OLIcyber – Make a Wish

```php
if(isset($_GET['richiesta'])) {
  if (preg_match("/.*/i", $_GET['richiesta'], $match))
    echo "No, mi dispiace non posso fare questo!";
        } else {
                echo "flag{TROVAMI}";
        }
} else {
  echo "Fai una richiesta e provero a realizzarla";
}
```

This challenge explicitly tells us the code that is running on the webpage

Make a Wish – PHP Code Analysis

```php
if(isset($_GET['richiesta'])) {
  if (preg_match("/.*/i", $_GET['richiesta'], $match))
    echo "No, mi dispiace non posso fare questo!";
        } else {
                echo "flag{TROVAMI}";
        }
} else {
  echo "Fai una richiesta e provero a realizzarla";
}
```

If the URL parameter richiesta (request) is provided, then it checks for a match in the request value

Make a Wish – PHP Code Analysis

```php
if(isset($_GET['richiesta'])) {
  if (preg_match("/.*/i", $_GET['richiesta'], $match))
    echo "No, mi dispiace non posso fare questo!";
        } else {
                echo "flag{TROVAMI}";
        }
} else {
  echo "Fai una richiesta e provero a realizzarla";
}
```

If there's a match, we don't get the flag, but if there's no match, we get the flag

Make a Wish – PHP Code Analysis

```
preg_match("/.*/i")

regular expression match
- matches any string
- including empty strings
```

The problem is that this function matches on any string given to it, so normally, we can't get the flag, no matter what

Make a Wish – Array Injection

```
preg_match(
    string $pattern,
    string $subject,
    array &$matches = null,
    int $flags = 0,
    int $offset = 0
): int|false
```

The trick here is to understand the PHP `preg_match` function that is used to match and deny our flag from being output

Make a Wish – Array Injection

```
preg_match(
    string $pattern,
    string $subject,
    array &$matches = null,
    int $flags = 0,
    int $offset = 0
): int|false
```

According to official docs, `preg_match` requires the subject (the thing to be compared) to be a string, but if we give it a non-string data type...

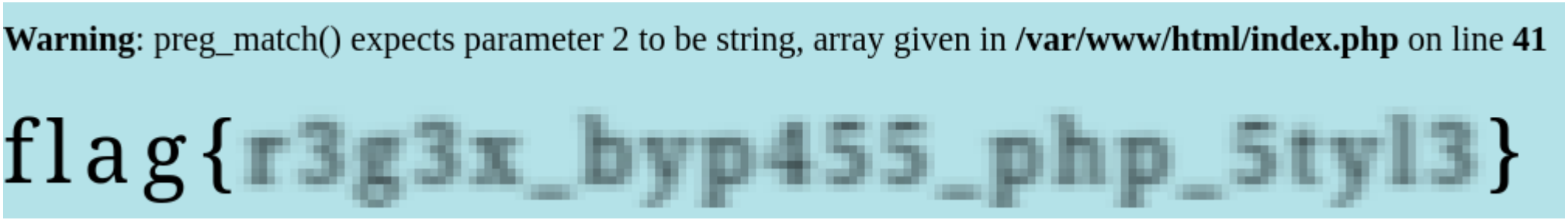
Make a Wish – Array Injection

```php
<?php
$array1 = array(
    "foo" => "bar"
);
preg_match("/.*/i", $array1, $matches);
?>
```

```
Uncaught TypeError: preg_match(): Argument #2
($subject) must be of type string,
array given in /home/user/scripts/code.php:5
```

Then the PHP engine will throw an error, but the error will count as the match returning False...

Make a Wish – Array Injection



Which will cause the page to echo out the flag