**CTF: Attack Vector Discovery with Nikto Scanner on SUIP.biz**



**Introduction**

****

Nikto is a web server scanner that performs comprehensive tests against web servers for multiple items, including dangerous files, outdated server software, and other vulnerabilities. In this challenge, you will use the Nikto scanner on SUIP.biz to analyze the website http://testphp.vulnweb.com/ and uncover potential attack vectors.

**Tools and Requirements**

To perform this CTF, you will need the following tools and resources:

* A web browser (e.g., Chrome)
* SUIP.biz Nikto Scanner: <https://suip.biz/?act=nikto>
* The target website: testphp.vulnweb.com: <http://testphp.vulnweb.com/>

**Scenario**

**A person sitting in front of several computer screens

Description automatically generated**

You are a cybersecurity analyst tasked with evaluating the security posture of a web application. Your mission is to use the Nikto scanner on SUIP.biz to scan the target website testphp.vulnweb.com for vulnerabilities. You will document the findings and answer specific questions based on the scan results.

**Process to Perform**

**Step 1: Visit SUIP.biz Nikto Scanner**

* Open https://suip.biz/?act=nikto in your browser.

**Step 2: Perform a Website Scan**

* Enter the target website URL "http://testphp.vulnweb.com/" into the provided field.
* Initiate the scan and wait for the results to be generated.

**Step 3: Analyze the Results**

* Review the detailed report provided by the Nikto scanner on SUIP.biz about the target website.
* Look for identified vulnerabilities, weak points, and potential attack vectors.
* Note down any significant findings, such as outdated software, server misconfigurations, or security vulnerabilities.

**Let's Begin the Challenge**

With the tools and techniques outlined above, let's dive into the challenge. Use the Nikto scanner on SUIP.biz to uncover potential attack vectors and security weaknesses in the target website. Document each step you take and any findings along the way.

**Questions**

1. What server software version is identified by the Nikto scanner?

Answer: nginx/1.19.0

2. What PHP version is indicated in the 'XPoweredBy' header?

Answer: 5.6.40

3. Which important security header is missing to prevent clickjacking?

Answer: X-Frame-Options

4. Which header that prevents MIME type sniffing is not set?

Answer: XContentTypeOptions

**Happy hunting!**A screenshot of a computer error

Description automatically generated