Assignment Report

Prepared by:

White Hat Group

Date:

04-10-2023

Table of content

Introduction

In an increasingly interconnected world, where digital information plays a pivotal role in our daily lives, the importance of safeguarding data and information cannot be overstated. The realm of cyber security is at the forefront of this battle, with individuals, organizations, and governments continually striving to protect their sensitive data from a growing arsenal of threats. This essay will delve into several critical cyber security topics, shedding light on the intricacies of each.

1. Brute Force Attack:

Brute force attacks represent a persistent and rudimentary threat in the world of cyber security. They involve the relentless trial-and-error method of guessing passwords or encryption keys. Through a sheer force of computational power, attackers systematically try every possible combination until they gain access to a system or an account. Brute force attacks, while straightforward, underscore the necessity of robust password and encryption practices in the digital age.

- By the help of brute force attack, we can get username or password or OTP.

2. Cross-Site Request Forgery (CSRF) Attack:

CSRF attacks are insidious attacks that manipulate a user's trust in a website. By tricking users into making unauthorized requests to a different site, attackers can initiate malicious actions without the user's knowledge. This essay will elucidate the mechanisms behind CSRF attacks and how they jeopardize the integrity and confidentiality of web applications.

3. Backdoor Creation Using SET:

The creation and exploitation of backdoors represent a particularly sinister facet of cyber threats. Social Engineering Toolkit (SET) is a potent tool used by attackers to manipulate human psychology and engineer backdoors into systems. This essay will examine how attackers exploit human vulnerabilities to create illicit access points in otherwise secure environments, illustrating the importance of educating users about social engineering tactics.

4. Cryptography:

Cryptography serves as the bedrock of information security, providing a shield against prying eyes and malicious actors. It is the science of encoding messages in such a way that only the intended recipients can decipher them. This essay will explore the principles of cryptography, highlighting its significance in securing sensitive information across the internet and other digital communication channels.

There are two types of Cryptography, they are:

- **Symmetric (Private Key):** Using single key that only sender and Receiver know.
- **Asymmetric (Public Key):** Using two keys, a private key - which is used by receiver and a public key - which is announced to the public.

5. SQL Injection:

SQL injection is a prevalent threat in the world of web applications. It involves injecting malicious SQL queries into an application's database, potentially exposing, altering, or deleting sensitive data. This essay will explore the techniques behind SQL injection attacks and how developers can safeguard their applications against this perilous vulnerability.

6. Cross-Site Scripting (XSS):

Cross-Site Scripting vulnerabilities allow attackers to inject malicious scripts into web pages viewed by other users. This can lead to the theft of session cookies, identity theft, and more. This essay will shed light on the different types of XSS attacks, their consequences, and mitigation strategies for web developers and administrators.

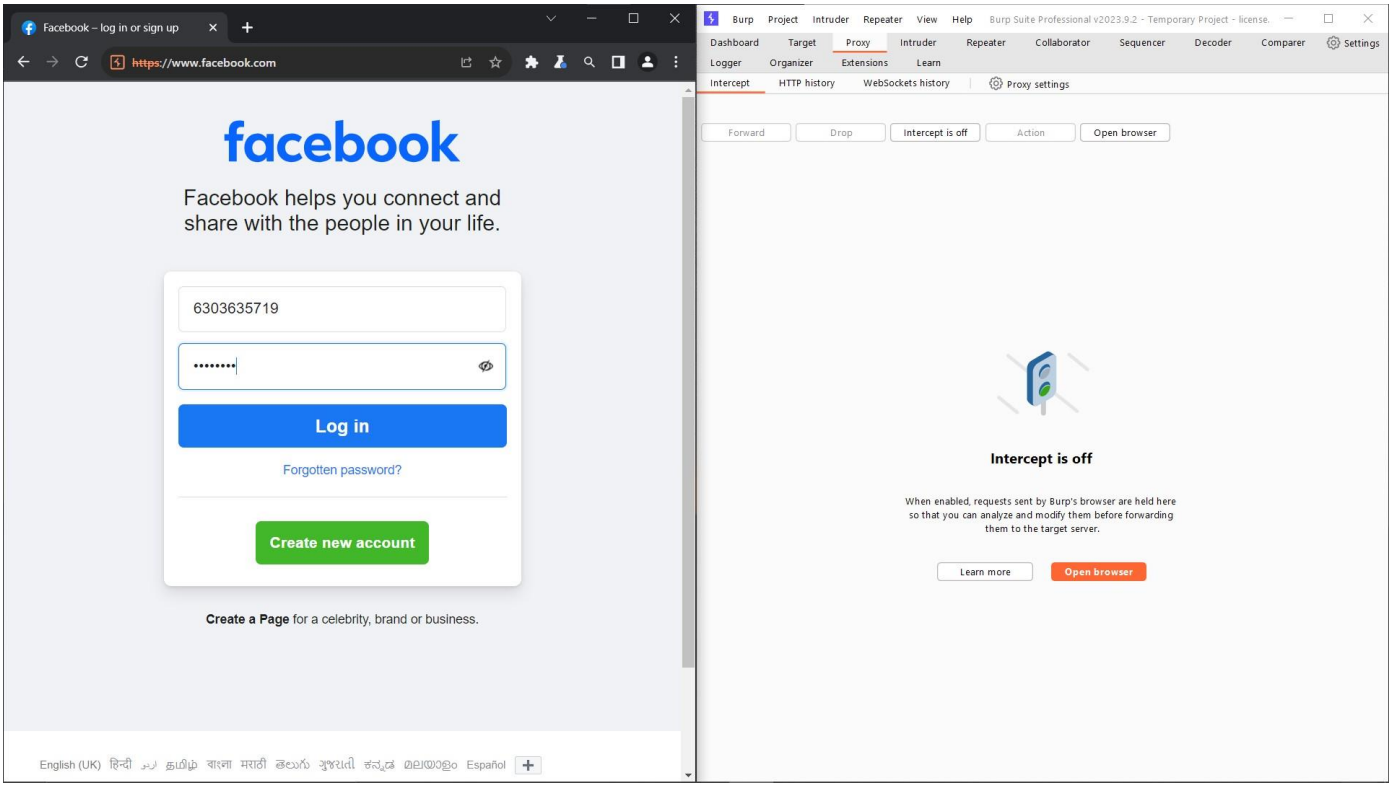
There are 3 types of XSS, they are:

- Stored XSS: where the malicious scripts comes from the website database.
- Reflected XSS: where the malicious script comes from the current HTTP request.
- DOM-based XSS: where the vulnerability exists in client-side code rather than server-side code.

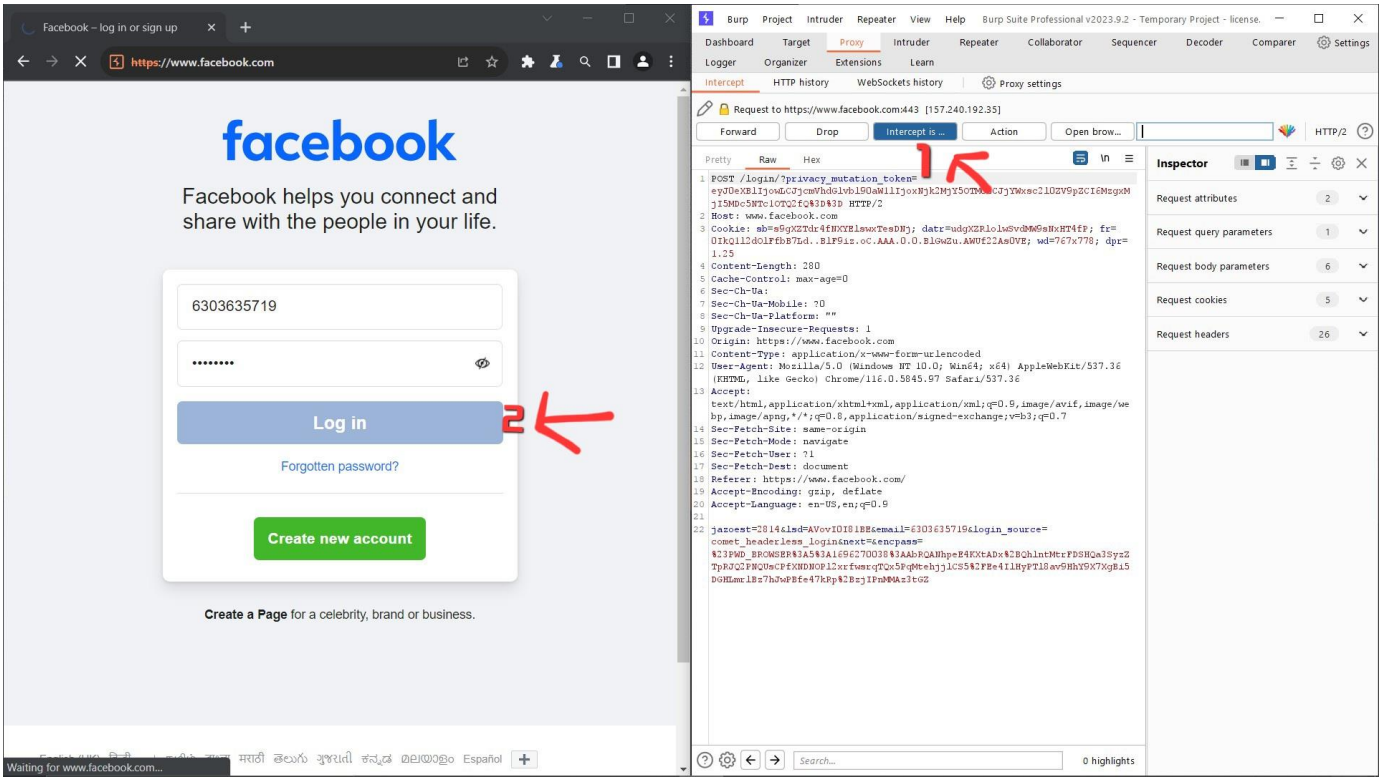
Brute Force Attack

Password cracking by brute force attack:

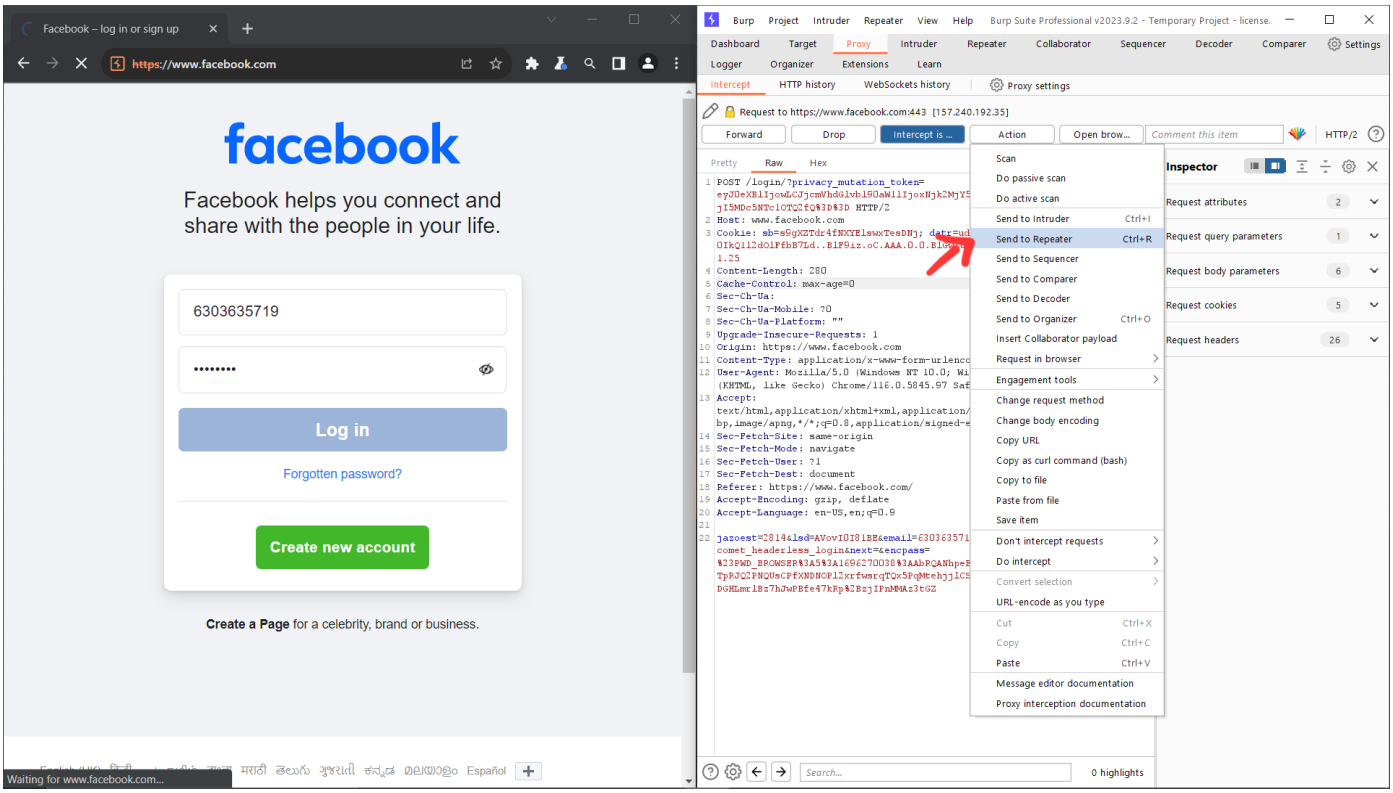
- Start Burp suite and Browser side by side, open website login page (example Facebook).



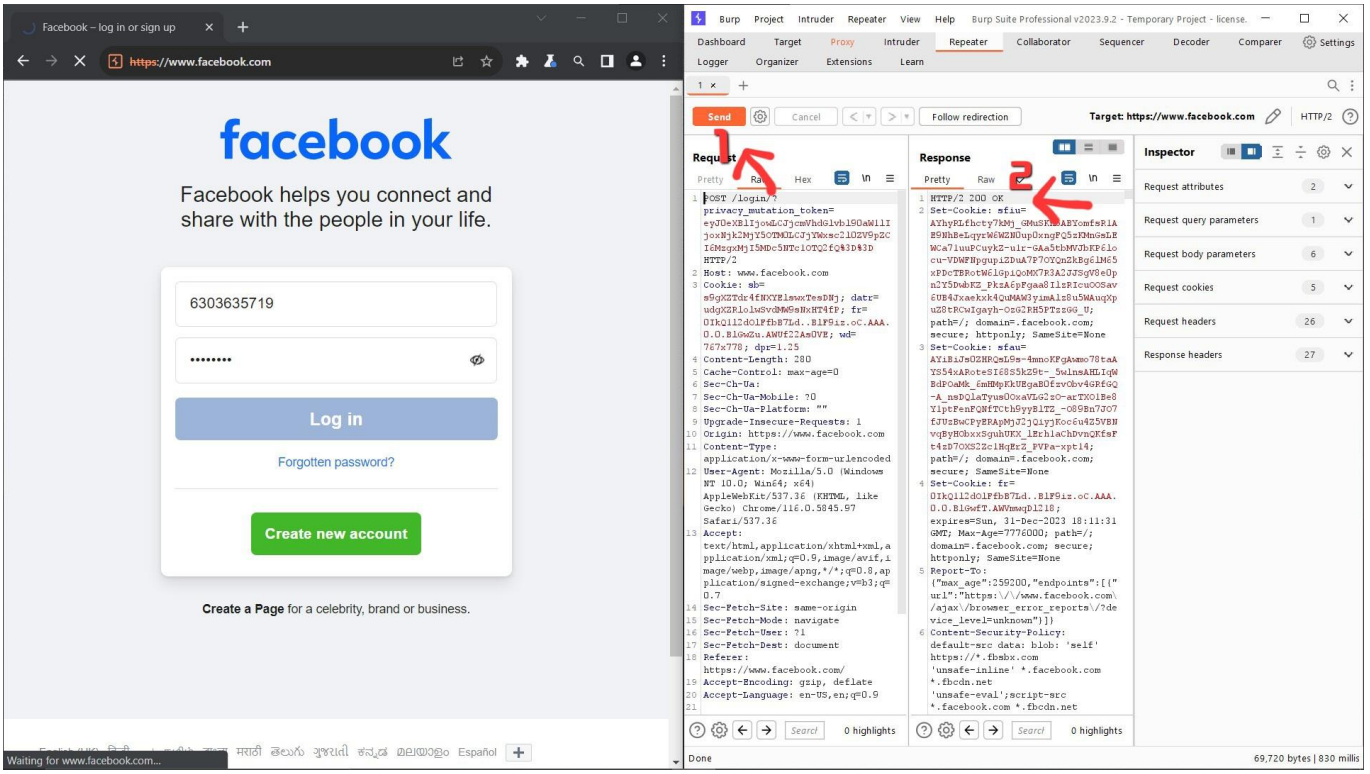
- Enter username of target and enter random password.



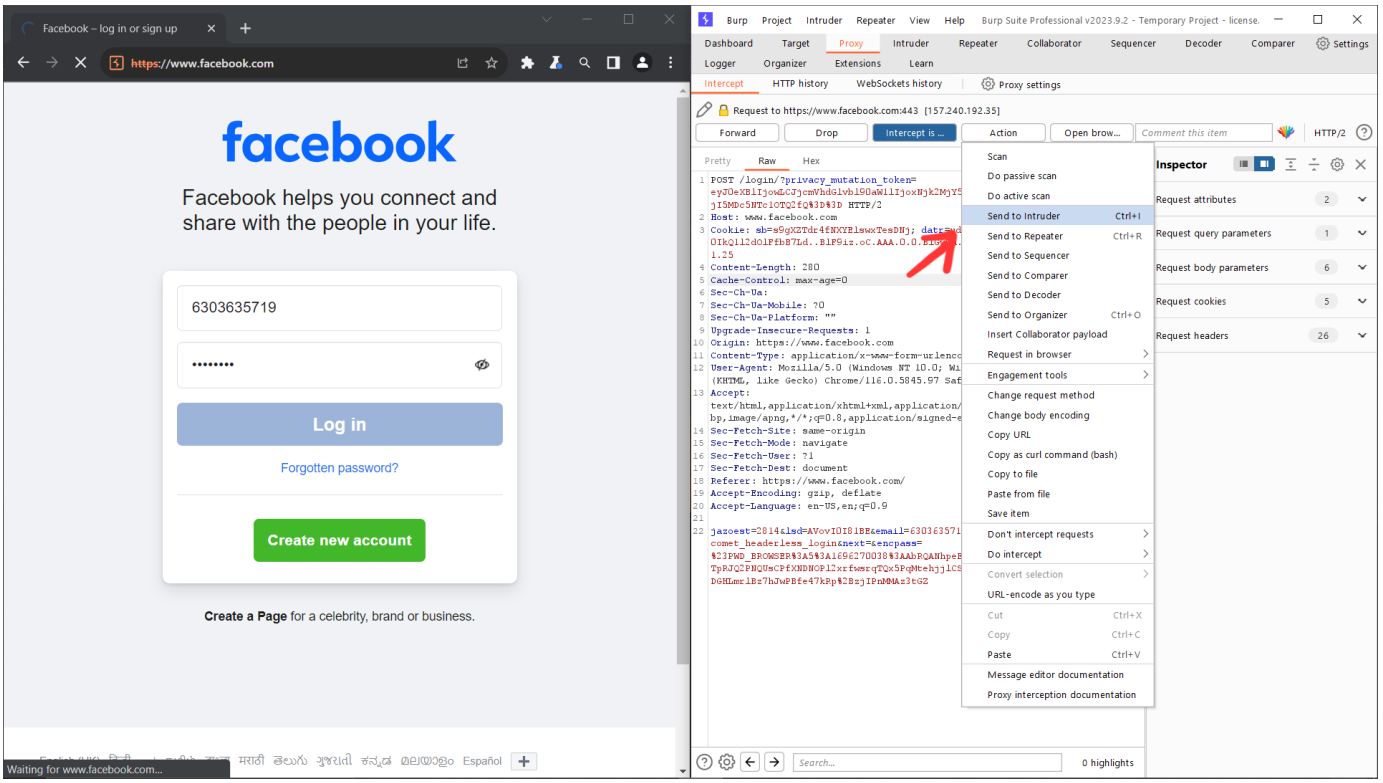
- Before clicking “Log in”, turn interception ON in burp suite (like 1 in above pic) and then click login (2).



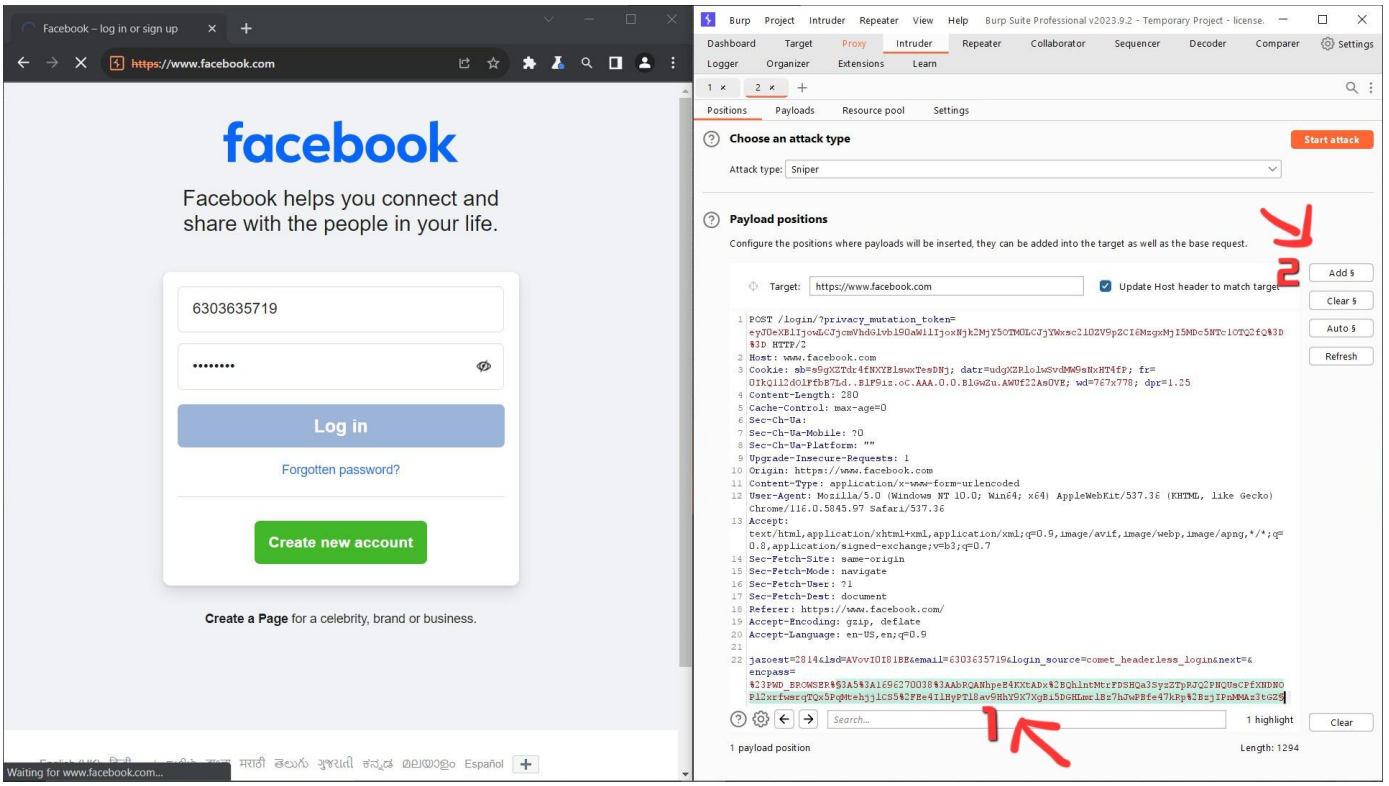
- Click on action and select “send to Repeater”.



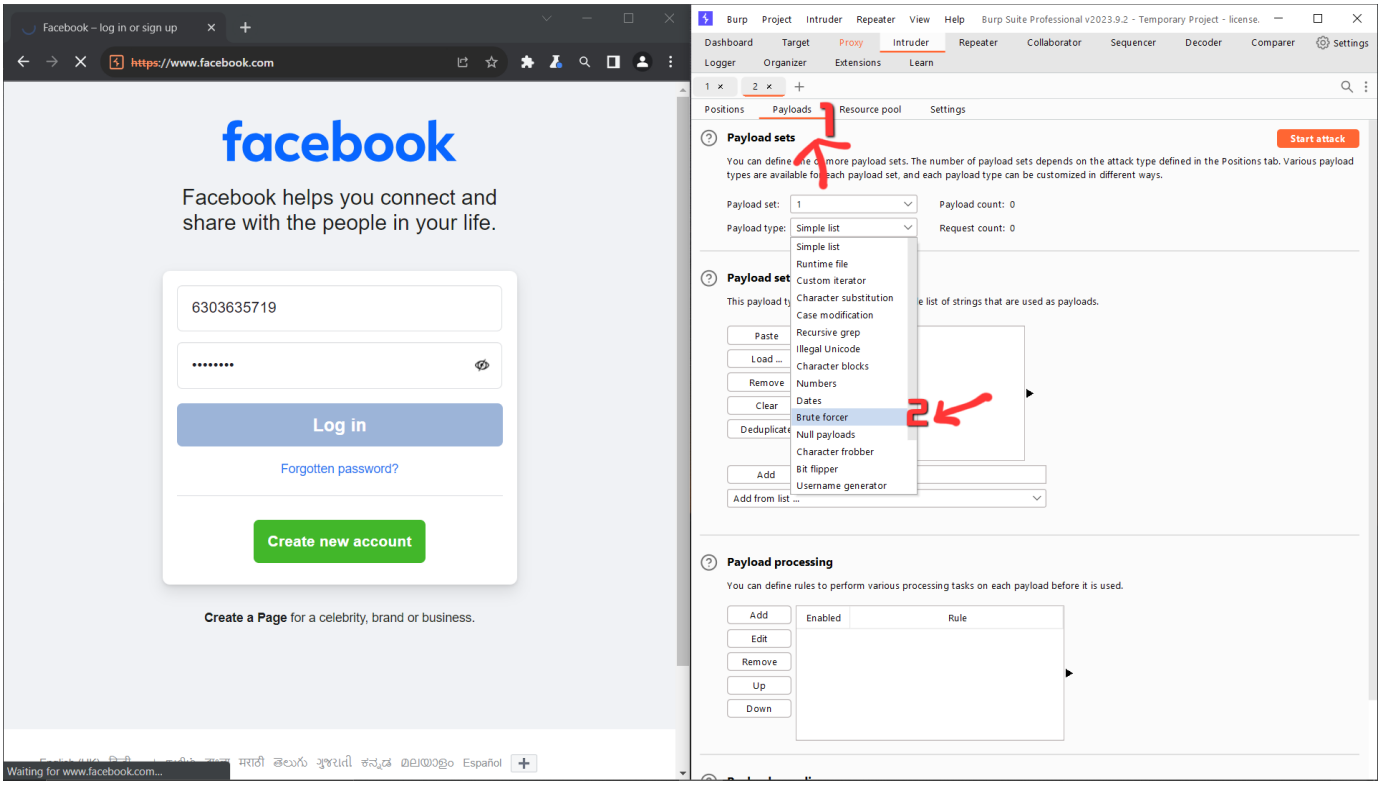
- Move to Repeater and click send button (1) and check whether there is “200 OK” is there in response or not (2)



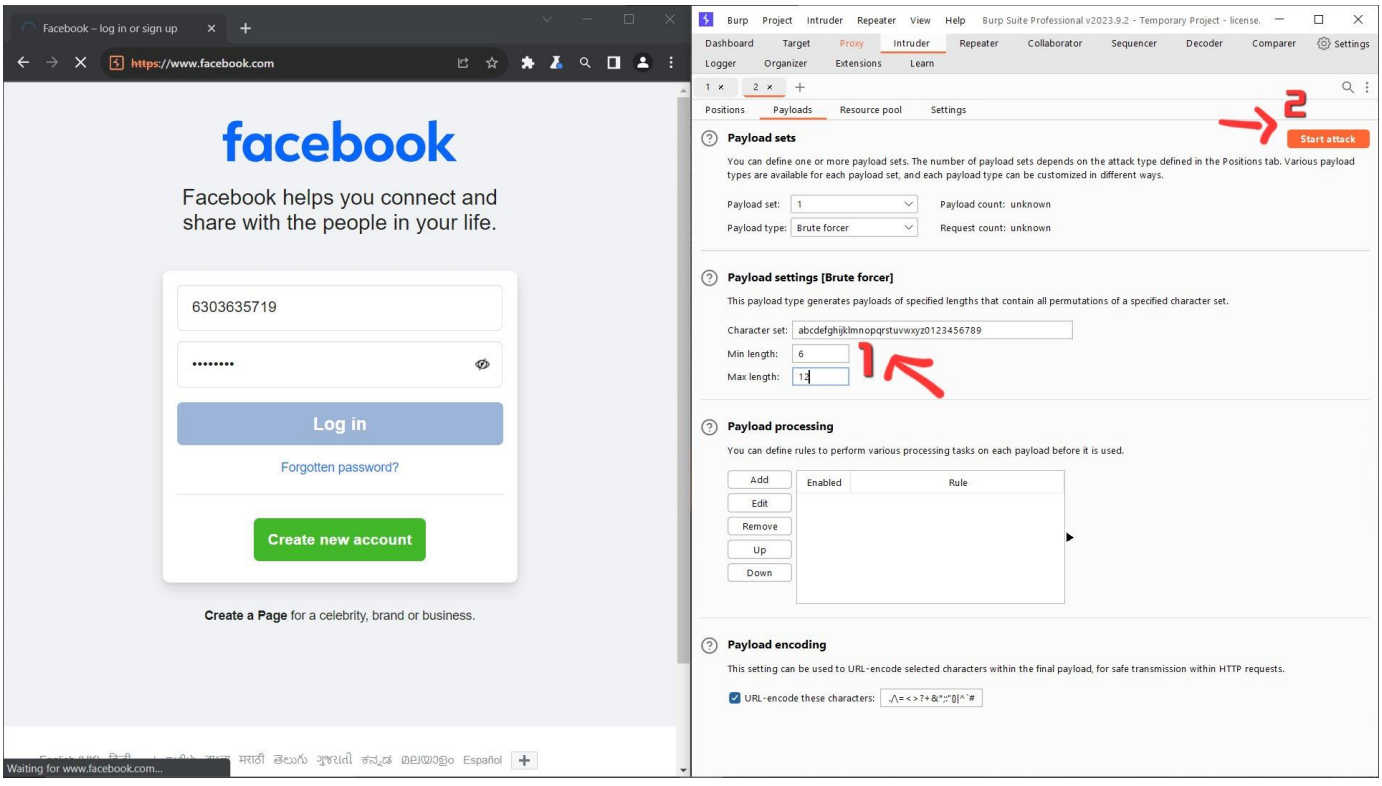
- If there is “200 OK” in response, move to Proxy and click on action and then select “Send to Intruder”.



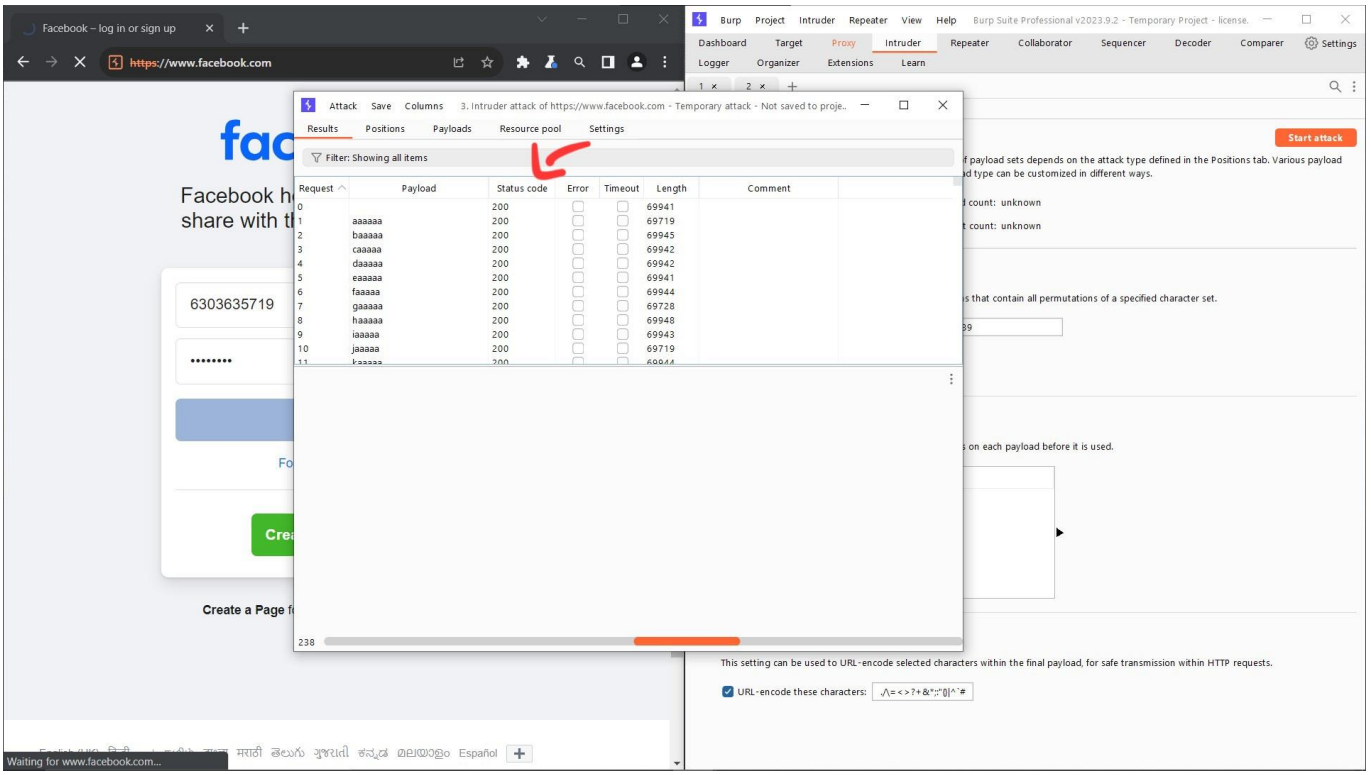
- Move to Intruder and select the encrypted format of password as shown above (1) and click on “ADD” (2).



➢ Move to Payloads (1) and select payload type as “Brute forcer” (2).



- Customize payload settings for searching password according to website (1) like alphabets in small letters and capital letters, numbers and special characters which might contain in passwords. Then click on “Start attack” (2).



- Then attack will get started and when it found password, we can see “302” in status code for that password and the length of that password will be higher than others and we can see true statement when we selected that password.
- This is the process of capturing the target’s password or username or OTP.

Mitigation:

1. Implement account lockout policies to temporarily suspend accounts after multiple failed login attempts.

2. Enforce the use of strong, complex passwords and encourage password changes at regular intervals.

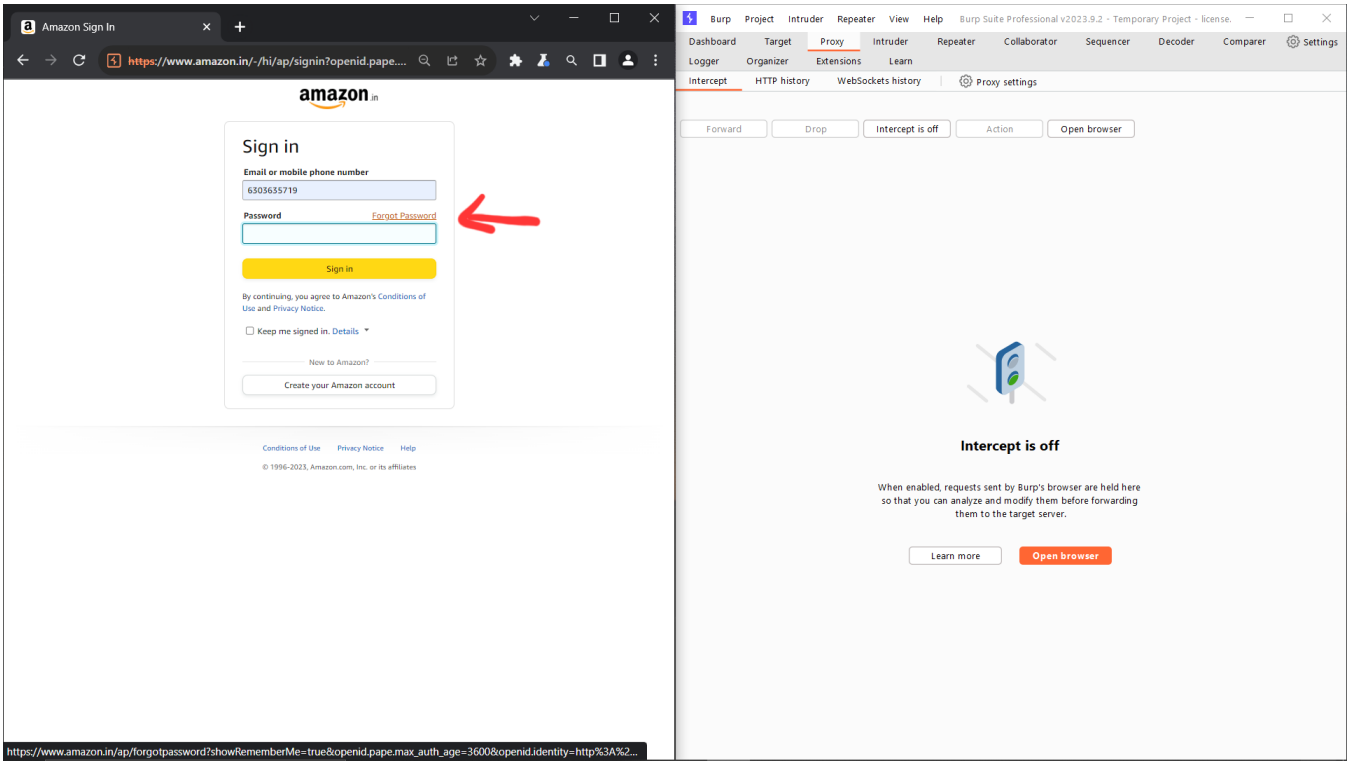
3. Consider implementing multi-factor authentication (MFA) to add an additional layer of security.

4. Monitor and analyze logs to detect and respond to unusual login activity promptly.

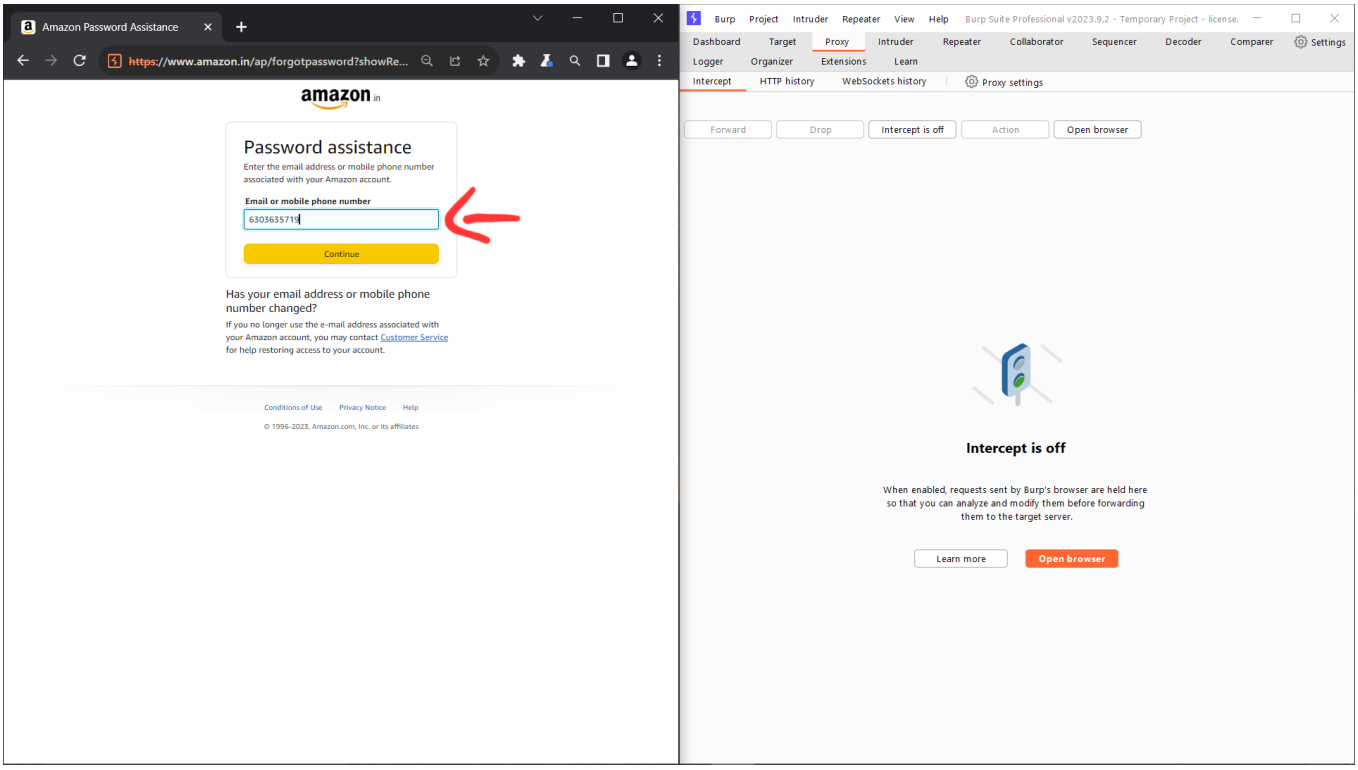
5. Implement rate limiting to restrict the number of login attempts from a single IP address.

Cross-Site Request Forgery (CSRF) Attack

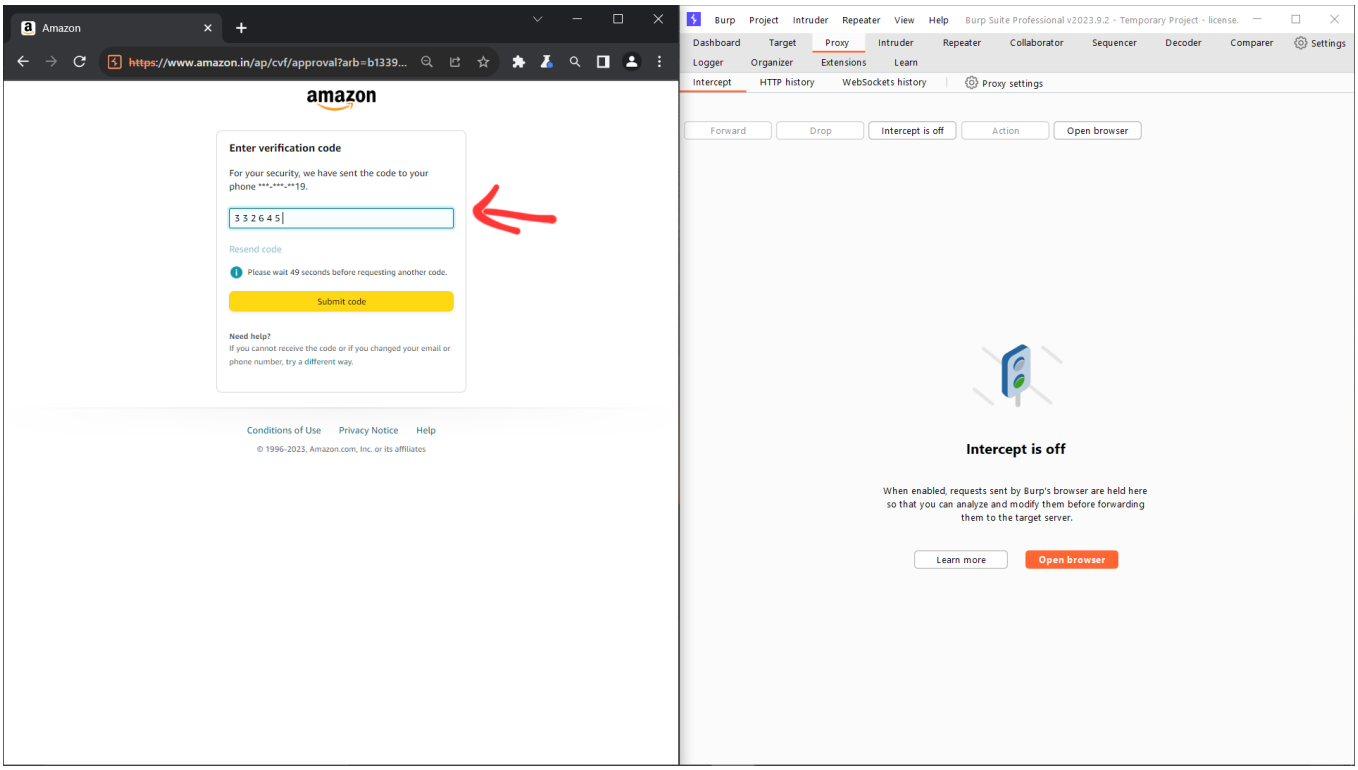
- Start Burp suite and Browser side by side, open website login page (example amazon).



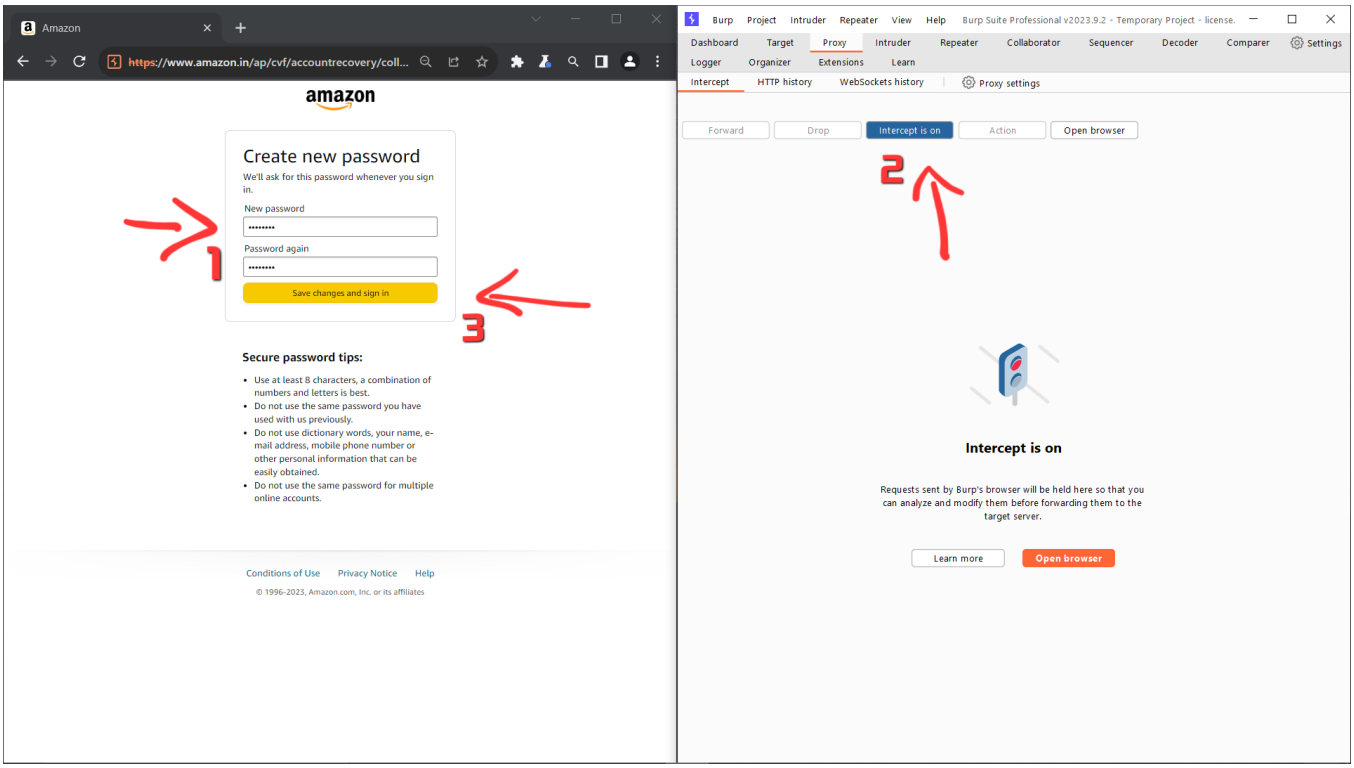
- Enter your mobile number or email and click forget password.



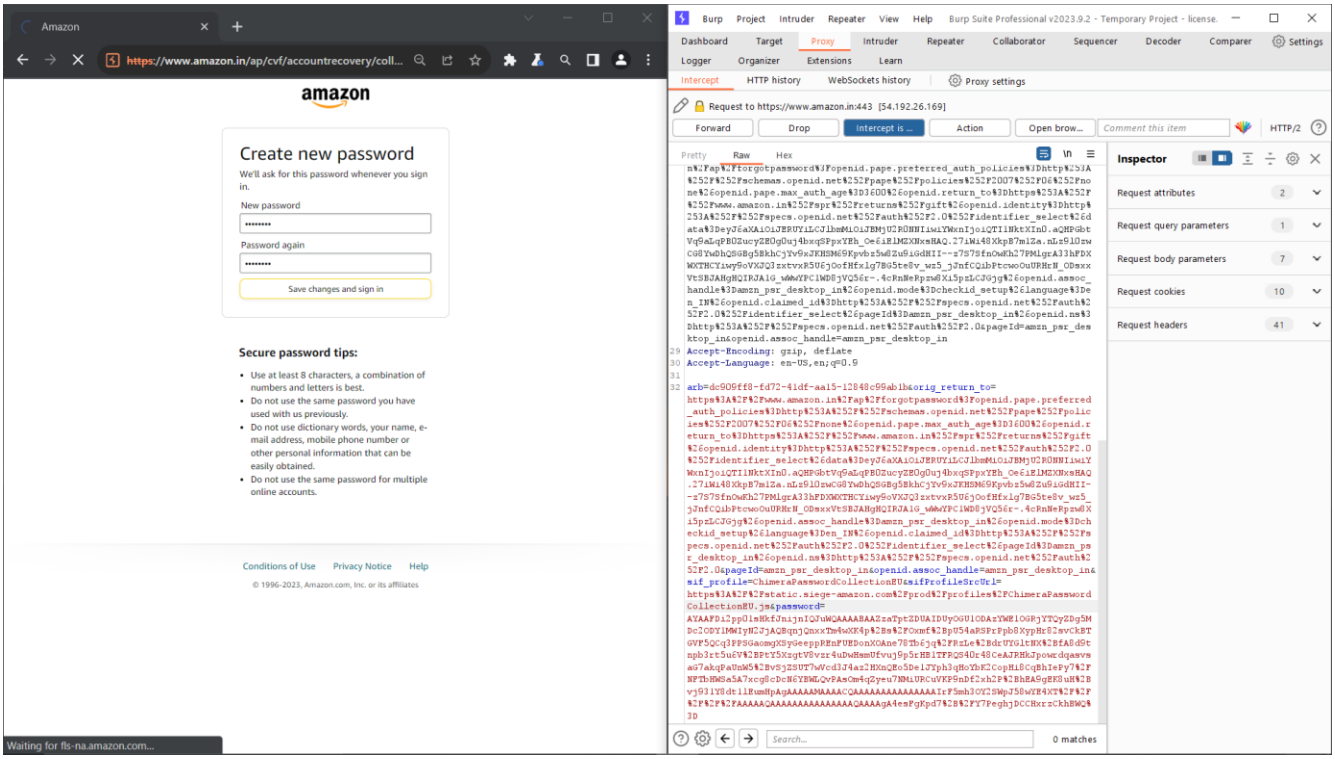
➢ Enter your mobile number again.



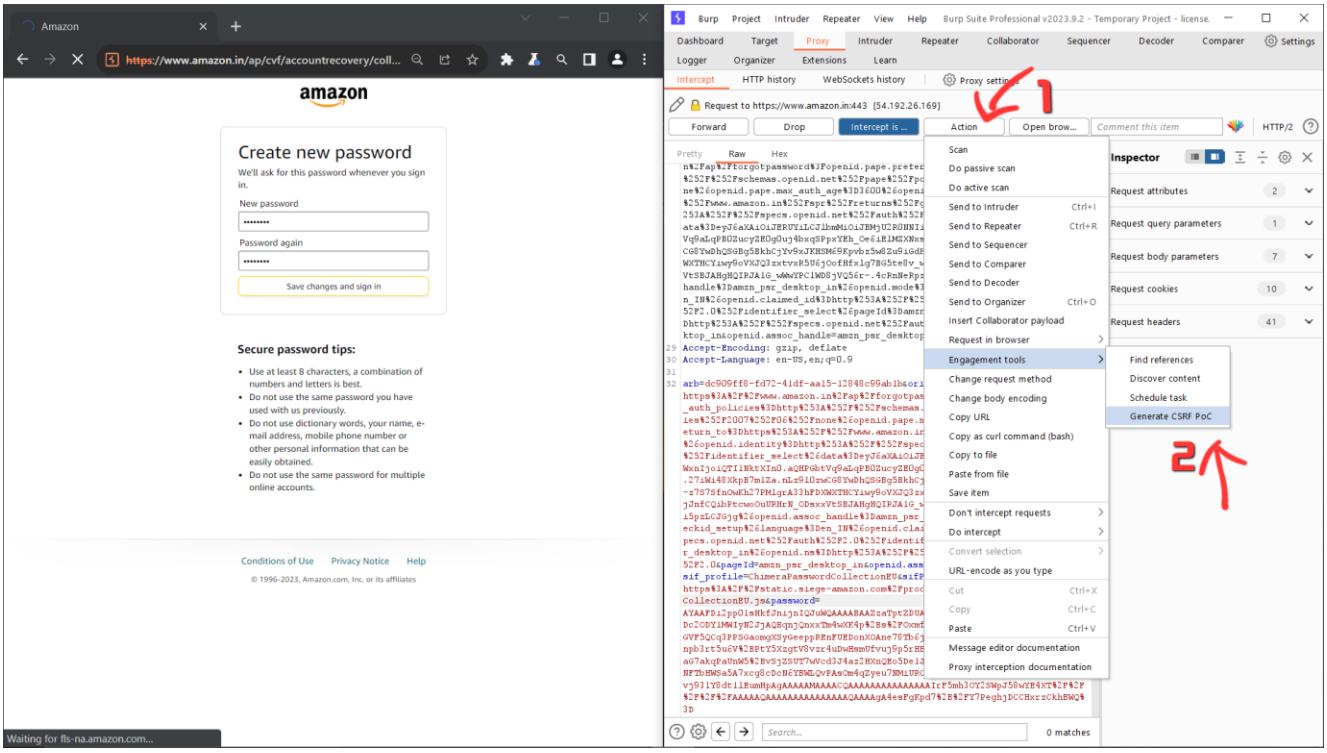
➢ Enter OTP which you will get to your given mobile number.



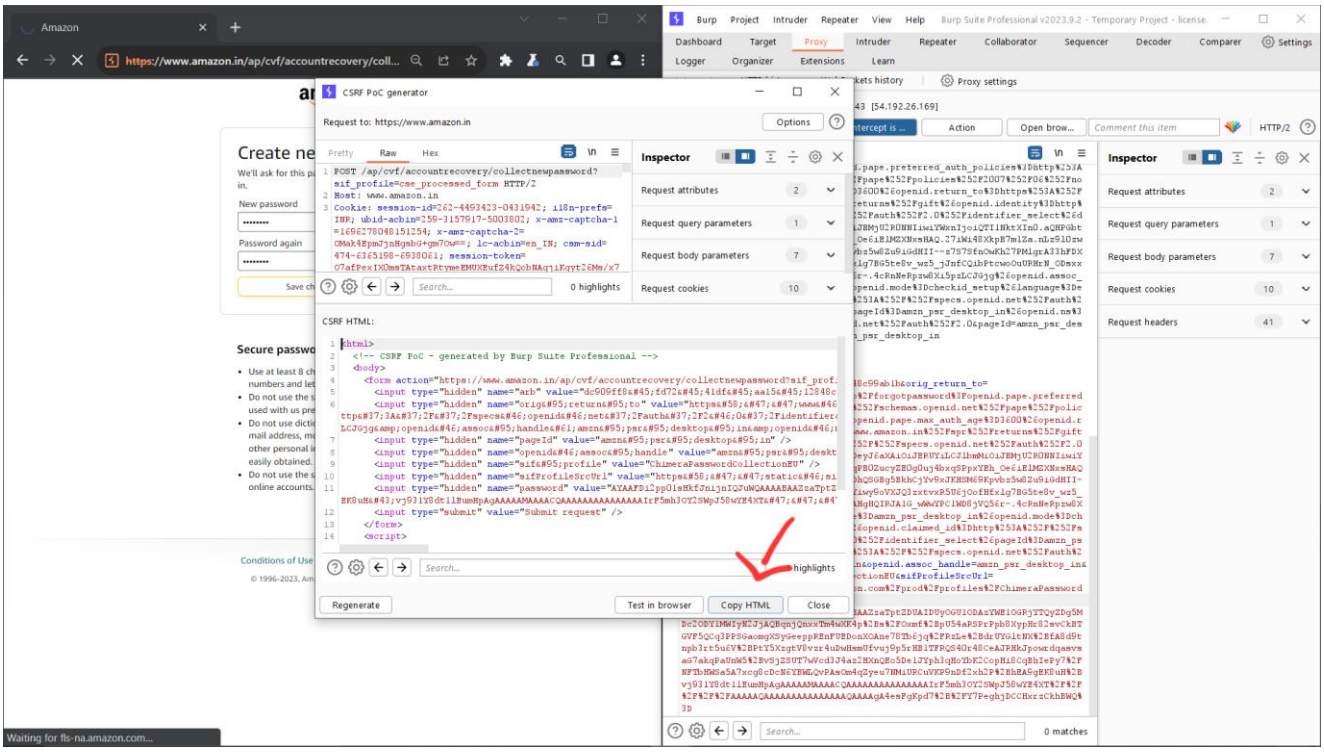
- Enter the new password which you want to change your target's account as well (1) and turn ON the interception in burp suite (2) and then click on "Save changes and sign in" (3).



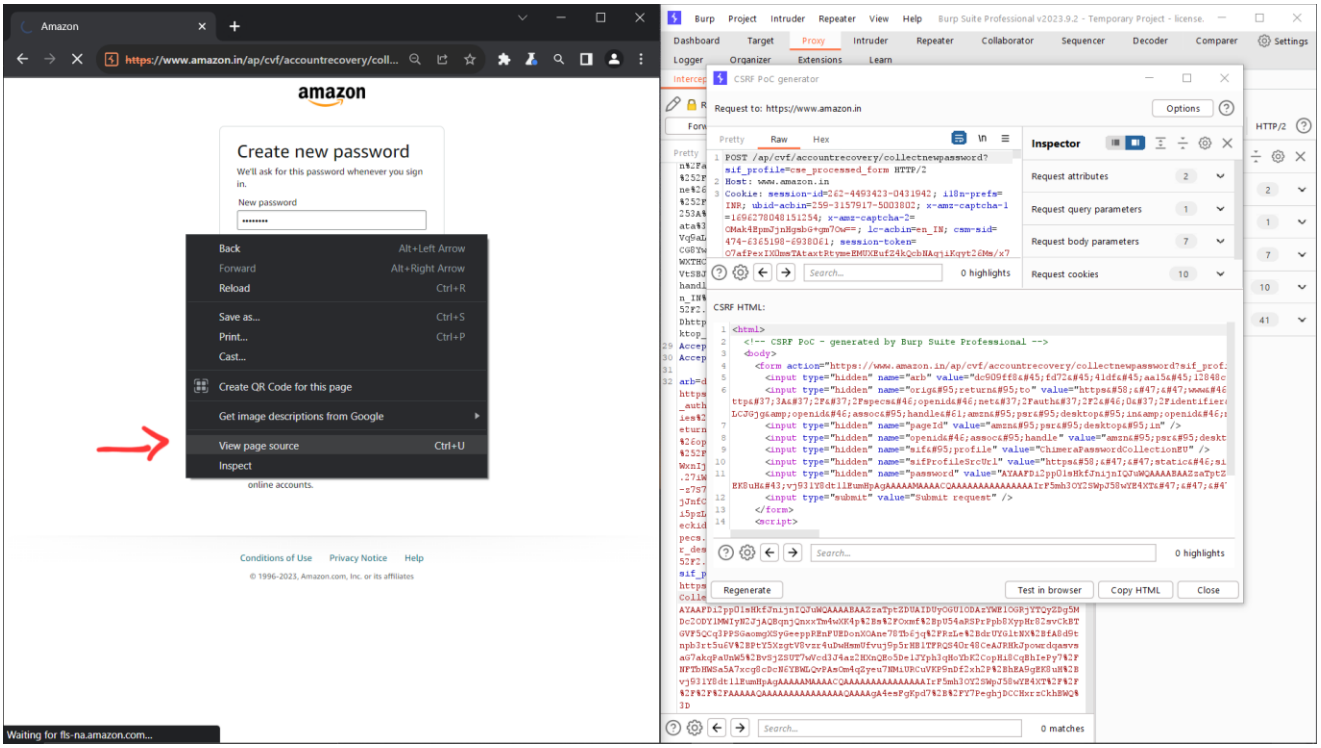
- Then you can see burp suite capturing the request, click on forward once.



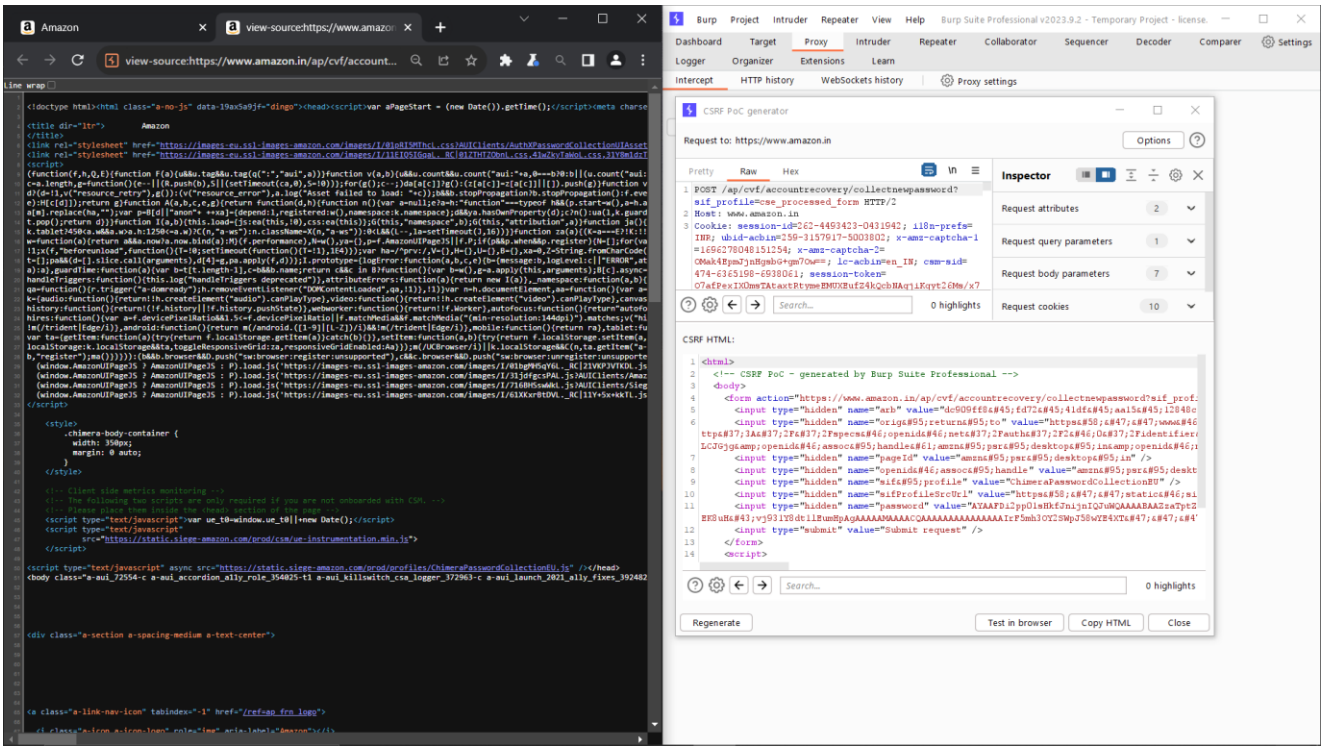
- Click on Action (1) and select “Engagement tools” and then select “Generate CSRF PoC” (2).



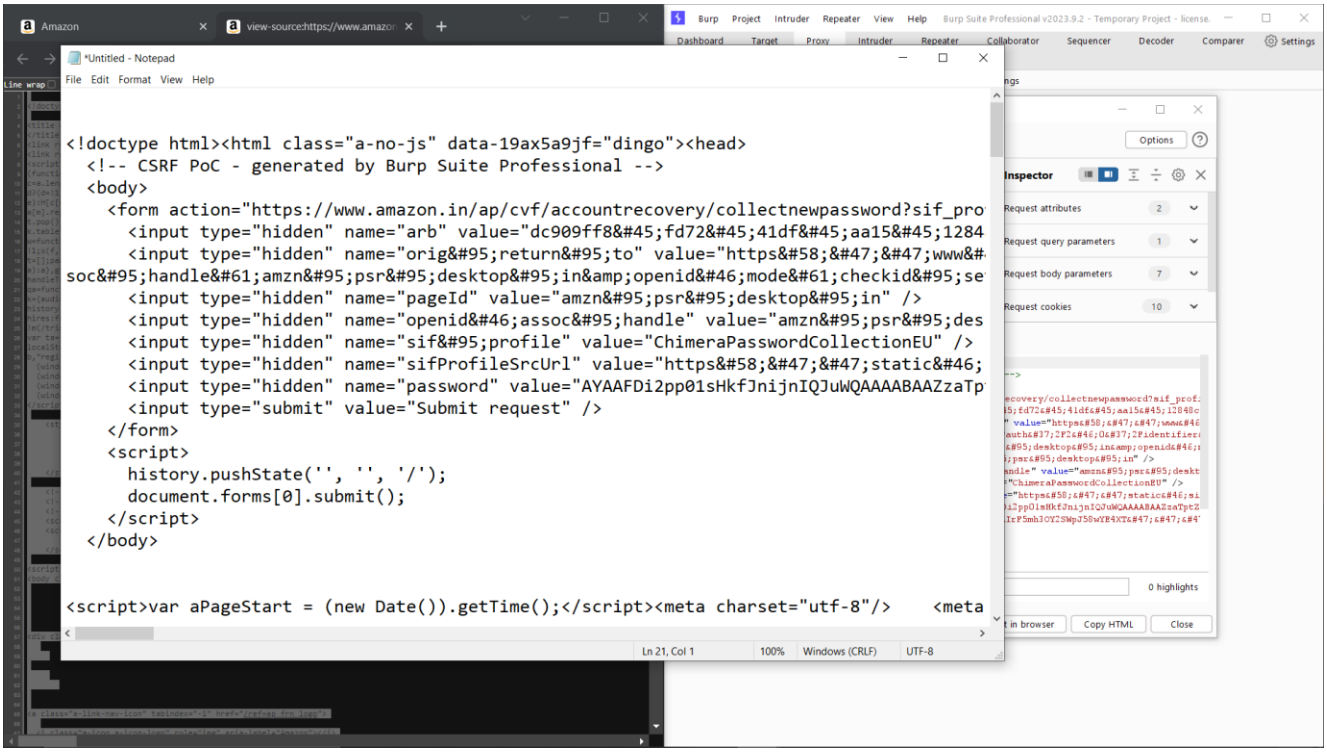
- Then you can find pop up window of CSRF code.



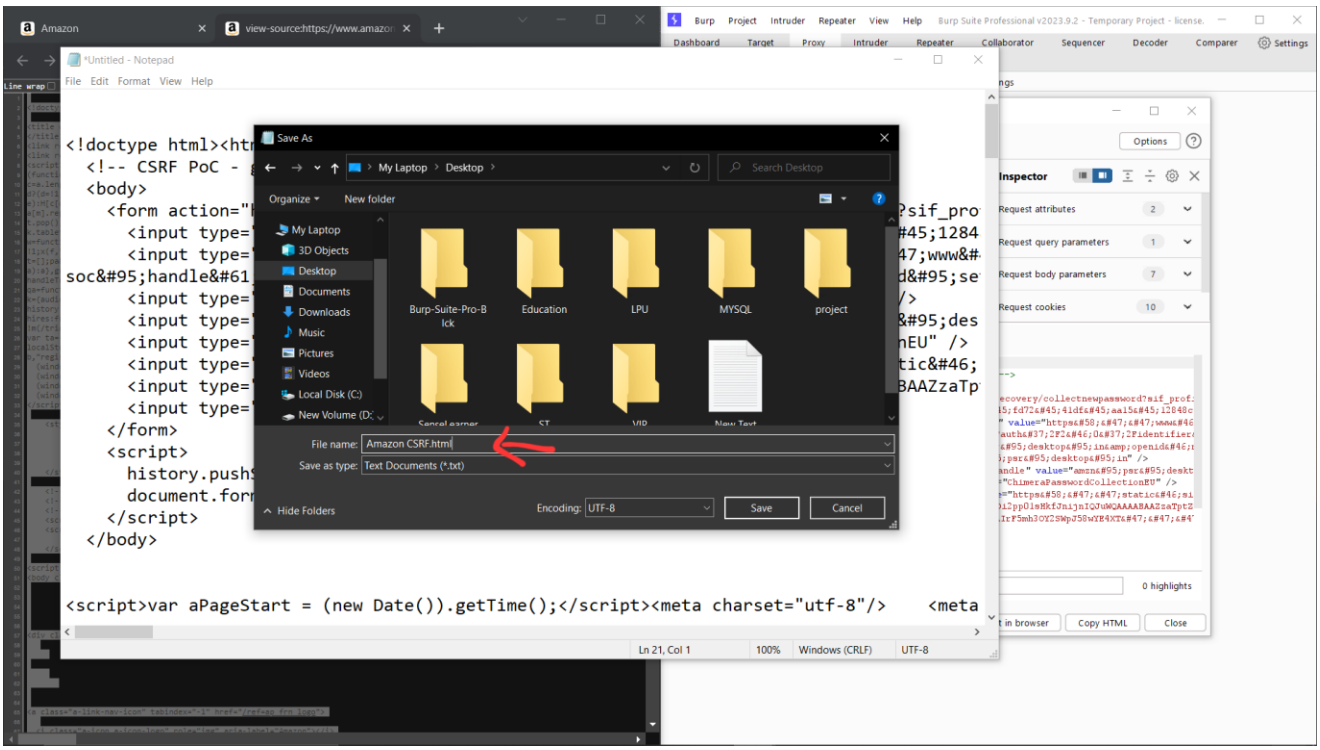
- Right click on browser and select “View page source”.



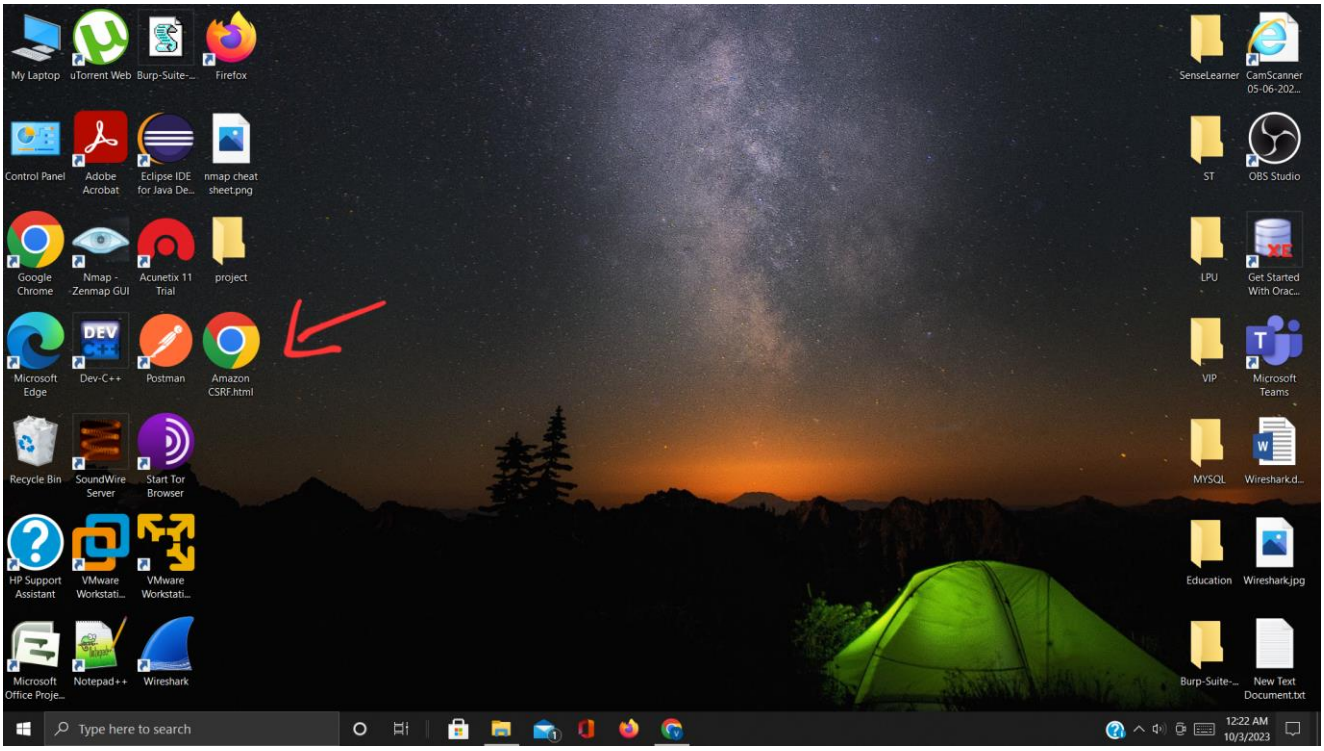
- Copy all the source code and paste it in notepad.



- Copy the CSRF code and paste it in notepad where you stored source code. Paste it below the "<head>" and remove "<html> and </html>" from CSRF code.



- Save it in ".html" format.



- Sending that file to target and if target clicks it and logged into his/her account will change their credentials.
- This is the process of CSRF attack to change the targets credentials as required and altering their account.

Mitigation:

1. Generate unique anti-CSRF tokens for each user session and validate them on form submissions to prevent unauthorized requests.

2. Implement the Same Site attribute on cookies to control cross-origin requests, reducing the risk of CSRF attacks.

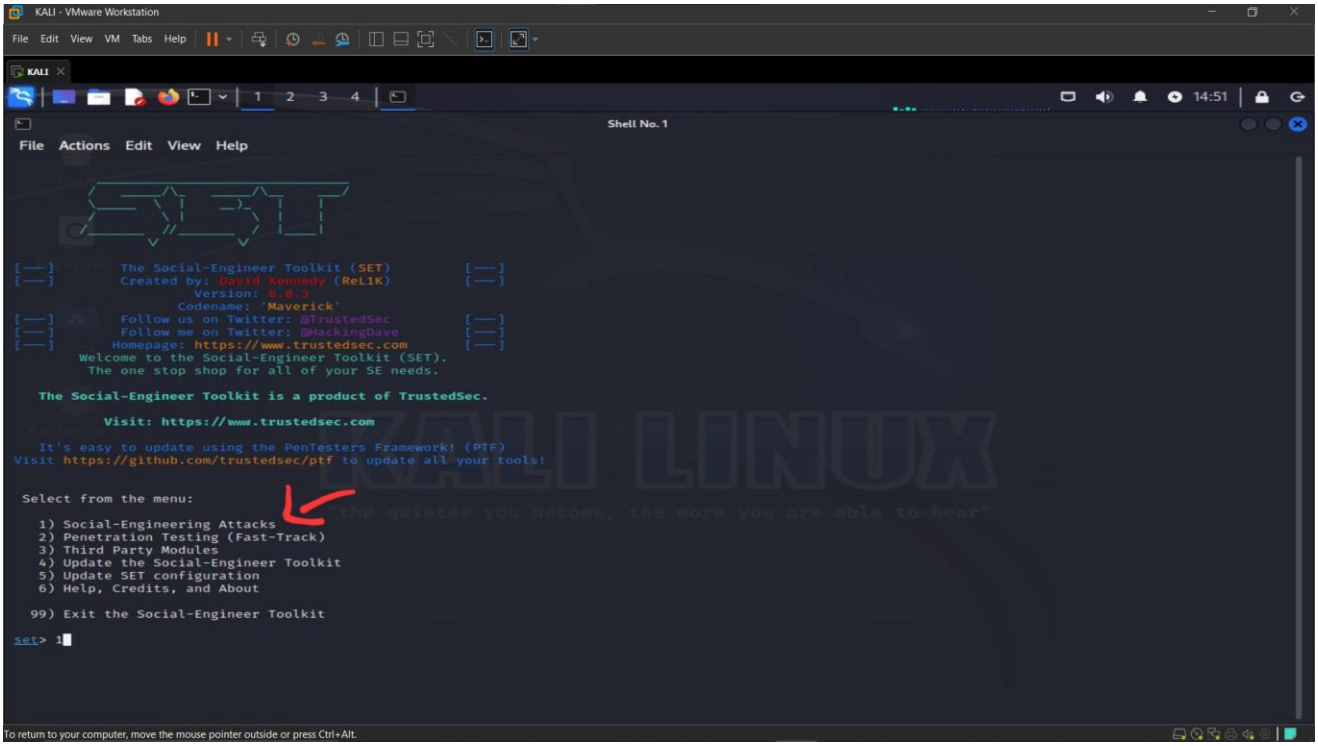
3. Employ security mechanisms like Content Security Policy (CSP) to restrict the execution of scripts from untrusted sources.

4. Utilize strong session management practices and ensure session cookies are secure and HttpOnly.

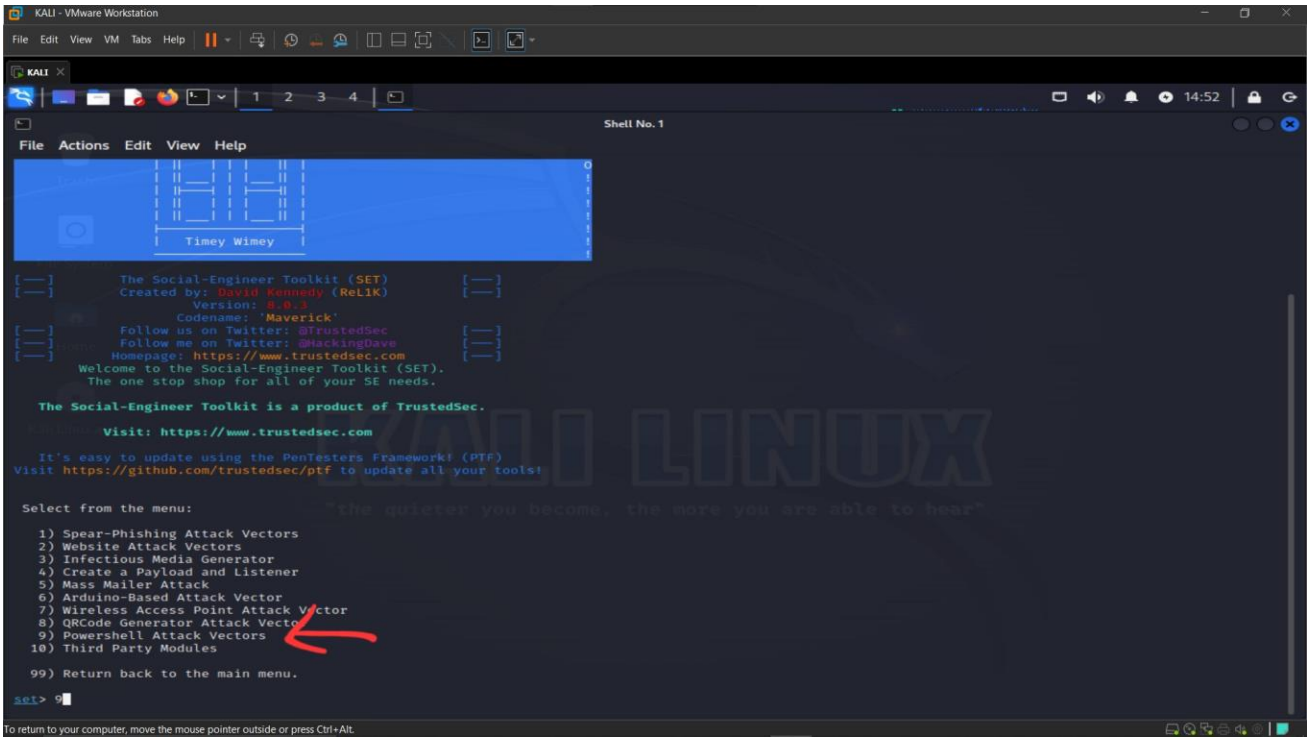
5. Regularly update and patch web applications and server software to protect against known vulnerabilities.

Backdoor Creation Using SET

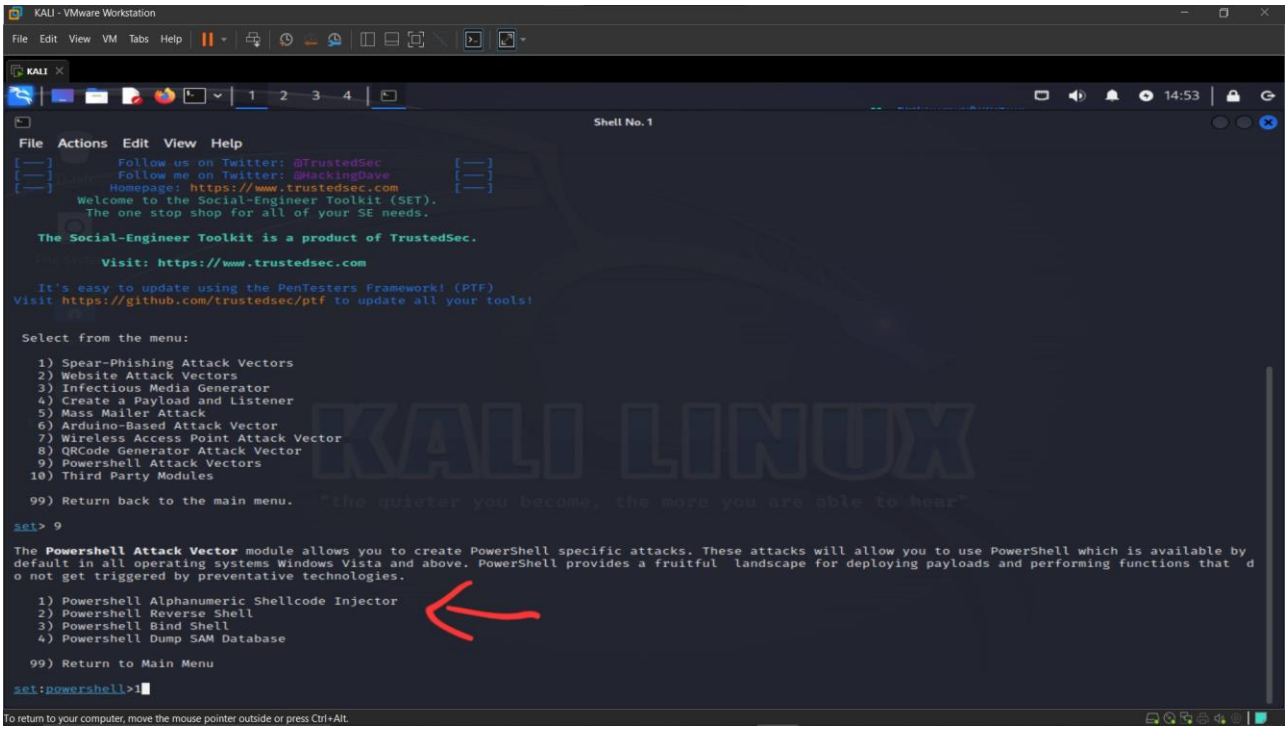
- Start Kali Linux, in applications, click on Social Engineering attacks and select Social-Engineering Toolkit (SET).



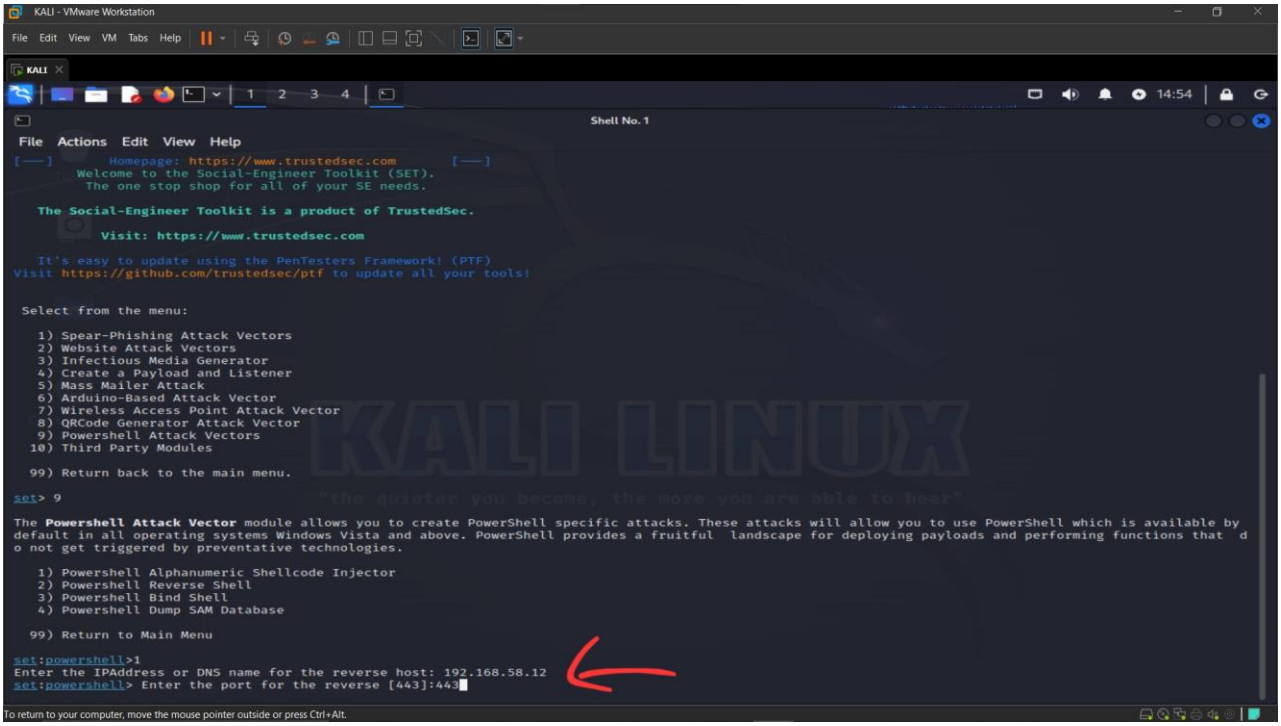
- Once it started, enter '1' which represents "Social-Engineering Attacks".



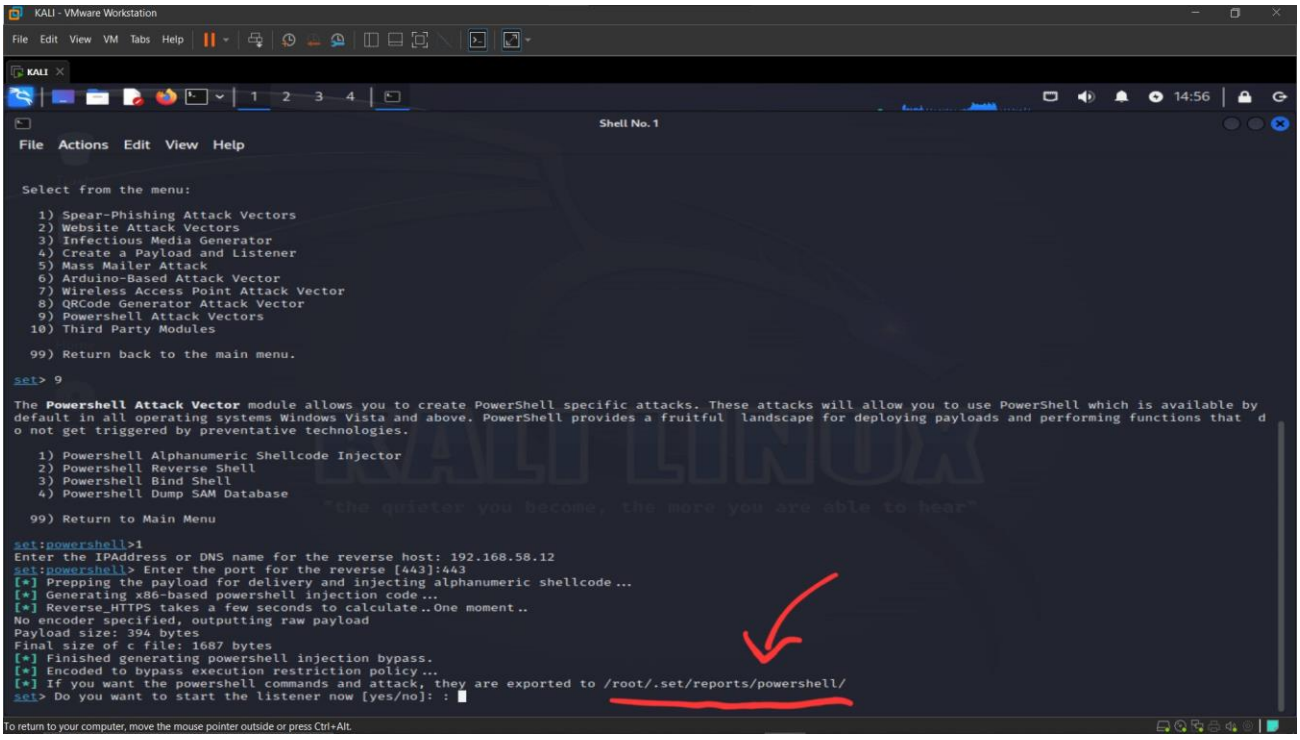
- Then enter '9' which represents "PowerShell Attack Vector".



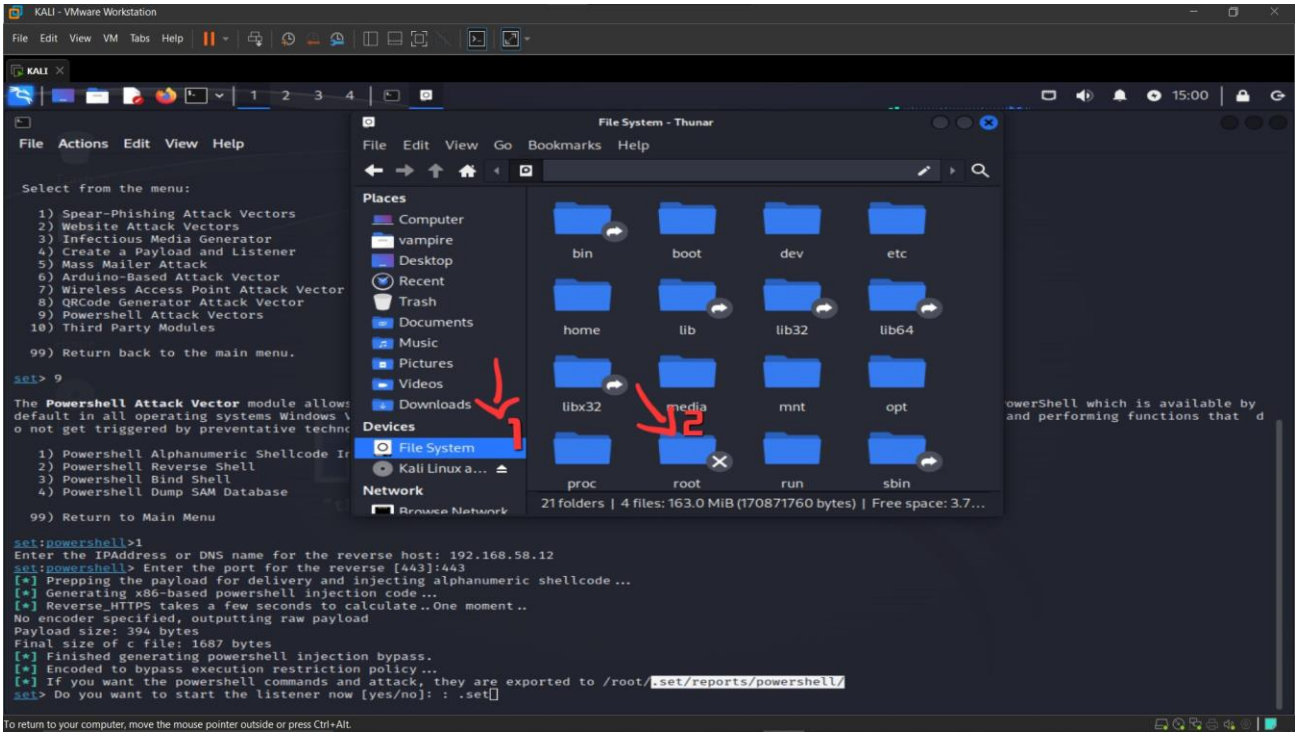
- Then enter '1' which represents "PowerShell Alphanumeric Shell code Injector".



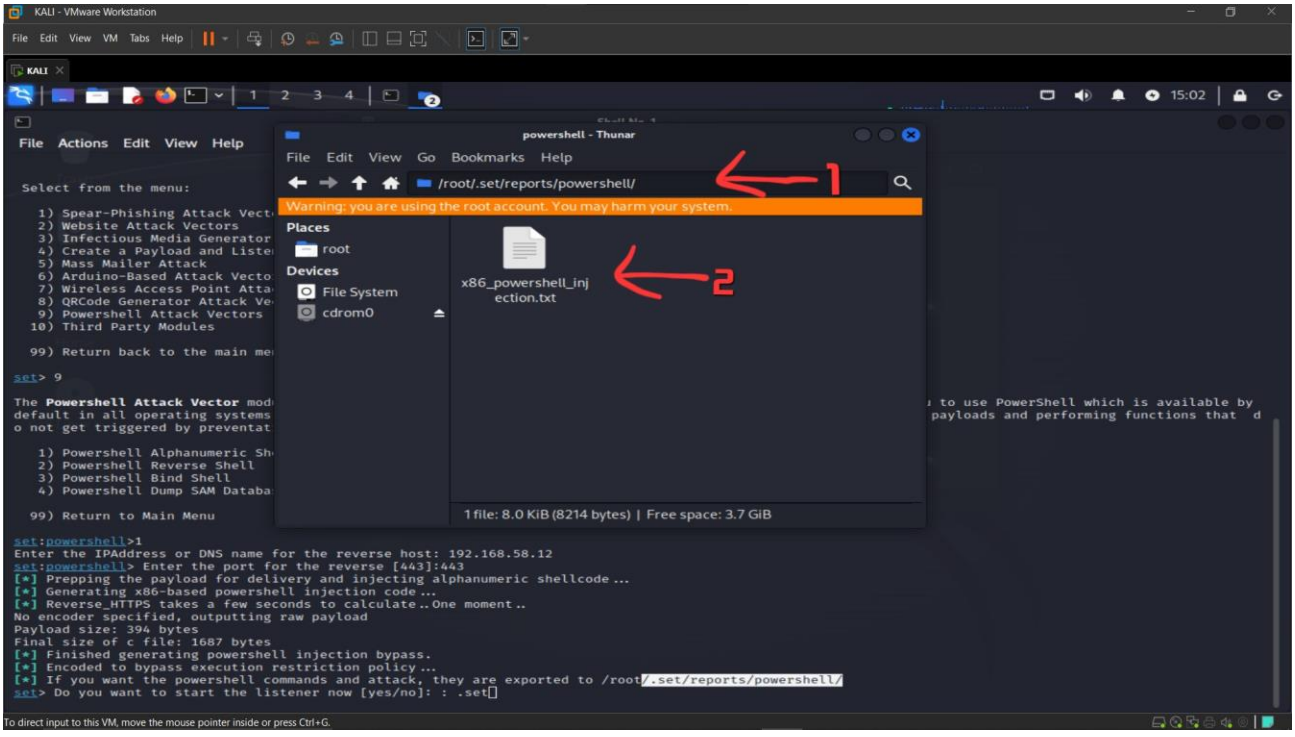
- Enter target's IP address and port number 443 which is default.



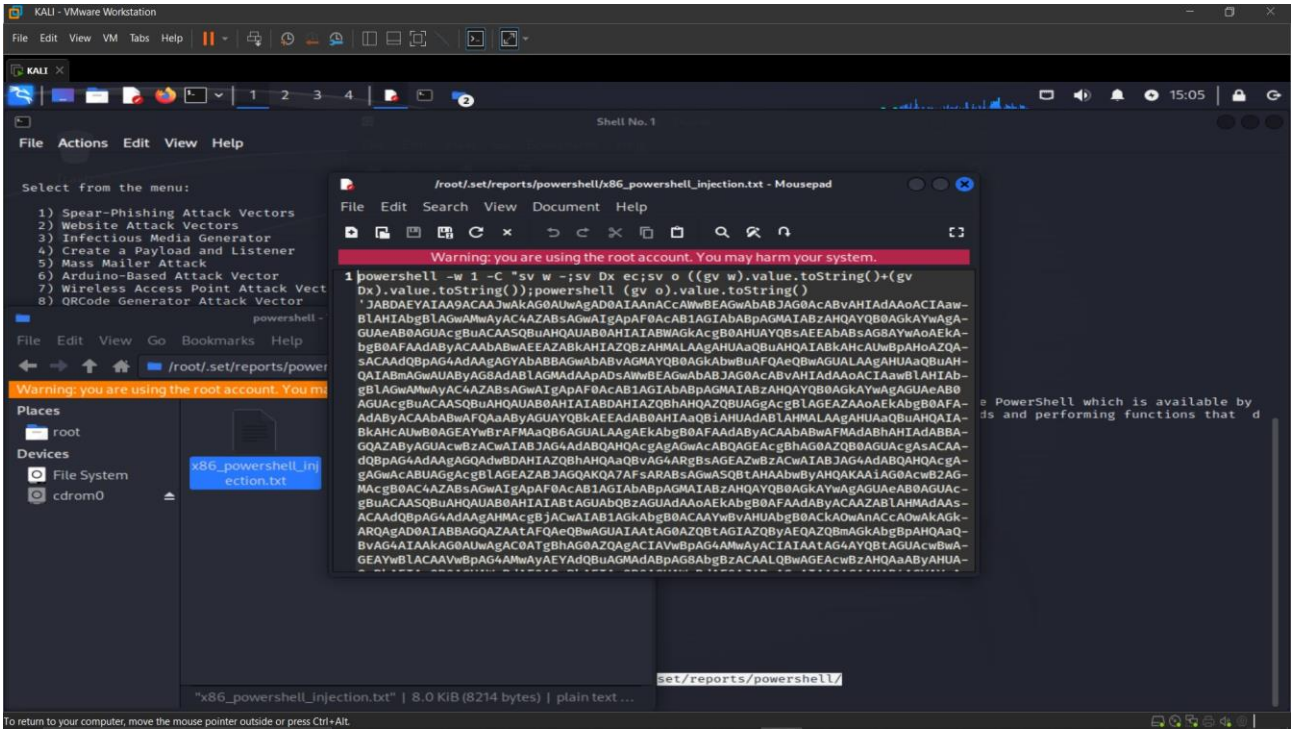
- Then we will get path to script which was created by SET, select it and copy the selection.



- Open folder, then click on File system (1) and click on Root folder (2), enter the password to open root folder.



- Paste the path which was copied earlier (1), there PowerShell Injection file is visible (2).



- Inside that file, Scripting is available to inject target, sending this file to target system and running in it will create backdoor for us.
- This is social engineering attack.

Mitigation:

1. Educate users and employees about social engineering tactics and the risks associated with unsolicited information requests or actions.

2. Enforce strict access controls and adhere to the principle of least privilege to limit unnecessary permissions.

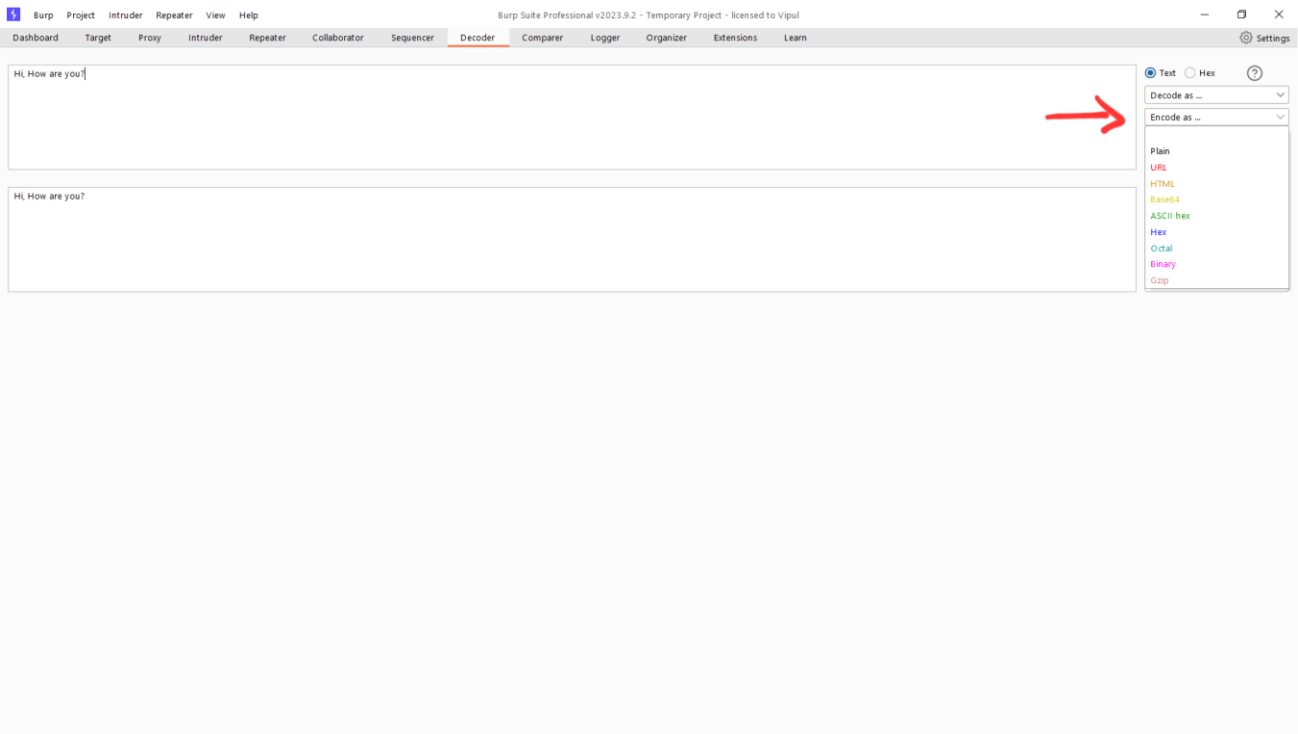
3. Deploy intrusion detection and prevention systems to detect and block unusual network activity and unauthorized access attempts.

4. Continuously update and patch software and systems to eliminate vulnerabilities exploited for backdoor creation.

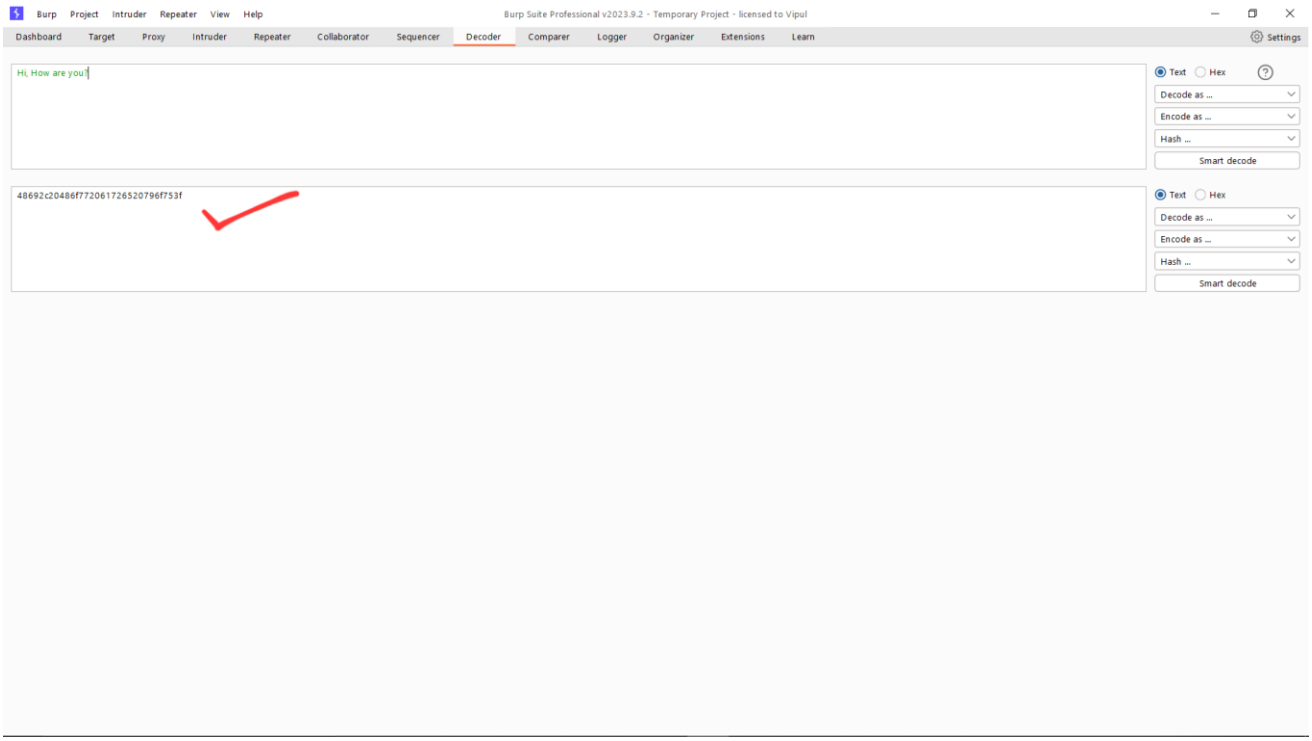
5. Regularly assess the security of third-party applications and maintain awareness of any potential risks they may introduce.

Cryptography

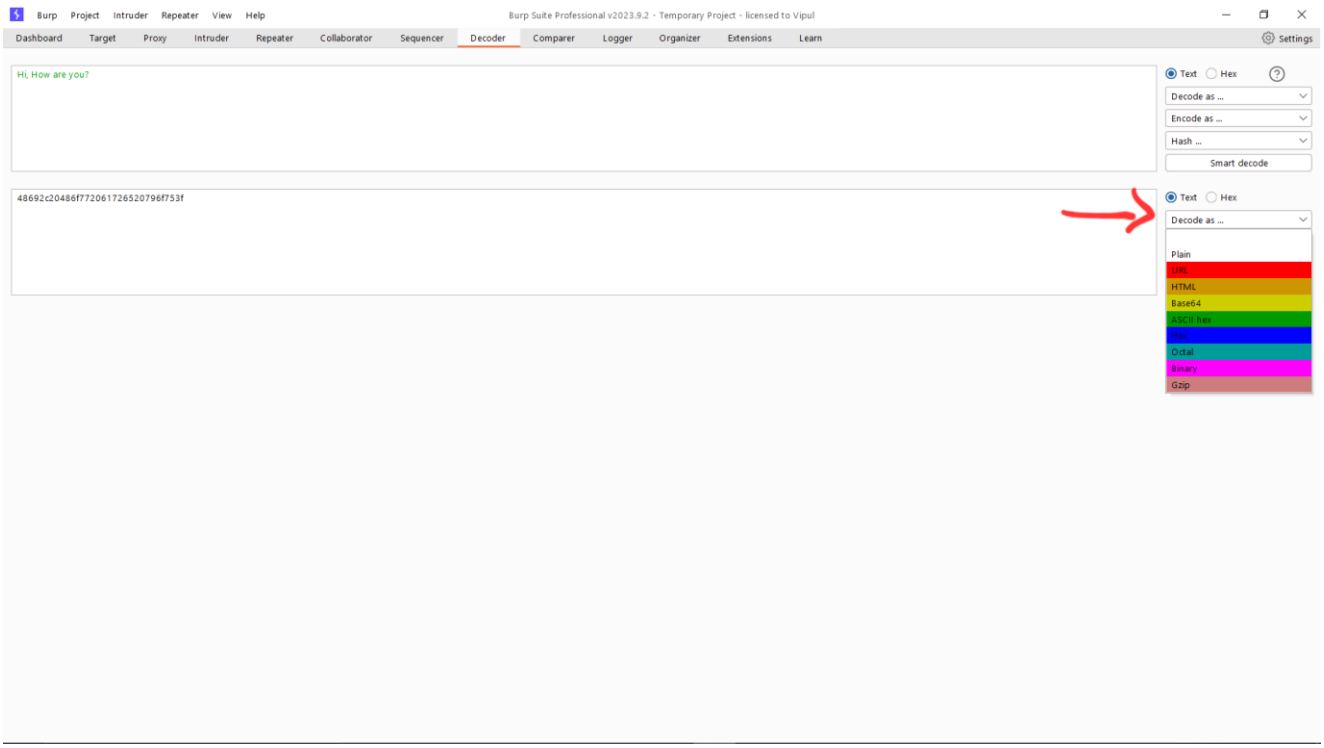
- Open Decoder in Burp Suite.



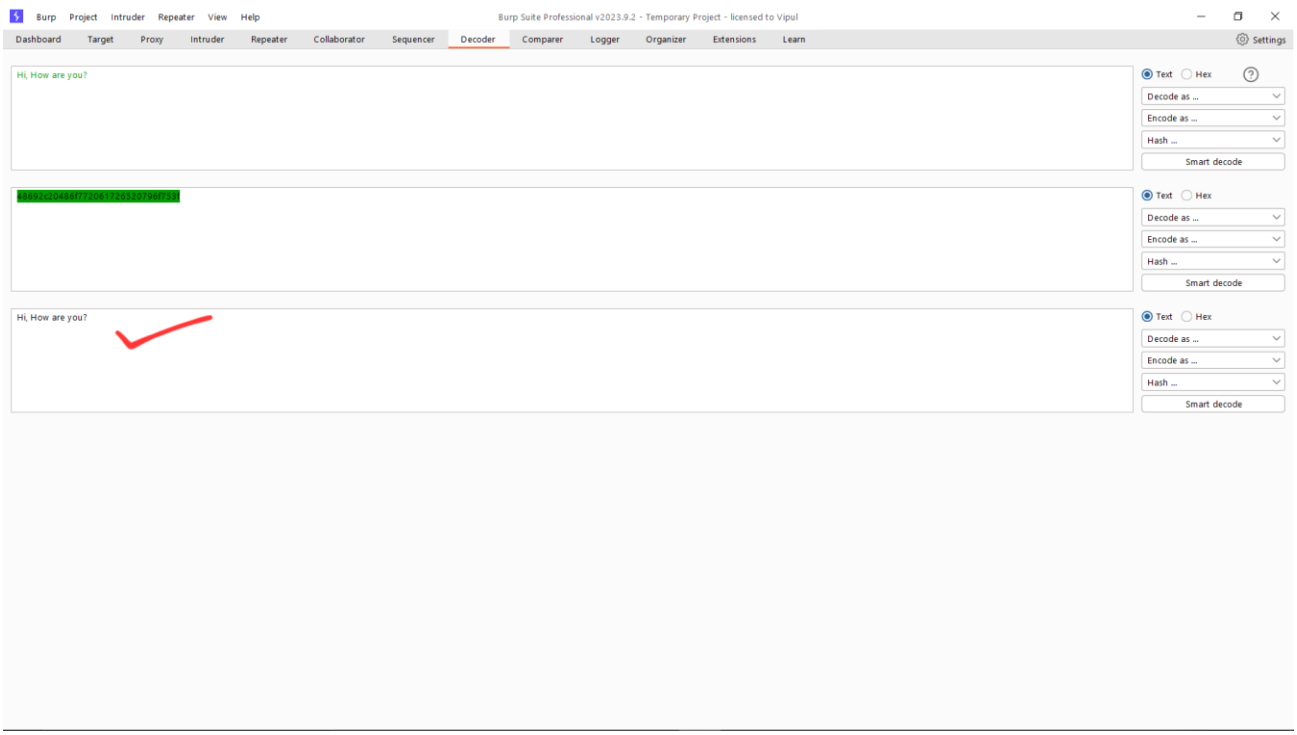
- Enter the text which is needed to encrypt and click on “encode as”.
- There will be list of encryption types, select one type which you wanted for example “ASCII hex”.



➢ The entered text successfully encrypted into selected type.



➢ Now click on decode as and select same type as it is encoded to decrypt the text.



- The encrypted message is successfully decrypted in to plain text again.
- This is known as Cryptography.

Mitigation:

1. Use the latest encryption algorithms and keep encryption protocols up to date to stay resilient against evolving threats.

2. Employ strong encryption for data at rest and in transit, and secure encryption keys in hardware security modules.

3. Regularly audit and review key management practices to ensure the security of cryptographic keys.

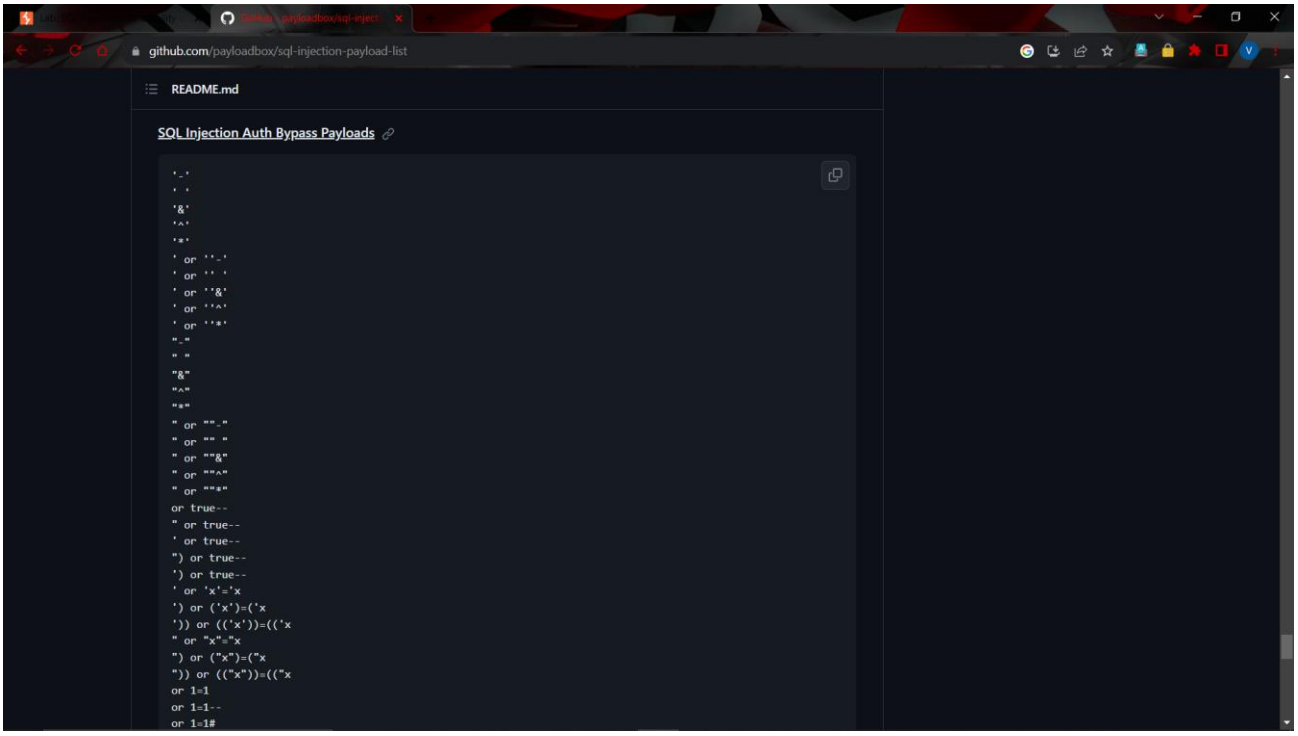
4. Implement end-to-end encryption for data transmission to protect against eavesdropping.

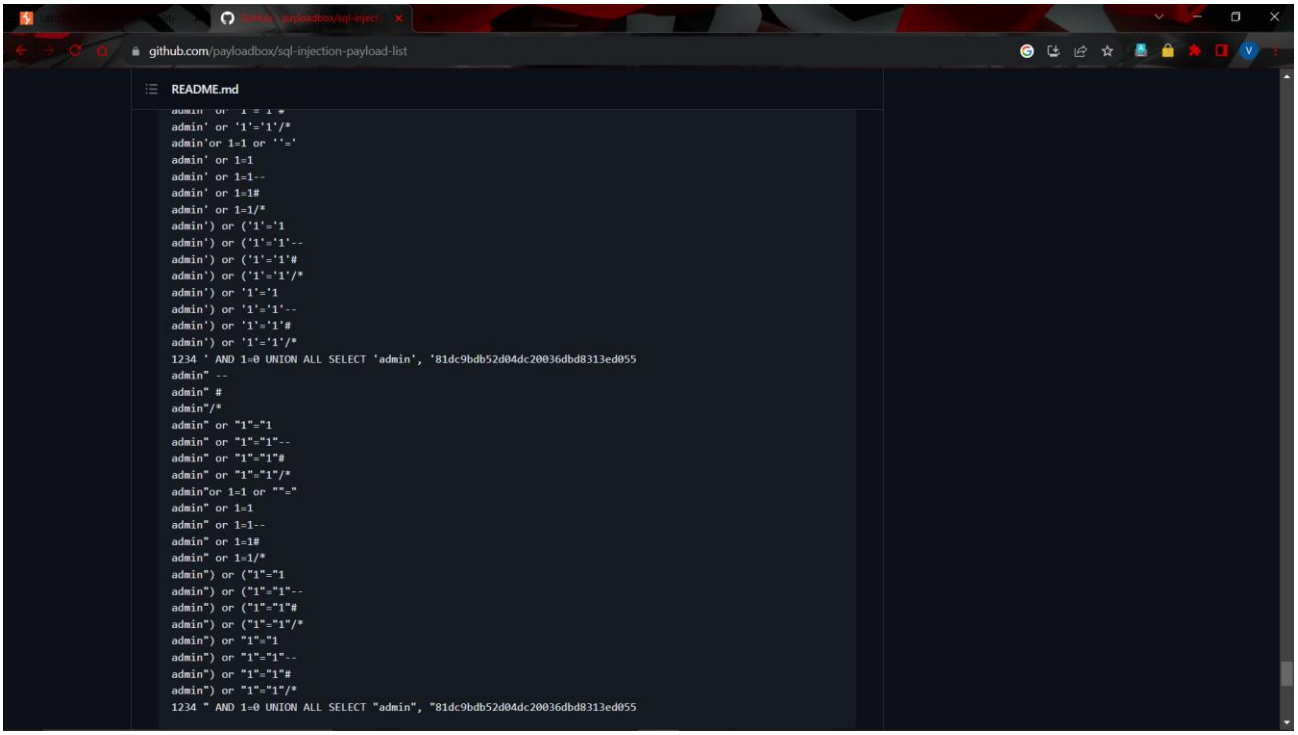
5. Keep a watchful eye on emerging cryptographic vulnerabilities and adapt as necessary.

SQL Injection

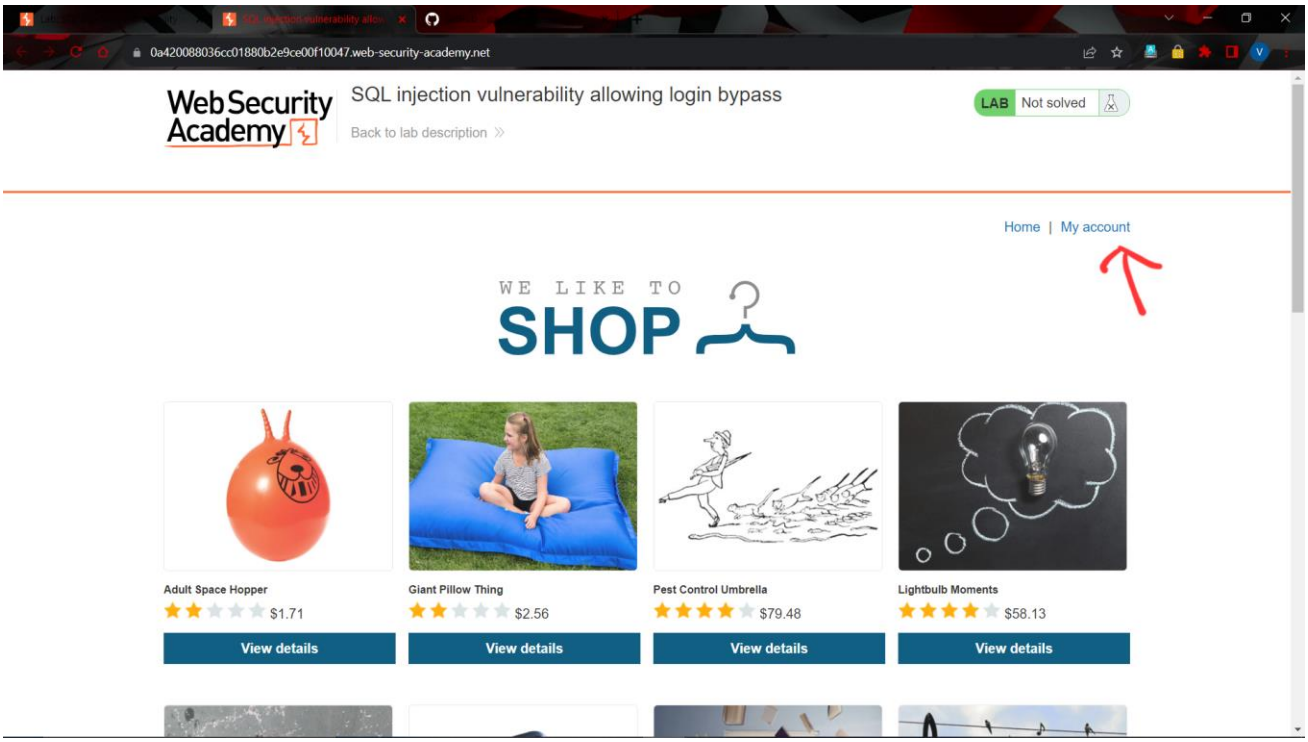
Authentication Bypass by SQL Injection:

- Search for Authentication bypass payloads for SQL injection in GitHub.

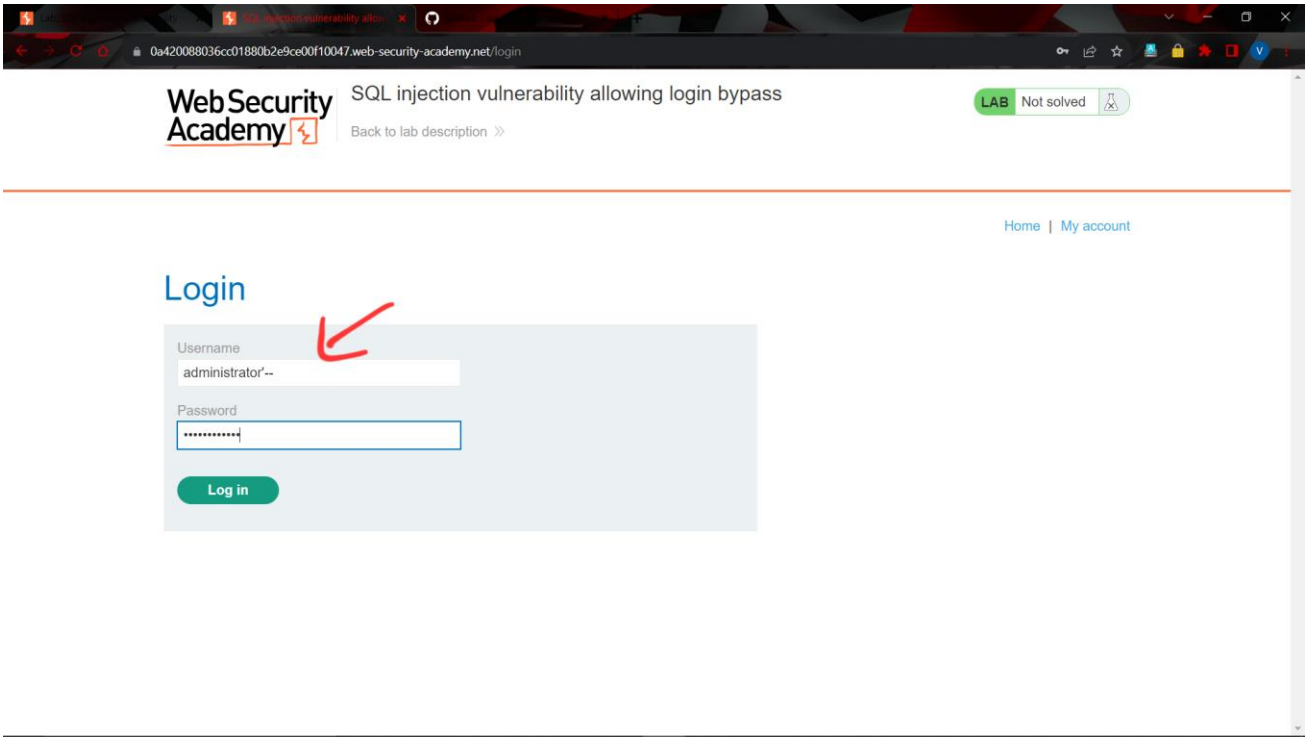




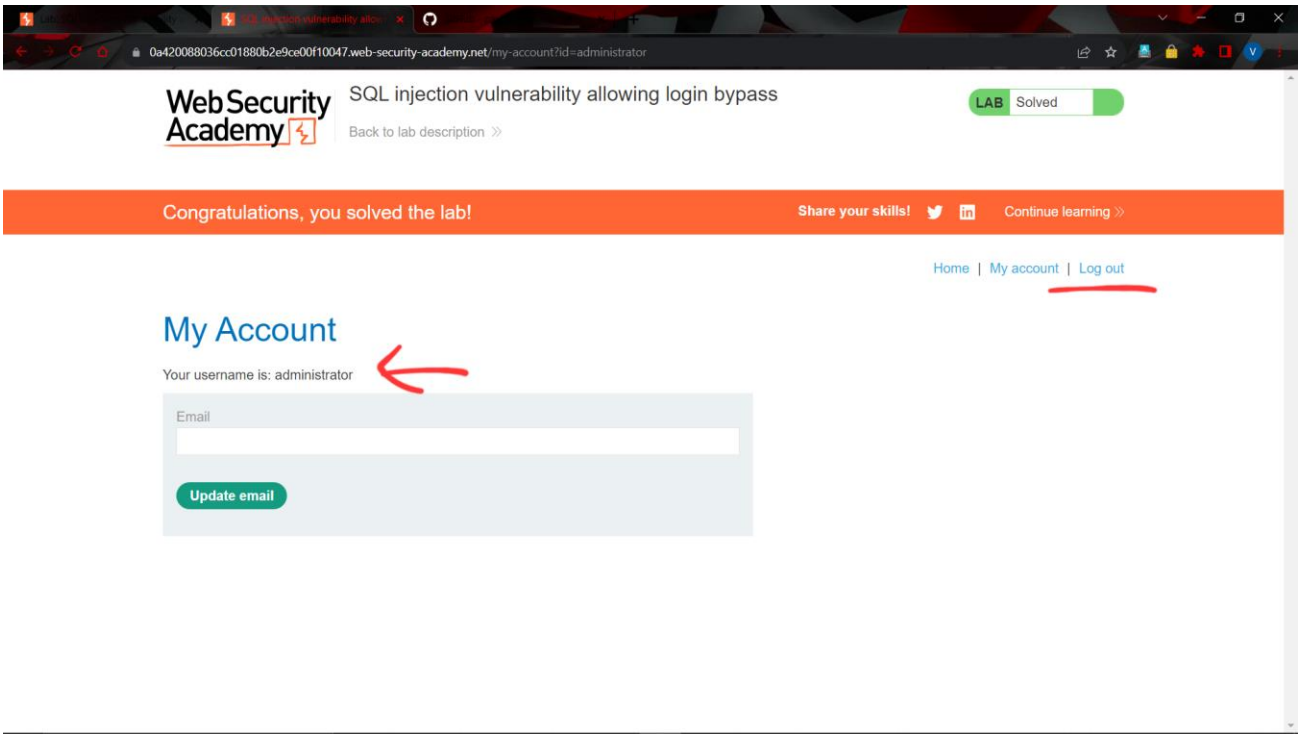
- There are so many payloads, in these only few might work on websites depends on their vulnerability.



- Select a website, click on my account or open login page of targeted website.



- Enter payload in username (such as [administrator'--]) and enter random password and click login.



- Here it is successfully logged into administrator account in the website using that payload.
- This is known as bypassing authentication using SQL Injection.

Mitigation:

1. Use parameterized queries and prepared statements to prevent malicious SQL code injection in database interactions.

2. Validate and sanitize user input to eliminate potential vulnerabilities in SQL queries.

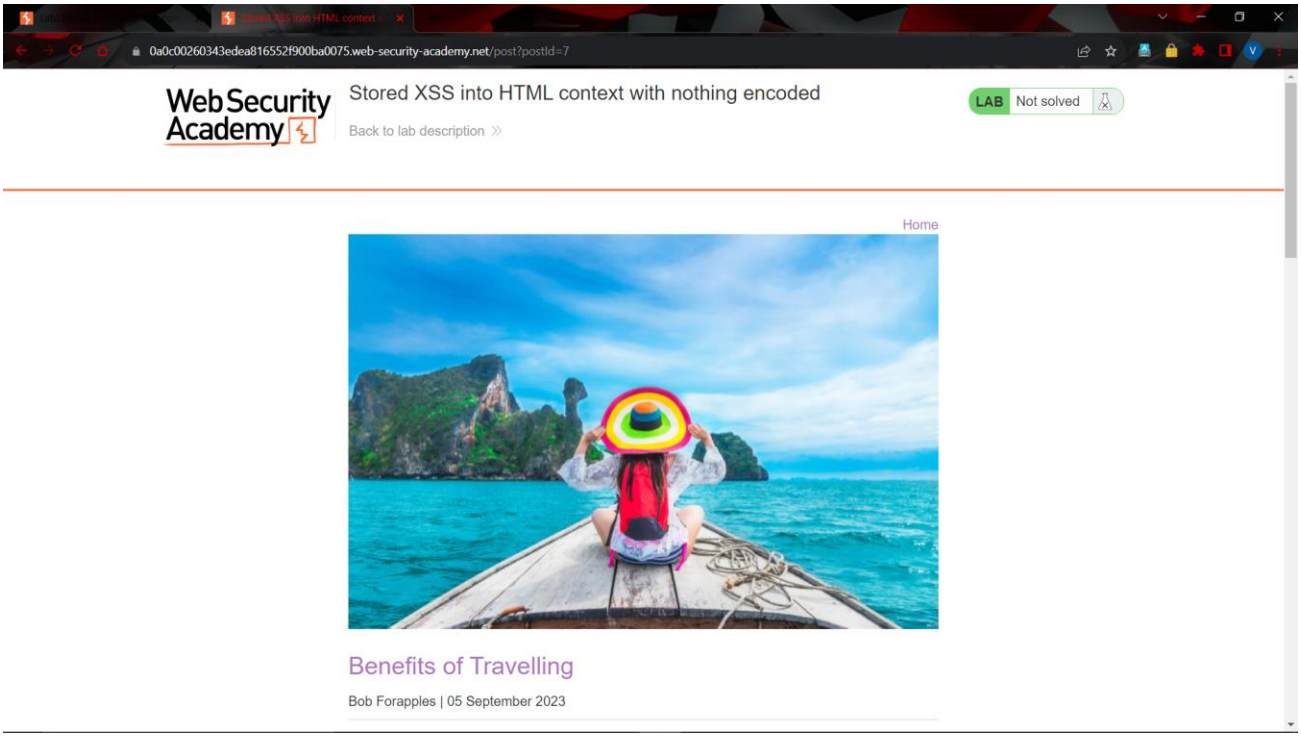
3. Regularly update and patch the database management system to address known security vulnerabilities.

4. Implement robust access controls to limit user access to only the necessary database functions.

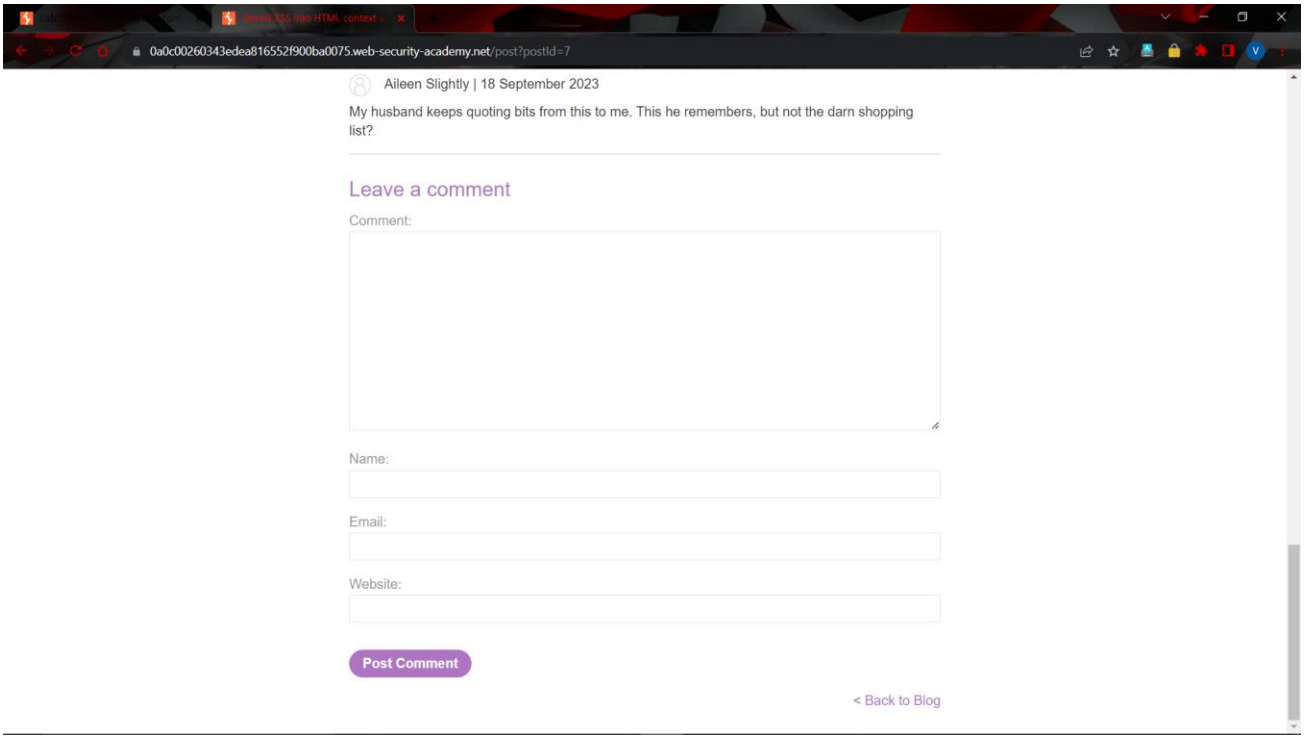
5. Perform regular security assessments and penetration testing to identify and address potential SQL injection vulnerabilities.

Cross-Site Scripting (XSS)

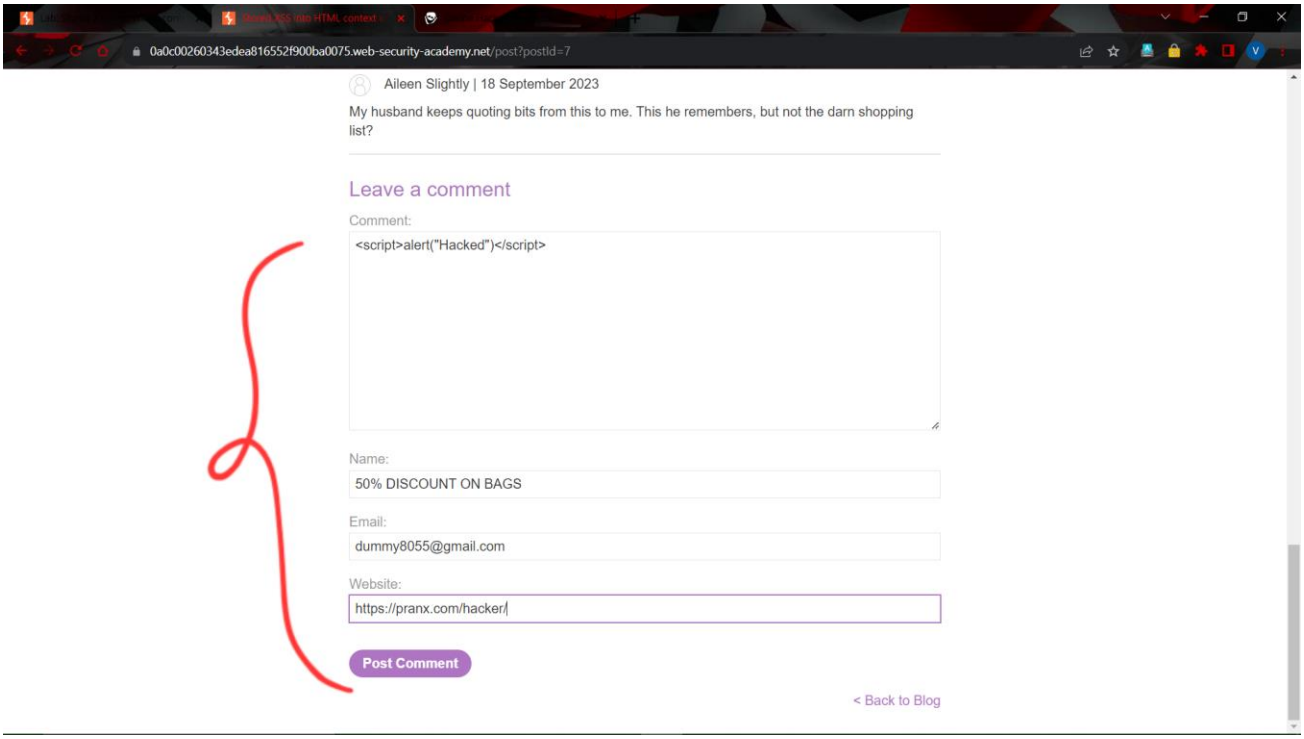
1- Stored XSS:



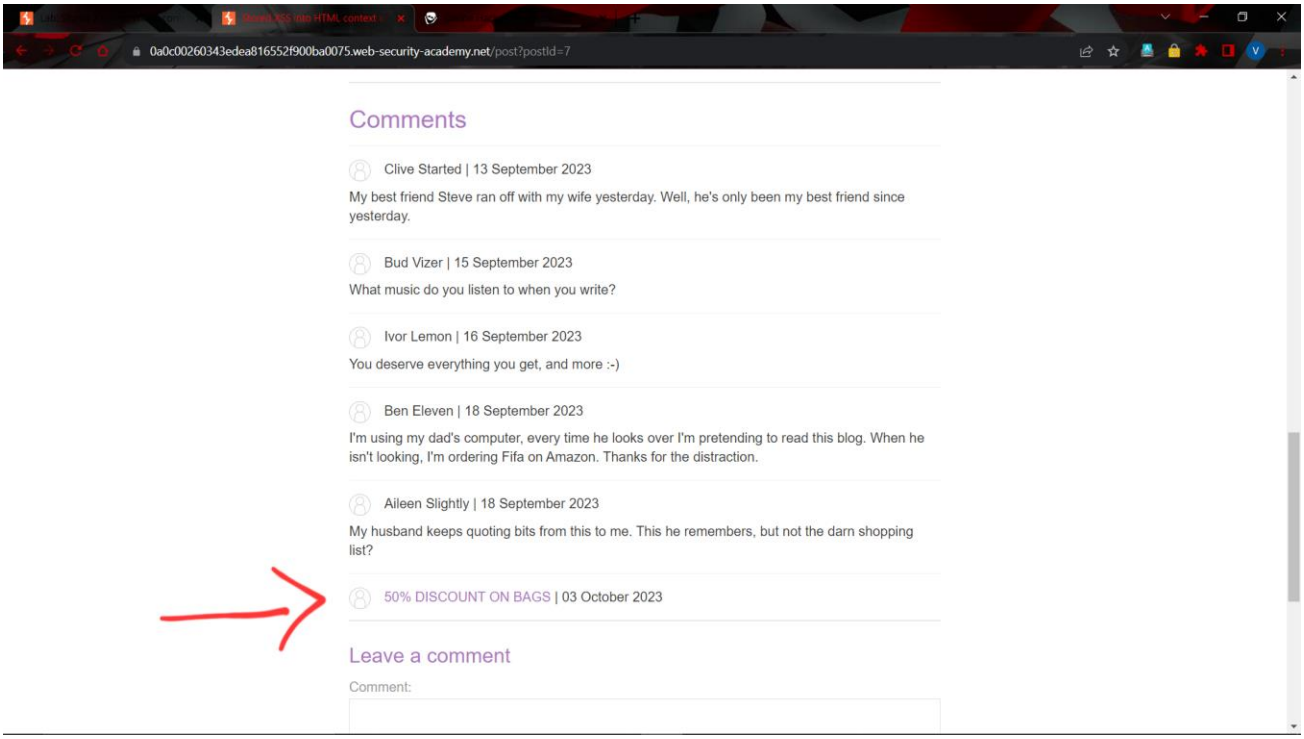
- Open ecommerce website or social media or blogs where you wanted to perform stored XSS, for example travelling blog.



- Open comment section in that website or page.



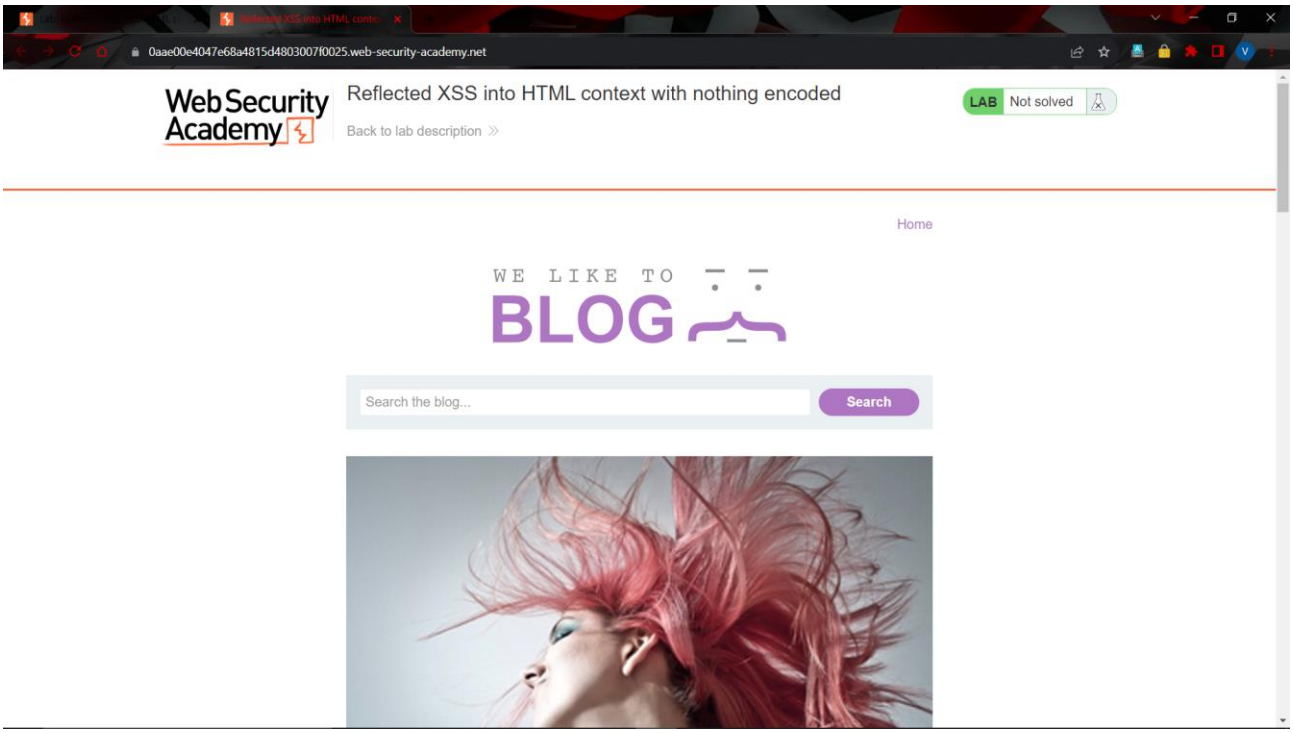
- Fill the sections with desired script and link to redirect users and good caption to attract users.



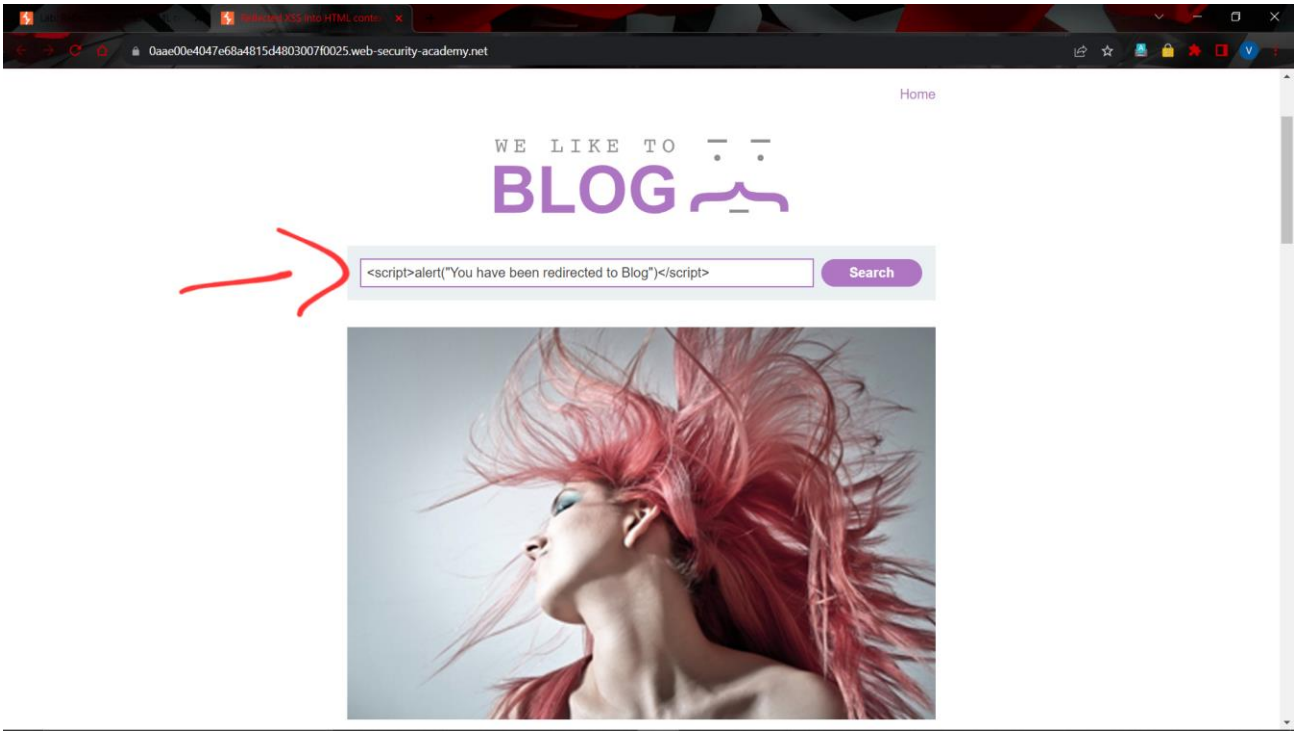
- Stored XSS script is hidden behind attractive caption.

- When users clicked comment, it will automatically redirected to mentioned link.
- This is Stored XSS which remains long term unless website or blog owner removes it.

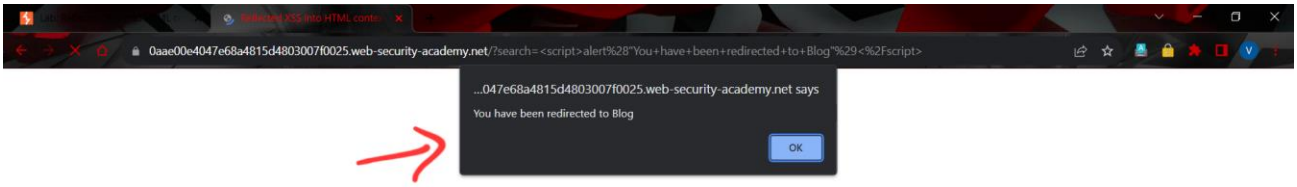
2- Reflected XSS:



- Open a target website to perform reflected XSS.



- Enter the script in search bar or where ever there is an input option in the website.



- The messaged entered in the script is shown in a pop up window.
- This is known as reflected XSS which is performed only once per script.

Mitigation:

1. Validate and sanitize user-generated content before rendering it in web pages to prevent script injection.

2. Implement security headers, such as X-XSS-Protection and Content Security Policy (CSP), to control script execution and sources.

3. Keep web application frameworks and libraries up to date to benefit from security patches and improvements.

4. Educate developers and users about the risks of XSS attacks and how to recognize and report suspicious activity.

5. Utilize browser security features like the 'sandbox' attribute to further restrict the execution of potentially harmful scripts

Conclusion

In the ever-evolving landscape of cyber security, the challenges posed by threats such as brute force attacks, cryptography, backdoor creation, CSRF attacks, SQL injection, and XSS vulnerabilities serve as constant reminders of the complex, multifaceted nature of the digital realm. As we've explored each of these topics in depth, it becomes evident that safeguarding our data and digital infrastructure demands both awareness and proactivity.

The brute force attack, with its relentless trial-and-error approach, underscores the importance of robust password and encryption practices. Cryptography, as the cornerstone of information security, is a testament to the power of encoding and decoding messages to protect sensitive information.

The creation of backdoors using tools like SET highlights the critical role of education in preventing social engineering attacks, where human psychology can be manipulated for malicious purposes. The CSRF attack reveals how trust in websites can be exploited, emphasizing the need for thorough validation of requests in web applications.

SQL injection is a cautionary tale for web developers, demonstrating the vital importance of input validation to prevent malicious database tampering. Lastly, the XSS vulnerability serves as a reminder of the need for developers and administrators to diligently sanitize user-generated content and protect against the injection of malicious scripts.

In conclusion, cyber security is a never-ending battle, where knowledge and preparedness are our most potent weapons. As technology advances, so too do the tactics of cybercriminals. Yet, through understanding these threats and implementing best practices, we can bolster our defenses and reduce the risk of falling victim to these ever-present dangers. The interconnected world we live in demands vigilance, adaptability, and collaboration to keep our digital lives secure. By actively addressing these cyber security challenges, we pave the way for a safer, more resilient digital future