



Università degli Studi di Padova



Catch em All - *CAPTCHA: Umano o Sovraumano?*

Email: [catchemallswe3@gmail.com](mailto:catchemallswe3@gmail.com)

# Manuale utente

<b>Versione</b>	1.0.0
<b>Approvazione</b>	Luca Brugnera
<b>Redazione</b>	Ana Lazic, Gabriele Da Re
<b>Verifica</b>	Sinicato Nicola, Matteo Stocco
<b>Stato</b>	Approvato
<b>Uso</b>	Esterno
<b>Distribuzione</b>	Zucchetti S.p.A, Prof. Vardanega Tullio, Prof. Cardin Riccardo, Gruppo Catch Em All

## Registro delle modifiche

Versione	Data	Descrizione	Autore	Ruolo
1.0.0	22/06/2023	Approvazione del documento	Luca Brugnera	Responsabile
0.1.0	21/06/2023	Verifica complessiva del documento	Matteo Stocco	Verificatore
0.0.6	20/06/2023	Modifiche alla sezione §4	Ana Lazic	Amministratore
0.0.5	16/06/2023	Stesura delle sezioni §2, §4, §5	Ana Lazic	Amministratore
0.0.4	11/06/2023	Verifica della sezione §3	Sinicato Nicola	Verificatore
0.0.3	09/06/2023	Verifica della sezione §1	Sinicato Nicola	Verificatore
0.0.2	08/06/2023	Stesura delle sezioni §1, §3	Gabriele Da Re	Amministratore
0.0.1	06/06/2023	Creazione bozza e struttura del documento	Gabriele Da Re	Amministratore

## Indice

<b>1</b>	<b>Introduzione</b>	<b>3</b>
1.1	Scopo del documento . . . . .	3
1.2	Scopo del prodotto . . . . .	3
1.3	Glossario . . . . .	3
<b>2</b>	<b>Requisiti minimi</b>	<b>4</b>
2.1	Requisiti hardware . . . . .	4
2.2	Browser <sub>G</sub> . . . . .	4
<b>3</b>	<b>Installazione</b>	<b>5</b>
3.1	Utilizzo dell'applicazione senza installazione . . . . .	5
3.2	Reinstallazione del prodotto software . . . . .	5
3.2.1	Installare il sistema operativo <sub>G</sub> . . . . .	5
3.2.2	Scaricare i pacchetti <sub>G</sub> . . . . .	5
3.2.3	Verifica delle estensioni <sub>G</sub> . . . . .	5
3.2.4	Clonare il repository <sub>G</sub> . . . . .	6
3.2.5	Installare il gestore di pacchetti <sub>G</sub> PHP <sub>G</sub> . . . . .	6
3.2.6	Impostazione dei permessi . . . . .	6
3.2.7	Modificare il file di configurazione di Nginx <sub>G</sub> . . . . .	6
3.2.8	Creare il file captcha.test . . . . .	8
3.2.9	Ottenere il percorso assoluto <sub>G</sub> . . . . .	9
3.2.10	Modificare il file captcha.test . . . . .	9
3.2.11	Creare il link simbolico <sub>G</sub> . . . . .	10
3.2.12	Riavviare Nginx <sub>G</sub> . . . . .	10
3.2.13	Configurare il file hosts . . . . .	10
3.2.14	Utilizzo dell'applicazione dopo l'installazione . . . . .	10
<b>4</b>	<b>Istruzioni per l'uso</b>	<b>11</b>
4.1	Inserimento delle credenziali e generazione del captcha <sub>G</sub> . . . . .	11
4.2	Superamento del test captcha <sub>G</sub> . . . . .	11
4.2.1	Test immagini . . . . .	12
4.2.2	Attesa operazioni in background <sub>G</sub> . . . . .	13
4.3	Verifica del test captcha . . . . .	14
4.4	Problemi comuni . . . . .	14
<b>5</b>	<b>Supporto tecnico e risoluzione dei problemi</b>	<b>15</b>
5.1	Documentazione API . . . . .	15

## **Elenco delle figure**

4.1	Form di inserimento credenziali . . . . .	11
4.2	Test immagini . . . . .	12
4.3	Test immagini con soluzione evidenziata . . . . .	13
4.4	Indicatore di progresso . . . . .	13
4.5	Pulsante di login . . . . .	14
4.6	Messaggio di errore . . . . .	14

## **Elenco delle tabelle**

2.1	Browser <sub>G</sub> compatibili . . . . .	4
-----	--	---

# 1 Introduzione

## 1.1 Scopo del documento

Questo documento contiene le indicazioni per l'utilizzo delle funzionalità di riconoscimento dei bot<sub>G</sub> fornite dal prodotto software.

## 1.2 Scopo del prodotto

Dal proponente Zucchetti S.p.A. viene evidenziato, nel capitolato da loro proposto, una criticità negli attuali sistemi di sicurezza sulla rilevazione dei bot<sub>G</sub> rispetto agli esseri umani. Oggi giorno il meccanismo più utilizzato per risolvere questo problema è il test CAPTCHA<sub>G</sub>.

Un bot<sub>G</sub> non è altro che una procedura automatizzata che, in questo caso, ha fini malevoli, come per esempio:

- Registrazione presso siti web;
- Creazione di spam<sub>G</sub>;
- Violare sistemi di sicurezza.

I bot<sub>G</sub>, grazie alle nuove tecnologie sviluppate con sistemi che utilizzano principalmente l'intelligenza artificiale, riescono a svolgere compiti che fino a poco tempo fa venivano considerati impossibili da svolgere per una macchina.

Ciò evidenzia che i CAPTCHA<sub>G</sub> attuali risultano sempre più obsoleti, non andando a individuare correttamente tutti i bot<sub>G</sub>, se non quasi nessuno.

Un'altra criticità individuata dal proponente è il sistema di classificazione delle immagini che sta effettuando Google grazie al proprio reCAPTCHA<sub>G</sub>, che attualmente è il sistema più diffuso.

Questa criticità nasce dal beneficio che questa azienda ottiene dall'interazione degli utenti nel risolvere le task<sub>G</sub> proposte, che portano alla creazione di enormi raccolte di immagini classificate che possono essere utilizzate per l'apprendimento dei propri sistemi di machine learning o vendibili a terzi.

Il capitolato C1 richiede di sviluppare una applicazione web costituita da una pagina di login provvista di questo sistema di rilevazione in grado di distinguere un utente umano da un bot<sub>G</sub>.

L'utente quindi, dopo aver compilato il form in cui inserirà il nome utente e la password, dovrà svolgere una task<sub>G</sub> che sarà il cosiddetto test CAPTCHA<sub>G</sub>.

## 1.3 Glossario

Per evitare ambiguità relative al linguaggio utilizzato nei documenti prodotti, viene fornito il **Glossario utente v 1.0.0**. In questo documento sono contenuti tutti i termini tecnici, i quali avranno una definizione specifica per comprenderne al meglio il loro significato.

Tutti i termini inclusi nel Glossario, vengono segnalati all'interno del documento Manuale utente con una G a pedice.

## 2 Requisiti minimi

Per poter utilizzare il prodotto software è necessario essere in possesso dei seguenti requisiti, che vengono specificati in questa sezione proprio per garantire il corretto funzionamento dell'applicazione.

### 2.1 Requisiti hardware

I requisiti hardware per l'utilizzo dell'applicazione sono facilmente soddisfacibili dai computer attualmente diffusi. Nello specifico:

- **Processore:** Pentium 4 3.00GHz;
- **RAM:** 8GB.

Inoltre, il computer utilizzato deve disporre di una connessione internet.

### 2.2 Browser<sub>G</sub>

Per poter utilizzare l'applicazione è necessario essere in possesso di un browser<sub>G</sub>. L'applicazione è stata resa compatibile con le versioni dei browser<sub>G</sub> riportate nella seguente tabella.

Browser <sub>G</sub>	Versione
Google Chrome	110
Microsoft Edge	113
Mozilla Firefox	114
Opera	99

Tabella 2.1: Browser<sub>G</sub> compatibili

## 3 Installazione

Il prodotto software fornito può essere utilizzato nelle seguenti modalità:

- **Senza installazione:** per l'utente che preferisce utilizzare l'applicazione disponibile online digitando l'indirizzo nella barra di ricerca del proprio browser<sub>G</sub>;
- **Reinstallazione:** per l'utente che desidera installare il prodotto software in locale.

L'utente, dopo aver scelto la modalità di utilizzo desiderata, potrà consultare la relativa sezione per ulteriori indicazioni.

### 3.1 Utilizzo dell'applicazione senza installazione

Di seguito vengono elencati i passaggi per avviare l'applicazione senza doverla installare:

- Avviare uno dei browser<sub>G</sub> compatibili con l'applicazione;
- Digitare il seguente indirizzo: <https://swe.gdr00.it> .

### 3.2 Reinstallazione del prodotto software

Di seguito vengono elencati i passaggi per l'installazione dell'applicazione in un server<sub>G</sub> locale. Si consiglia di seguire i passaggi di questa sezione della guida nell'ordine in cui vengono presentati.

#### 3.2.1 Installare il sistema operativo<sub>G</sub>

Sul computer scelto come server<sub>G</sub> dell'applicazione installare il seguente sistema operativo<sub>G</sub>:

Ubuntu 20.04.6 LTS (Focal Fossa)

#### 3.2.2 Scaricare i pacchetti<sub>G</sub>

Eseguire il seguente comando per scaricare i pacchetti<sub>G</sub> per l'utilizzo di PHP<sub>G</sub>, Nginx<sub>G</sub>, SQLite<sub>G</sub>, FPM<sub>G</sub>, cURL<sub>G</sub>, mbstring<sub>G</sub>:

```
sudo apt update && sudo apt full-upgrade -y &&  
apt install nginx php php-fpm php-sqlite3 php-curl php-mbstring -y &&  
systemctl enable nginx.service && systemctl enable php-fpm php-dom
```

#### 3.2.3 Verifica delle estensioni<sub>G</sub>

Verificare se le seguenti estensioni<sub>G</sub> sono abilitate, e in caso contrario abilitarle:

- OpenSSL PHP Extension;
- PDO PHP Extension;
- Mbstring PHP Extension;
- Tokenizer PHP Extension;

- XML PHP Extension;
- CType PHP Extension;
- JSON PHP Extension;
- BCMath PHP Extension.

### 3.2.4 Clonare il repository<sub>G</sub>

Spostarsi nella cartella `/var/www` del web server<sub>G</sub>, in modo che poi esso abbia tutti i permessi necessari, e poi clonare il repository<sub>G</sub> da GitHub<sub>G</sub>:

```
cd /var/www
git clone https://github.com/catchEmAll-SWE/dev.git
```

### 3.2.5 Installare il gestore di pacchetti<sub>G</sub> PHP<sub>G</sub>

```
php -r "copy('https://getcomposer.org/installer', 'composer-setup.php');"
sudo php composer-setup.php --install-dir=/bin --filename=composer
composer global require laravel/installer
echo 'export PATH="$PATH:$HOME/.config/composer/vendor/bin"' >> ~/.bashrc
source ~/.bashrc
cd /dev/captcha
cp .env.example .env
composer install
composer require --dev knuckleswtf/scribe
php artisan key:generate
php artisan scribe:generate
```

### 3.2.6 Impostazione dei permessi

Spostarsi nella cartella `cd/dev/captcha` ed eseguire i seguenti comandi, in modo che Nginx<sub>G</sub> abbia i permessi per modificare i file nelle cartelle dedicate. Attenzione: la parte **username** dei comandi **chown** va sostituita con l'effective userID<sub>G</sub>. Se non lo si conosce, lo si può ottenere con il comando **whoami**.

```
cd/dev/captcha

sudo chmod -R 775 storage
sudo chmod -R 775 bootstrap/cache

sudo chown -R username:www-data /full/path/to/dev/captcha/bootstrap/cache
sudo chown -R username:www-data /full/path/to/dev/captcha/storage
```

### 3.2.7 Modificare il file di configurazione di Nginx<sub>G</sub>

Aprire in modifica il file **nginx.conf** che si trova al percorso `/etc/nginx/nginx.conf` e impostarlo come segue:



```
#user www-data;
worker_processes 1;

#error_log logs/error.log;
#error_log logs/error.log notice;
#error_log logs/error.log info;

#pid logs/nginx.pid;

events {
    worker_connections 1024;
}

http {
    charset utf-8;
    sendfile on;
    tcp_nopush on;
    tcp_nodelay on;
    server_tokens off;
    log_not_found off;
    types_hash_max_size 4096;
    client_max_body_size 16M;

    # MIME
    include mime.types;
    default_type application/octet-stream;

    # logging
    access_log /var/log/nginx/access.log;
    error_log /var/log/nginx/error.log warn;

    # load configs
    include /etc/nginx/conf.d/*.conf;
    include /etc/nginx/sites-enabled/*;

    #log_format main '$remote_addr - $remote_user [$time_local] "$request" '
    #                '$$status $body_bytes_sent "$http_referer" '
    #                '"$http_user_agent" "$http_x_forwarded_for"';

    #access_log logs/access.log main;

    #keepalive_timeout 0;
    keepalive_timeout 65;
```

```
#gzip on;

server_names_hash_bucket_size 64;


# another virtual host using mix of IP-, name-, and port-based configuration
#
#server {
#    listen      8000;
#    listen      somename:8080;
#    server_name somename alias another.alias;


#    location / {
#        root    html;
#        index   index.html index.htm;
#    }
#}


# HTTPS server
#
#server {
#    listen      443 ssl;
#    server_name localhost;


#    ssl_certificate      cert.pem;
#    ssl_certificate_key  cert.key;


#    ssl_session_cache    shared:SSL:1m;
#    ssl_session_timeout  5m;


#    ssl_ciphers  HIGH:!aNULL:!MD5;
#    ssl_prefer_server_ciphers on;


#    location / {
#        root    html;
#        index   index.html index.htm;
#    }
#}

}
```

### 3.2.8 Creare il file `captcha.test`

Eseguire il seguente comando:

```
sudo touch /etc/nginx/sites-available/captcha.test
```

### 3.2.9 Ottenere il percorso assoluto<sub>G</sub>

Eseguire i seguenti comandi, e salvare l'output del comando **pwd** che sarà utile nel paragrafo successivo **3.2.10**:

```
cd/dev/captcha/public
pwd
```

### 3.2.10 Modificare il file **captcha.test**

Aprire in modifica il file **captcha.test** che si trova al percorso */etc/nginx/sites-available/captcha.test* e impostarlo come segue. Attenzione: il percorso indicato alla voce **root** deve essere l'output del comando **pwd** ottenuto al precedente paragrafo **3.2.9**.

```
server {
    listen 80;
    listen [::]:80;
    server_name captcha.test;
    root /path/to/web/root/dev/captcha/public;

    add_header X-Frame-Options "SAMEORIGIN";
    add_header X-Content-Type-Options "nosniff";

    index index.php;

    charset utf-8;

    location / {
        try_files $uri $uri/ /index.php?$query_string;
    }

    location = /favicon.ico { access_log off; log_not_found off; }
    location = /robots.txt  { access_log off; log_not_found off; }

    error_page 404 /index.php;

    location ~ \.php$ {
        fastcgi_pass unix:/var/run/php-fpm/php-fpm.sock;
        fastcgi_param SCRIPT_FILENAME $realpath_root$fastcgi_script_name;
        include fastcgi_params;
    }

    location ~ /\.(!well-known).* {
        deny all;
    }
}
```

### 3.2.11 Creare il link simbolico<sub>G</sub>

Eeguire il seguente comando per creare il link simbolico<sub>G</sub> del file **captcha.test** nella cartella **sites-enable** usata da Nginx<sub>G</sub>:

```
sudo ln -s /etc/nginx/sites-available/captcha.test /etc/nginx/sites-enabled
```

### 3.2.12 Riavviare Nginx<sub>G</sub>

Ora che la configurazione di Nginx<sub>G</sub> è completata, sarà necessario riavviare il servizio<sub>G</sub>:

```
sudo systemctl restart nginx.service
```

### 3.2.13 Configurare il file hosts

Aprire in modifica il file **hosts** che si trova al percorso */etc/hosts* e aggiungere la riga seguente, in modo da poter avviare l'applicazione più intuitivamente:

```
127.0.0.1 captcha.test
```

### 3.2.14 Utilizzo dell'applicazione dopo l'installazione

Se tutti i passaggi sono stati eseguiti correttamente, sarà possibile aprire l'applicazione seguendo questi passaggi:

- Avviare uno dei browser<sub>G</sub> compatibili con l'applicazione;
- Digitare il seguente indirizzo: `captcha.test` .

## 4 Istruzioni per l'uso

L'applicazione è composta da un'unica pagina web che prevede l'esecuzione di una serie operazioni ordinate da parte dell'utente:

- Inserimento delle credenziali e generazione del  $\text{captcha}_G$ ;
- Superamento del test  $\text{captcha}_G$ ;
- Verifica delle credenziali e del superamento del test.

### 4.1 Inserimento delle credenziali e generazione del $\text{captcha}_G$

Una volta aperta la pagina web dell'applicazione viene visualizzata la pagina di login, dove l'utente deve:

- Inserire l'username nell'apposito campo: **CatchEmAll**;
- Inserire la password nell'apposito campo: **captcha**;
- Premere il tasto **Genera captcha**.

Per evitare un afflusso di richieste, prima di generare il captcha vengono verificate le credenziali. La richiesta verrà accettata solo nel caso queste ultime siano corrette.

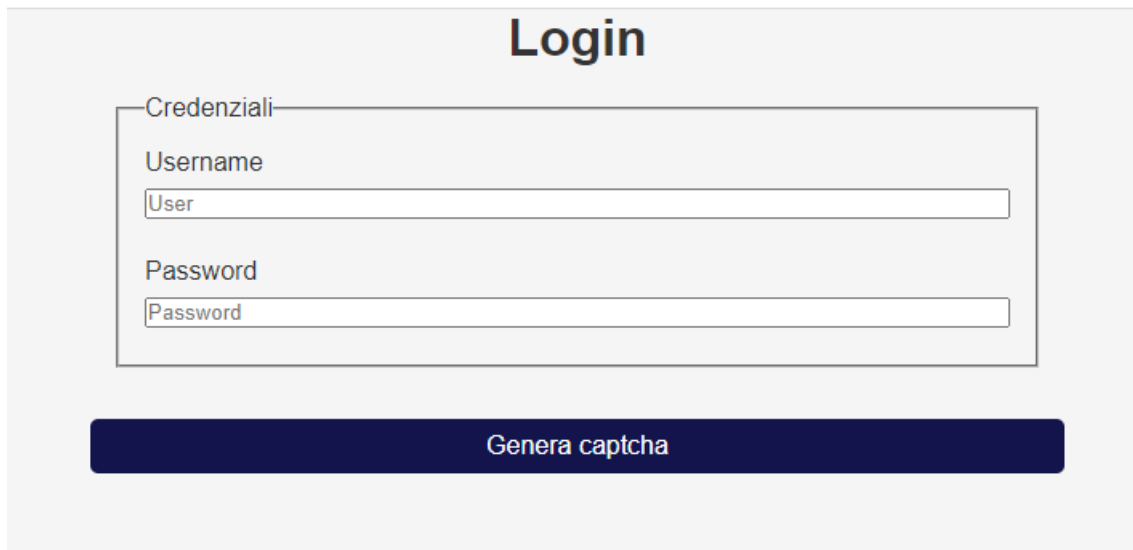


Figura 4.1: Form di inserimento credenziali

### 4.2 Superamento del test $\text{captcha}_G$

Il test  $\text{captcha}_G$  è composto da due parti visibili all'utente:

- Test immagini;
- Attesa operazioni in background<sub>G</sub>.

#### 4.2.1 Test immagini

Per poter essere riconosciuto come utente umano e non come un bot<sub>G</sub>, l'utente deve superare il test immagini. Questo test è composto da:

- Una tipologia di immagini da selezionare;
- Una griglia 3x3 su cui sono disposte 9 immagini cliccabili, di cui solo alcune appartengono alla tipologia di immagine da selezionare.

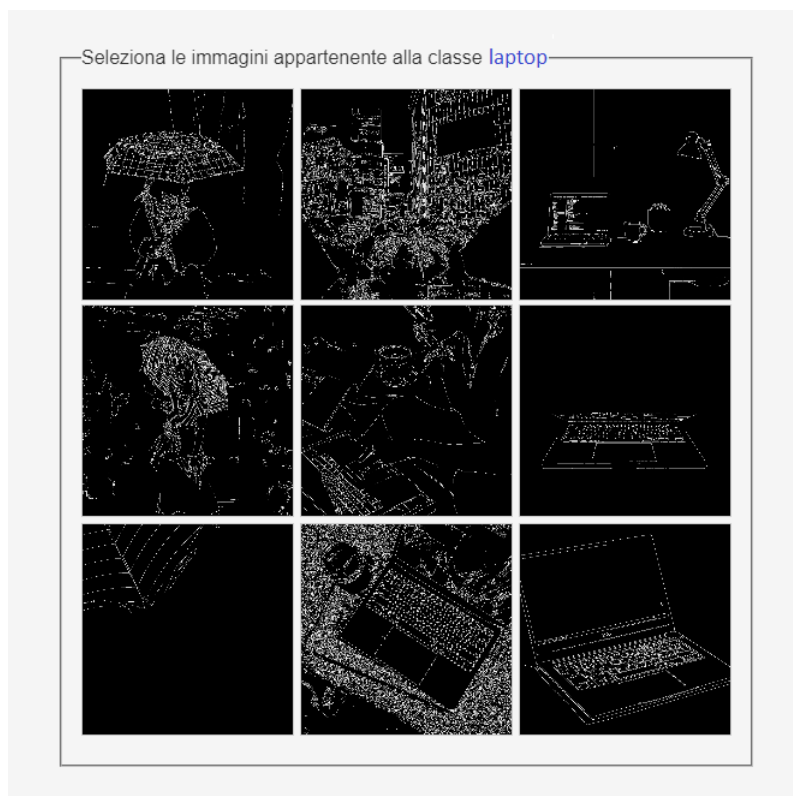


Figura 4.2: Test immagini

L'utente dovrà selezionare solo le immagini che ritiene facciano parte della tipologia richiesta - per esempio, nell'immagine sottostante è richiesto di selezionare le immagini appartenenti alla classe **laptop**, e le immagini corrette da selezionare vengono evidenziate in rosso:

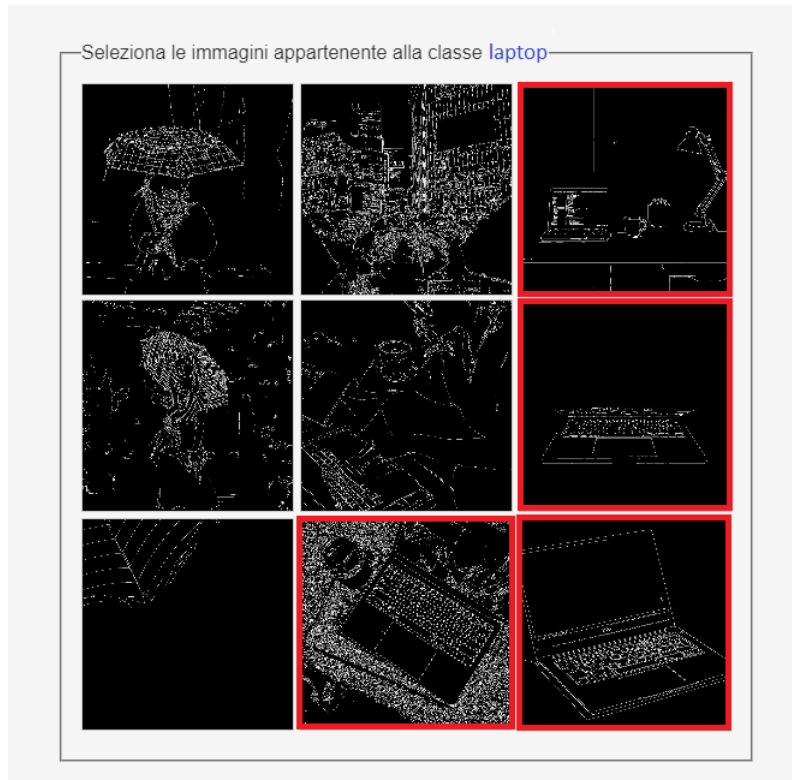


Figura 4.3: Test immagini con soluzione evidenziata

#### 4.2.2 Attesa operazioni in background<sub>G</sub>

L'utente per poter completare il captcha dovrà svolgere un proof of work, permettendoci di avere uno strato di sicurezza in più contro degli attacchi burst. Infatti si potrà procedere all'operazione successiva solo dopo che l'indicatore di progresso ha raggiunto il 100%, come indicato nella seguente immagine:

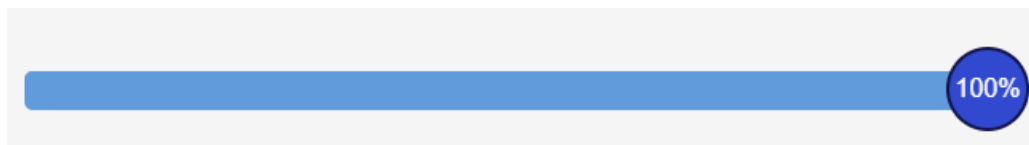


Figura 4.4: Indicatore di progresso

Osservazione:

- Questa è un'operazione che richiede pochi secondi, e normalmente quando l'utente ha terminato la compilazione del test immagini l'avanzamento ha già raggiunto il 100%.

### 4.3 Verifica del test captcha

Una volta effettuati i passaggi illustrati nei paragrafi precedenti, l'utente potrà procedere con l'autenticazione cliccando sul tasto **Login**. Se questa è andata a buon fine, l'utente verrà reindirizzato ad una pagina con un messaggio che indica la riuscita dell'operazione; altrimenti visualizzerà un messaggio di errore e potrà ritentare il login ripetendo i passaggi.

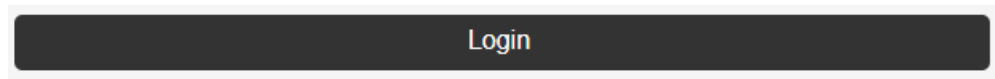


Figura 4.5: Pulsante di login



Figura 4.6: Messaggio di errore

### 4.4 Problemi comuni

Di seguito vengono elencati alcuni suggerimenti in merito alle operazioni alle quali prestare particolare attenzione nel caso in cui l'utente non riesca ad autenticarsi sul sistema:

- L'utente non ha inserito correttamente le credenziali indicate al paragrafo 4.1;
- L'utente ha compilato erroneamente il test captcha<sub>G</sub> illustrato al paragrafo 4.2.2;
- L'utente non ha aspettato il completamento delle attività in background<sub>G</sub> come indicato al paragrafo 4.2.2.



## **5   Supporto tecnico e risoluzione dei problemi**

In caso di problemi tecnici o richieste di ulteriori informazioni il fornitore del prodotto software è contattabile al seguente indirizzo email:

`catchemallswe3@gmail.com`

Al fine di consentire l'erogazione di un servizio di assistenza efficace si richiede all'utente di fornire nel contenuto dell'email:

- Una chiara descrizione del problema;
- L'elenco dei passaggi per riprodurre il malfunzionamento;
- Eventuali screenshot che possono essere utili a comprendere meglio l'anomalia.

### **5.1   Documentazione API**

Viene inoltre fornita dagli sviluppatori la documentazione dell'API sviluppata in caso si voglia utilizzare il servizio per il proprio sito web. La documentazione specifica chiaramente di quali parametri le varie richieste necessitano e della risposta che verrà fornita.

La documentazione di può trovare al seguente link:

- <https://swe.gdr00.it/docs>.

Si specifica che per poter fare richieste direttamente al nostro servizio è necessario un BEARER TOKEN<sub>G</sub>, così da poter gestire solo richieste legittime, e che per richiederne uno valido sarà necessario inviare una mail all'indirizzo citato precedentemente.