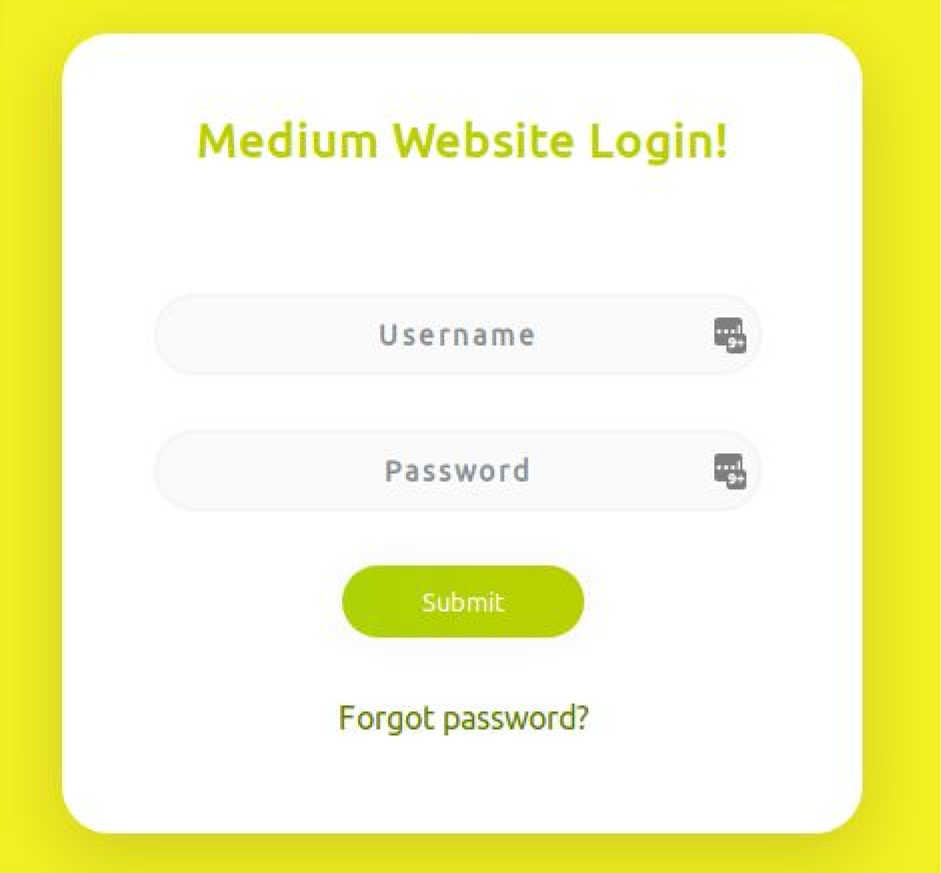
Medium Login

This challenge requires some OSINT, or Open Source Intelligence. Both the good guys and bad guys don't just start breaking in without doing some research first. Information that can be found on the open internet about companies and employees can be very informative. Your LinkedIn page listing all of your experience with specific technologies could be very useful to a hacker as it may tell them what technologies your company leverages. As could secrets in open github repositories, or maybe even personal details found on social media sites like Twitter. Or maybe a website you've got an account on (like the IRS website) has bad security questions. This challenge is meant to show how that kind of OSINT research can play out.

The challenge:

> *You'll have to do a little OSINT (Open Source Intelligence) work to get this flag. It's elementary!*
>
> *http://redacted-url*

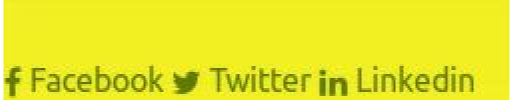
The page has the very ugly mustard yellow login page pictured here:


Medium Website Login!

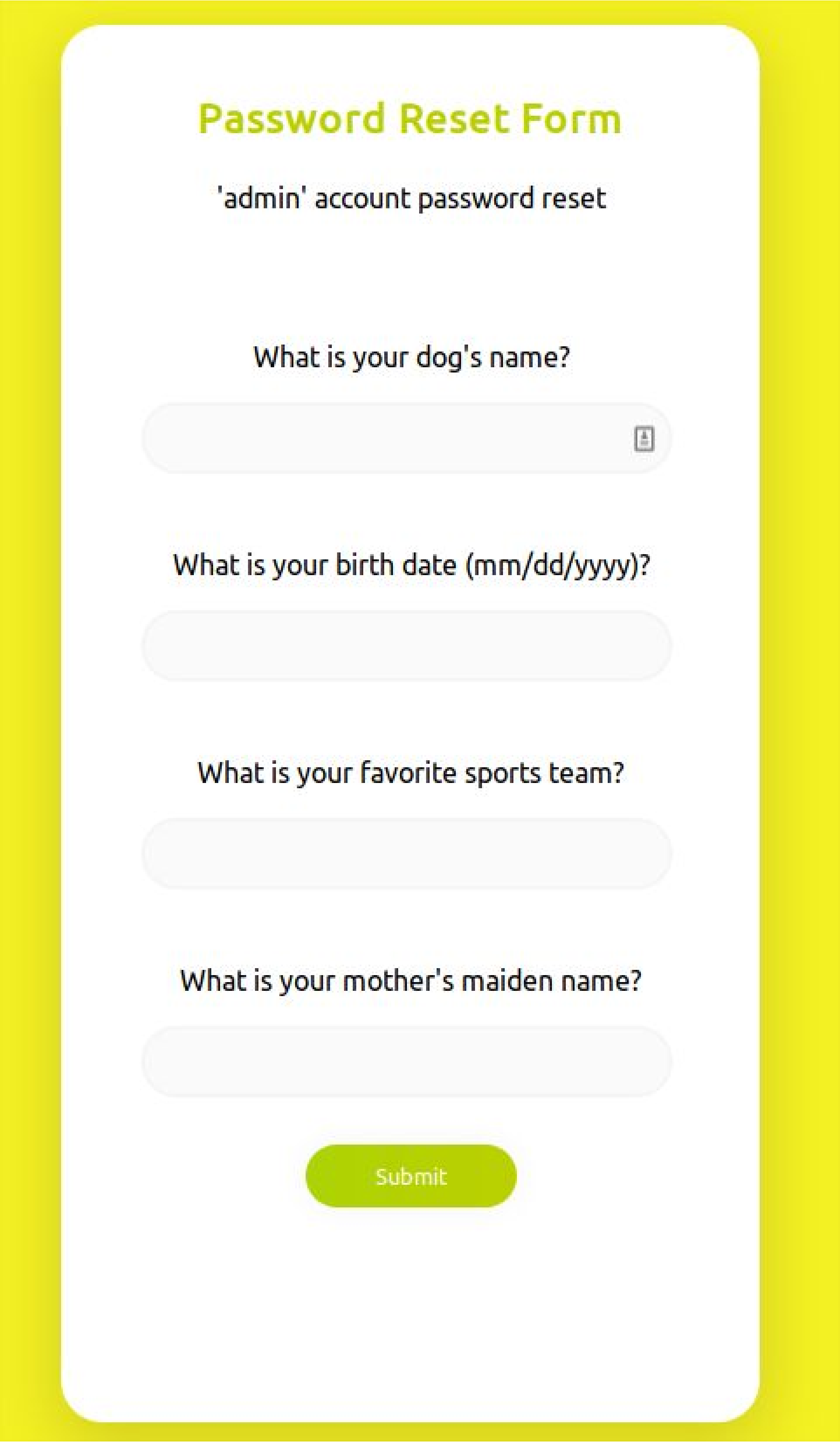
Username

Password

You may also may have noticed the links at the bottom of the page:



Clicking the "Forgot Password?" Link takes you the this page:



Password Reset Form

'admin' account password reset

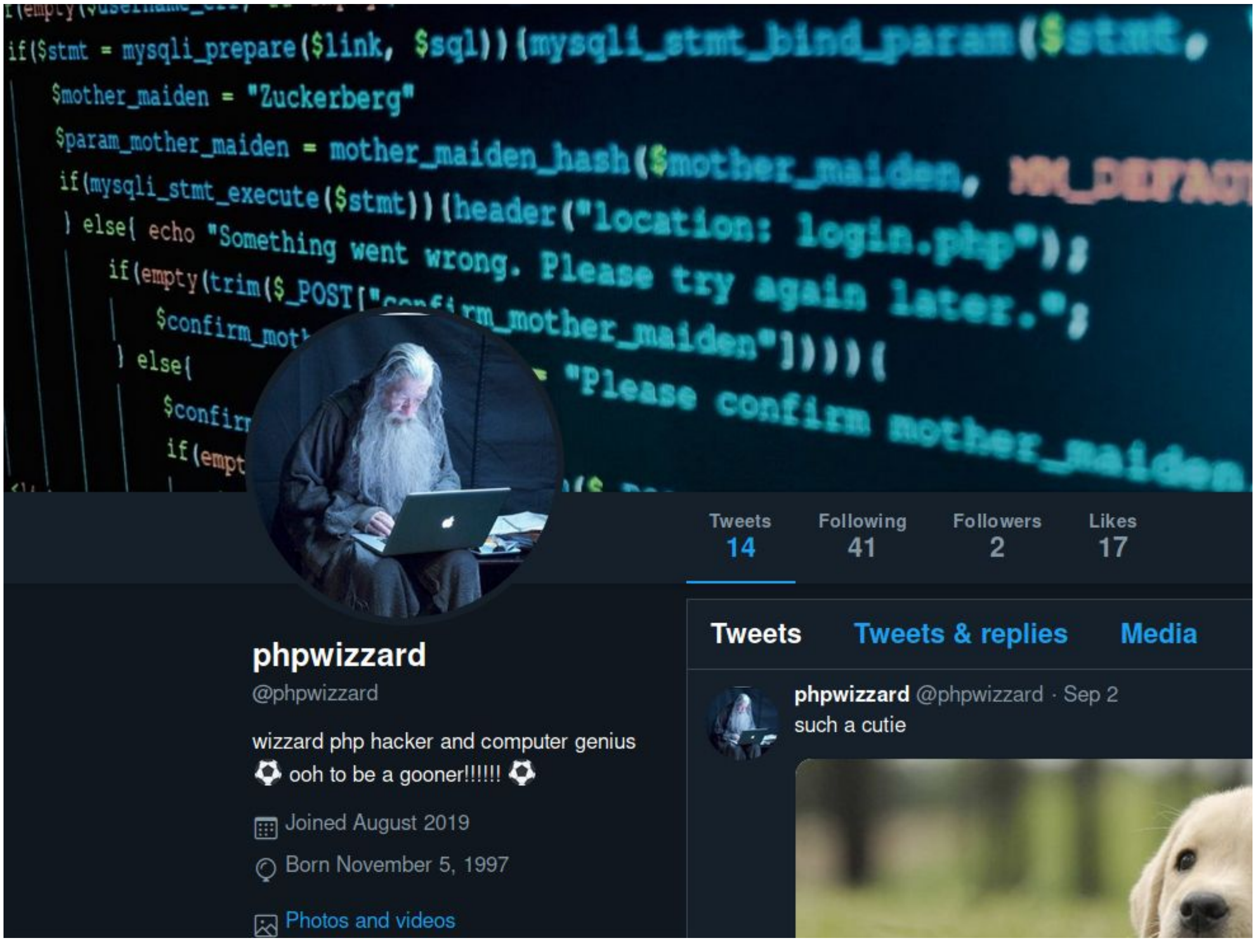
What is your dog's name?

What is your birth date (mm/dd/yyyy)?

What is your favorite sports team?

What is your mother's maiden name?

On this page you can see that the login is in fact “admin”, and that there is a password reset feature with some suspicious security questions. The source code on both pages won’t give you anything useful, but you can see that there is a Twitter account linked on both. Let’s take a look at that account, which must belong to the owner of this site: https://twitter.com/phpwizzard



```
if($stmt = mysqli_prepare($link, $sql)){mysqli_stmt_bind_param($stmt,
    $mother_maiden = "Zuckerberg"
    $param_mother_maiden = mother_maiden_hash($mother_maiden, MM_DEFAU
    if(mysqli_stmt_execute($stmt)){header("location: login.php");
    } else{ echo "Something went wrong. Please try again later.";
        if(empty(trim($_POST["confirm_mother_maiden"]))){
            $confirm_mot                     = "Please confirm mother_maiden
        } else{
            $confir
            if(empt
```

phpwizzard
@phpwizzard

wizzard php hacker and computer genius
⚽ ooh to be a gooner!!!!!! ⚽

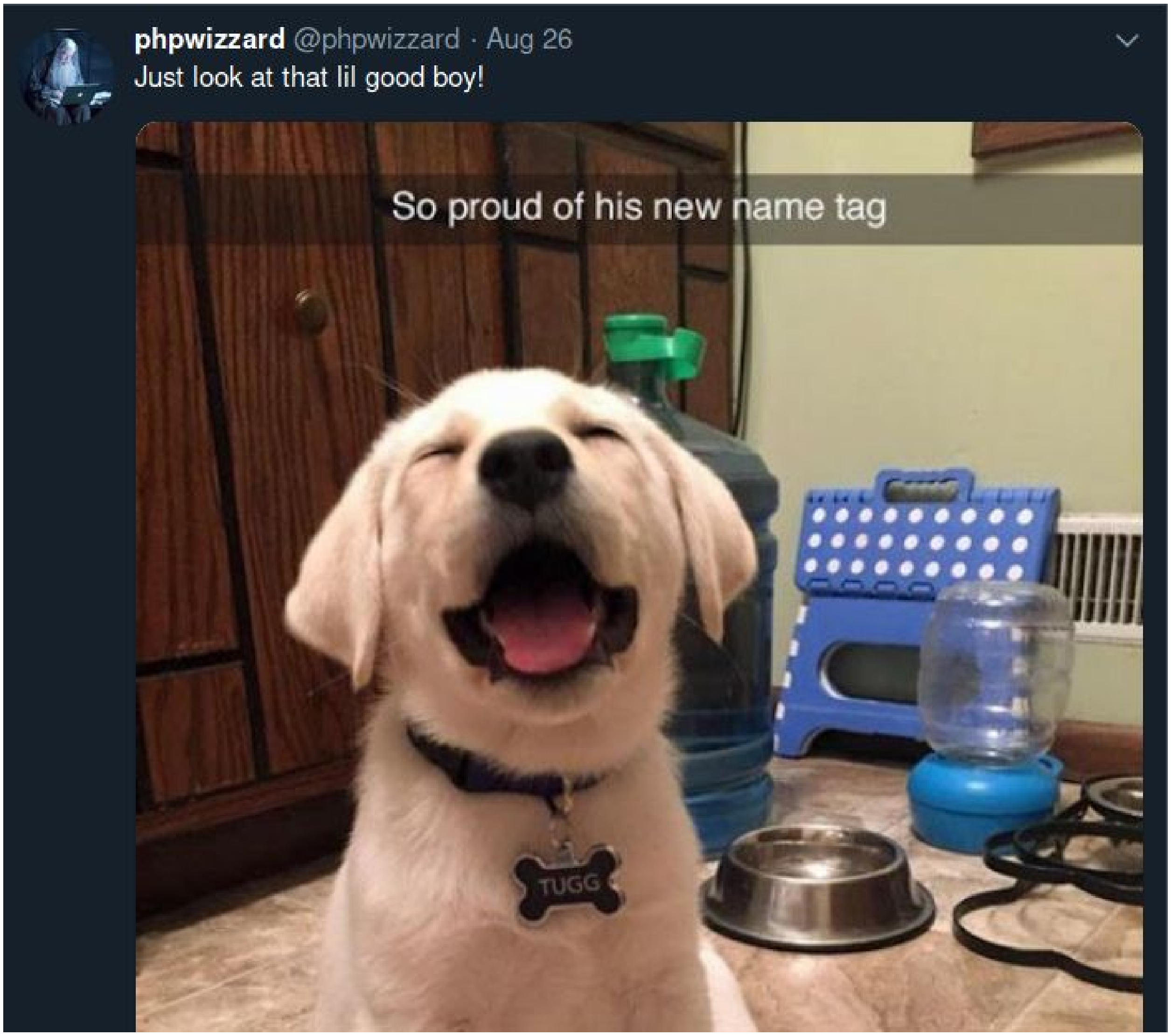
Joined August 2019

Born November 5, 1997

Photos and videos

phpwizzard @phpwizzard · Sep 2
such a cutie

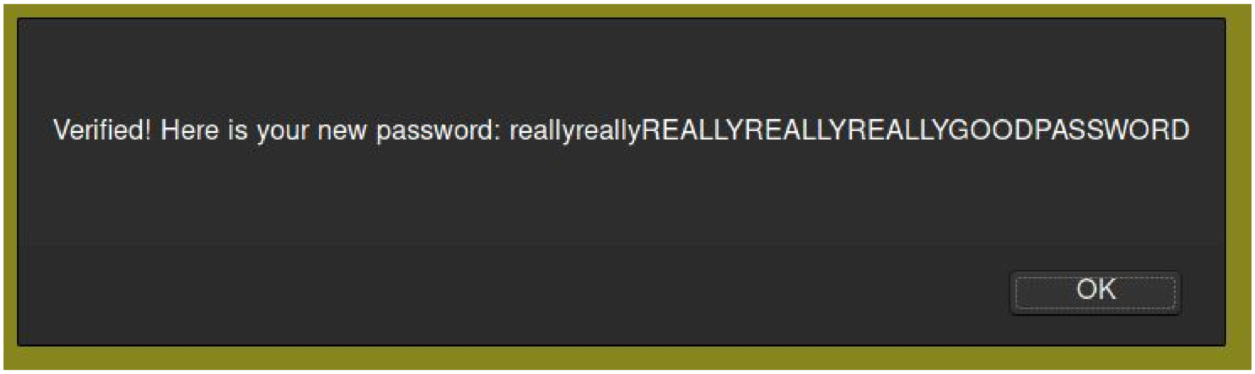
In the screenshot above 2 of the answers are clearly visible. The birthdate of the admin is 11/05/1997. The admin’s mother’s maiden name is in the banner image of the twitter account in the source code. The admin was definitely not practicing good opsec when trying to make a cool source code banner! The third is a hint that should lead you to the admin’s favorite sports team. [soccerball]ooh to be a gooner!!!!!![soccerball] is a clue. If you google that you’ll find that this is a chant for the Arsenal soccer team. That is the 3rd answer. The 4th is found in one of the pics of the admin’s dog that was uploaded in a tweet. You can find the pup’s name on his nametag in the picture below.



phpwizzard @phpwizzard · Aug 26

Just look at that lil good boy!

Enter those 4 answers (case does not matter): Tugg, 11/05/1997, Arsenal, Zuckerberg and you will be presented with a new password:



Verified! Here is your new password: reallyreallyREALLYREALLYREALLYGOODPASSWORD

Go back to the login page and enter the creds to get the flag:
That is a good password!! Here is the flag: flag{who_was_your_favorite_teacher}