

## Curling in the cloud

Ici nous avons un service web qui va aller chercher une page donnée en paramètre.



Enter a URL to fetch

URL:

Il va ensuite afficher à l'utilisateur quelques mots du code source. Pourquoi ? Pourquoi pas...

Suite à une recherche avec les mots clés « curl php » sur Google nous pouvons voir que Curl est une bibliothèque « qui vous permet de vous connecter et de communiquer avec différents types de serveurs, et ce, avec différents types de protocoles. »

<http://php.net/manual/fr/intro.curl.php>

La suite logique serait de faire une deuxième recherche sur curl. Cependant, nous allons rechercher s'il y existe des vulnérabilités ou de mauvaises implémentations connues.

curl vulnerability php

Tous

Images

Vidéos

Actualités

Shopping

Plus

Paramètres

Outils

Environ 7 250 000 résultats (0,39 secondes)

Subtle vulnerabilities with PHP and cURL - Lukas's Random Thoughts

<https://statuscode.ch/2016/.../subtle-vulnerabilities-with-php-and-cu...>

Traduire cette page

Subtle vulnerabilities with PHP and cURL. Jan 25, 2016. This post tries to prove that vulnerabilities can in fact be very subtle and that even people who master ...

PHP curl\_exec() url is controlled by user - Vulnerabilities - Acunetix

[https://www.acunetix.com/vulnerabilities/.../php-curl\\_exec---url-is-...](https://www.acunetix.com/vulnerabilities/.../php-curl_exec---url-is-...)

Traduire cette page

This script is using the PHP function curl\_exec(). The url used by curl is based on user input. This is not recommended as it can lead to various vulnerabilities.

Is allowing unfiltered curl request from a website a vulnerability?

<https://security.stackexchange.com/.../is-allowing-unfiltered-curl-re...>

Traduire cette page

1 août 2015 - It could be XML, txt, HTML, any reachable path via curl. ... but a quickly hacked PHP page on my Windows machine happily consumed the URL:

curl - Vulnerability Table

<https://curl.haxx.se/docs/vulnerabilities.html>

Traduire cette page

This is the exhaustive list of all curl versions and which releases that are ... Each version number link shows a vulnerability summary for that specific release.

Are there any security vulnerabilities to allowing unfiltered user input ...

<stackoverflow.com/.../are-there-any-security-vulnerabilities-to-allo...>

Traduire cette page

!!

## PHP curl\_exec() url is controlled by user

Web Vulnerabilities / 10000 Medium Severity / 10000 PHP curl\_exec() url is controlled by user

Description

Manual confirmation is required for this alert.

This script is using the PHP function **curl\_exec()**. The url used by curl is based on user input. This is not recommended as it can lead to various vulnerabilities.

For example, an attacker can use the **file://** protocol to read arbitrary files from the server (by using an url like **file:///etc/passwd**). It's also possible to access computers behind the firewall using URLs like **http://192.168.0.1** or **ftp://192.168.0.1**.

An older version of libcurl compiled to support SCP can get tricked to get a file using embedded semicolons, which can lead to execution of commands on the given server. "scp://name:passwd@host/a" ;date >/tmp/test" ;"

Severity

LEVEL 3 - MEDIUM

Classification

CWE CVE-2009-0037

CWE CVE-352

Voilà quelque chose d'intéressant.

Si l'entrée d'un utilisateur n'est pas bien filtrée. Celui-ci sera en mesure de changer le fonctionnement prévu ! Essayons file://

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
c2:2:bin:/bin:/usr/sbin/nologin
:65534:sync:/bin:/bin/sync:c3:3:sys:/dev:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
s:x:9:9:news:/var/spool/news:/usr/sbin/nologin
games:x:5:60:games:/usr/games
spool/pd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
```

```
c:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
```

Enter a URL to fetch

URL:

Et voilà le fichier passwd du serveur. Il nous reste qu'à chercher notre flag !

FLAG-LECURLINGCESTUN'

Enter a URL to fetch

URL:

<http://www.acunetix.com/blog/articles/server-side-request-forgery-vulnerability/>

[https://www.acunetix.com/vulnerabilities/web/php-curl\\_exec---url-is-controlled-by-user](https://www.acunetix.com/vulnerabilities/web/php-curl_exec---url-is-controlled-by-user)