

# juggling-flea – PHP Type Juggling

```
<?php
if (empty($_POST))
{
    highlight_file(__FILE__);
    exit;
}
header("Access-Control-Allow-Origin: *");
header("Content-Type: application/json; charset=UTF-8");
$flag=require_once(' ../flag.php');
```

The web application is explicitly gives us the app's PHP code. We should inspect the code to understand how it works

# juggling-flea – PHP Type Juggling

```
$randno=intval(rand()%10);  
$mypassword=$randno.md5(time());
```

To form the password variable, the app generates a random number from 0 to 9, then appends an MD5 hash value to that number, e.g., 7 + cfc208495d565ef66e7dff9f98764da

# PHP Type Juggling – String / Integer

```
<?PHP
if (7 == "7cfcd208495d565ef66e7d
echo "Returned true!";
} else {
    echo "This won't execute\n";
```

When PHP compares strings and integers in a loose comparison, if the leading numbers match, then the comparison will always return True