**Kaushal Kotkar**

**BE-15**

**Roll no: 54**

**Experiment No. 5**

**Aim:** Use OSINT Tools to identify the technologies and frameworks used by the website, such as content management systems (CMS), server software, programming languages, or analytics tools and create vulnerability reports.

**Lab outcome:** Get familiar with Technical Foot printing websites for mitigating various threats.

**Theory:**

The aim here is to utilize OSINT (Open-Source Intelligence) tools to determine the technologies and frameworks used by a website. This includes identifying content management systems (CMS), server software, programming languages, and analytics tools. Additionally, we aim to create vulnerability reports by analysing the identified technologies for potential security weaknesses.

**Tools:**

1. **BuiltWith:**

BuiltWith is an OSINT tool designed to reveal the technology stack of a website. It provides information on CMS platforms, server software, web frameworks, analytics tools, and more. It helps in understanding the website's architecture.

1. **WhatWeb:**

WhatWeb is an OSINT tool specifically designed for web fingerprinting. It scans websites to identify the software and technologies employed, including CMS, frameworks, and server details.

1. **Netcraft:**

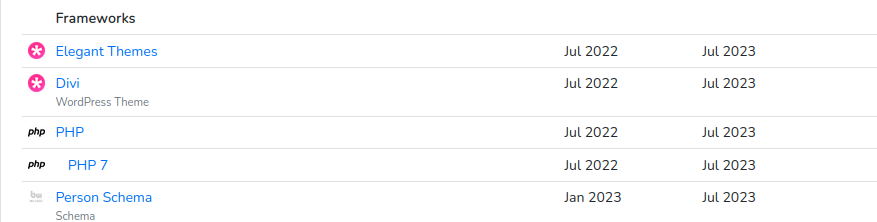
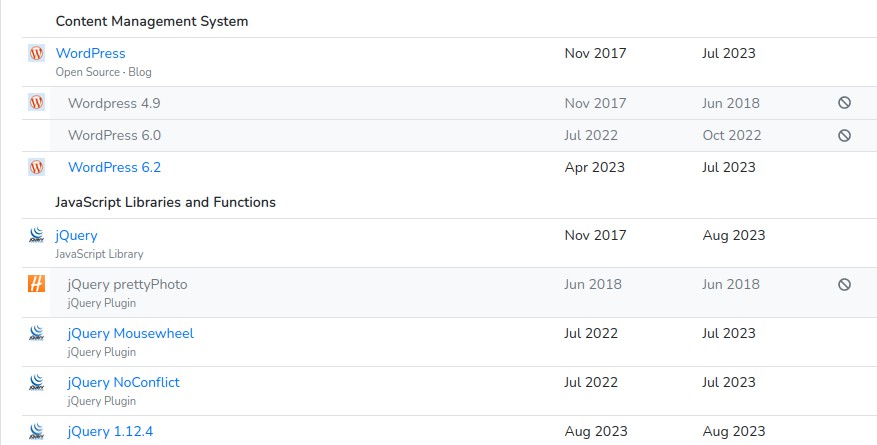
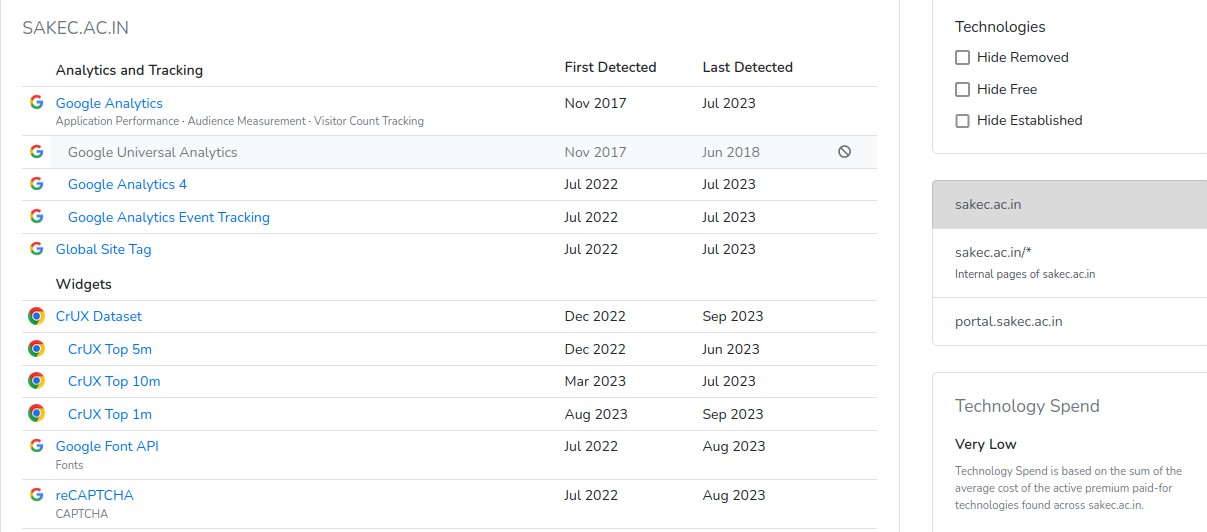
Netcraft is an OSINT tool that focuses on internet security. It can provide information about a website's hosting infrastructure, server software, and historical data, aiding in vulnerability assessment.

1. **Wappalyzer:**

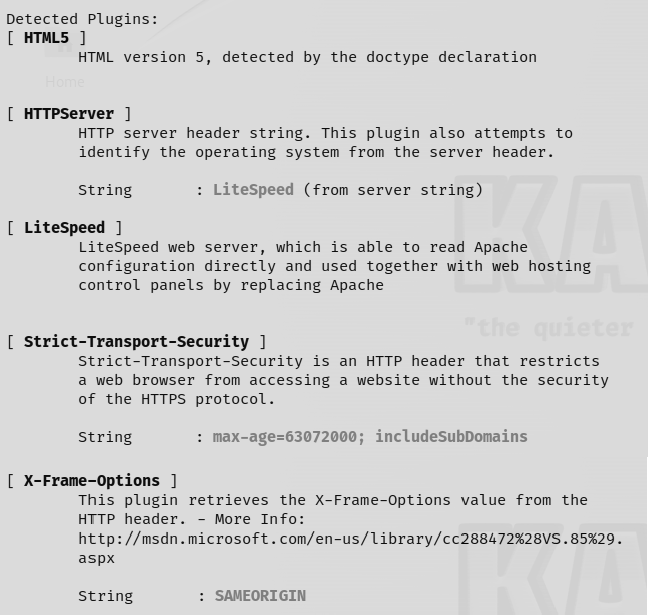
Wappalyzer is a browser extension that detects the technologies used by websites. It identifies CMS, JavaScript frameworks, web servers, and more. While not a standalone OSINT tool, it's a handy resource for technology discovery.

**Result:**

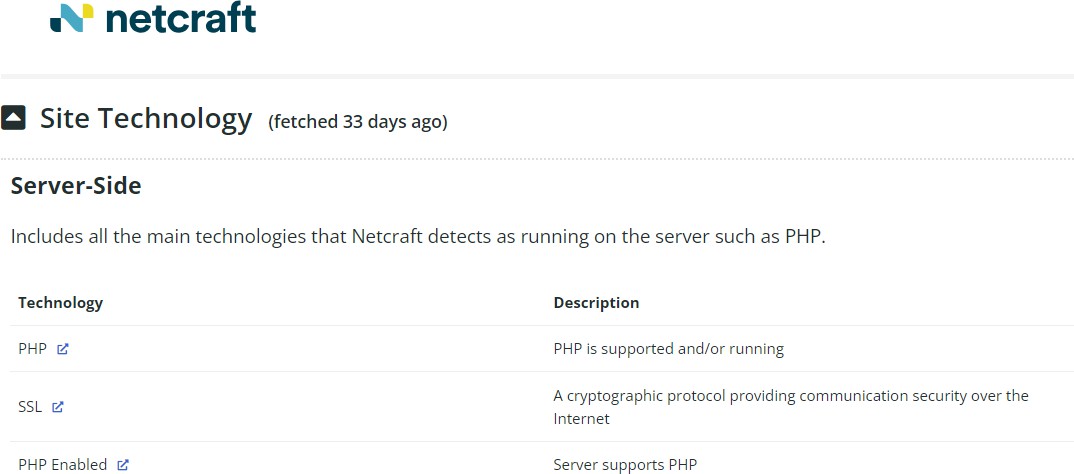
**Built with:** BuiltWith provides a comprehensive list of technologies used by the website, including the CMS, web server, JavaScript frameworks, analytics tools, and more.



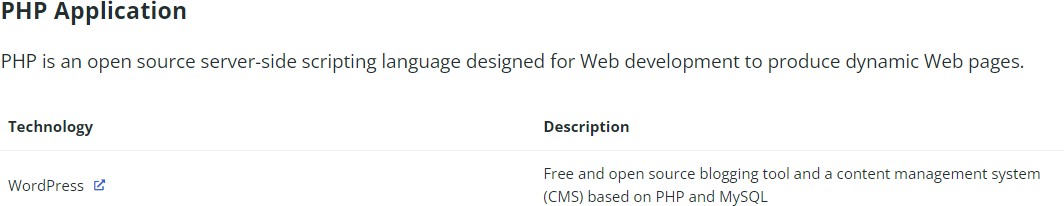
**WhatWeb:** WhatWeb scans and identifies CMS, web frameworks, server software, and more, offering a detailed breakdown of the technologies in use.



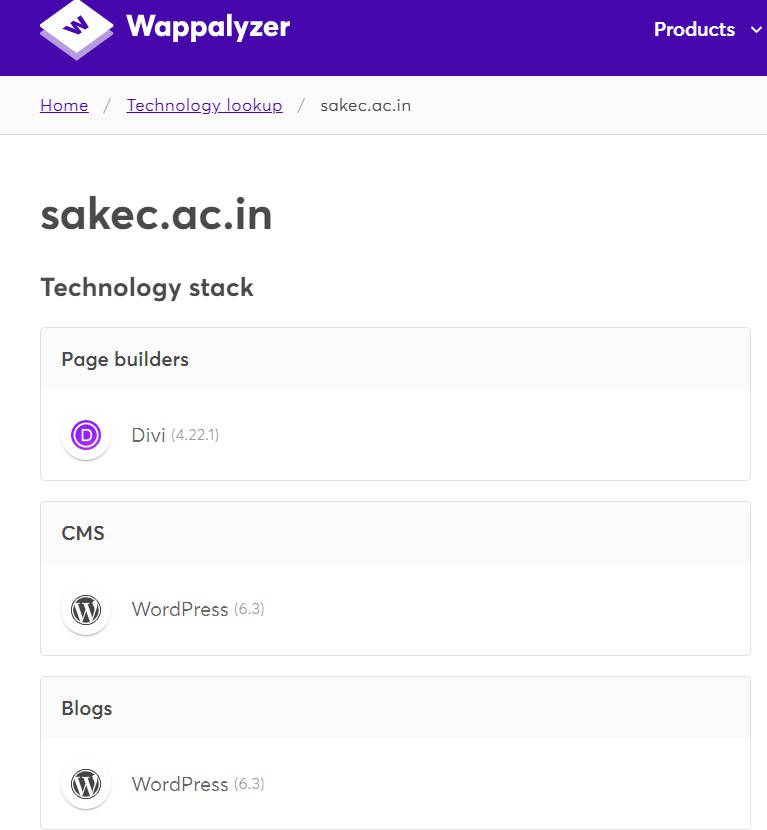
**Netcraft:** Netcraft provides information about the website's hosting infrastructure, server software, and historical data related to the domain.

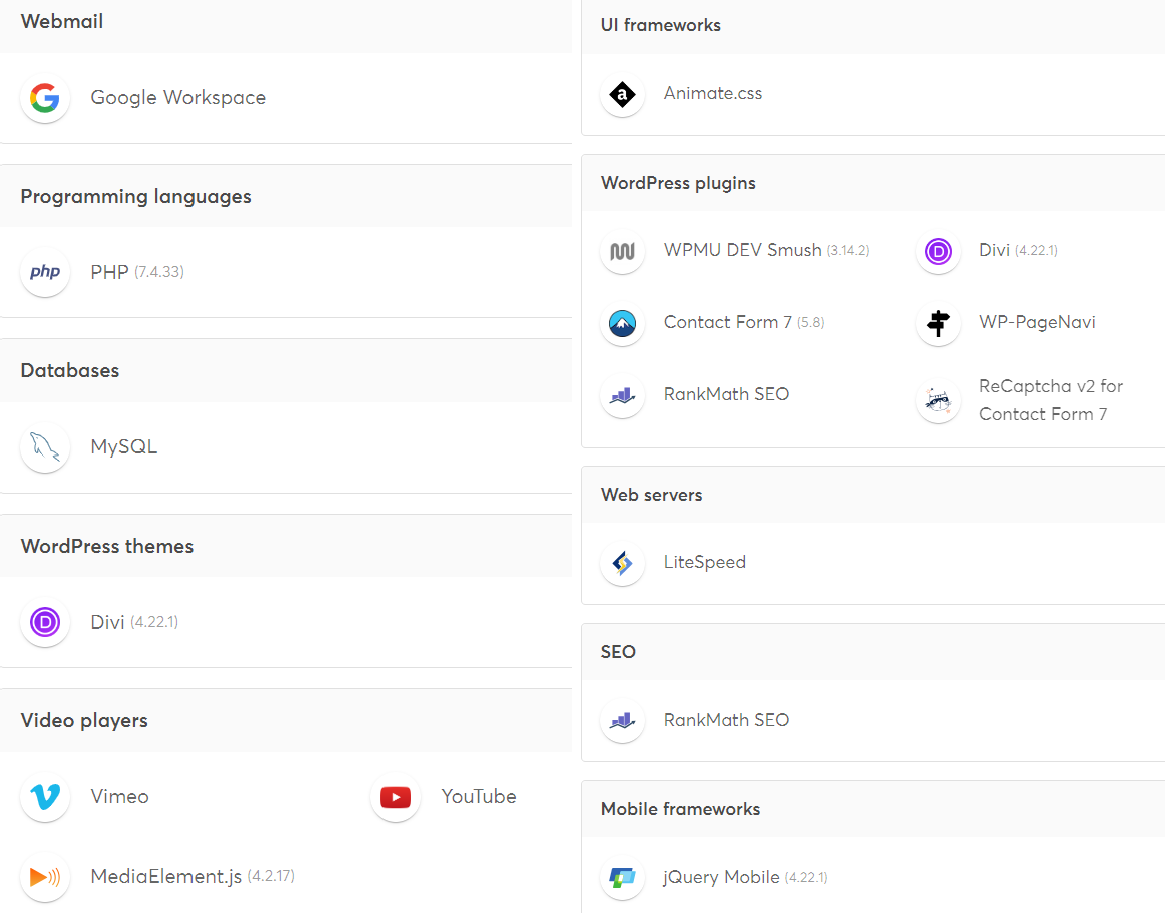
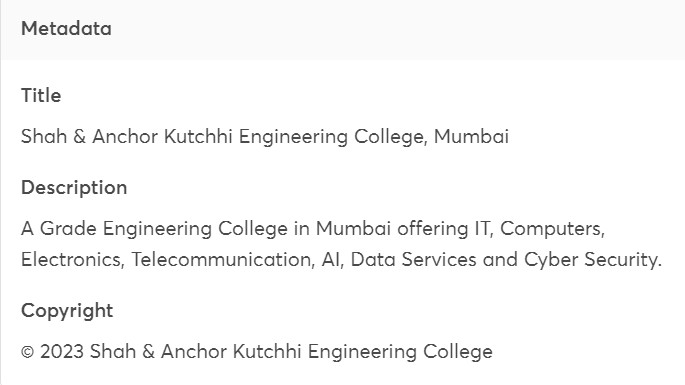






**Wappalyzer:** Wappalyzer, as a browser extension, identifies the technologies and frameworks employed by the website, including CMS, JavaScript frameworks, and web servers.





**Conclusion:**

Utilizing these OSINT tools, we successfully identified the technologies and frameworks used by the target website. This knowledge is essential for creating vulnerability reports and assessing potential security weaknesses associated with the website's technology stack. Understanding the technology landscape enables us to proactively address security risks and enhance the overall security posture of the website.