LONDON METROPOLITAN UNIVERSITY

islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CC5004NI Security in Computing

Assessment Weightage & Type

30% Individual Coursework 2

Year and Semester

2023 -24 Spring

Student Name: Raj Bhattarai

London Met ID: 22067111

College ID: np01nt4a220078@islingtoncollege.edu.np

Assignment Due Date: 7th May 2024

Assignment Submission Date: 7th May 2024

Word Count (Where Required):

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Table of Contents

Table of Figures.

1. Introduction.

A brute force attack is the process of hacking a computer system which uses the method of trial and error to crack passwords, login credentials, and encryption keys. Brute force attack is a simple but reliable way for getting unauthorized access to user accounts and organization's systems and networks. In brute force attack the hacker tries multiple usernames and passwords in order to find the correct combination of letters, numbers, and symbols. This process is greatly aided by the use of a computer to generate multiple random combinations of characters in order to gain the access. The name brute force comes from the attackers using forceful ways to gain access to the information systems and private networks (Fortinet, n.d.). Brute force at least in theory can be used to decrypt any encrypted data. Since brute force attack require the hacker to calculate every possible combination and checking each one as the length of the password increases the time to find the correct combination for the hacker increases exponentially (Kaspersky, 2018). What makes brute force attacks unique in a way is that the attack does not rely on the vulnerabilities on the system or the network or exploit sophisticated techniques. Instead, the attack relies on the sheer volume of attempts to overwhelm the authentication mechanism present in the system. With higher computational power the automated tools and software attackers are able to execute brute force techniques at scale amplifying the threat potential of the involved hackers. The resources required for a brute force attack rises exponentially with the increase I the key size. The attackers use brute force attacks mainly to crack passwords, Decrypt encrypted data, and gain unauthorized access to the systems, software , websites, and networks.

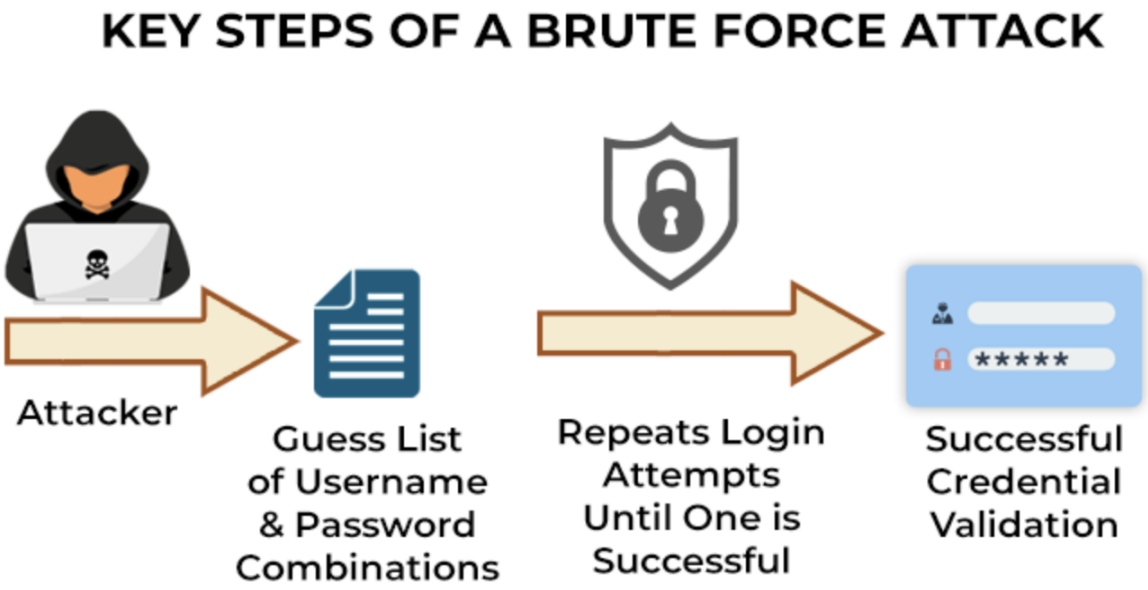


Figure 1: a figure showing how brute force attack works.

In this report we will delve deep into the intricacies of brute force attack on information technology devices and systems. Through various means we will demonstrate a brute force attack and analyze the mitigation methods in order for us to understand more about this method of hacking and be well prepared to safeguard against the hackers employing brute force attacks. As Sun Tzu once said “If you know your enemy and yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.” (Tzu, n.d.). Therefore, by understanding the inner workings of the brute force attack we can fortify our defenses and safeguard against such cyber threats.

Statistics of brute force attacks and cyber-crimes in general:

1. 6% of network intrusions worldwide were caused by brute force attack.

2. In theory brute force attacks are the best cyber-attack method as it has a 100% success rate in theory but realistically about 80% in cracking passwords especially in web applications and services.

3. In 2020, FBI reported that annually cyber-crimes and attacks caused damages worth 4.2 billion dollars rising the five year total to 13.3 billion dollars.

4. Brute force attack rose 671% in 2020. (hill, 2020)

5. On average 10% of companies experience a brute force attack every week.

6. 71% of all data breaches are financially motivated.

7. 80% of hacking breach relies on brute force attacks.

8. 83% of Americans create weak password both in length and complexity and 53% of Americans use the same password in multiple different sites and services.

1.1. Aims and objectives.

The main aim of this course work is to be to *research*, *describe*, *analyse*, *evaluate*, to *demonstrate* and to provide *mitigation* techniques and cases for brute force attacks to the information technology systems.

The various objectives of this coursework are listed below.

1. Learn what brute force attack is how it is performed and know about the various methods and types of brute force attacks.
2. Analyse the vulnerabilities of the information system from which the hackers are able to breach using brute force attack.
3. Demonstrate the findings and perform brute force attacks in a secure environment.
4. Find the mitigative measures of the attack to be better protected against these types of exploits.

2. Background.

The evolution of information technology has revolutionized the way that individuals, businesses, and societies operate, communicate, and interact fundamentally changing the landscape of modern society at large the presence of these technology has made the world more interconnected. This makes the world incredibly vulnerable since massive amount of information about an individual are Heald in these devices which are exploitable. Brute force attacks are incredibly common in the early phases of cyber kill chain, such as reconnaissance and invasion. The attackers are required to gain an access point into their victim's system, most brute force hackers employ the philosophy of set and leave to get access to the victim's server. The real threat then continues as hackers compromise the encryption operations in the victim's computers making the hackers freer to conduct their tasks. (Basumallick, 2022)

The cyber criminals employ the methods of using scripts and programs as brute force weapons. To get around the authentication process these tools use a variety of password protections in some cases the attackers will look into various factors of assonating the correct session id of the victim. Though some hackers use the brute force methods manually nowadays due to computers hackers have employed the use of bots in almost all brute force cases. Automated programs are used widely as to predict all the default combinations till the username and password inputted into the system is correct. It is difficult to estimate the time required to crack the password using brute force method. As weak passwords may be compromised in just a few seconds while a strong password like mine might require hours if not days to break into. Many big organizations and co operations use very strong passwords consisting of letters numbers and symbols in order to safeguard the system and buy more time to prepare for resistance towards the data breach.

2.1. Types of Brute force attacks.

Brute force attacks might utilize various ways and tactics to break into the computer system. The various brute force attacks are listed below .

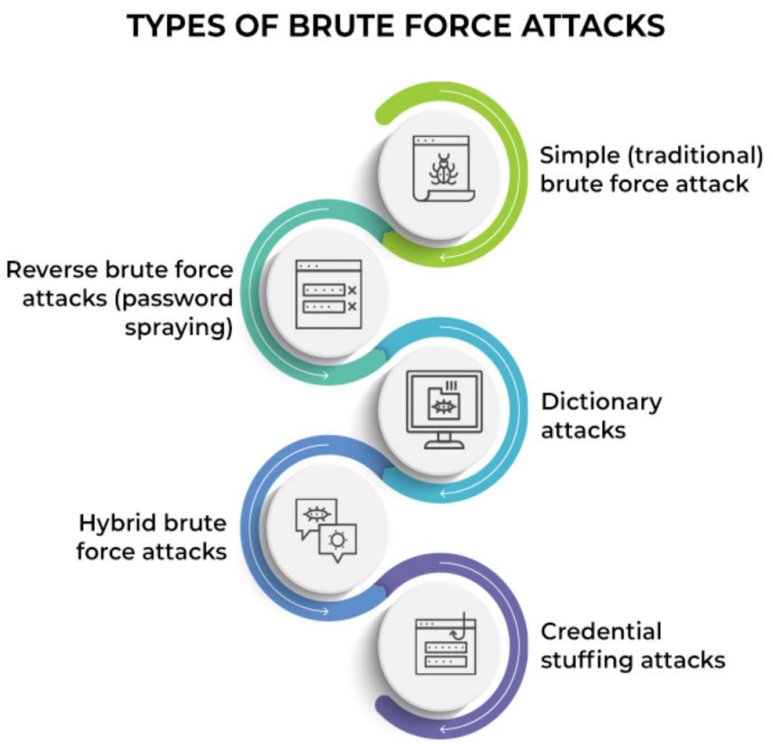


Figure 2: Figures showing the types of brute force attacks.

1. Simple or traditional brute force attack.

   Simple brute force attack is a type of brute force attack where an attacker guesses many passwords to target a specific individual and repeat the process of guesswork until the password is compromised. In this type of brute force attack the attacker employs the use of various password attempts to target a certain individual through the use of random assortment of characters. This method is incredibly time and resource intensive as it requires creating every combination of characters, numbers, and special characters. Due to this very reason this type of brute force attack is incredible in order to break into shorter passwords and is very hard against longer passwords. (Rajput, 2023)

Figure 3: Basic or Traditional brute force attack.

2. Reverse brute force attacks.
   Reverse brute force attacks are exact opposite to the simple brute force attack. In this type of brute force attack the attacker uses a targeted number of passcodes to predict multiple potential identities in a credential spraying attack. The attacker employs the method of spraying pre-determined set of passwords while cycling through their vast list of user IDs and passcodes and wait to see which hits the home run. In this case the hacker already knows your old password. Hackers may use the older password to look into database to make a calculated guess about your new password. (Gillis, 2017)

3. Dictionary brute force attacks.
   Dictionary brute force attacks are the types of brute force attacks where the hacker uses a pre-defined collection of popular slang and phrases which are found in a dictionary format. This type of brute force attack is more complicated and specializes on the individual than a direct brute force attack. To employ this strategy the hackers, use all phrases and character sets and employ the use of password cracking tools and wordlist producers. Since this brute force approach is tailored for a certain individual the examination of the victim's profile is vital for the hackers. They find the individuals work, passions, family members, birthdays, hobbies and add these phrases to create a more focused attack. (Aakashpa, 2022)

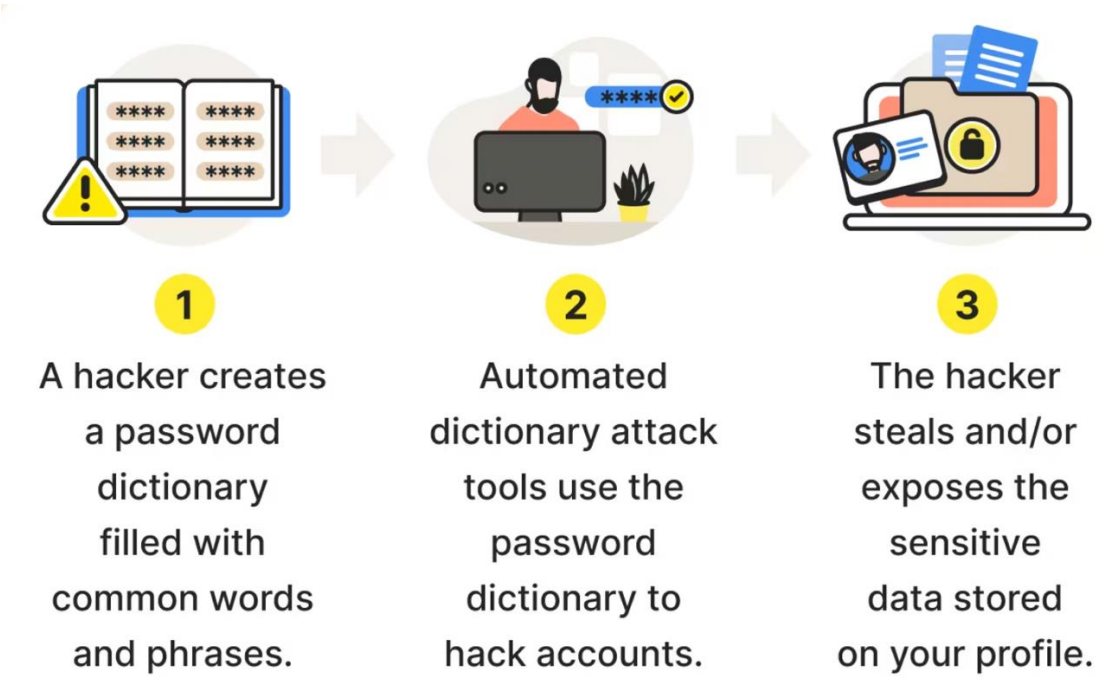


Figure 4: Figure showcasing how dictionary brute force attack works,

4. Hybrid brute force attacks.
   Hybrid brute force attacks are the type of brute force attack where two different kinds of brute force attacks are merged. An example of this could be a hacker using dictionary and reverse brute force attack in conjunction. Where the hacker gains the important intel about the victim's identity and uses password spraying technique in order to compromise the passcode protecting their device. (Rajput, 2023)

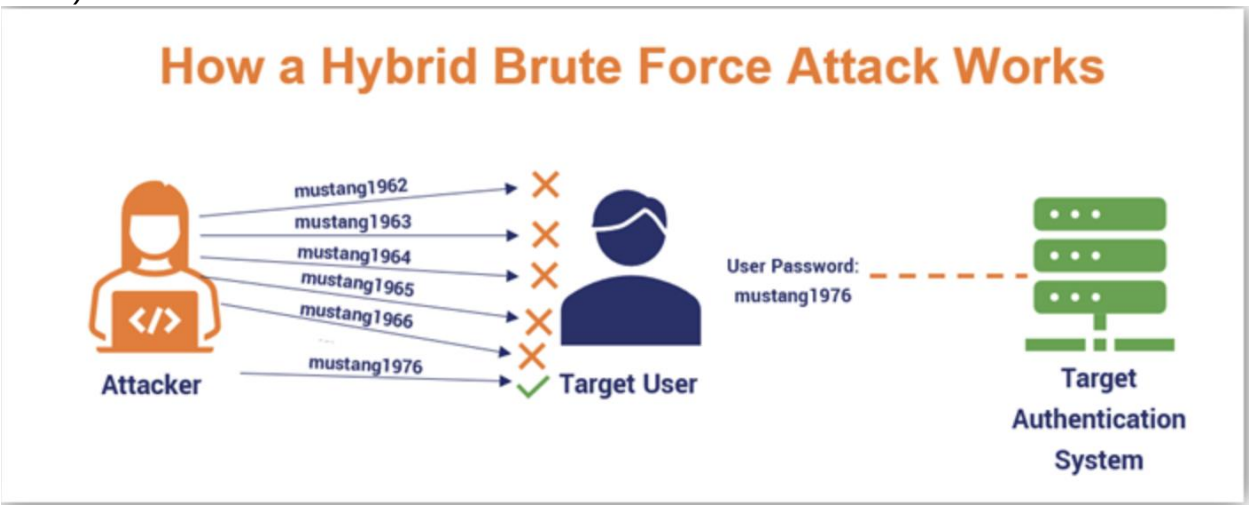


Figure 5: Picture showing how hybrid brute force attack works.

5. Credential stuffing brute force attacks.
   Credential stuffing brute force attacks are the types of brute force attacks where the attacker entails a cybercriminal regularly “stuffing” identified passwords into the login fields on various sites. This act shows known passwords to the test on various websites. In theory the hacker will get unlawful access to some or all of the applied websites. This type of brute force attack relies heavily on botnets to get unauthorized access to multiple different websites by using the stolen information from a directory. It exploits a flaw in human psyche where an individual uses the same passwords on various different sites and platforms.

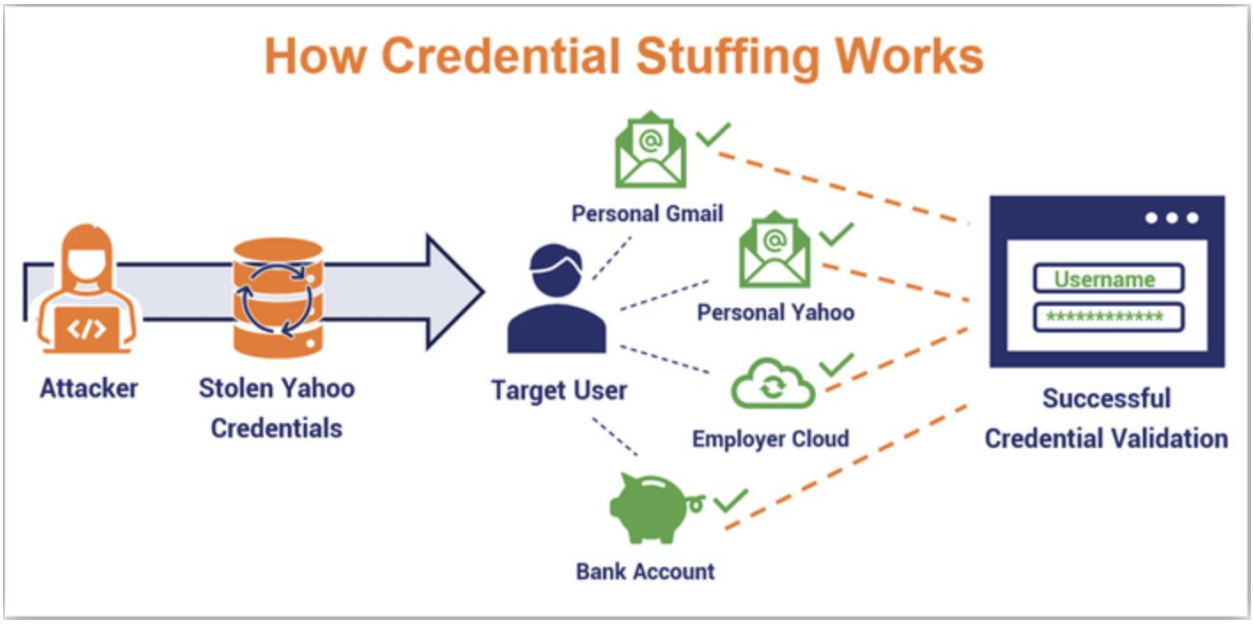


Figure 6:a figure Credential stuffing works.

2.2. How is brute force attack conducted.

Brute force attacks can be done manually too though it is a very tedious process and requires multiple individual large amounts of time to crack a single password. Many hackers choose brute force attacks as it is well known that most Individuals Create a weak password. In addition, many account credentials include the personal information which could be a clue to the individuals passcodes like user’s name, birthdate, hobbies, anniversaries, and interests. Due to the advent of technology giving rise to the computational power and rise in technological know-how hackers are using various tools and services to perform brute force are learning about the subject like us are given below:

1. Hash cat.

Hash cat is a penetration testing platform which facilitates the users to use known hashes which are a password ran through a formula and are converted to a string of random generated characters not changing the length of the characters irrespective to the change in the data contained by the password. Once the hashes are found the directory can help to revert the password to human readable text. (Magunsson, 2024)

2. Jhon the Ripper.

   Jhon the Ripper is an open-source software which allows the users to run dictionary attacks ad detect weak passwords through multitude of methods regarding various cracking and decryption techniques. (Magunsson, 2024)

3. Aircrack-ng.

   Aircrack-ng is an open-source software just like Jhon the Ripper which specializes in penetration testing of wireless network security through the employment of dictionary attacks against network protocols. (Magunsson, 2024)

4. Rainbow Crack.
   Rainbow crack is a widely used brute force tool which is mainly used for password cracking. The tool generates a rainbow table to use while performing the brute force attack. Since rainbow tables are pre-computed the tool it provides helps us in reducing the time required while conducting the brute force attack. (Shankdhar, 2020)

5. THC Hydra.

   THC Hydra a well-known and popular tool for pen testers focuses on cracking passwords of well protected network authentications by performing brute force attacks. THC Hydra helps in performing dictionary attacks against more than 30 protocols which includes Telnet, HTTP, SMB and many more. (Shankdhar, 2020)

2.3. Brute-force attack cases.

There are various brute-force attacks targeted towards big organizations and firms. Some of the influential cases which redefined cybersecurity as a defensive mechanism some of these cases are mentioned below:

1. Dunkin Donuts.

In 2015 a brute force attack involving Dunkin Donuts took place. The hackers targeted Dunkin Donuts customer accounts through the use of previously stolen customer information and used those credentials to implement a brute force algorithm. The hackers were successful in their attempt as they gained the access to 19,715 user accounts from the customer loyalty application. The hackers gained tens of thousands of dollars' worth of customer cash rewards also known as loyalty rewards. This hacked caused Dunkin Donuts to face both legal and reputational consequences as Dunkin had to pay $650,000 in fines and damages. Dunkin Donuts later upgraded their security policies and reset all the user passwords. (Magnusson, 2024)

2. Alibaba.

   In 2016, Hackers took advantage of a breached database with over 99 million credentials for multiple web applications. The hackers used brute force approach using credential stuffing to access 20% of the accounts which they targeted. This resulted in over 20.6 million Alibaba accounts to be compromised. The result of this hack caused millions of individuals to get their personal information stolen including their credit card information and much more. (Magnusson, 2024)

3. Magento.

   In 2018, Magento a popular ecommerce platform suffered from a devastating brute force attack. With an agenda to steal credit card information of account holders and install a malware into the victim's devices to harness the computational power to mine crypto the attackers victimized over 1,000 different account credentials finding them from the dark web. Later Magneto found out that the breach exploited weak passcodes of their users. (ODOGWU, 2021)

4. Northern Irish Parliament.

   In 2018, Not even the government of Ireland was spared as hackers used brute force approach to compromise accounts of some of the most powerful individuals in the country. After investigations it was founded the attackers accessed the mailboxes of assembly members by simple brute force approach of trying various passwords as random letters. (ODOGWU, 2021)

5. Canadian Revenue Agency.

Even a powerful government like Canadian government could not escape a brute force attack in 2020. The attack on Canadian Revenue Agency compromised more than 11,000 accounts belonging to the CRA and other Governmental bodies. Investigations led to the conclusion that the attackers targeted CRA and GCKey through the use of previously stolen login information like usernames and passcodes to hack the already affected. (ODOGWU, 2021)

3. Demonstration.

1. Password brute force through the use of password change.

1. Step 1.
   Open burp suite and open a browser tab which has proxied to burp suite. Make sure the interceptor is off.

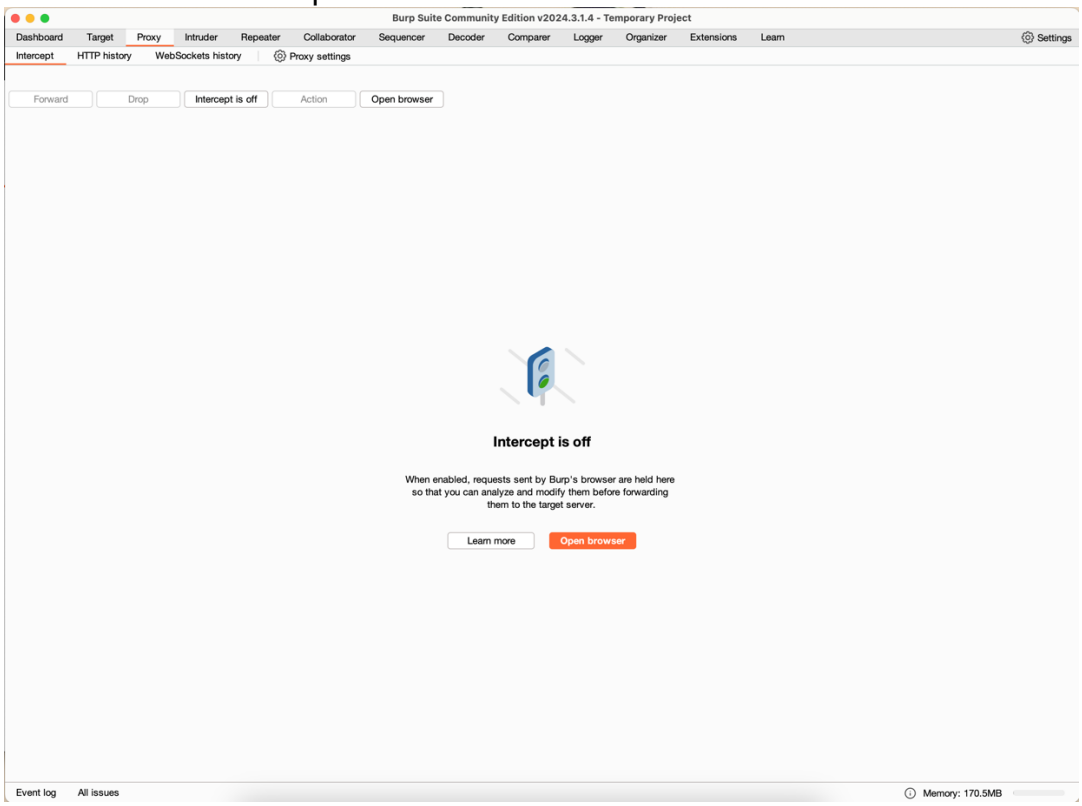


Figure 7: Step 1 preparation.

2. Step 2.
   Start port swigger through the proxy browser and access the given lab. Open the credentials password in a different tab. Then click on my account on the following page which will allow you to enter your credentials to login and login in with your credentials.

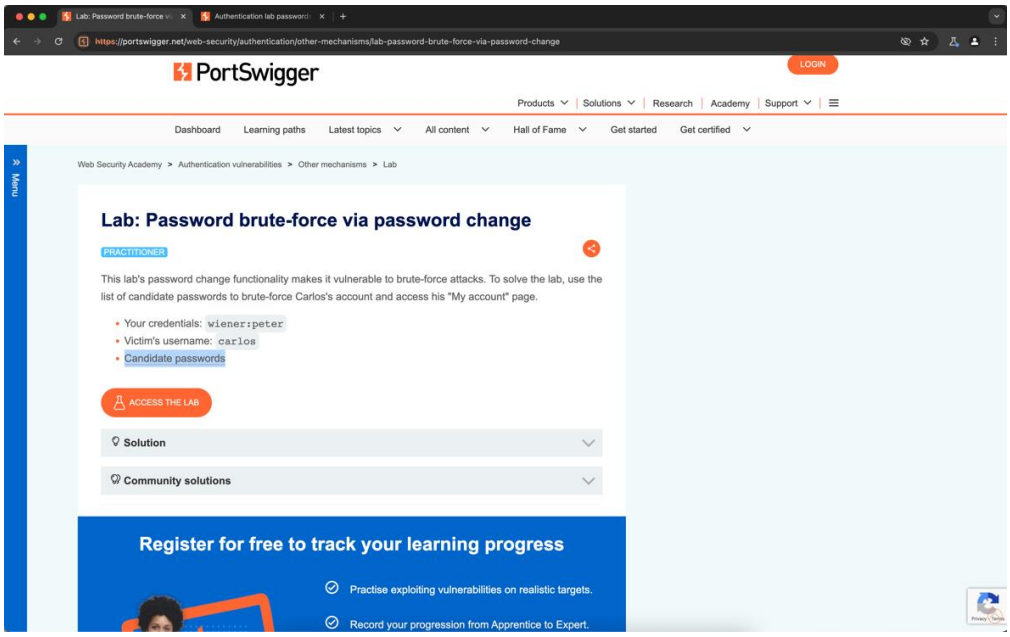


Figure 8: Step 2 Accessing the lab.

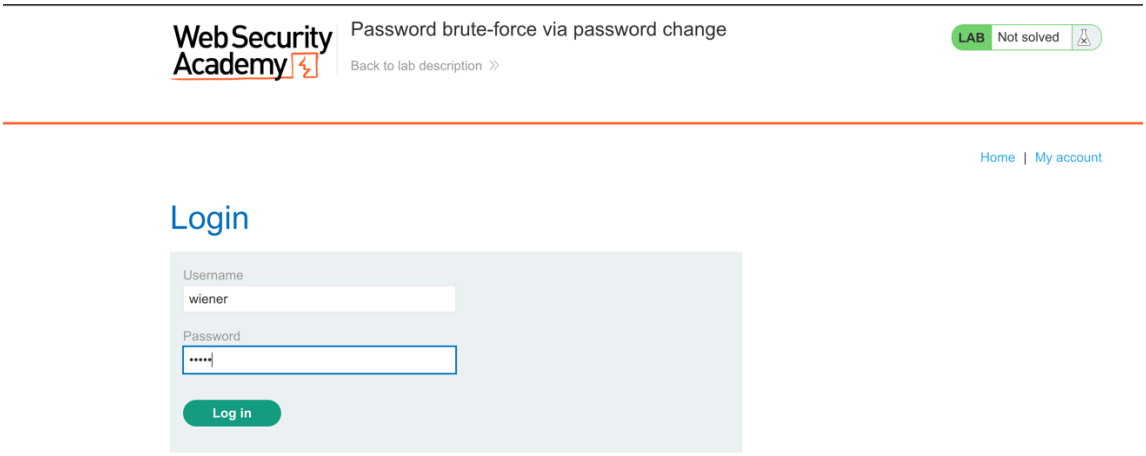


Figure 9: Step 2 part 2 logging in by using the credentials given.

3. Step 3.
   Change the password. For burp suite community users turn the intercept on and then change the password. Click on forward and turn the intercept off. This will update your password.

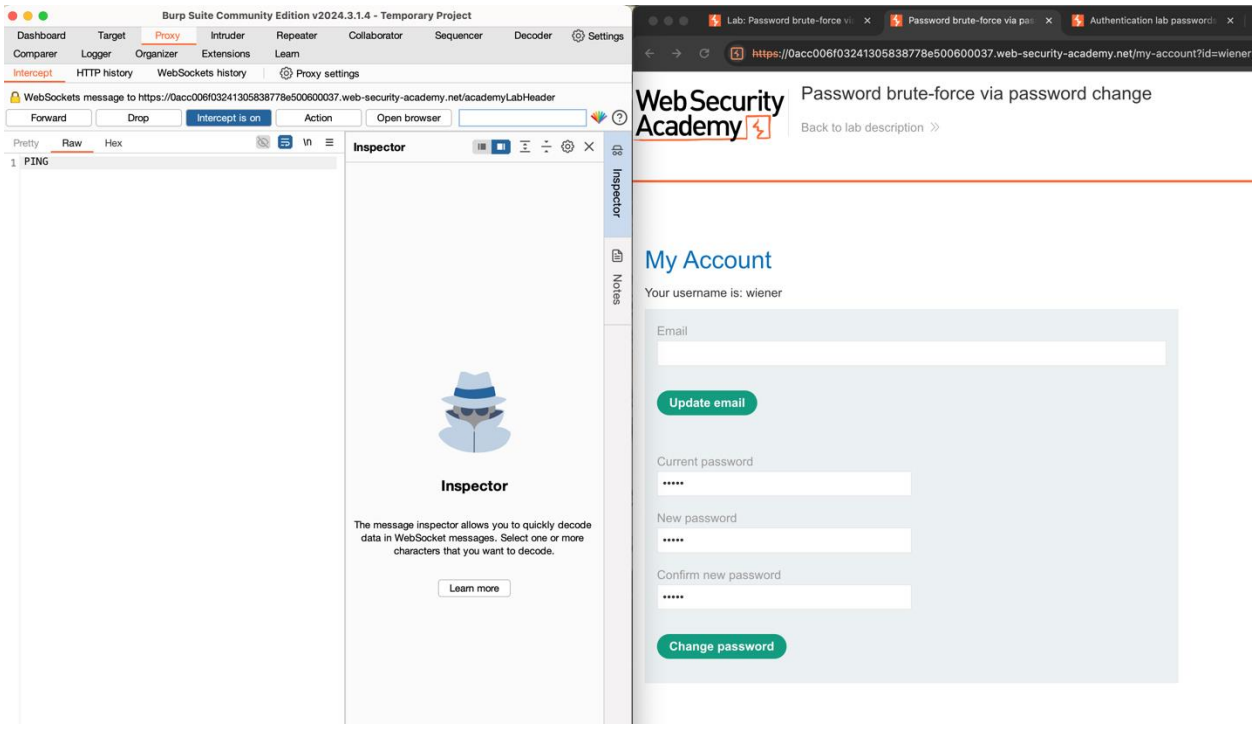


Figure 10: step 3 changing the password.

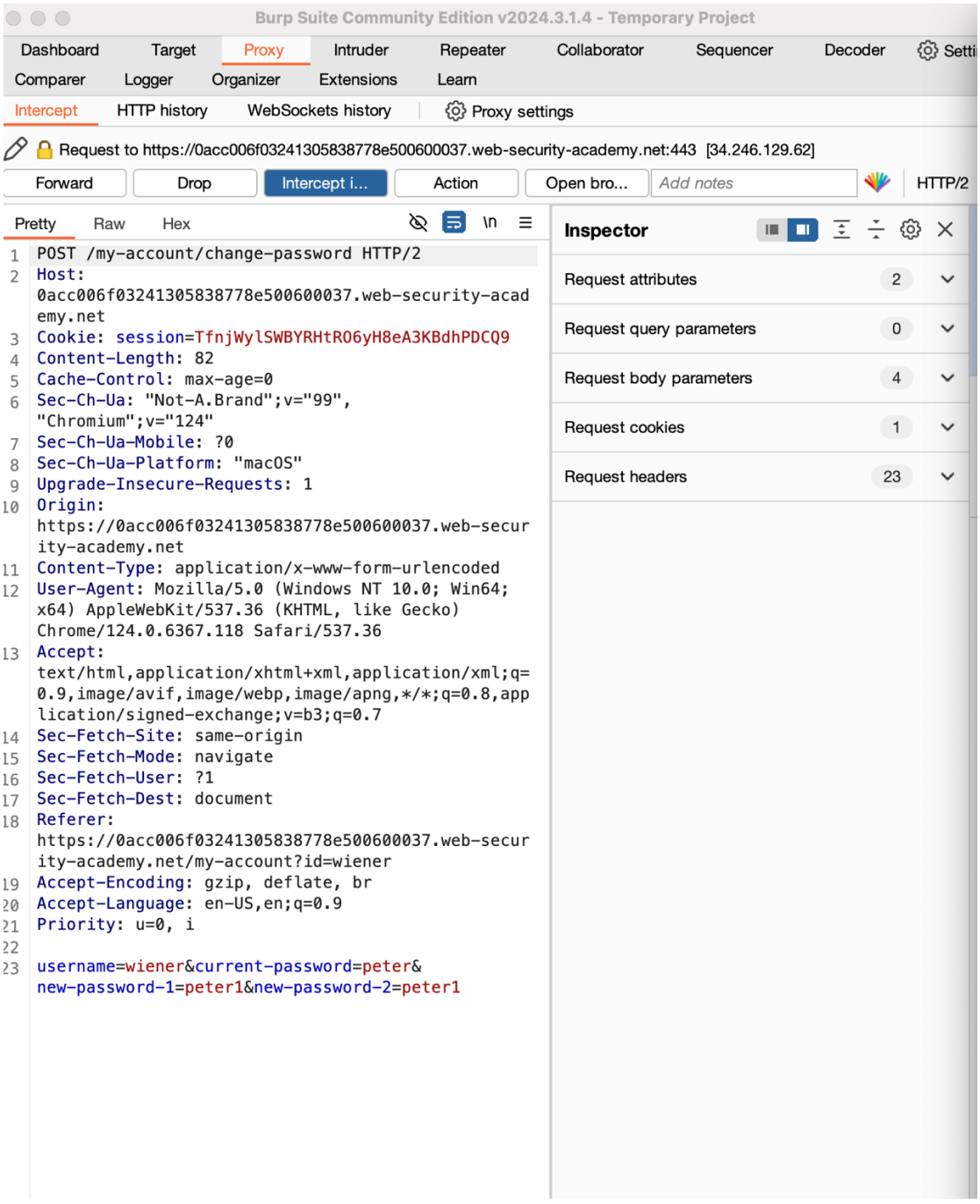


Figure 11: Step 3 part 2 showing the interception of the new password.

4. Step 4.

Try to change the password again but now use the incorrect password but same new passwords.

Figure 12: Step 4 using incorrect password to try and change the password.

5. Step 5.
   Again, try to change the password with different new non matching passwords and the wrong conformation password.

Figure 13: Step 5 changing the password with incorrect password and non-matching new passwords.

6. Step 6.

   Now change the password while using the correct current passcode but different new and confirm passcodes.

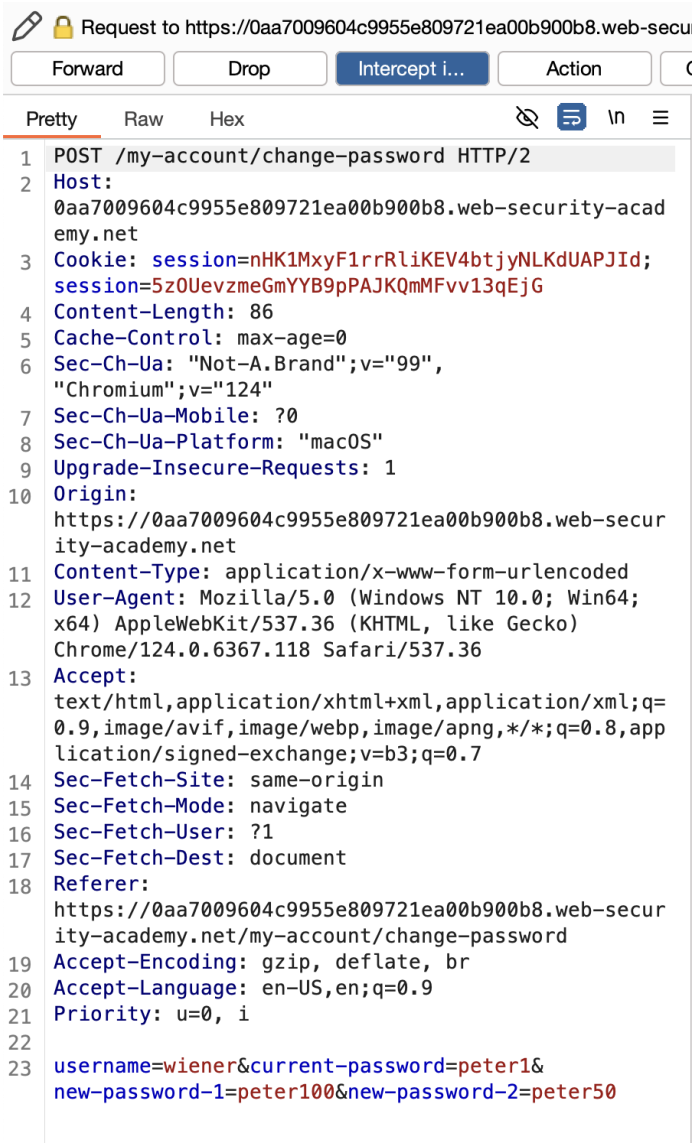


Figure 14: Step 6 Using correct password but non matching new password.

7. Step 7.
   Head over to proxy then search for the URL my-account/change-password and transfer the request to the burp intruder. Then click on payload intruder press clear on the left side of the screen and then press add on top of the clear button after pressing at the new password and change the username.

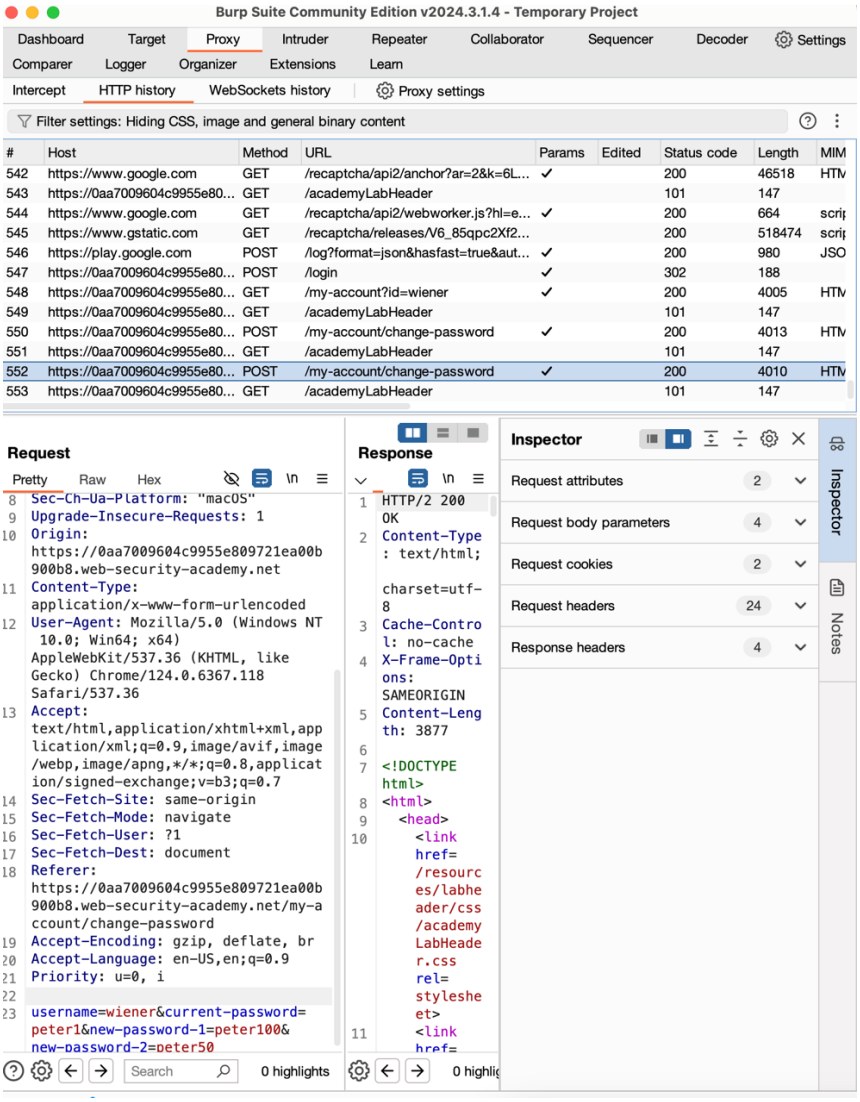


Figure 15: step 7 going through the request and transferring to intruder.

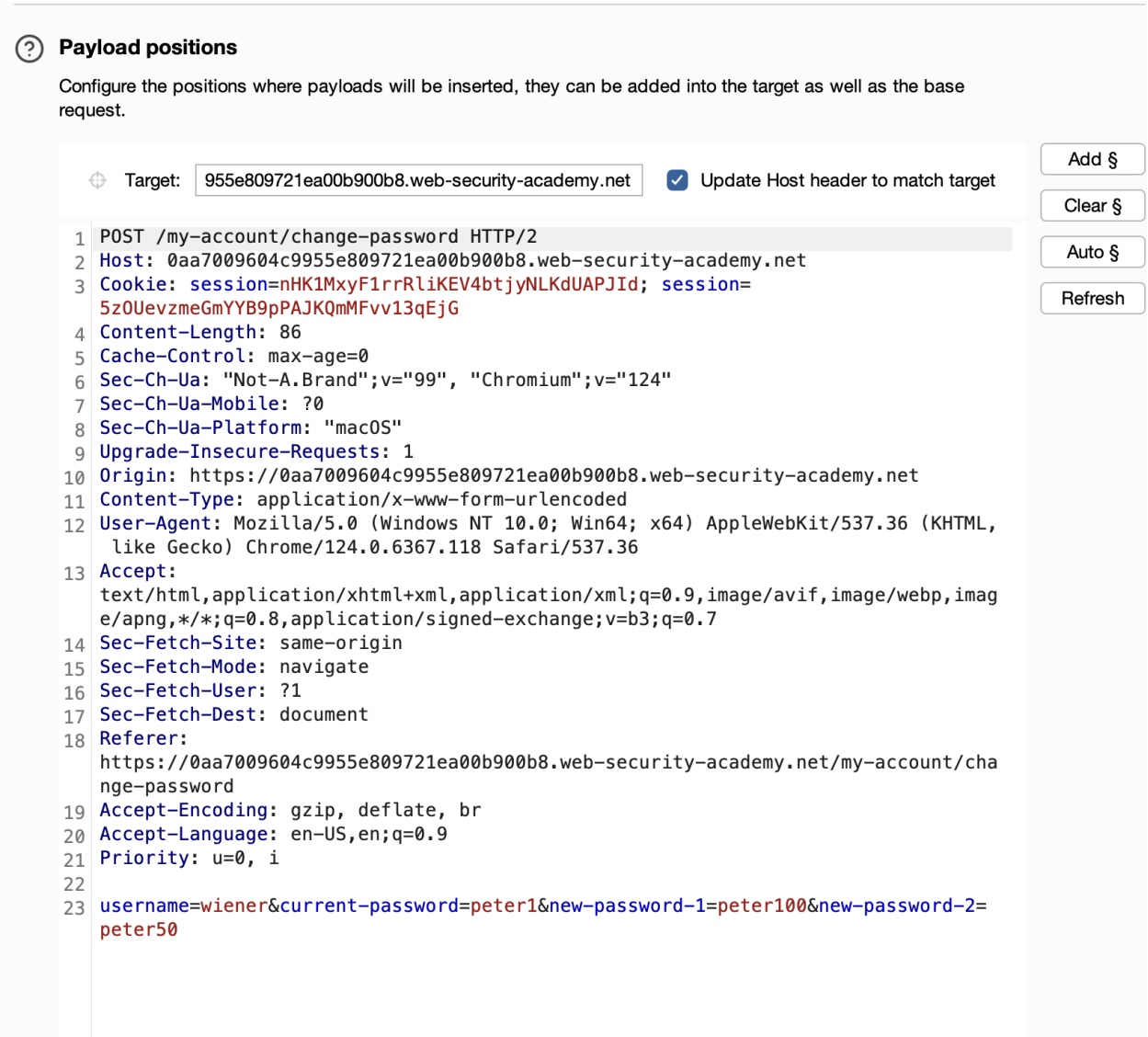


Figure 16: Step 7 part 2 payload pssition.

8. Step 8.
   Go to payloads and move the authentication lab passwords to the payload settings and go to the settings and clear the Grep match. Then start the attack.

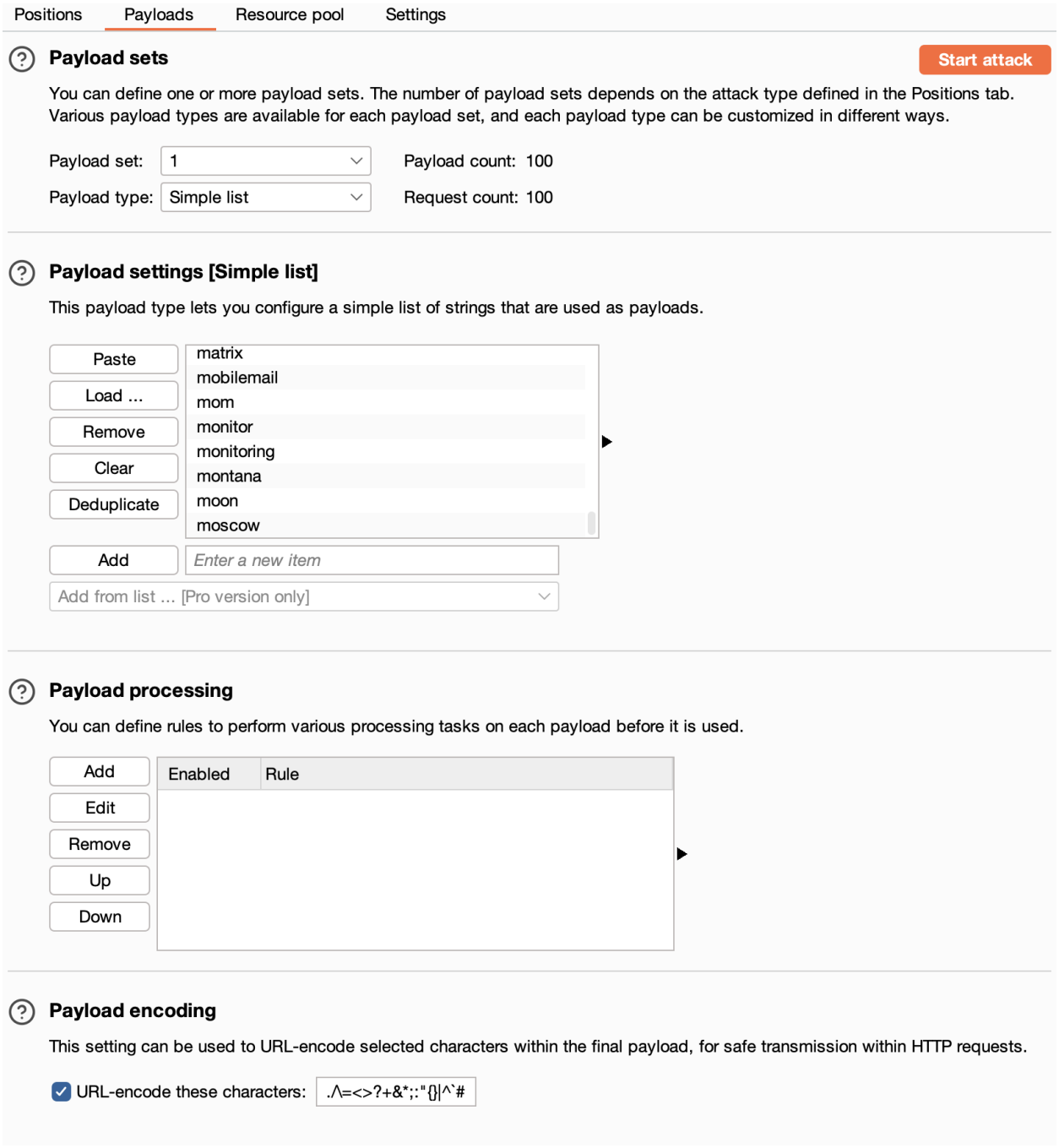


Figure 17: Step 8 setting in they payload.

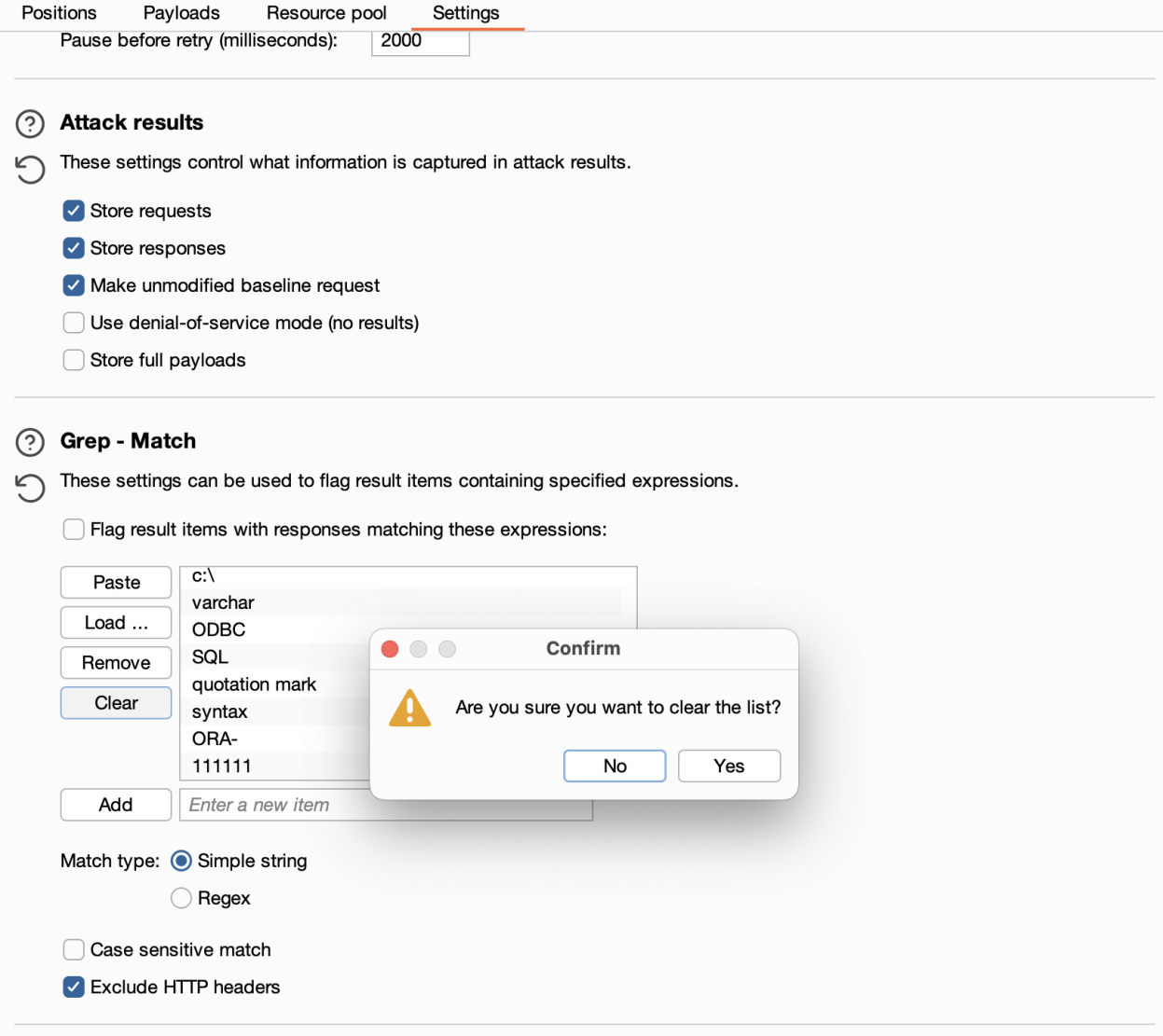


Figure 18: Step 8 part 2 clearing the payload from Grep - Match.

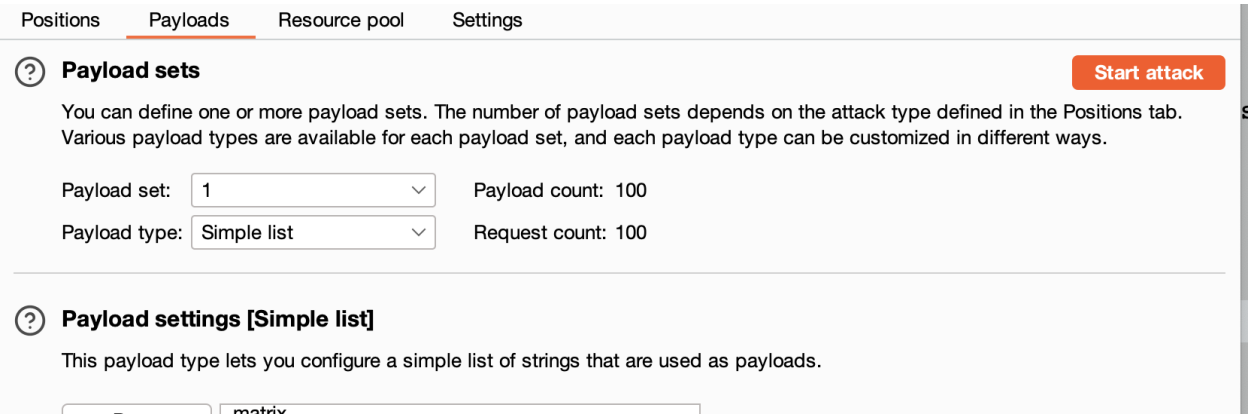
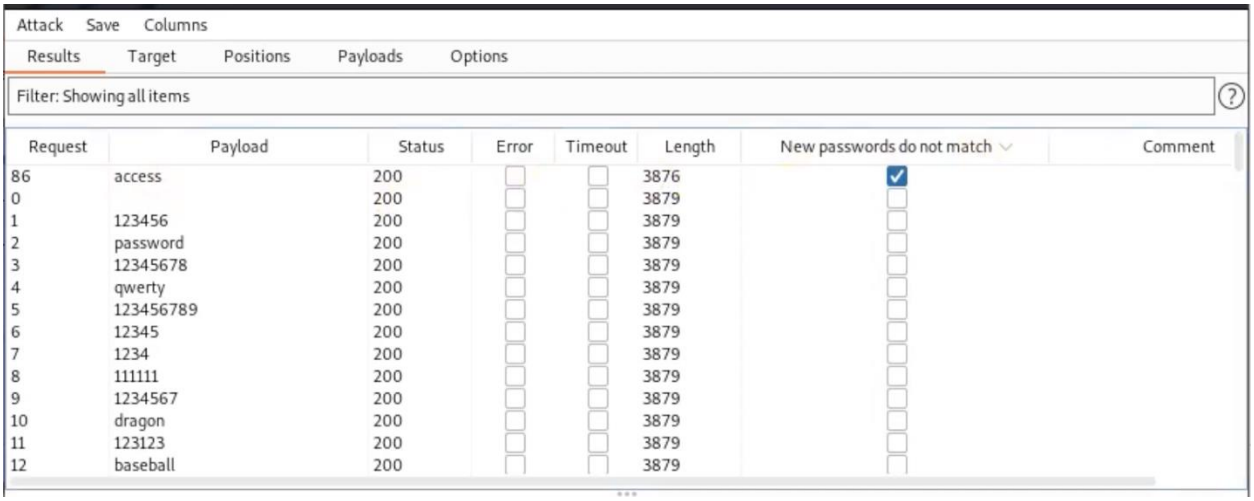


Figure 19: Step 8 part 3 Starting the attack.

9. Step 9.
   After the attack is completed you will see that tyou have gained the password. Note that this is your new password which you would be required to enter inorder to break into the system.



Request	Payload	Status	Error	Timeout	Length	New passwords do not match	Comment
86	access	200			3876	☑	
0		200			3879		
1	123456	200			3879		
2	password	200			3879		
3	12345678	200			3879		
4	qwerty	200			3879		
5	123456789	200			3879		
6	12345	200			3879		
7	1234	200			3879		
8	111111	200			3879		
9	1234567	200			3879		
10	dragon	200			3879		
11	123123	200			3879		
12	baseball	200			3879		

Figure 20: Step 9 finding the password .

10. Result.
    The access has been gained by the use of password changing through the use of brute force method.

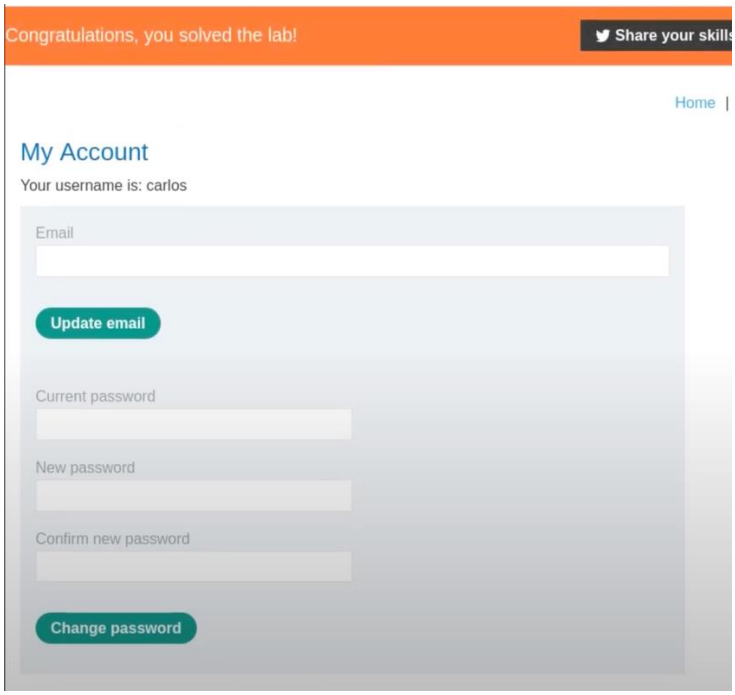


Figure 21: Result for Password changing method.

2. Bypassing Graph QL brute force protections.

1. Step 1.

   Log in into burp suit open the burp suite proxy browser try logging in with the wrong credentials. Use random login credentials to test the response of the login page.

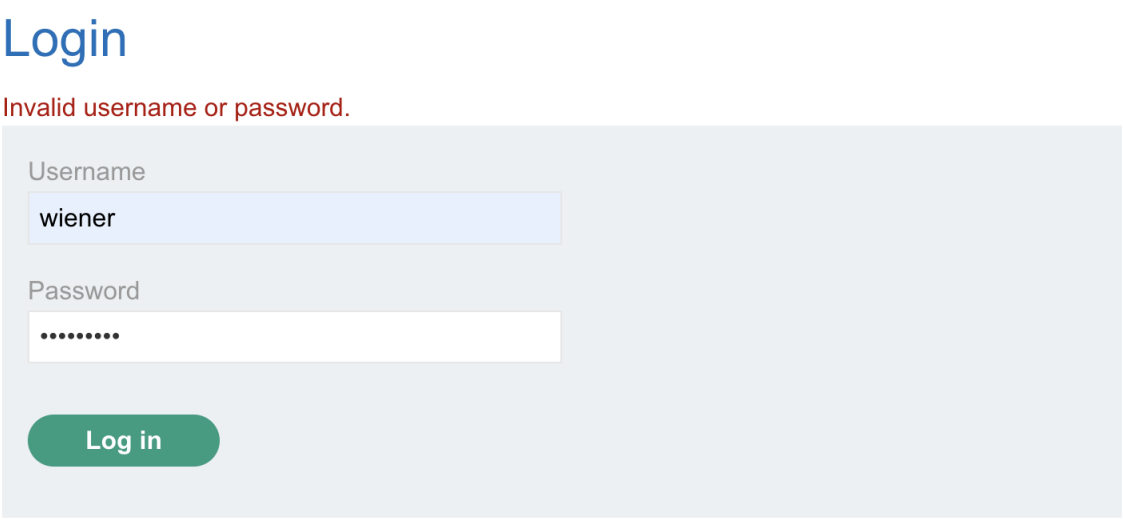


Figure 22: Step 1 using random password in login page.

2. Step 2.
   Go to burp suite and open Http history, open URL /graphql/v1 and send the request to the Repeater.

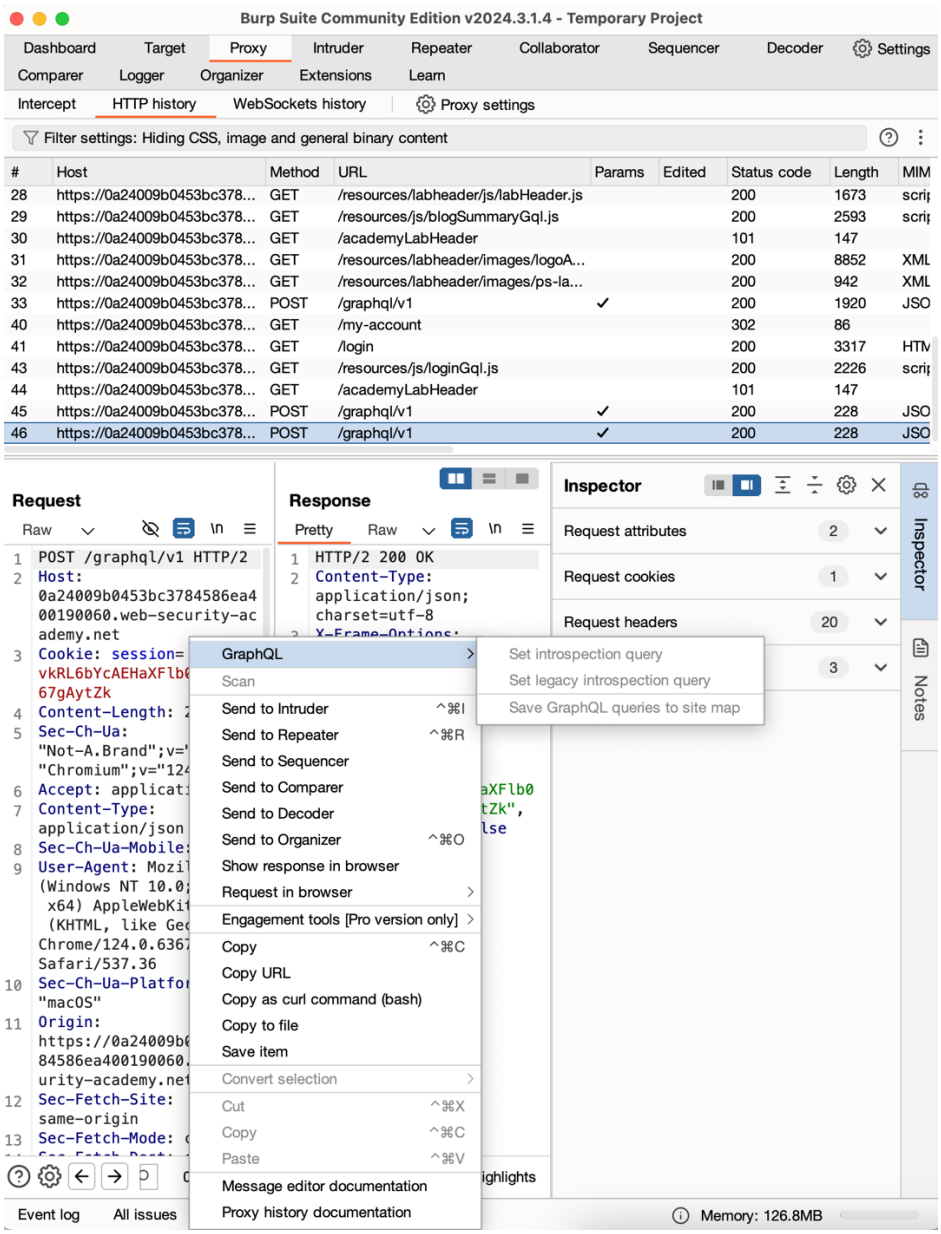


Figure 23: Step 2 Sending the proxy request to the repeater.

3. Step 3.

Head over to the repeater and go to Graph QL and watch the response you might get a penalty for multiple attempts.

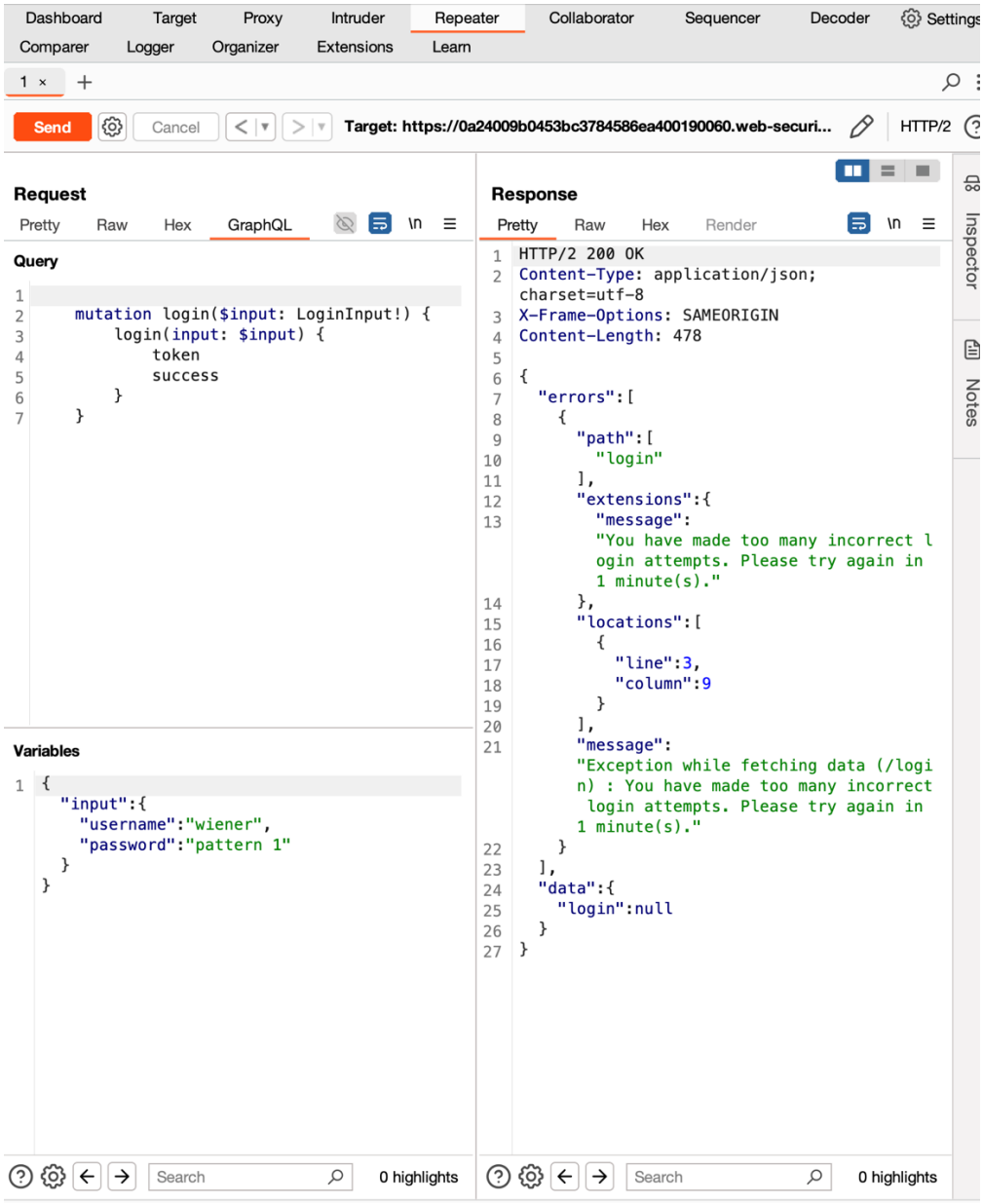


Figure 24: Step 3 sending multiple requests .

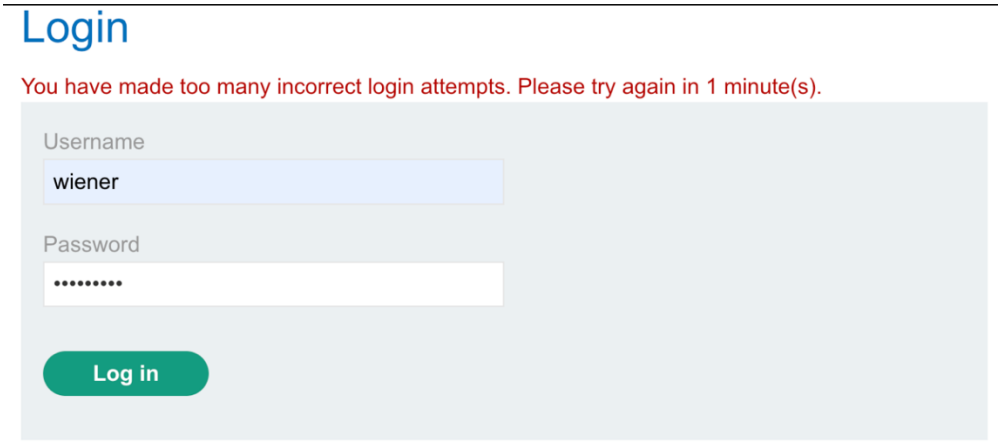


Figure 25:Showcasing Graph Ql brute force defenses.

4. Step 4.

Change the query request to mutation login{
Login (array of numbers)(input: {password: " ---", username: "carlos")
{
token
success}}
Put a passwords from the authentication lab passcodes. Send 100 request at once.

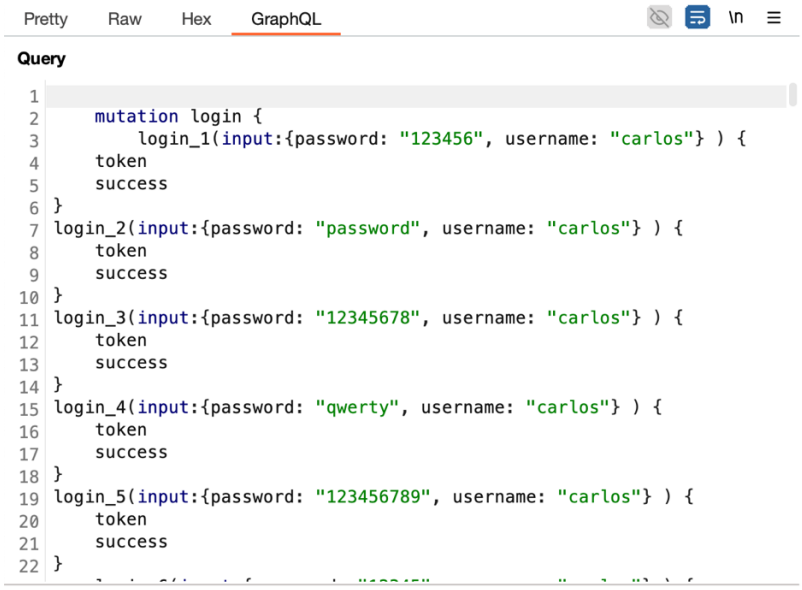


Figure 26: Sending multiple query request at once.

5. Step 5.
   Look for multiple responses and find the one that says true in the success portion. And track the login number of the response. The request corresponding to the response is the password.

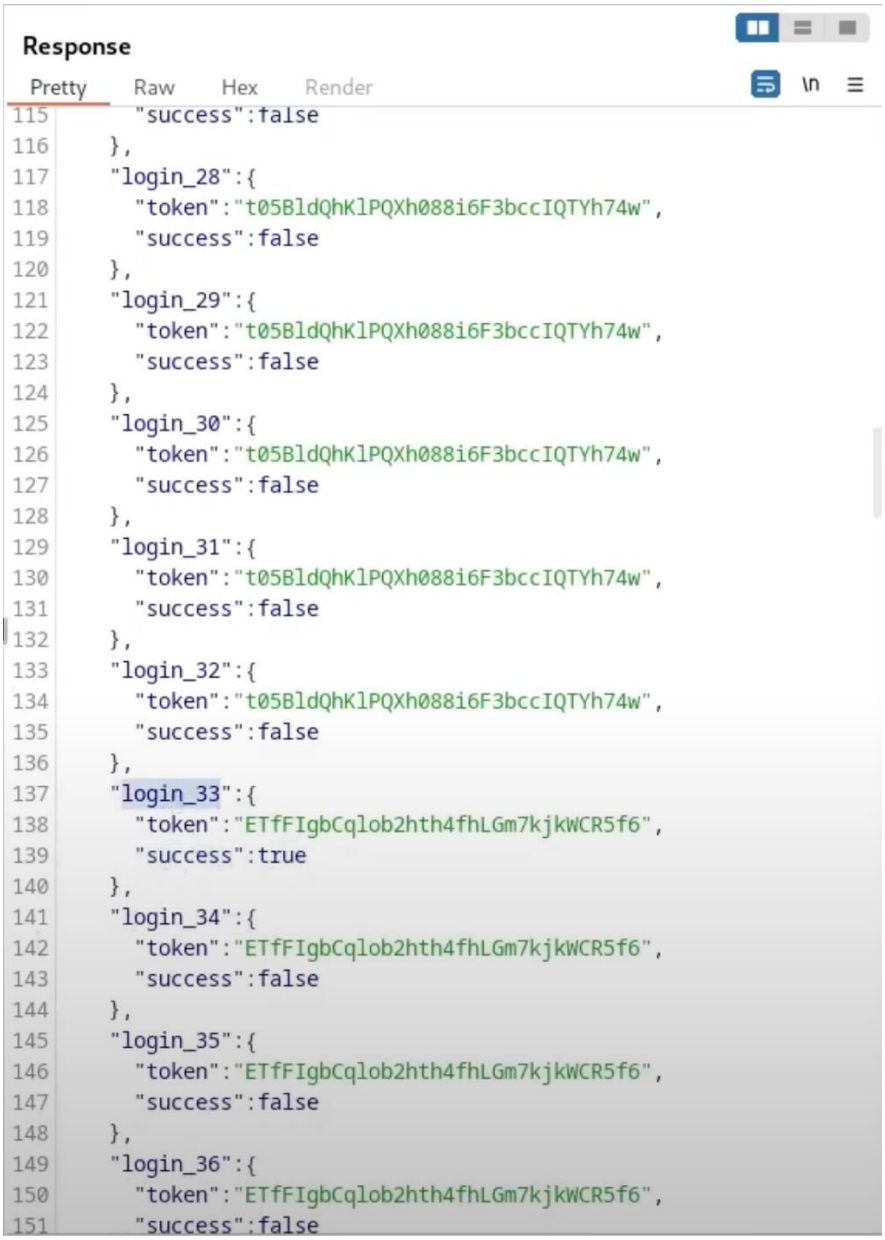


Figure 27: Step 5 watching for true response.

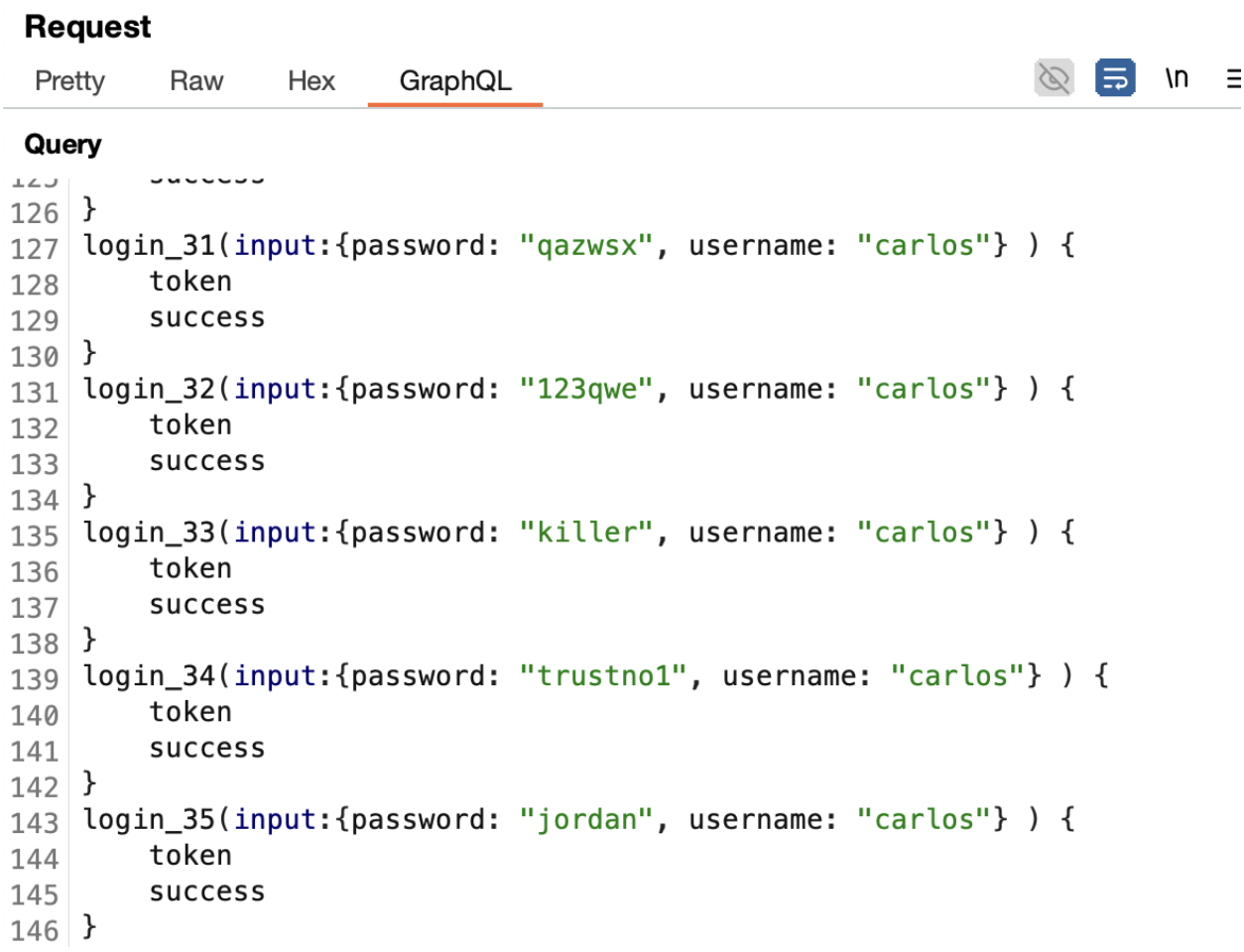


Figure 28: Step 5 finding the corresponding request and the password.

6. Step 6 Results.
   Insert the username carlos and recently found password killer in the login in page.

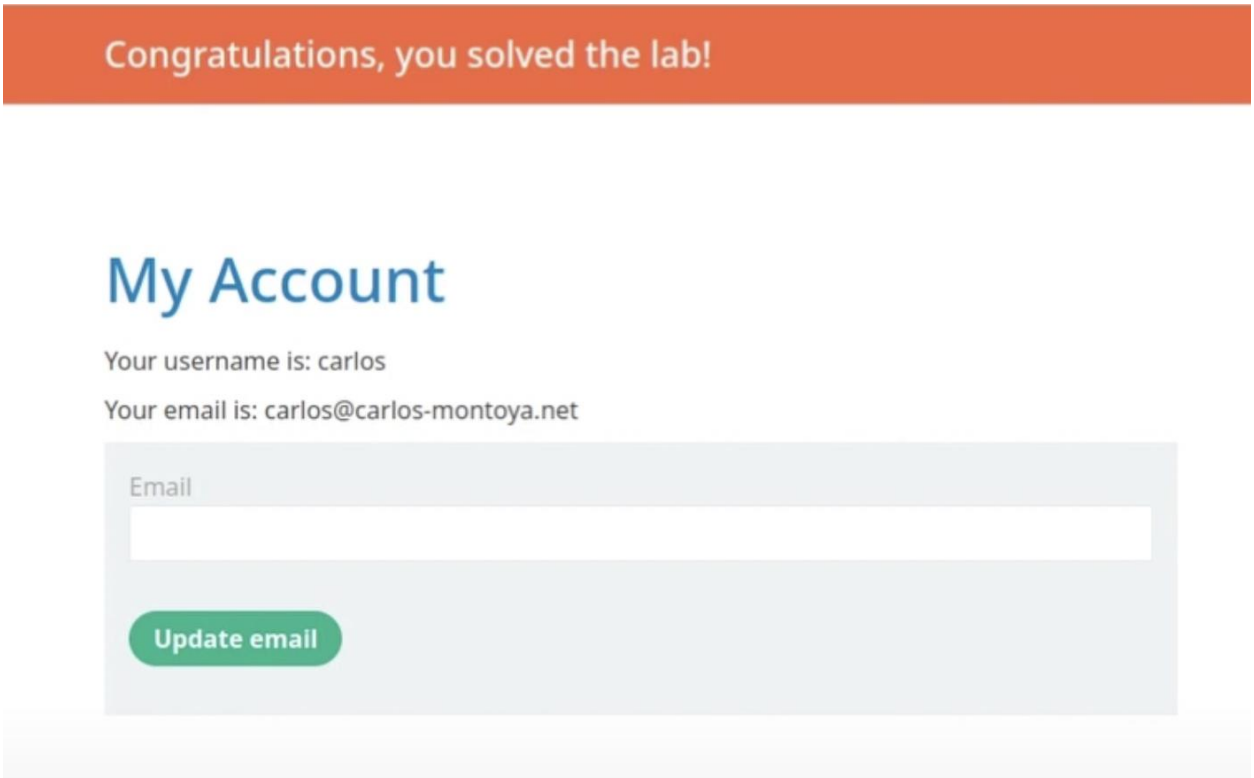


Figure 29: Result.

4. Mitigation.

There are various mitigative methods which can be used to prevent and minimize the damages which can potentially cause massive damages. These Mitigative measures are listed below.

1. Employing the use of strong passwords.
   Having a strong password is the simplest yet the most optimum defense against a brute force attack. Using a strong password policy is incredibly effective and an easy way of finding the various sector. Some of the important steps to keep in mind are the individuals should never recycle their password and should avoid using their personal information like using names, birthdays, and anniversary dates. Most people do not need to be worried about brute force attacks if they used strong passwords containing letters, numbers, and symbols. In order to have a strong password the password should also be long ideally a password should be longer than 15 characters. It also would be better to use random combination of various strings together than something that has meaning since hackers can target your identity while targeting a victim. (Descalso, 2022)

2. Limit login Attempts.
   Today, most websites allow unlimited login attempts. In terms of brute force attacks and in general cyber-attacks attacks it is incredibly risky to allow unlimited login attempts. It is incredibly easy as a website administrator to limit the login attempts to be safe from brute force attacks. There are various plugins like Jetpack, Shield Security, and loginizer. The web developer or an application should employ a mechanism to record the login attempts of the users along with the interval between each attempt. It a user exceeds this limit the account must be locked until one can verify it was the right user who just forgot their password. The User must be notified if anything suspicious is happening to their personal accounts. (Descalso, 2022)

3. Employ the use of two factor authentication.
   Two factor authentication or multi-factor authentication adds a layer of security to the users. Two factor authentication requires the user to either enter a code or more recently the authentication process might require you to open a certain app on your phone and confirm the number they are seeing on their phone screen against the device the users were adding before. Two factor authentication can be incredibly useful as user's account is not compromised even if their password is compromised. (Securi, n.d.)

4. Using CAPTCHAs.
   CAPTCHA are the tools through which web applications and web services can differentiate between a human and a bot. CAPTCHAs are constantly evolving and are becoming more difficult. A few years ago captchas required the users to identify between different things which were easy to distinguish from each other. But now due to the developments made in the field of artificial intelligence and machine learning captchas are required to be harder. Since brute force attacks require multiple attempts to break into a system using captcha in between every login attempt it will make the hacking process using it tedious. (Novell, n.d.)

5. Use of Web application firewalls.
   A web application firewall helps protect the applications by filtering and monitoring HTTP traffic between a web application and the internet. Web application firewalls are effective to defend against brute force and various other kinds of cyber-attacks such as SQL injection attacks and DOS attack.

5. Evaluation.

1. Advantages of implemented mitigation strategy.

1. Comprehensive Defense:
   By Implementing the combination of mitigation approaches listed above which include Two factor authentication, CAPTCHAs, strong password, login attempt limiting and web application firewall an organization can create an expansive and a multi-layered defensive mechanism ensuring the survival rate of a system or an account.

2. Increased Resilience.
   Strong passwords and login attempt limiting directly targets brute force attacks as I proposed the mitigation methods that directly counters the brute force approach. Two factor authorization is directly counter to bots making these mitigation process well defended against DOS attacks too.

3. Adaptability to evolving threats.
   Combining various different strategies allowing the adaptability of the evolving cyber threat making the mitigation technique extremely well rounded in terms of flexibility and adaptability.

2. Disadvantages.

1. False alarms.

Monitoring tools and intrusion detection systems may generate false alerts, flagging legitimate user actions as potential brute force attacks. These false alarms can result in unnecessary delays, additional workload during investigation, and administrative burdens during alert management and resolution.

2. Impact on user experience.

Some security measures such as CAPTCHAs are incredibly annoying and frustrating for the regular user experience of the attackers go bad resulting in loss. Even though it is security is important but the users prefer convenience due to ignorance.

6. Conclusion.

To sum up, this research has thoroughly examined the complexities of attacks using brute force in the context of information technology. By means of a thorough analysis of their operational methods and their consequences, we have emphasized the vital significance of taking proactive measures to counter these dangers. The integrity and security of information systems and networks are seriously threatened by brute force assaults, which can take many different forms, such as guessing encryption keys or breaking passwords. Their dynamic character necessitates constant attention to detail and flexible defensive strategies.

Furthermore, investigating mitigation techniques has shown the way to strengthening protections from brute force attacks. Organizations can greatly increase their resistance to these hostile acts by promoting strong password management procedures, such as the use of multifactor authentication as well as intrusion detection systems. Case studies from the real world have shown to be incredibly insightful, demonstrating how primitive security measures can effectively lessen the damage of brute force attacks.

It is clear from the future that the defence against brute force attacks is a continuous process that calls for cooperation and dedication. As technology advances, our defensive tactics also need to adapt. Through constant monitoring of new threats and the application of creative solutions, we can strengthen our defences and ensure the security of our technological infrastructure. By means of cooperation, attentiveness, and a proactive security strategy, we may confidently and resiliently traverse the intricacies of the digital terrain.