

Web_Crypto


Description

CHALLENGE

265 SOLVES



Webcrypto

 200

I think we can all agree that most of us grew up watching the iconic cartoon Tom & Jerry. Every kid would feel that surge of adrenaline during the thrilling chases and chaotic conflicts between the mischievous mouse and the ever-determined cat. The excitement of those scenes—the heart-pounding moments of escape—sometimes felt almost real.

But then, I heard a little rumor: what if all those chases were fake? What if Tom and Jerry were actually friends all along? That revelation shook me. I had no one to ask about this mind-bending twist, so I decided to take matters into my own hands—I created a web app to settle this question once and for all.

I know the truth now. Do you think you can uncover it too?

<https://chal.acectf.tech/Webcrypto/>

Flag

Submit

Category

#web

Solution

Accessing the site we see that it is actually a PHP code

```
<?php
include('flag.php');
highlight_file(__FILE__);

// Check if parameters 'tom' and 'jerry' are not equal
if ($_GET['tom'] != $_GET['jerry']) {
    echo "<br>Parameter 1 Met!<br>";

    if (md5('ACECTF' . $_GET['tom']) == md5('ACECTF' . $_GET['jerry'])) {
        echo $FLAG; // If the condition is true, print the flag
    }
}
?>
```

This PHP asks for two param, tom and jerry. There value has to be different

This then compare the MD5 hash value when concatenate with ACECTF

Since this is using a double equal == It is vulnerable to magic hash attack

```
<?php
include('flag.php');
highlight_file(__FILE__);

// Check if parameters 'tom' and 'jerry' are not equal
if ($_GET['tom'] != $_GET['jerry']) {
    echo "<br>Parameter 1 Met!<br>";

    if (md5('ACECTF' . $_GET['tom']) == md5('ACECTF' . $_GET['jerry'])) {
        echo $FLAG; // If the condition is true, print the flag
    }
}
?>
```

Parameter 1 Met!

If we change this to array, the parameter stays the same as tom and jerry.

The only difference is PHP can't convert an array to a string, it only throws an error and only hashes the ACECTF string.



https://chal.acectf.tech/Webcrypto/?tom[]=1&jerry[]=2

```
<?php
include('flag.php');
highlight_file(__FILE__);

// Check if parameters 'tom' and 'jerry' are not equal
if ($_GET['tom'] != $_GET['jerry']) {
    echo "<br>Parameter 1 Met<br>";

    if (md5('ACECTF' . $_GET['tom']) == md5('ACECTF' . $_GET['jerry'])) {
        echo $FLAG; // If the condition is true, print the flag
    }
}
?>
```

Parameter 1 Met!

ACECTF{70m_4nd_j3rry_4r3_4ll135}