Notes Keeper

- **Author :** Ala Loghmari
- **Difficulty : Friendly/Easy**

Description

Notes Keeper is a web application where one can keep his notes, in this challenge, you will need to find your way through the web app by enumerating the website logging in/signing up, and then retrieving notes of other users through an IDOR vulnerability.

Skills Required

- Web Enumeration

Skills Learned

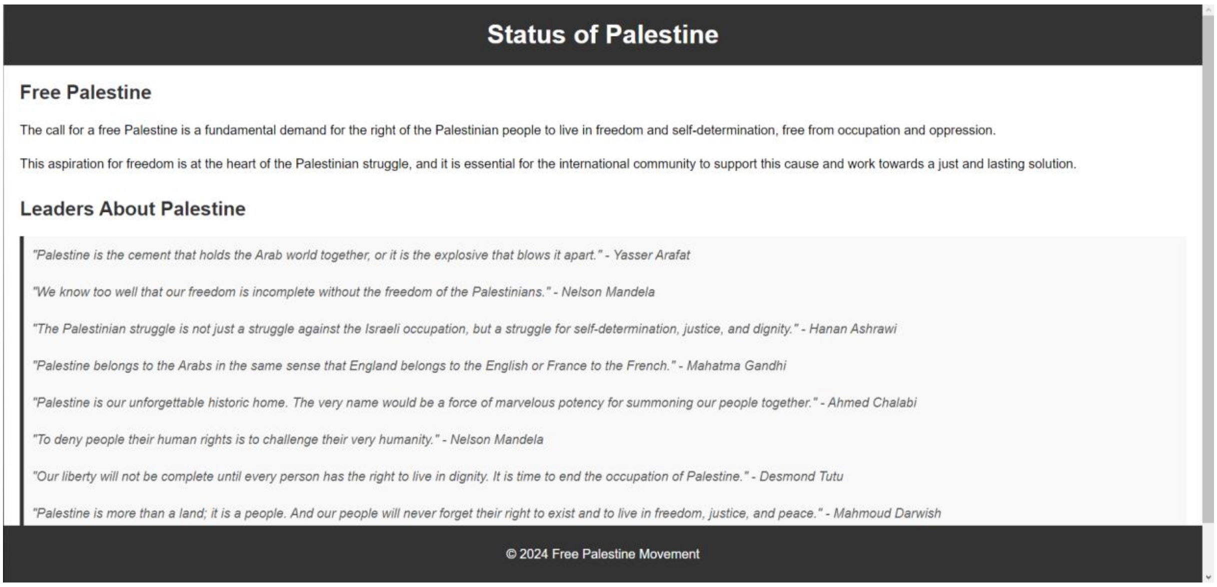
- Web Fuzzing
- Insecure direct object references (IDOR)

References & Guides

- https://portswigger.net/web-security/access-control/idor (Port Swigger)

Enumeration

Accessing the web application, we come across a “Status of Palestine” index page.



Status of Palestine

Free Palestine

The call for a free Palestine is a fundamental demand for the right of the Palestinian people to live in freedom and self-determination, free from occupation and oppression.

This aspiration for freedom is at the heart of the Palestinian struggle, and it is essential for the international community to support this cause and work towards a just and lasting solution.

Leaders About Palestine

"Palestine is the cement that holds the Arab world together, or it is the explosive that blows it apart." - Yasser Arafat

"We know too well that our freedom is incomplete without the freedom of the Palestinians." - Nelson Mandela

"The Palestinian struggle is not just a struggle against the Israeli occupation, but a struggle for self-determination, justice, and dignity." - Hanan Ashrawi

"Palestine belongs to the Arabs in the same sense that England belongs to the English or France to the French." - Mahatma Gandhi

"Palestine is our unforgettable historic home. The very name would be a force of marvelous potency for summoning our people together." - Ahmed Chalabi

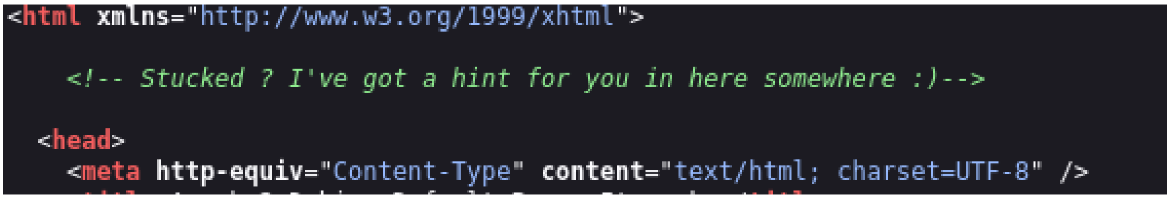
"To deny people their human rights is to challenge their very humanity." - Nelson Mandela

"Our liberty will not be complete until every person has the right to live in dignity. It is time to end the occupation of Palestine." - Desmond Tutu

"Palestine is more than a land; it is a people. And our people will never forget their right to exist and to live in freedom, justice, and peace." - Mahmoud Darwish

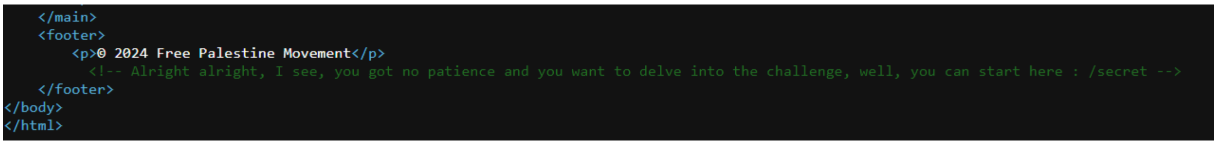
© 2024 Free Palestine Movement

Nothing seems helpful at first but taking a look at the source code of the page we can see some hidden comments that might help us to move further in our enumeration process.



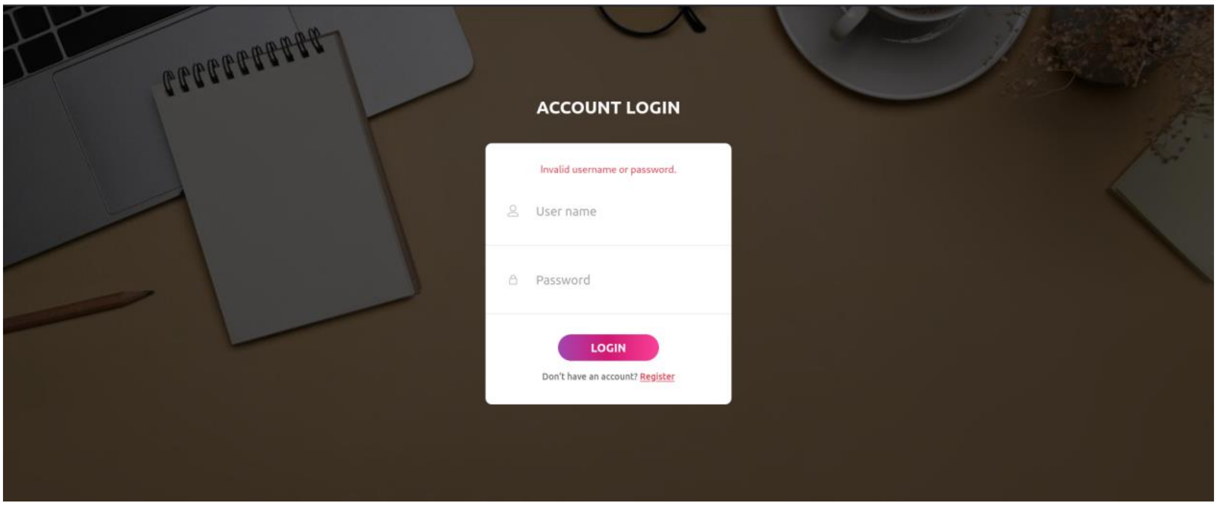
```
<html xmlns="http://www.w3.org/1999/xhtml">

    <!-- Stucked ? I've got a hint for you in here somewhere :)-->

  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
```

Going down a bit, we get our way through the web application.



```
    </main>
    <footer>
        <p>© 2024 Free Palestine Movement</p>
          <!-- Alright alright, I see, you got no patience and you want to delve into the challenge, well, you can start here : /secret -->
    </footer>
</body>
</html>
```

A /secret route seems to exist, a login page appears, after visiting it, asking for a user name and a password.



ACCOUNT LOGIN

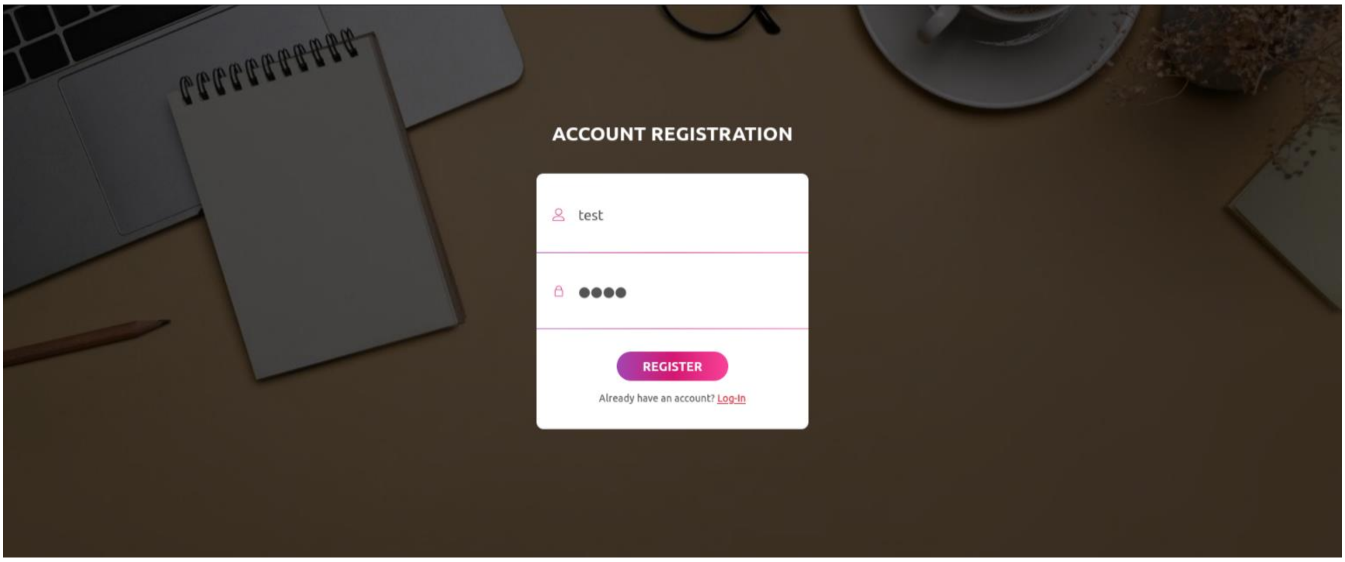
Invalid username or password.

User name

Password

Trying some of the most known combinations (admin:admin, root:root, user:user…) doesn't seem to work as well.

From here, and in order to go further, we decide to create an account by clicking the Register link redirecting us to /register.php.

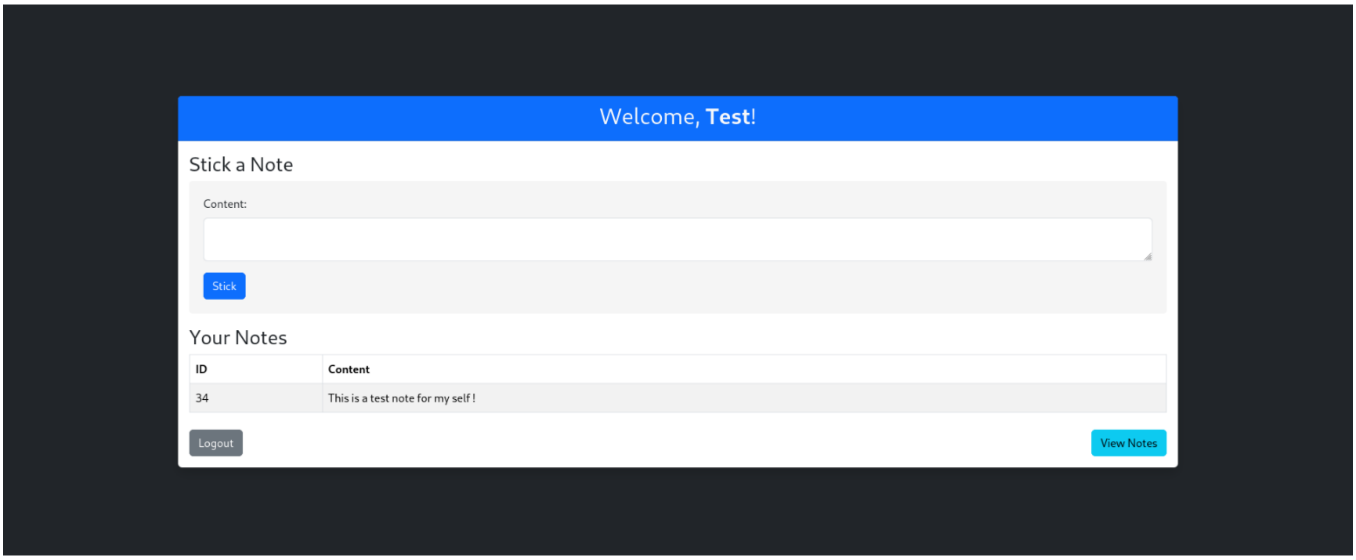


ACCOUNT REGISTRATION

test

●●●●

Once the account is created we get redirected to /home.php where we can, from what it seems, write notes to keep for ourselves.



Welcome, **Test**!

Stick a Note

Content:

Your Notes

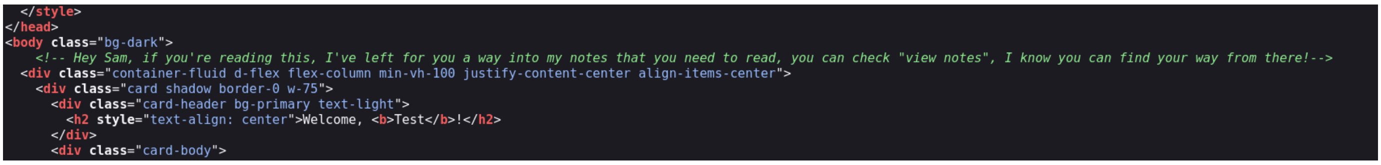
ID	Content
34	This is a test note for my self !

Trying to create a note we notice something odd, the id of the note does not begin at 1, for instance, the one we created has been assigned to it the id "34".

Keeping that in mind, we checked the source code of the page looking for a hint or something that could help us with our enumeration.

Hitting **CTRL U** to view the source code we come across a new hidden message/comment.

```
〝 Hey Sam, if you're reading this, I've left for you a way into my notes
that you need to read, you can check "view notes", I know you can find your
way from there! 〝
```

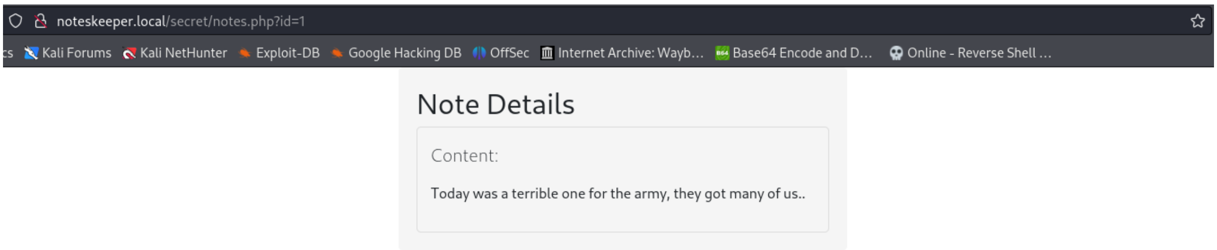


```
  </style>
</head>
<body class="bg-dark">
    <!-- Hey Sam, if you're reading this, I've left for you a way into my notes that you need to read, you can check "view notes", I know you can find your way from there!-->
  <div class="container-fluid d-flex flex-column min-vh-100 justify-content-center align-items-center">
    <div class="card shadow border-0 w-75">
      <div class="card-header bg-primary text-light">
        <h2 style="text-align: center">Welcome, <b>Test</b>!</h2>
      </div>
      <div class="card-body">
```

Doing what the message say we get a redirection to /notes.php with our first note displayed.

Looking at the URL we see an id parameter which apparently is fetching the database and getting us the noted based on the id value, for instance, our first note id.

After trying to manipulate the id value we come across a note that is clearly not ours.



noteskeeper.local/secret/notes.php?id=1

Note Details

Content:

Today was a terrible one for the army, they got many of us..

Exploitation

Time for the exploitation phase, after discovering the correct GET parameter that the web app is using to fetch notes we figured out that the application is vulnerable to an IDOR.

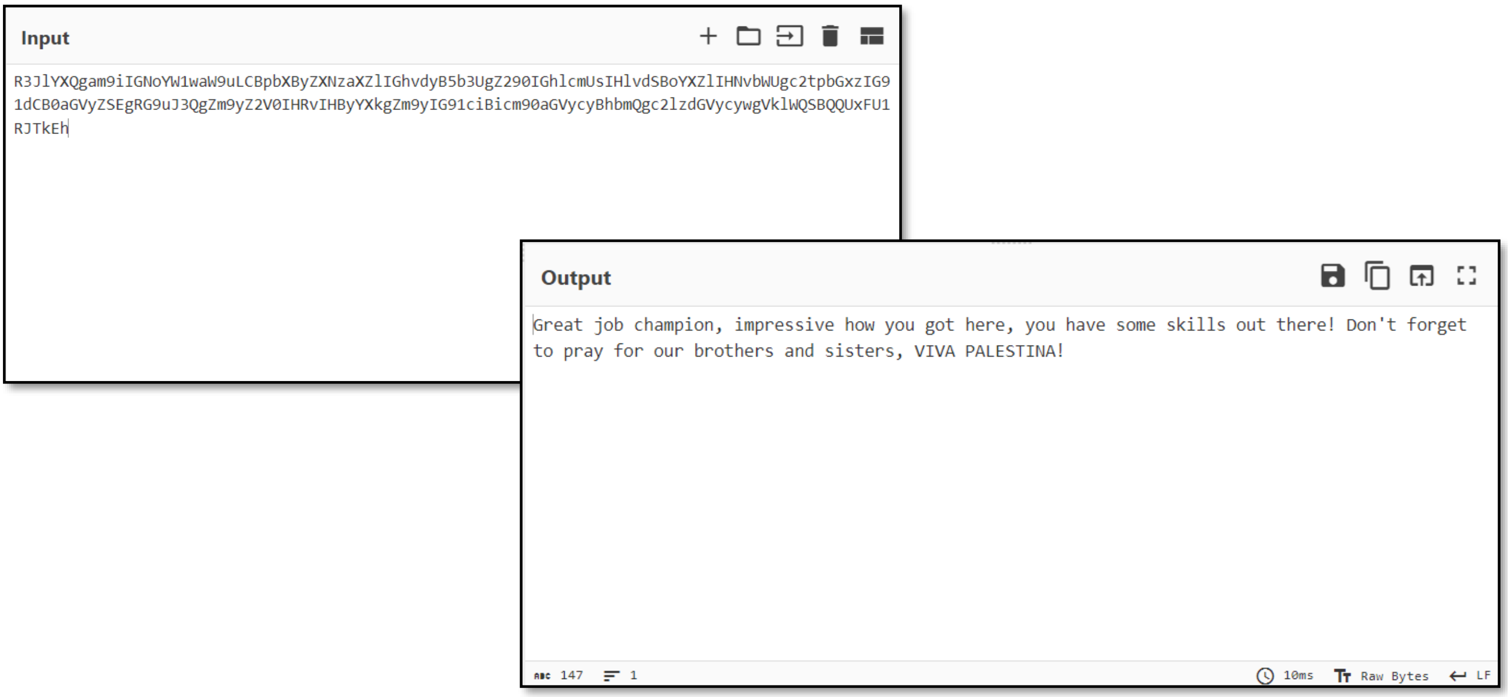
Going through the different IDs we get different existing notes listed in the table below :

ID	Content
1	Today was a terrible one for the army, they got many of us..
2	How could someone imagine some unarmed guys could set such traps and kill this many.. things are getting serious!
3	Note to Self: Don't forget to call Sam at 2PM
4	URGENT: WE NEED MORE BACKUP !!!!!
5	SAM if you're seeing this, tell my family that i love them this might be my last day! these Palestinians are stronger than we thought..
6	I almost forgot, here's the key to my house Sam : **Securinets{N0T3S_L34KED}** get in there and open the book I left on the table, check page number 32!
…	
32	R3JlYXQgam9iIGNoYW1waW9uLCBpbXByZXNzaXZlIGhvdyB5b3UgZ290IGhlcmUsIHlvdSBoYXZlIHNvbWUgc2tpbGxzIG91dCB0aGVyZSEgRG9uJ3QgZm9yZ2V0IHRvIHByYXkgZm9yIG91ciBicm90aGVycyBhbmQgc2lzdGVycywgVklWQSBQQUxFU1RJTkEh

As we go through the IDs one by one, we can retrieve our flag ! but, the challenge is not over yet as the 6th note is talking about a book and a page number, could it be a note id?

Indeed, after supplying the id we get some sort of an encrypted text.
Different tools on the web can help us decode the text, one of the most known is, **Cyberchef**.

Giving it the text we got, we'll see a magic wand that we can click on to decrypt the text and it's a base64 encoded text.



Input

```
R3JlYXQgam9iIGNoYW1waW9uLCBpbXByZXNzaXZlIGhvdyB5b3UgZ290IGhlcmUsIHlvdSBoYXZlIHNvbWUgc2tpbGxzIG9
1dCB0aGVyZSEgRG9uJ3QgZm9yZ2V0IHRvIHByYXkgZm9yIG91ciBicm90aGVycyBhbmQgc2lzdGVycywgVklWQSBQQUxFU1
RJTkEh
```

Output

```
Great job champion, impressive how you got here, you have some skills out there! Don't forget
to pray for our brothers and sisters, VIVA PALESTINA!
```