To identify vulnerabilities and perform a Vulnerability Assessment and Penetration Testing (VAPT) on a website, you can utilize various online tools and platforms that specialize in web security testing. Here are some popular online resources and tools you can use:

**Online Vulnerability Scanners**

1. **Qualys FreeScan**:
   * **Description**: A free online vulnerability scanner that helps identify security vulnerabilities in your network.
   * **URL**: [Qualys FreeScan](https://www.qualys.com/products/freescan/)
2. **HackerTarget**:
   * **Description**: Offers a variety of tools for network and web security testing.
   * **URL**: [HackerTarget](http://www.hackertarget.com/)
3. **SecurityHeaders**:
   * **Description**: Checks the security headers of a website to ensure they are properly configured.
   * **URL**: [SecurityHeaders](https://securityheaders.com/)
4. **CyberChef**:
   * **Description**: A web-based tool that allows you to perform data encoding, decoding, and analysis.
   * **URL**: [CyberChef](https://gchq.github.io/CyberChef/)
5. **Sucuri SiteCheck**:
   * **Description**: A free online scanner to check your website for malware, blacklisting, and other security issues.
   * **URL**: [Sucuri SiteCheck](https://sitecheck.sucuri.net/)
6. **Burp Suite Online**:
   * **Description**: A web-based version of the popular Burp Suite tool for web security testing.
   * **URL**: [Burp Suite Online](https://portswigger.net/burp)

**Manual Testing Tools**

1. **OWASP ZAP (Zed Attack Proxy)**:
   * **Description**: An open-source web application security scanner.
   * **URL**: [OWASP ZAP](https://www.zaproxy.org/)
2. **Nikto**:
   * **Description**: An open-source web server scanner which performs comprehensive tests against web servers for multiple items.
   * **URL**: [Nikto](https://cirt.net/Nikto2)
3. **SQLmap**:
   * **Description**: An open-source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws.
   * **URL**: [SQLmap](https://sqlmap.org/)
4. **W3AF (Web Application Attack and Audit Framework)**:
   * **Description**: An open-source web application security scanner.
   * **URL**: [W3AF](https://w3af.org/)

**Online Courses and Tutorials**

1. **Hack The Box**:
   * **Description**: An online platform offering a wide range of cybersecurity challenges and labs.
   * **URL**: [Hack The Box](https://www.hackthebox.eu/)
2. **TryHackMe**:
   * **Description**: An online cybersecurity learning platform with interactive labs and challenges.
   * **URL**: [TryHackMe](https://tryhackme.com/)
3. **PortSwigger Web Academy**:
   * **Description**: Free online training and resources for web security.
   * **URL**: [PortSwigger Web Academy](https://portswigger.net/web-security)

**Community Forums and Resources**

1. **Stack Exchange - Information Security**:
   * **Description**: A Q&A platform for information security professionals.
   * **URL**: [Stack Exchange - Information Security](https://security.stackexchange.com/)
2. **OWASP (Open Web Application Security Project)**:
   * **Description**: A nonprofit organization focused on improving the security of software.
   * **URL**: [OWASP](https://owasp.org/)

By using these online resources and tools, you can effectively identify vulnerabilities and perform a comprehensive VAPT on your target website.