

**AKADEMIA GÓRNICZO-HUTNICZA
IM. STANISŁAWA STASZICA W KRAKOWIE**

Wydział Informatyki, Elektroniki i Telekomunikacji
Katedra Informatyki



PROJEKT INŻYNIERSKI

**GRA TYPU CAPTURE-THE-FLAG
OPARTA O REVERSE ENGINEERING**

CAPTURE-THE-FLAG GAME BASED ON REVERSE ENGINEERING

PIOTR SZCZYGIEŁ

KIERUNEK:
Informatyka

OPIEKUN:
dr inż. Łukasz Faber

Kraków, 2020

Uprzedzony o odpowiedzialności karnej na podstawie art. 115 ust. 1 i 2 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz.U. z 2006 r. Nr 90, poz. 631 z późn. zm.): „Kto przywłaszcza sobie autorstwo albo wprowadza w błąd co do autorstwa całości lub części cudzego utworu albo artystycznego wykonania, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3. Tej samej karze podlega, kto rozpowszechnia bez podania nazwiska lub pseudonimu twórcy cudzy utwór w wersji oryginalnej albo w postaci opracowania, artystycznego wykonania albo publicznie zniekształca taki utwór, artystyczne wykonanie, fonogram, wideogram lub nadanie.”, a także uprzedzony o odpowiedzialności dyscyplinarnej na podstawie art. 211 ust. 1 ustawy z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (t.j. Dz. U. z 2012 r. poz. 572, z późn. zm.): „Za naruszenie przepisów obowiązujących w uczelni oraz za czyny uchybiające godności studenta student ponosi odpowiedzialność dyscyplinarną przed komisją dyscyplinarną albo przed sądem koleżeńskim samorządu studenckiego, zwanym dalej «sądem koleżeńskim».”, oświadczam, że niniejszą pracę dyplomową wykonałem(-am) osobiście, samodzielnie i że nie korzystałem(-am) ze źródeł innych niż wymienione w pracy.

.....

PODPIS

Spis treści

| | | |
|----------|--|-----------|
| 1 | Cel prac i wizja produktu | 4 |
| 1.1 | Wprowadzenie | 4 |
| 1.2 | Dostępne platformy | 6 |
| 1.3 | Języki programowania i narzędzia | 6 |
| 2 | Zakres funkcjonalności | 7 |
| 2.1 | Platforma | 7 |
| 2.2 | Użytkownicy | 7 |
| 2.3 | Prezentacja interfejsu użytkownika | 8 |
| 3 | Wybrane aspekty realizacji | 17 |
| 4 | Organizacja pracy | 17 |
| 5 | Wyniki projektu | 17 |

1. Cel prac i wizja produktu

1.1. Wprowadzenie

Gra typu Capture-the-Flag jest to rodzaj zawodów z ogólnie pojętego bezpieczeństwa komputerowego. Ich celem zwykle jest edukacja uczestników o zabezpieczeniach systemów oraz możliwość pokazania im jak reagować na wypadek wystąpienia rzeczywistych ataków. Zawody takie podzielone są zazwyczaj na poszczególne zadania z różnych kategorii. Aby rozwiązać takie zadanie należy znaleźć "flagę", którą następnie podaje się w interfejsie udostępnionym przez organizatora zawodów. Flagą w tym wypadku jest ciąg znaków, który możemy uzyskać poprzez rozwiązanie zadania. Przykładowo w najprostszych zadaniach z dziedziny eksploatacji stron internetowych, flagę możemy znaleźć klikając "Pokaż źródło strony" w przeglądarce internetowej.

```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4     <meta charset="UTF-8">
5     <title>Source Me 1</title>
6 </head>
7 <body>
8 <h2>Welcome to the admin portal!</h2>
9 Currently, only the user who can login is 'admin'.
10 <br>
11 <!-- Shh, don't tell anyone. The admin password is f7s0jkl -->
12 <form action="/login.php" method="get">
13 Username:<input type="text" name = "user"><br>
14 Password:<input type="text" name = "pass"><br>
15 <input type="submit" value="Submit">
16 </form>
17 </body>
18 </html>
```

Rysunek 1: Flaga **f7s0jkl** ukryta w źródle strony internetowej

W tej pracy zaprezentowana będzie jednak grę oparta wyłącznie o Reverse Engineering (ang. Inżynieria Wsteczna). Inżynieria wsteczna oprogramowania może odbywać się na różne sposoby. Może to być przykładowo wykorzystanie tzw. snifferów do analizy protokołów komunikacyjnych aplikacji internetowej. W tym wypadku będzie ona jednak zazwyczaj oznaczała proces analizy programu, aby zrozumieć co robi oraz w jaki sposób. Przedstawione zadania można by też podpiąć do kategorii eksploatacji binarnej (ang. Binary Exploitation), która w pewny sposób pokrywa się z zagadnieniami Reverse Engineeringu. Jest to mianowicie proces wykorzystywania niedoskonałości programów w celu zmuszenia ich do zrobienia czegoś, czego w normalnej sytuacji nie powinny robić. Te dwie kategorie pokrywają się ze sobą, ponieważ zazwyczaj nie jest możliwe rozwiązanie zadania z kategorii eksploatacji binarnej, bez wykorzystania do tego inżynierii wstecznej.

Produktem końcowym będzie zbiór kilku zadań udostępniony na platformie webowej. Platforma sama w sobie nie jest niczym specjalnym, udostępnia jedynie takie powszechne funkcjonalności jak rejestracja użytkowników, ranking najlepszych graczy, pobieranie zadań oraz interfejs umożliwiający wprowadzanie znalezionych flag. Z tego względu użyta zostanie gotowa platforma CTFd [2]. Użycie takiego gotowego rozwiązania pozwoli w pełni skupić się na samych zadaniach, a ominąć takie kwestie jak np. gracze łamiący zabezpieczenia platformy.

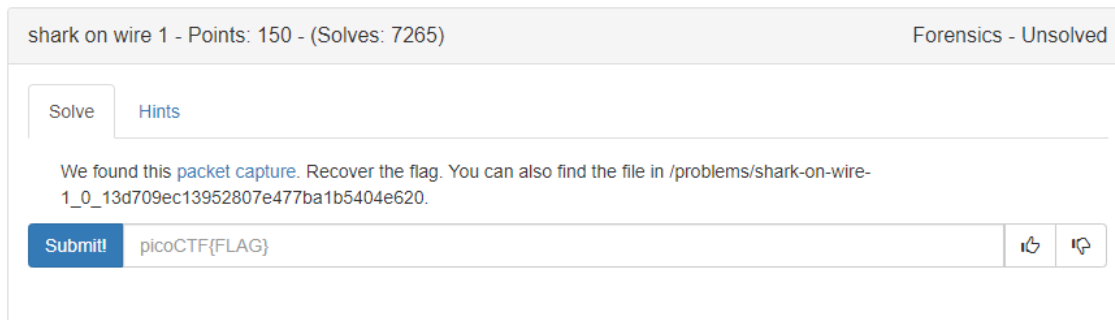


Rysunek 2: Przykładowe zadanie na stronie demonstracyjnej CTFd

W tej pracy opisany zostanie zarówno proces tworzenia poszczególnych zadań, jak i przykładowe ich rozwiązania. Użyte zostało słowo "przykładowe", ponieważ w takiej kategorii jak Binary Exploitation / Reverse Engineering liczba sposobów na rozwiązanie danego zadania jest ograniczona jedynie przez wyobraźnię uczestnika. Nie ograniczymy się również do korzystania ciągle z tych samych narzędzi. Pokazane zostaną różnorodne podejścia do analizy i rozwiązywania wyzwań. Zadania będą tworzone z zamiarem zachowania rosnącego stopnia trudności. Na początku uczestnik będzie miał szansę rozwiązać proste zadania, zachęcające go do dalszej rozgrywki. Finalne zadania powinny stanowić wyzwanie nawet dla doświadczonych graczy.

1.2. Dostępne platformy

Aktualnie istnieje wiele różnych zawodów CTF online. Jednym z popularniejszych jest picoCTF [5]. Można tam wejść kiedykolwiek, zalogować się i zająć się rozwiązywaniem problemów.



Rysunek 3: Zadanie z kategorii Forensics na stronie picoCTF

Główną motywacją do napisania tej pracy jest fakt, że strony tego typu często skupiają się na zadaniach w takich kategoriach jak Forensics czy Web Exploitation. Mnie natomiast bardzo interesuje temat inżynierii wstecznej i chciałem przygotować wyzwania oparte o zadania tylko z tej kategorii.

1.3. Języki programowania i narzędzia

Zadania będą tworzone w języku C. Jest to powszechnie znany język, który z wyłączoną zbyt agresywną optymalizacją ze strony kompilatora, generuje w miarę przewidywalny kod maszynowy. Zaletą tego jest to, że narzędzia do debugowania, dezasemblacji oraz wykonywania innych analiz programów dobrze radzą sobie z takimi plikami. Dzięki temu język ten zapewni nam kontrolę nad tym w jakim stopniu graczowi ułatwimy lub utrudnimy rozgrywkę. W celu zapewnienia większej różnorodności środowisk korzystać będziemy zarówno z systemu Windows jak i Linux.

Do rozwiązywania zadań posłużymy się różnorodnymi rodzajami narzędzi. Poczynając od linuxowych programów linii poleceń takich jak *strings* czy *gdb*, pisania własnych narzędzi w języku *Python*, czy w końcu korzystając z pełnoprawnych narzędzi z interfejsem graficznym takich jak używana przez NSA *Ghidra*, *Cutter*, czy debugger dla systemu Windows *RemedyBG*.

2. Zakres funkcjonalności

2.1. Platforma

Do interfejsu webowego skorzystamy z gotowej platformy CTFd [2]. Finalny produkt będzie dostępny pod adresem <https://ctf.szczygiel.dev>. Strona postawiona będzie na prywatnym serwerze VPS. Platforma będzie uruchomiona w środowisku docker [3], a wystawiona do świata będzie poprzez serwer Caddy [1], który w prosty sposób zapewni nam HTTPS, dzięki organizacji Let's Encrypt [4].

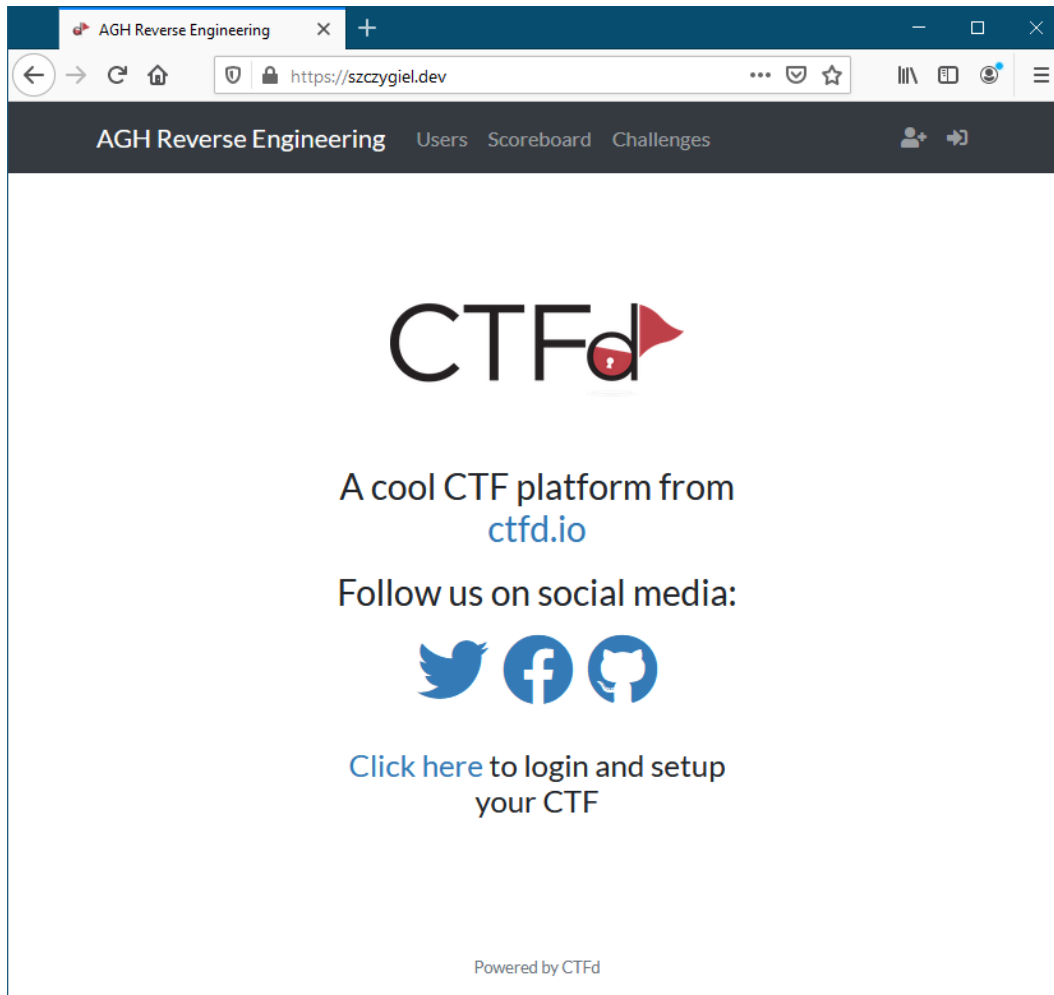
2.2. Użytkownicy

Użytkownikiem systemu będzie każda osoba zainteresowana rozwiązywaniem tego rodzaju zadań. Może to być zarówno ktoś kształcący się lub pracujący w dziale informatycznym, jak i osoba dla której jest to jedynie hobby.

Wszystkie gotowe zadania zostaną wrzucone na platformę, dzięki czemu każda zainteresowana osoba będzie mogła spróbować swoich sił.

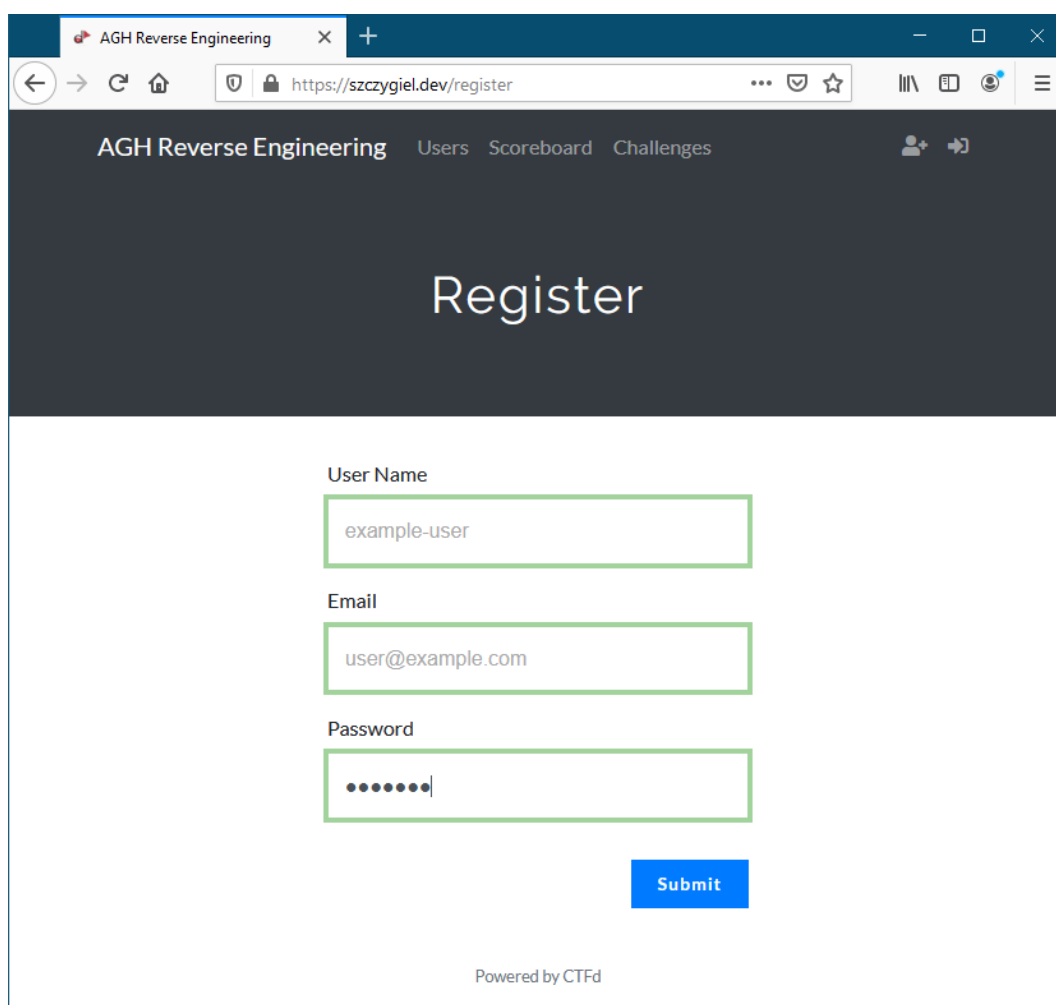
2.3. Prezentacja interfejsu użytkownika

Pierwsze co zobaczy każdy użytkownik wchodzący na platformę, to strona główna. Będzie z niej można przejść do reszty podstron, takich jak logowanie, rejestracja, wylogowanie, spis graczy, tabela wyników oraz lista dostępnych zadań.



Rysunek 4: Strona główna platformy CTF

Poniżej przedstawiony jest interfejs rejestracji nowego użytkownika. Nie będzie to nic skomplikowanego - wystarczy podać login, email oraz hasło.



The image shows a web browser window with the title "AGH Reverse Engineering". The address bar displays "https://szygiel.dev/register". The page has a dark blue header with the site name and navigation links: "Users", "Scoreboard", and "Challenges". The main content area has a dark blue background with the word "Register" in large white text. Below this, on a white background, are three input fields: "User Name" with the value "example-user", "Email" with the value "user@example.com", and "Password" with masked characters. A blue "Submit" button is positioned to the right of the password field. At the bottom of the white area, it says "Powered by CTFd".

AGH Reverse Engineering Users Scoreboard Challenges

Register

User Name
example-user

Email
user@example.com

Password
●●●●●●

Submit

Powered by CTFd

Rysunek 5: Rejestracja nowego użytkownika

Jeśli użytkownik posiada konto to będzie się mógł na nie zalogować.

AGH Reverse Engineering Users Scoreboard Challenges

Login

User Name or Email

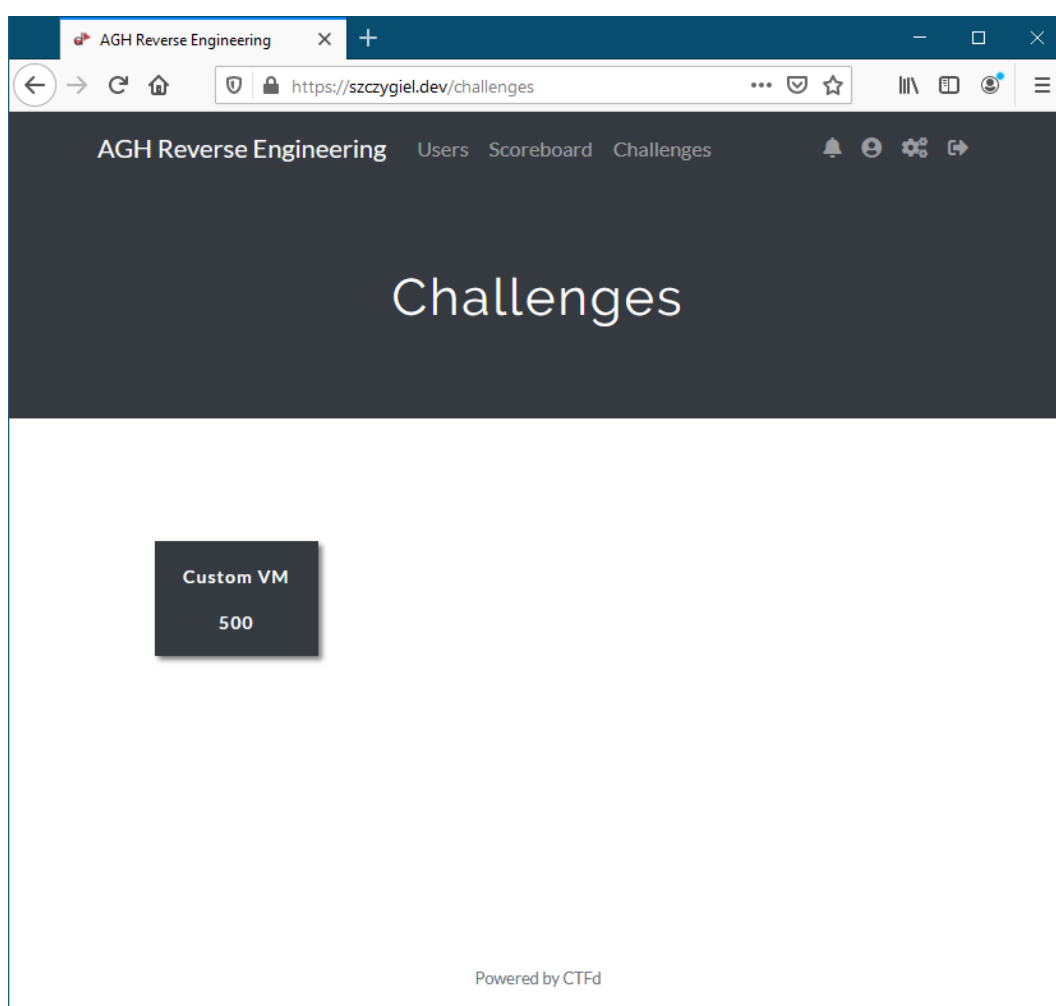
Password

[Forgot your password?](#) [Submit](#)

Powered by CTFd

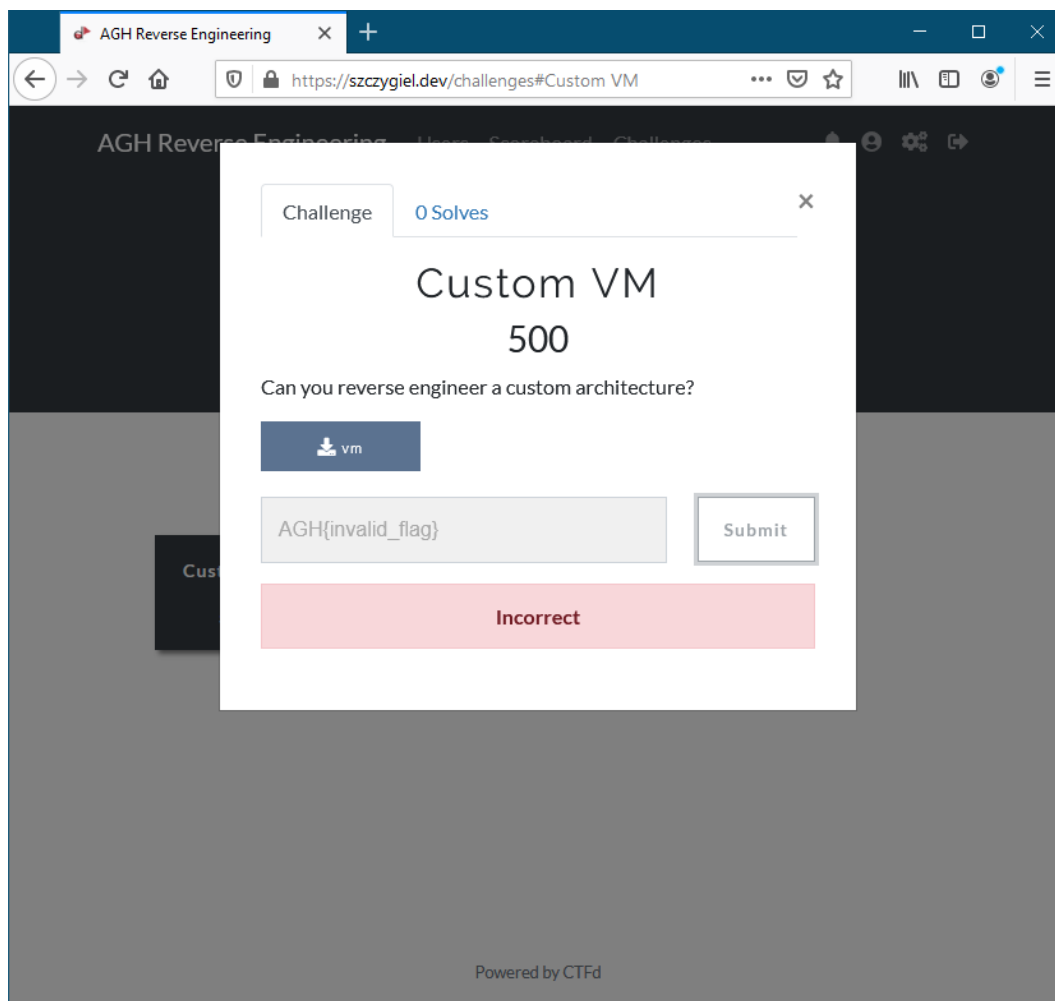
Rysunek 6: Panel logowania dla istniejącego użytkownika

Będąc zalogowanym, można wybrać zadanie które ma się ochotę rozwiązać.



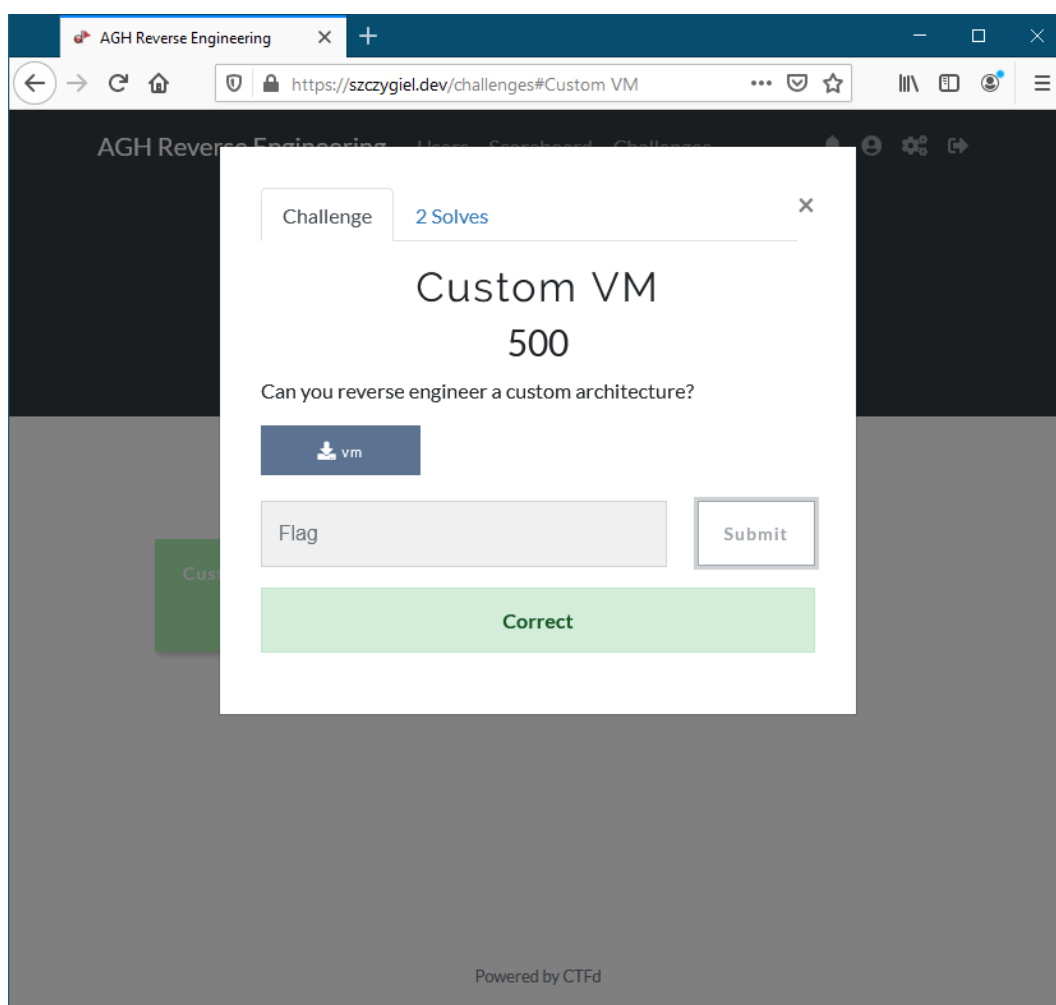
Rysunek 7: Wybór zadania do rozwiązania

Po wybraniu interesującego nas zadania, można pobrać dostarczony plik, a następnie po rozwiązaniu zadania wprowadzić prawidłową (lub nie) flagę.



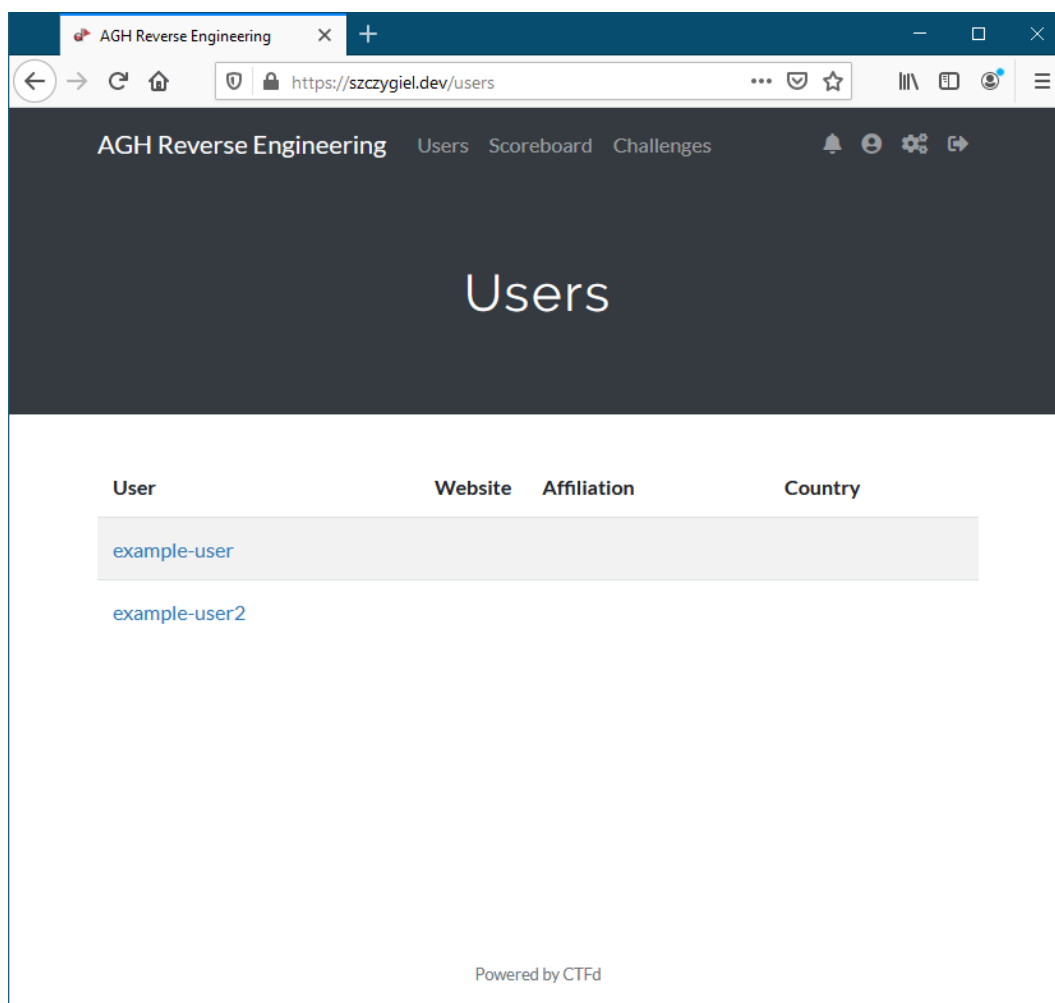
Rysunek 8: Interfejs zadania oraz wprowadzenie nieprawidłowej flagi

Po wprowadzeniu prawidłowej flagi otrzymamy stosowny komunikat. Można również zauważyć, że zadanie w tle zmieniło kolor na zielony.



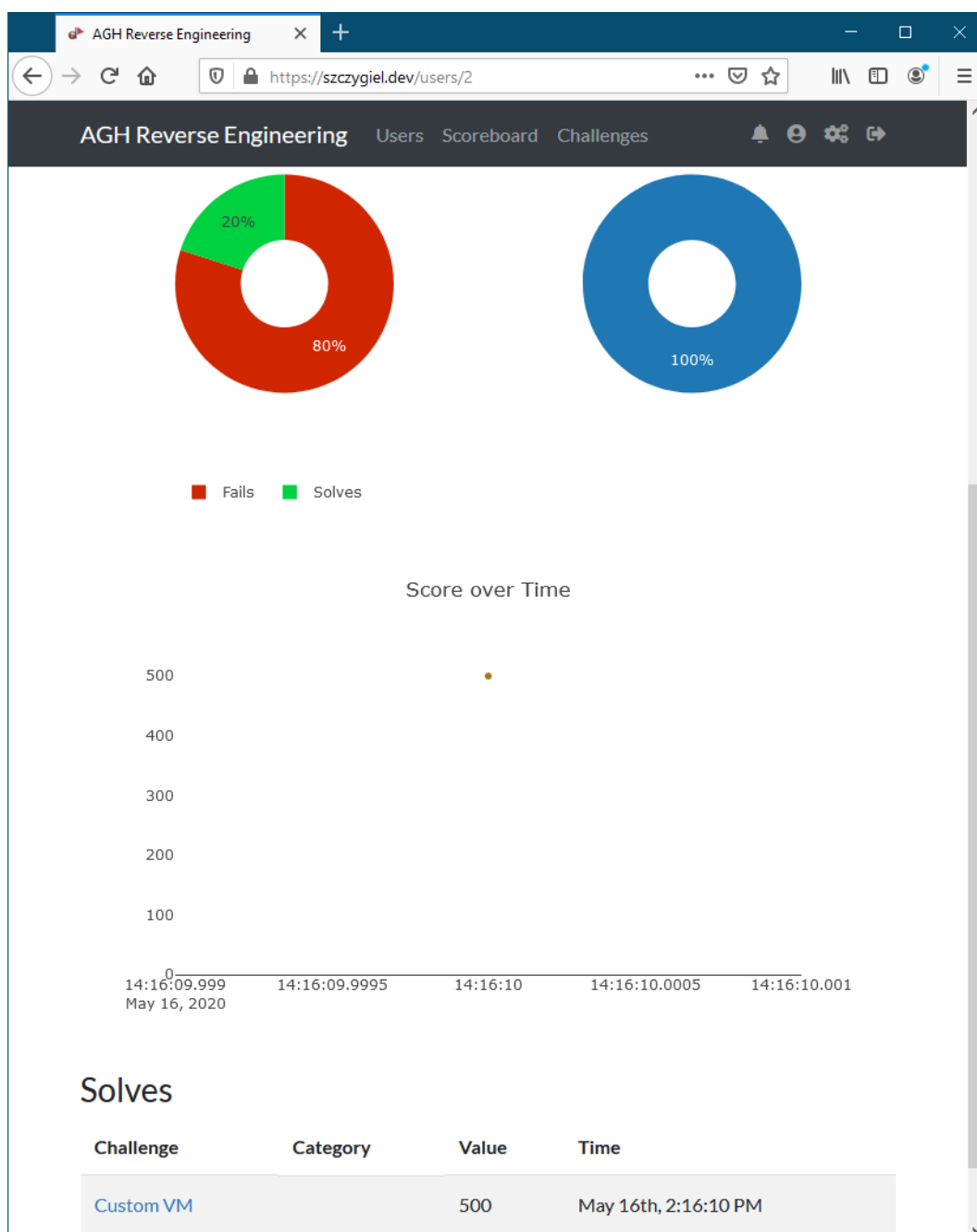
Rysunek 9: Efekt wprowadzenia prawidłowej flagi

Dostępna jest również lista zarejestrowanych użytkowników. Można wejść w profil każdego użytkownika i zobaczyć jego postępy.



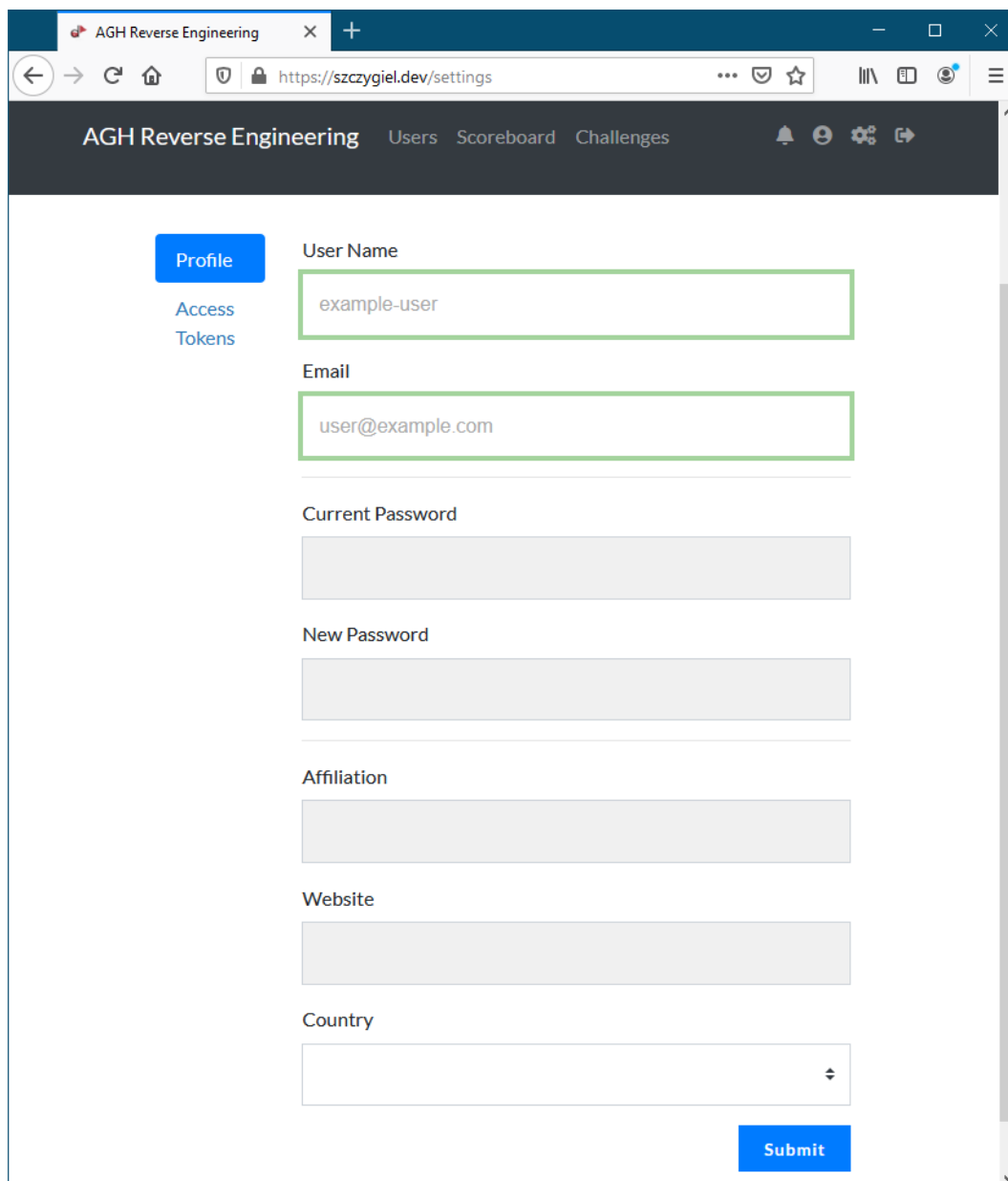
Rysunek 10: Spis zarejestrowanych użytkowników

Wchodząc na profil użytkownika można zobaczyć o nim różne informacje. Jest to przede wszystkim rozkład prawidłowych oraz nieprawidłowych wprowadzeń flag oraz wykres posiadanych punktów w czasie. Na dole widzimy również wszystkie rozwiązane przez użytkownika zadania.



Rysunek 11: Szczegóły postępów konkretnego użytkownika

Każdy użytkownik może również zmienić oraz dodać informację o sobie. Będzie mógł zmienić nazwę użytkownika, email, hasło, oraz dodać takie szczegóły jak strona internetowa, firma dla której pracuję czy kraj pochodzenia.



The screenshot shows a web browser window with the title "AGH Reverse Engineering". The address bar displays "https://szczygiel.dev/settings". The page has a dark blue header with the site name and navigation links: "Users", "Scoreboard", and "Challenges". On the left, there is a sidebar with a blue "Profile" button and links for "Access" and "Tokens". The main content area contains several form fields: "User Name" (with "example-user" entered), "Email" (with "user@example.com" entered), "Current Password", "New Password", "Affiliation", "Website", and "Country" (a dropdown menu). A blue "Submit" button is located at the bottom right of the form.

Rysunek 12: Edycja profilu użytkownika

3. Wybrane aspekty realizacji

Przyjęte założenia, struktura i zasada działania systemu, wykorzystane rozwiązania technologiczne wraz z uzasadnieniem ich wyboru, istotne mechanizmy i zastosowane algorytmy.

4. Organizacja pracy

Struktura zespołu (role poszczególnych osób), krótki opis i uzasadnienie przyjętej metodyki i/lub kolejności prac, planowane i zrealizowane etapy prac ze wskazaniem udziału poszczególnych członków zespołu, wykorzystane praktyki i narzędzia w zarządzaniu projektem.

5. Wyniki projektu

Wskazanie wyników projektu (co konkretnie udało się uzyskać: oprogramowanie, dokumentacja, raporty z testów/wdrożenia, itd.), prezentacja wyników i ocena ich użyteczności (jak zostało to zweryfikowane — np. wnioski klienta/użytkownika, zrealizowane testy wydajnościowe, itd.), istniejące ograniczenia i propozycje dalszych prac.

Materiały źródłowe

- [1] Serwer caddy. <https://caddyserver.com>.
- [2] Platforma ctfid. <https://ctfid.io>.
- [3] Docker. <https://docker.com>.
- [4] Organizacja let's encrypt. <https://letsencrypt.org>.
- [5] Zawody picoctf. <https://picoctf.com>.