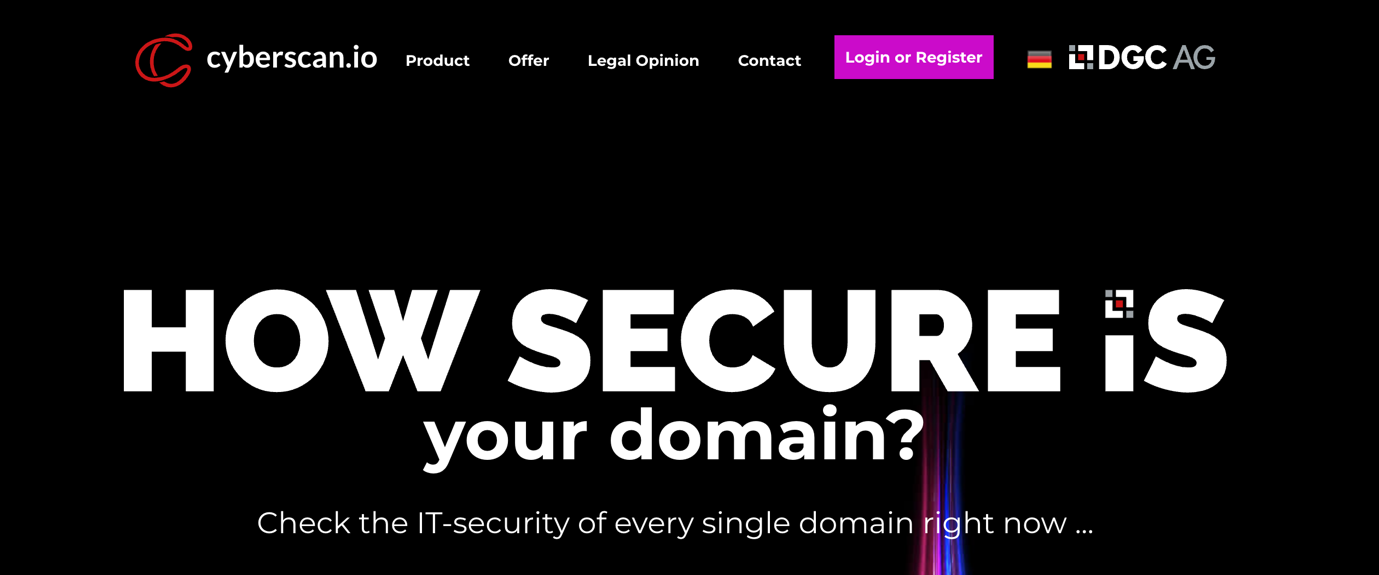
**CTF: Comprehensive Website Security Analysis with Cyberscan.io**



**Introduction**

Cyberscan.io is a tool that performs a comprehensive security assessment of websites, identifying various vulnerabilities and configuration issues. This CTF challenge involves analyzing the security report for the website "https://testphp.vulnweb.com" and identifying security misconfigurations, vulnerabilities, and potential risks.

**Tools and Requirements**

* Access to cyberscan.io: <https://www.cyberscan.io/>
* Basic understanding of web security concepts

**Scenario**

As a cybersecurity analyst, you are tasked with performing a security assessment of the website "https://testphp.vulnweb.com". Using the scan results from Cyberscan.io, you aim to identify vulnerabilities, configuration issues, and potential security risks. You will provide detailed analysis and recommendations for improving the website's security posture.

**Process**

1. Open the website “cyberscan.io”: [www.cyberscan.io](http://www.cyberscan.io)
2. After that scan the website “testphp.vulnweb.com”:

: <http://testphp.vulnweb.com/>

1. Capture the Flag

**Questions**

Flag 1: What hostname is associated with the IP address "8.20.241.107"?

Answer: ns1.eurodns.com

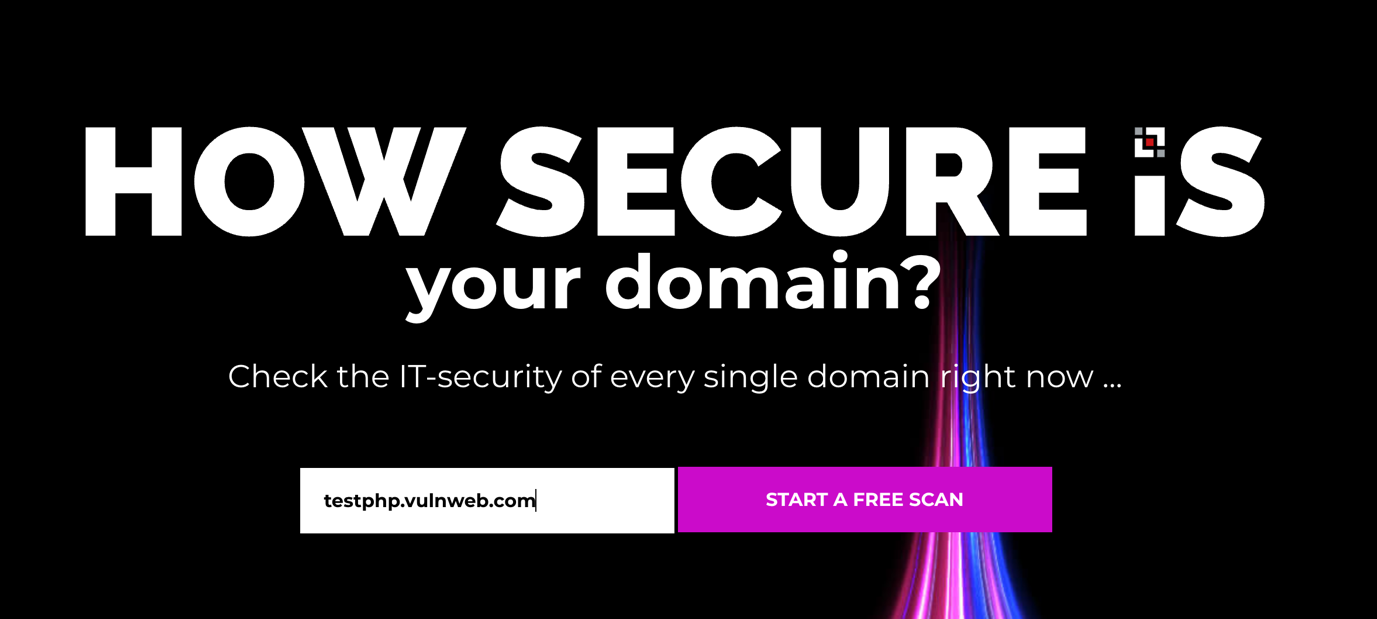
Flag 2: What ISP is for the IP range "8.20.243.0 - 8.20.243.255"?

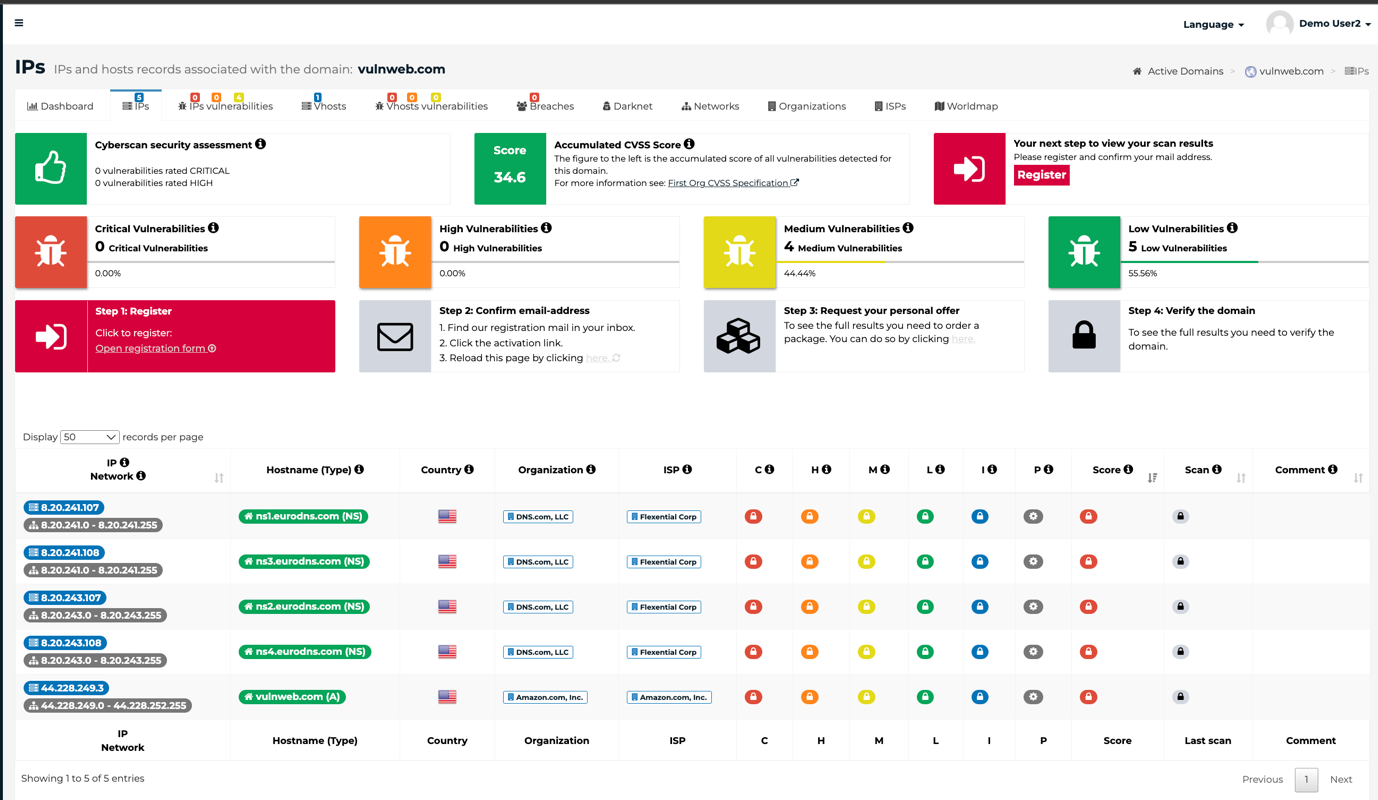
Answer: Flexential Corp

Flag 3: Which organization is associated with the IP address "8.20.241.108"?

Answer: DNS.com, LLC

**Hint**

****



This challenge should test the participants' ability to interpret comprehensive security scan results and understand the importance of various security configurations and vulnerabilities in web security.