

Category:

Web

Name:

Find origin server – Basic.

Message:


A benign user reported a fake anti-virus vendor site in <https://trendymicro.ajccbc-cyber-sea-game.net/> . But we think this site uses a CDN (or a reverse proxy) to hide their identity. Your task is finding the way to find origin server behind the CDN.

Objective:

You can learn there is a case you can find the origin server behind CDN.


Write-up instructions:

You see a fake site in the given address like the below.



What Is Credit Card Fraud? & How to Avoid It

June 20, 2024



You might not realize it, but a quick swipe of your card or an innocent entry of its details onto a shopping site could turn into a financial nightmare. In this article, we delve into the nuances of credit card fraud, how it happens, and, most importantly, how you can protect yourself from it.

What Is Credit Card Fraud?

Credit card fraud is a type of identity theft that involves the unauthorized use of someone's credit card information to make purchases or withdraw funds. It can range from small-scale theft of an individual's credit card information to massive data breaches affecting thousands of people.

How Does Credit Card Fraud Happen?

Credit card fraud can occur in several ways. Here are some of the most common methods:

- **Physical theft:** The classic case of pickpocketing, where the actual card is stolen.
- **Skimming:** Devices installed on ATMs or card readers that steal your card information.
- **Phishing:** Scams via email or phone designed to trick you into providing your card details.
- **Data breaches:** When hackers infiltrate a company's secure data storage to steal credit card information.
- **Public Wi-Fi:** Unsecured networks can be a hotbed for intercepting financial details during transactions.

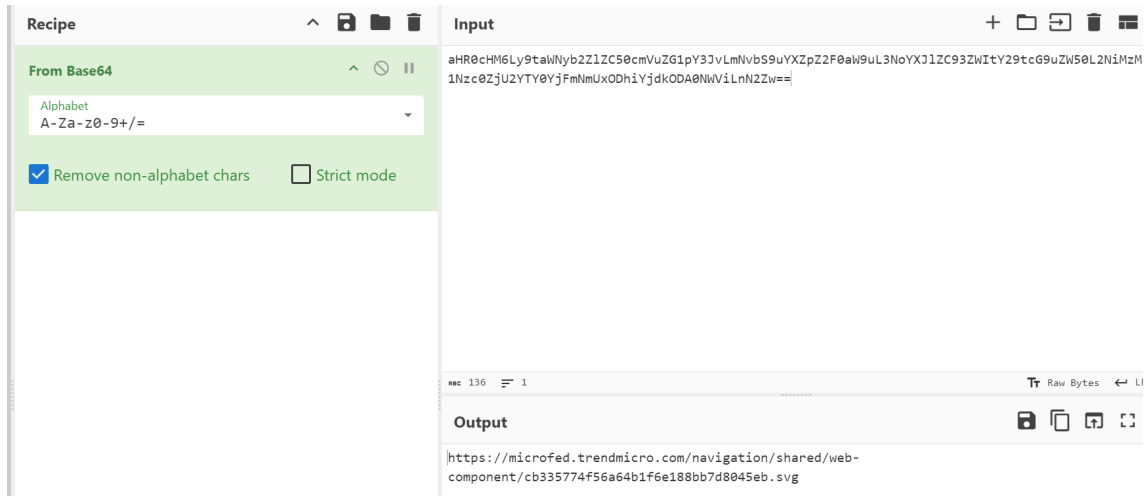
Reading the source you can find /imgcdn.php whose parameter is a base64-encoded string.

```

<div class="nav_logo" src="/imgcdn.ahc7a1c-sH0cHMLv3ta8Wb2Z1ZC50cnUzG1eY3JyLnHb59vYXZaZ2FbBmUd3WcYXU1ZC93Zm1Y29tCG9uZm50L2NlZm91bnR5c0ZlU2YTY0YjFmNmUwODhYfj80040MMlLnkZem" srcset="">
<h1>What Is Credit Card Fraud? & How to Avoid It</h1>
<p>June 20, 2024</p>

```

Try decode the strings as usual. You will see the original URL of the picture.



As the extension implies a PHP script, that should run on the origin server when it receives a request. You may think “pic” should be a picture URL, but is this true? You can check it by inputting an encoded URL. For example, <https://google.com/>, encoding to “aHR0cHM6Ly9nb29nbGUuY29tLw==”

Accessing to <https://trendmicro.ajccbc-cyber-sea-game.net/imgcdn.php?pic=aHR0cHM6Ly9nb29nbGUuY29tLw==> returns a corrupted data, but it has 23492 bytes.

Name	X	Headers	Payload	Preview	Response	Initiator	Timing
imgcdn.php?pic=aHR0cHM6Ly9nb29nbGUuY29tLw==		▼ General					
favicon.ico		Request URL:			https://trendmicro.ajccbc-cyber-sea-game.net/imgcdn.php?pic=aHR0cHM6Ly9nb29nbGUuY29tLw==		
		Request Method:			GET		
		Status Code:			200 OK		
		Remote Address:			10.80.22.80:8080		
		Referrer Policy:			strict-origin-when-cross-origin		
		▼ Response Headers					
		Content-Length:			23492		
		Content-Type:			image/jpeg		
		Date:			Thu, 26 Sep 2024 04:37:21 GMT		
		Server:			CherryPy/18.10.0		

Download and check it. You can find this is a HTML source from google.

User is challenger, password is FQDN

As stated, username is “challenger”, and the password is “trendymicro.ajccbc-cyber-sea-game.net”.

CSG_FLAG{Claim_Abuse_to_Network_Admin}

Then you will get the flag “CSG_FLAG{Claim_Abuse_to_Network_Admin}”.

References:

Tools

- Cyberchef: <https://gchq.github.io/CyberChef/>