SCENARIO

The application contains a hidden blog page which contains a secret password which we can be accessed by using GraphQL queries. We will try to exploit this vulnerability and get the secret password hidden within the hidden page.

**PROCEDURE**

1. Open the web application and study the request made to the server.
2. We see that there are 5 posts in total but only 4 of them are visible to us and those post are equipped with a serialized **postID.**
3. Now we will scan the GraphQL endpoint and get to know that the BlogPost type has a **postPassword** field available which causes the site to make a GraphQL query that fetches the relevant post data via a direct reference to the post's ID.
4. Navigate to any post, send the request to the BurpSuite’s Repeater modify the id variable to 3 and add the postPassword field to the query like the Payload.
5. Now, in the response we will get the hidden blog with the desired secret key.

PAYLOAD

{"variables": {"id": 3}, "query": "\n query getBlogPost($id: Int!) {\n getBlogPost(id: $id) {\n image\n title\n author\r\n\t\t\t\t\t\tpostPassword\n date\n paragraphs\n }\n }", "operationName": "getBlogPost"}

REMEDIATION