# **CTF Topic: HostedScan**

# **Introduction**

Hosted scans are security assessments conducted through third-party services to identify vulnerabilities and security issues in web applications or networks. These scans are typically done via cloud-based platforms, providing comprehensive reports on potential threats. This CTF challenge will guide you through using a hosted scan service and understanding its results.

# **Tools and requirements**

**Hosted Scan Service:** A service like Qualys, Tenable.io, or a similar platform. For this challenge, we'll use a fictional service called "SecureScan".

**Sample Website URL or IP Address:** A URL or IP address of a web application or network to scan.

# **Link (File)**

<https://hostedscan.com/scans>

# **Scenario**

You are a cybersecurity analyst responsible for ensuring the security of your organization's web assets. You have been given a URL to a web application and need to perform a hosted scan using SecureScan to identify any potential vulnerabilities.

# **Process to Perform**

**Access SecureScan:** Open your web browser and navigate to the SecureScan platform.

**Input the URL/IP:** Enter the URL or IP address of the web application or network you want to scan in the provided input field.

**Configure the Scan:** Choose the type of scan (e.g., web application scan, network scan) and configure any advanced settings if needed.

# **Let's Begin The Challenge**

You have been provided with the following URL to scan: <https://kavyaschool.edu.np/>. Use SecureScan to scan this URL and answer the following questions:

# **Question**

**Flag 1:** How many vulnerabilities were detected?

**Ans:** 6

**Flag 2:** What vulnerabilities were detected?

**Ans:** Generic Padding Oracle, Cookie No HttpOnly Flag

# **Hint**

Pay close attention to the detailed report provided by SecureScan. Look for the CVE identifiers and severity ratings (e.g., low, medium, high, critical). The mitigation steps are usually provided alongside the vulnerability descriptions.

