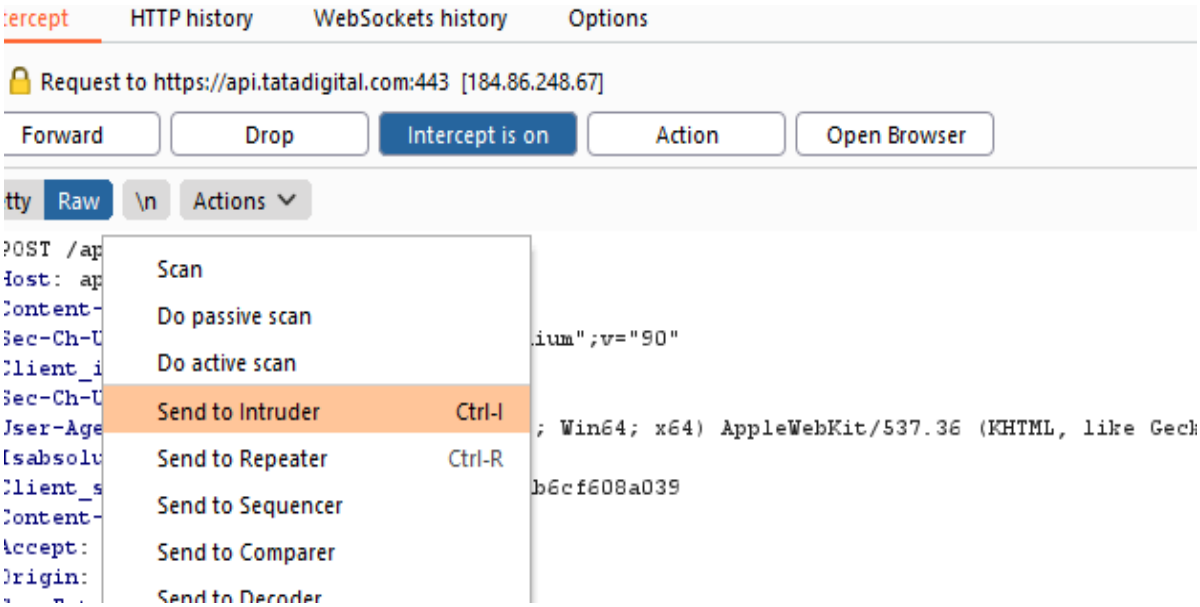

Figure 21: burp suit proxy tool page

On this page, we use to send the raw (or) dummy OTP to the intruder for finding the OTP.

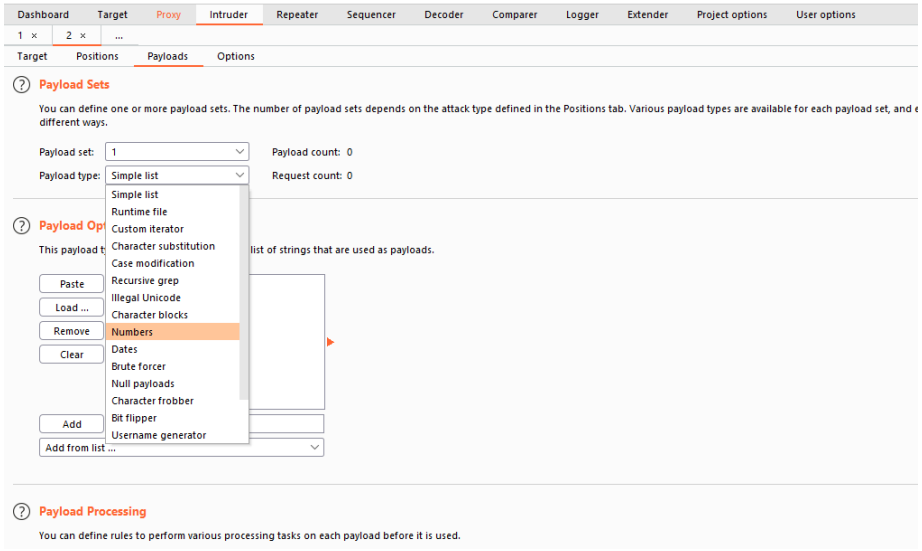

Figure 22: burp suit intruder tool page

Figure 21 represents the intruder tool page where the payloads place we can select the type of payloads and the range and it can able to report the count too.

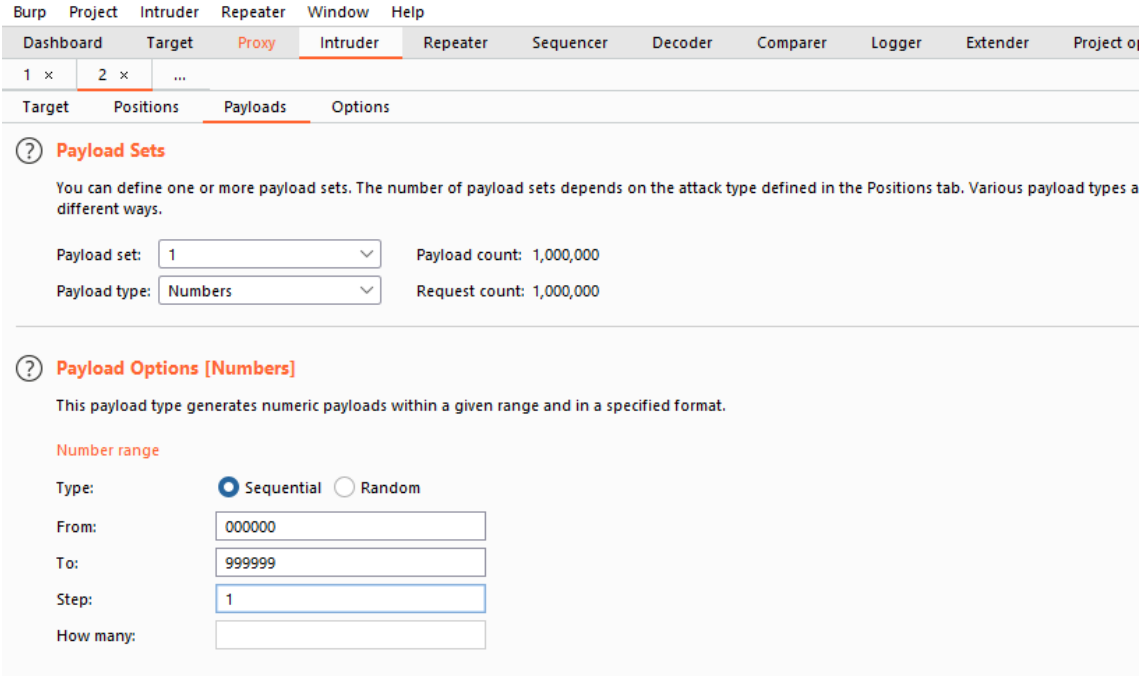

Figure 23: burp suit intruder tool page

Figure 22 represents the selection of payload options like number range and number format.

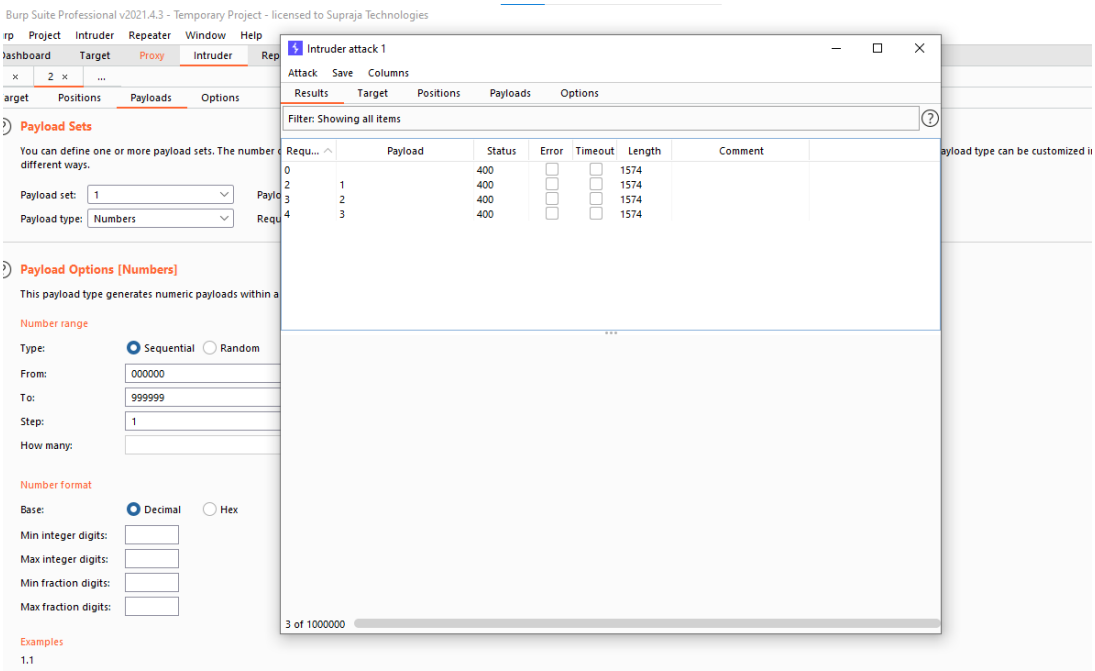

Figure 24: burp suit intruder tool page

Figure 23 represents the attack of the real OTP which is generated in the mobile of a particular person.

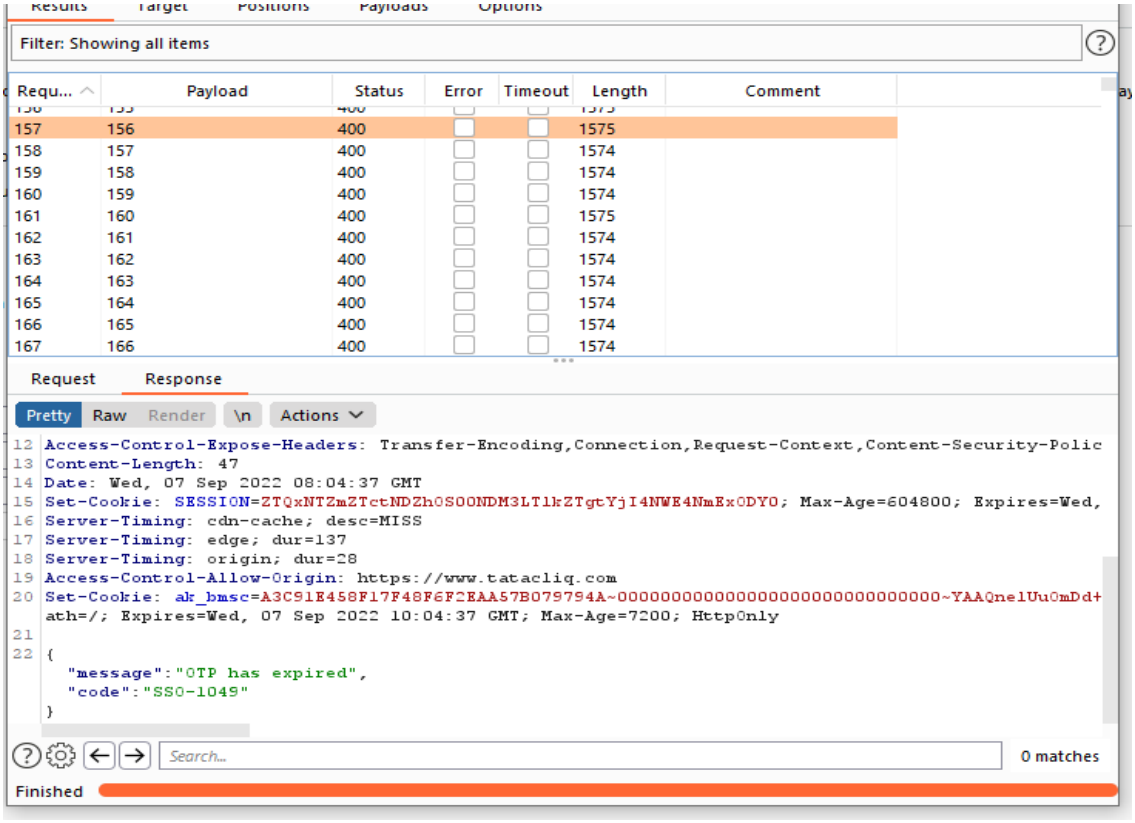

Figure 25: burp suit intruder tool page

Figure 24 represents the attack page where all the OTP combinations are generated. We need to select the OTP where the abnormal increase of the length is shown in the figure. So we choose the OTP.

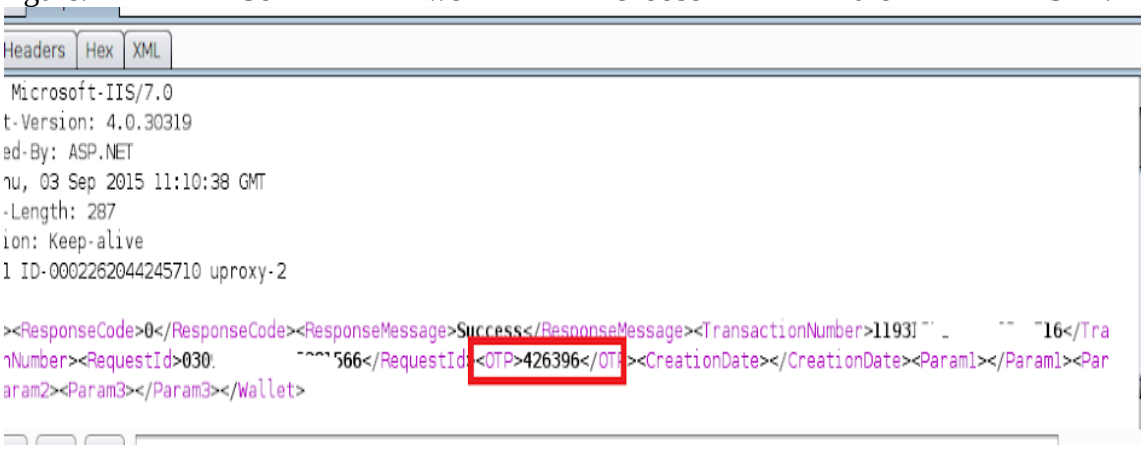

Figure 26: burp suit intruder tool page

This page represents the OTP generation in the response page of the intruder attack page. Thus the OTP has been given in the message as "OTP is successful" or "valid OTP".

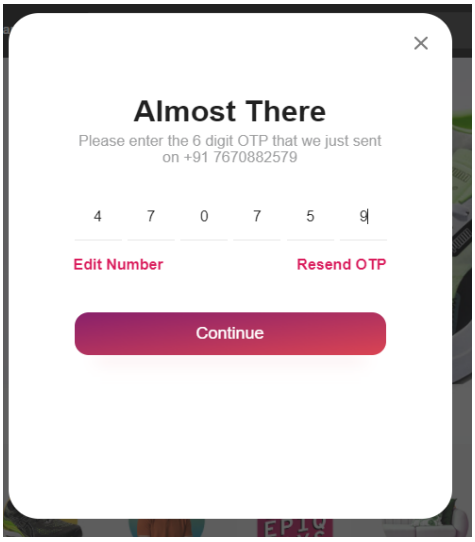

Figure 27: web page of tatacliq website.

Figure 26 represents the login page where the actual OTP (generated OTP) is entered. And click continue for logging into the website.

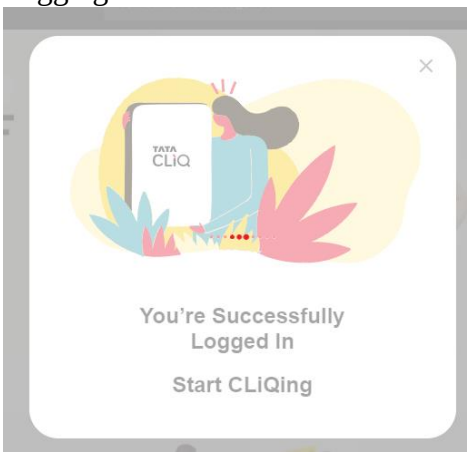

Figure 28: log in pop up

Figure 27 represents the successful logged in of specific users into the tatacliq website.

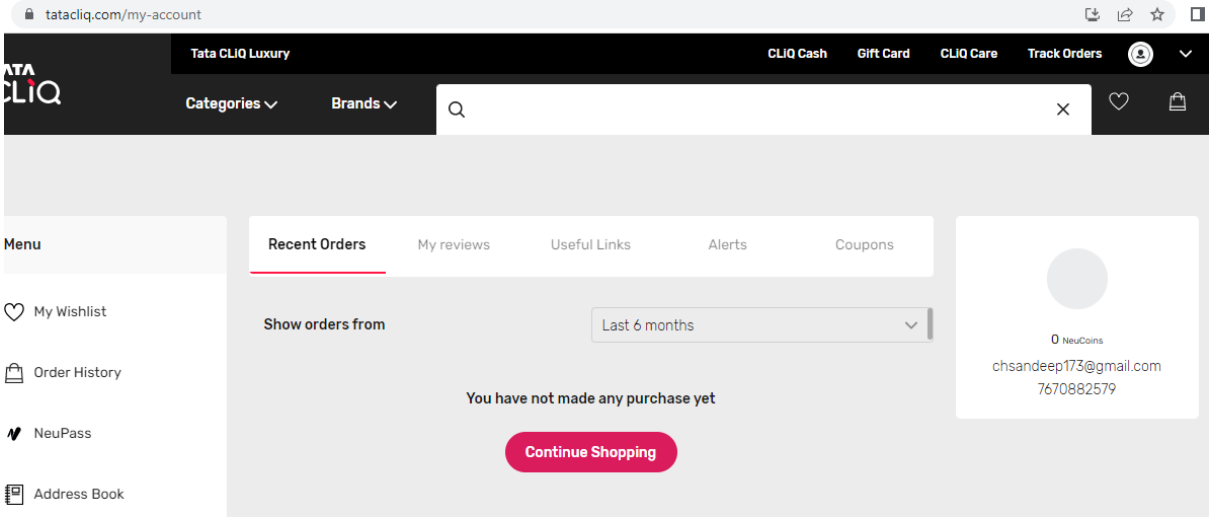

Figure 29: TataCliq website

Figure 28 represents the successfully logged-in page where it used to purchase on this website.

Conclusion

The project sought to get some awareness of the OTP bypass attack among normal people by getting so they will know what is meant by an OTP bypass attack. The attackers use so many different types of tools that which you can get knowledge about how the attackers will work. So, in this, some websites and applications are has a basic login page as a mobile number and OTP with knowing the mobile number yours the attackers start an attack on your social media accounts to get the personal credientials of yours and they will sell it in the dark web otherwise they will blackmail you. If any private things are found in your account .they will publish in public or they will harass you and do some criminal things. Let's see how the attackers start an attack on you. They will get your mobile number of yours and start an attack on you. If you are entered in any website that has no time limit to enter the OTP then you are in the hands of hackers they will monitor you so you must have to be safe on it. So, this is the reason the website and applications have a time limit for the OTP. But even some websites do not have a time limit .some other websites have a the time-limit of 2 to 3 minutes. For that the beginner hacker cannot get it, if the hackers are professional hackers they can sufficient with that 2-minutes to enter into your account of any websites. So, the top and most popular MNCs have used only a time limit of 30 sec. If the hacker has tried to enter into the website which has a 30-sec timelimit. So, their process in the tools is automatically terminated by themselves. If the time limit is reached to 30 sec. So, the company and any other business websites must keep inn the time limit of otp is just 30 sec. Then the hackers cannot log in to their users of the websites and companies. so, please use the websites which have a maximum time limit for OTP. Then you will be protected from hackers."Be brave while using the technology." Hacker's motto: "Information is wealth."

References

In[1] Brute-force Attack, https://en.wikipedia.org/wiki/Brute-force_attack

In[2] Social Engineering, https://en.wikipedia.org/wiki/Social_engineering_(security)

In[3] Payment Card Industry (PCI) Data Security Standard, "Requirements and Security-Assessment-Procedures", May 2018 https://www.pcisecuritystandards.org/document_library

In[4] SecureString Class, https://docs.microsoft.com/en-us/dotnet/api/system.security.securestring?redirectedfrom=MSDN&view=netframework-4.7.2.

In[5] System.Security.Cryptography.RNGCryptoServiceProvider class, https://docs.microsoft.com/en-us/dotnet/api/system.security.cryptography.rngcryptoserviceprovider?redirectedfrom=MSDN&view=netframework-4.7.2

In[6]Securing-Vulnerable-Web-Applications:https://webthesis.biblio.polito.it/9578/1/tesi.pdf

In[7]Three-Layer-Defence_in_Authentication_Mechanism https://www.ijres.org/papers/Volume-10/Issue-4/Ser-11/F10043238.pdf

In[8] Menggunakan Algoritma AES dan One-Time Password Studi Kasus https://pdfs.semanticscholar.org/f277/4330d1db92ab2db30e39f7622719bbab8ac1.pdf.