Detoxio.ai

Conduct a black-box assessment to identify critical vulnerabilities in the provided web application and/or APIs.

Input

1. [app.pfbeta.com](http://app.pfbeta.com/) --- Don’t use illegal activities for the websites in the Documents and testing Websites also.

2. Log files containing API request traces (It will be provided once you complete 1 to 4th step)

Instructions

1. Discover the web application structure.

2. Identify any running APIs.

3. Use Burp Suite or OWASP ZAP to scan for web application vulnerabilities.

4. Check for hidden directories or data exposure.

5. Identify any exposed APIs.

## **Recon**

1. First, confirm that the target is active and the web application is running (use Nmap, Dig or any other tool)

2. Explore the target thoroughly. Interact with the web application by filling out forms and identifying backend APIs, as well as gather any additional relevant information.

Scanning

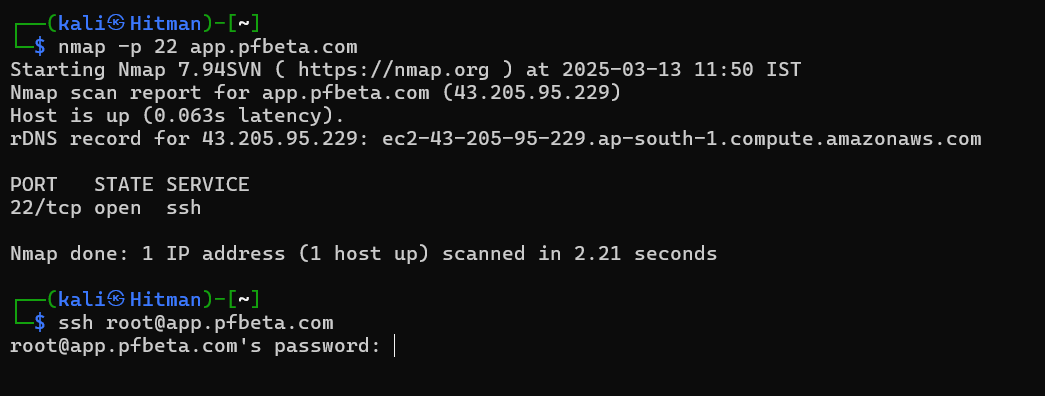
1. Utilize Nuclei to identify any vulnerabilities at the framework level (<https://github.com/projectdiscovery/nuclei>)

2. Execute a vulnerability API tool on the API endpoints to uncover potential vulnerabilities (<https://github.com/cerberauth/vulnapi>)

3. Employ Burp or Zap scanner on the web apps to discover any vulnerabilities.

Custom Tools

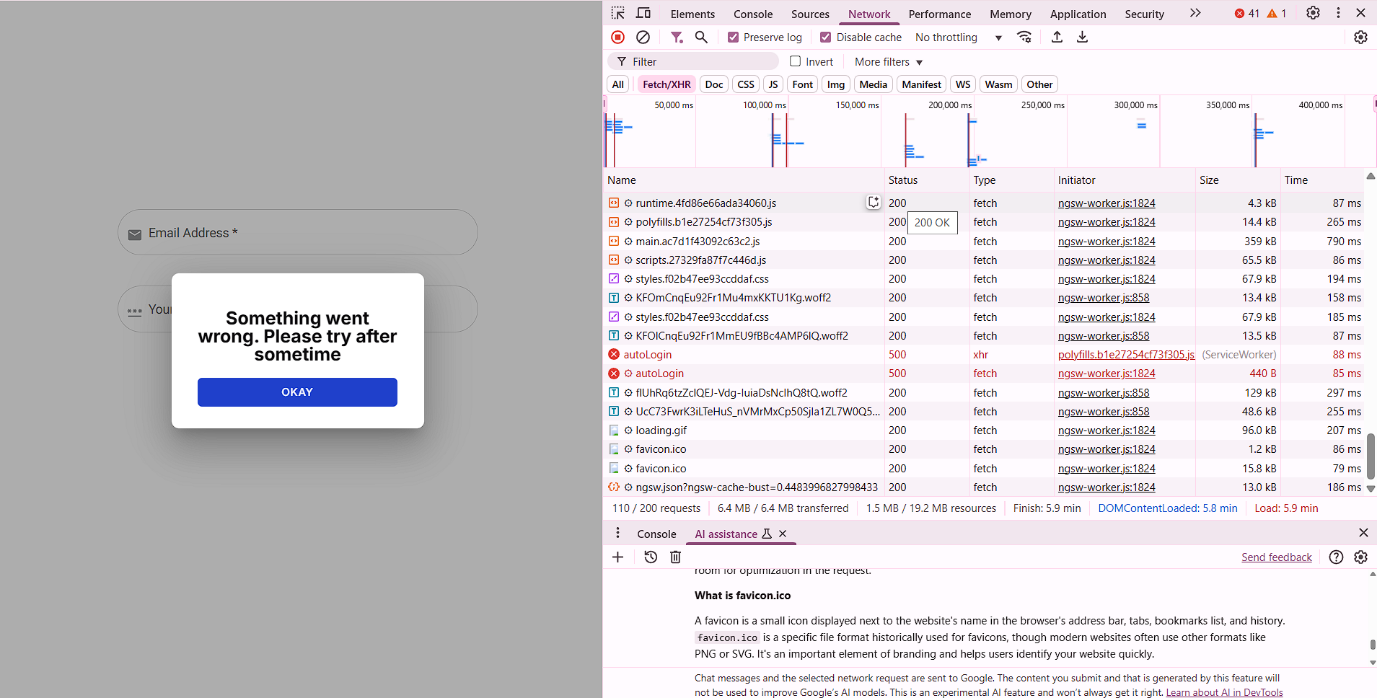
1. If you identify the need for any additional tools to run, proceed accordingly.

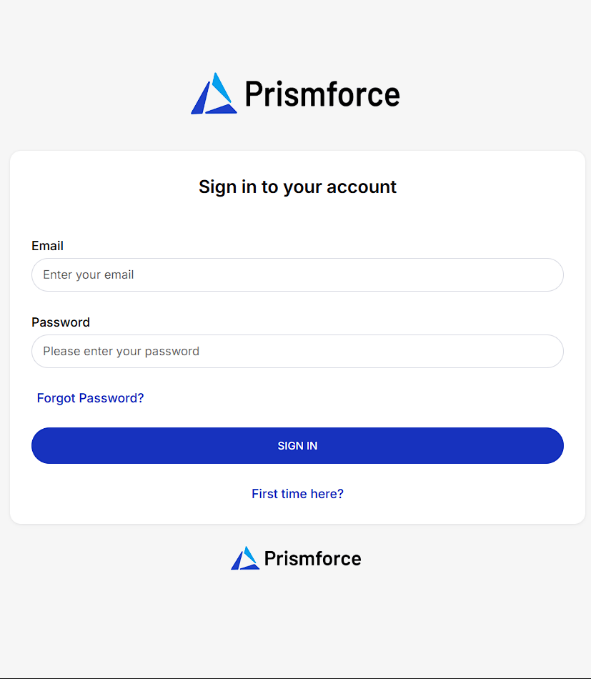
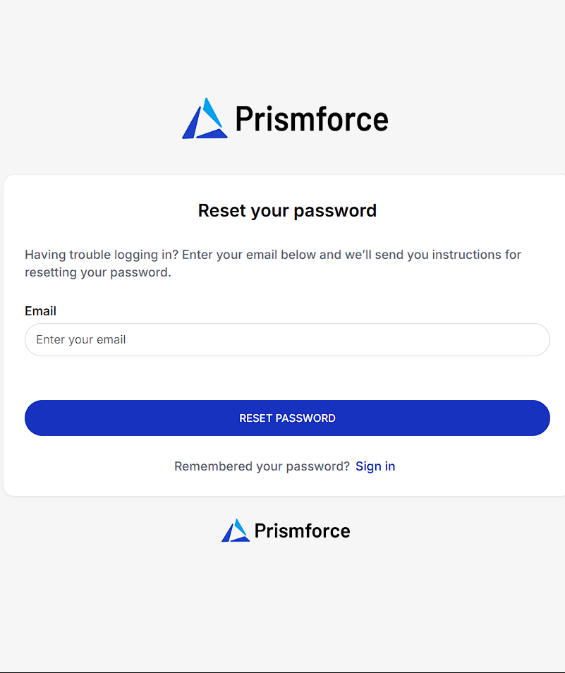


### This is Black Box Assignments so there is no input Credentials or Default Credentials

### 🛠️ Technologies and Services Overview

| **Technology / Service** | **Details** |
| --- | --- |
| **Content Delivery Network (CDN)** | Amazon CloudFront |
| **Hosting Provider** | Amazon Web Services (AWS) |
| **Web Server** | Nginx |





**Functional Issue Report**

**Issue Title:**

Incorrect Link Mapping – "First time here?" and "Forgot Password?" Redirecting to the Same Page

**Category:**

Functional Bug (Non-Security)

**Issue Description:**

During a routine functional review of the web application's login interface, it was observed that both the **"First time here?"** and **"Forgot Password?"** hyperlinks are directing users to the **password reset page**. These two options are meant to serve different user intents and therefore should not redirect to the same destination.

### ****Expected Behavior:****

* **"First time here?"** – Should redirect to the **new user registration** or **onboarding** page.
* **"Forgot Password?"** – Should redirect to the **password recovery** page.

**Actual Behavior:**

* Both links currently redirect to the **password reset** page, which may confuse users, especially new users attempting to create an account.

**Steps to Reproduce:**

1. Navigate to the login page.
2. Click on **"First time here?"** – redirected to the password reset page.
3. Click on **"Forgot Password?"** – same redirection as above.

**Recommendation:**

* Reconfigure the **"First time here?"** link to point to the correct **registration or onboarding page**.
* Perform link validation on all user navigation elements to ensure proper routing.
* Conduct a usability test to confirm that user journeys align with expected behaviors.

### ****Conclusion:****

Although this is **not a security vulnerability**, it is a significant **functional issue** affecting user interaction. Timely correction is recommended to enhance the usability and professionalism of the web interface.

## 🔍 Directory Enumeration Report

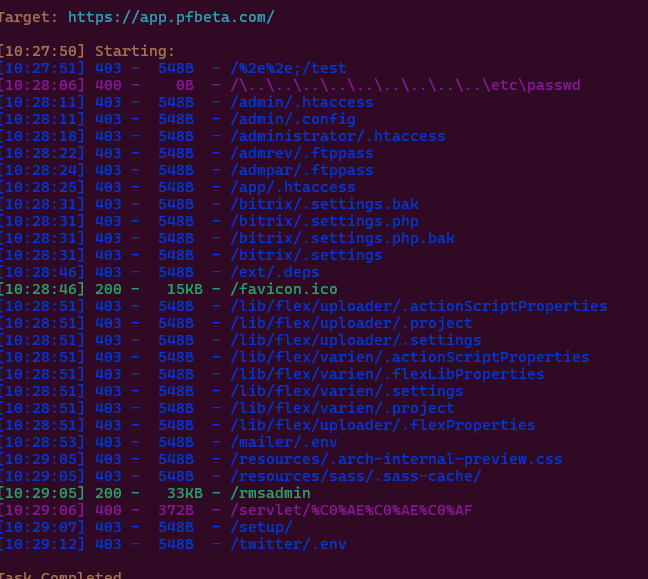
### ****Tool Used:****

Gobuster – Directory/URL Brute-forcing Tool

Command Executed: gobuster dir -u https://app.pfbeta.com -w /usr/share/wordlists/dirb/big.txt -b "200"

 **Purpose:** To enumerate hidden or unlisted directories and files in the web application.

 **Wordlist Used:** big.txt from the default dirb wordlists.



* **Target URL:** https://app.pfbeta.com
* **Wordlist:** /usr/share/wordlists/dirb/big.txt
* **Filter:** Status code 200 (OK)

|  |
| --- |
| Subdomain - /rmsadmin |

|  |
| --- |
| 200 OK |

|  |
| --- |
| 33KB |

|  |
| --- |
| ✅ Active endpoint — may serve a web interface or admin panel |
| **Target Application:** <https://app.pfbeta.com/rmsadmin>  **Accessible Endpoint (/rmsadmin):Medium Level Bug**  Returned a 200 OK with a 33KB response — likely a functional panel or interface that should be reviewed manually for vulnerabilities such as:   * + Broken Access Control   + Sensitive Information Disclosure |

**Conclusion:**

The enumeration process successfully uncovered potential entry points and sensitive paths within the application. Although many were properly protected with 403 status codes, their visibility alone can aid an attacker in crafting targeted attacks. It is crucial to secure both access and disclosure of these resources.