

Browser Extensions

Intro

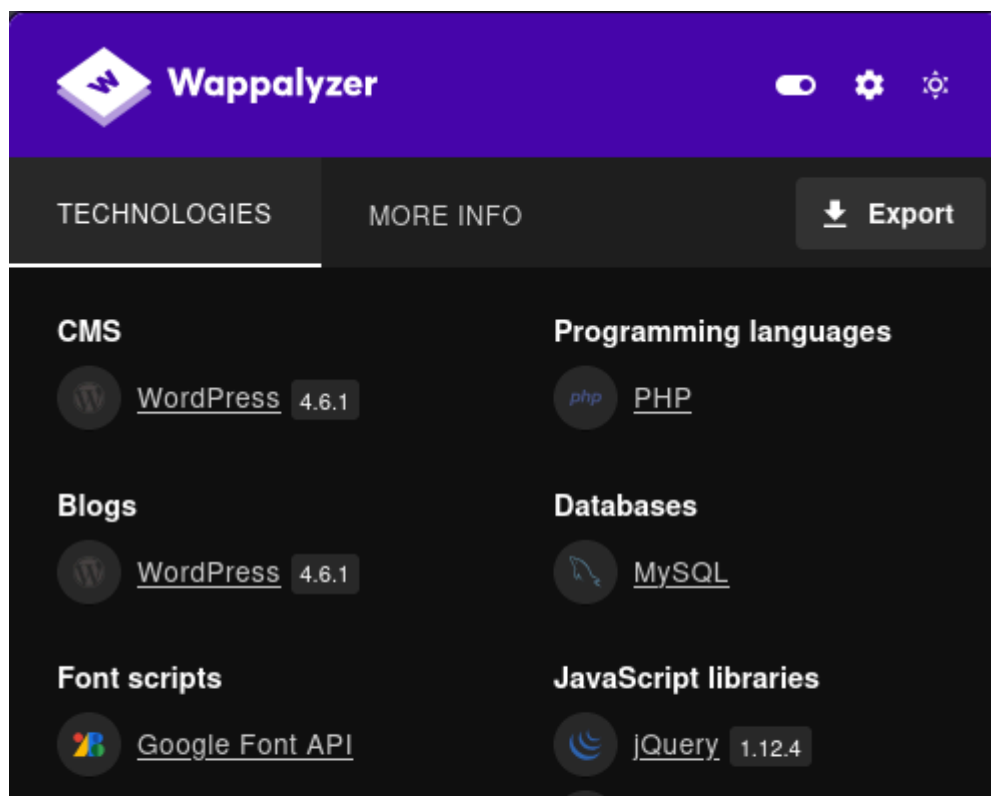
The last point we'll review in this section is **browser extensions** and how they will help us not only perform reconnaissance tasks, but can also be useful for certain **exploitation tasks**.

Browser extensions are small programs that extend the functionality of a web browser. In the context of cybersecurity, they can be used as both defensive and offensive tools. Browser extensions can be key tools during the reconnaissance phase of cybersecurity, allowing us to passively or actively gather valuable information about a target and, as we mentioned at the beginning, expand our capabilities in the exploitation phase.

So, let's see some browser extensions that will be useful on a web hacking exercise.

Wappalyzer and TechsFound

Wappalyzer is, probably, the most popular Browser Extension using web penetration testing. This extension is dedicated **to identify the technologies** that run on a website like CMS, servidores, frameworks, JS library, etc. Similar to **whatweb** does. Here a example:



Another tool that will be very useful on the detection of the technologies that runs on a web site and will complement **Wappalyzer** is **TechsFound**. Here the example:

Technologies

SSL Details

Valid Untill:
Day(s) Remaining:

CMS

WordPress

Programming languages

php PHP

Operating systems

Windows Server

Web server extensions

Shodan

The **Shodan** extension allows us to use the IoT capabilities of this powerful search engine to view detailed information about the IP address of the website that we are visiting directly from our browser such as **open ports and detected services**, banner information. **scan history and known vulnerabilities**, and more. Here's an example of this:

www.hackthissite.org

IP Address

137.74.187.103

Hostname(s)

hackthisjogneh42n5o7gbzrewxee3vyu6e
www.hackthissite.org
hackthissite.org

Tags

onion

Vulnerabilities

CVE-2019-11358, CVE-2012-6708, CVE-20
CVE-2015-9251, CVE-2020-11023

Open Ports

80

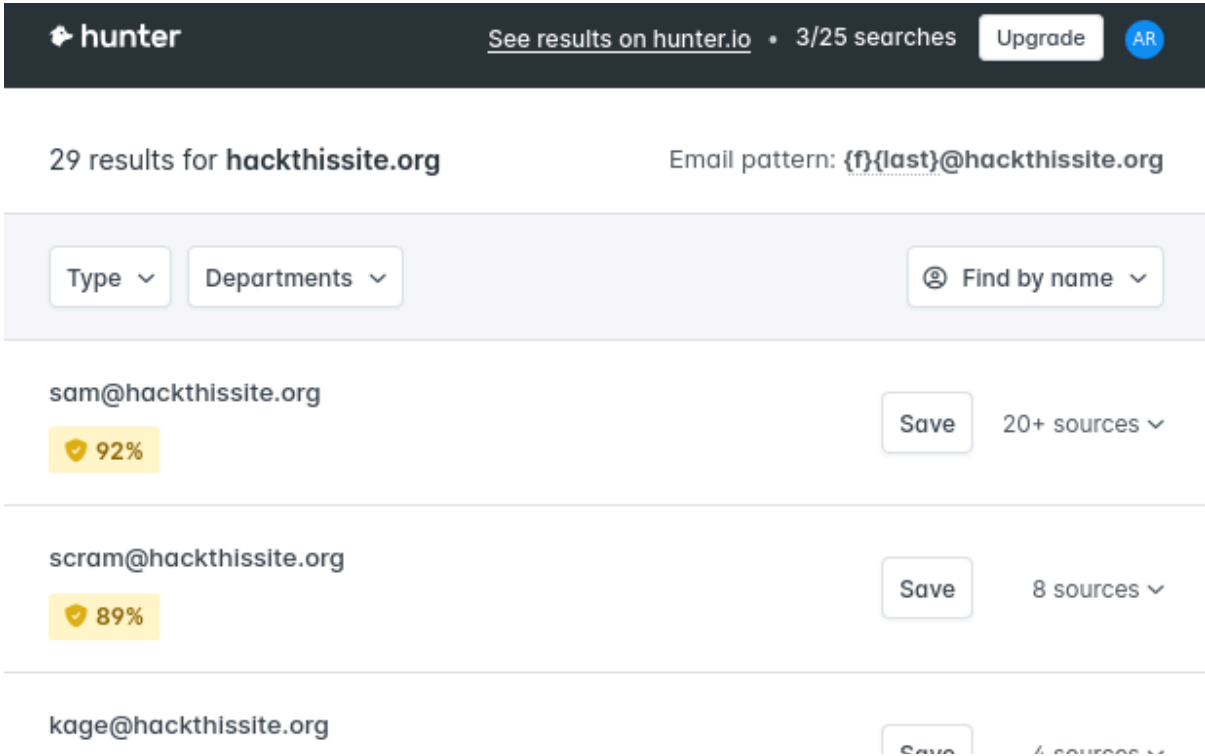
443

VIEW IP DETAILS

VIEW DOMAIN DETAILS

Hunter

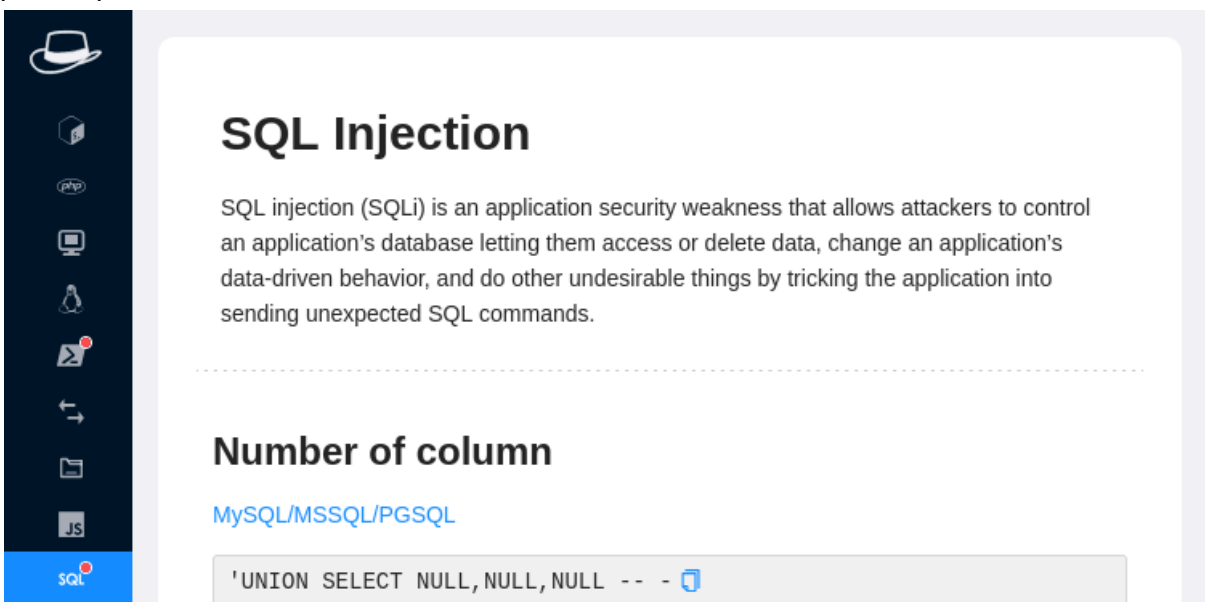
The **Hunter.io** extension allows us to **find email addresses** associated with a domain directly from the browser while visiting a website. This is especially useful during OSINT or reconnaissance phases of an audit. Here a example:



The screenshot shows the Hunter.io extension interface. At the top, there's a dark header with the 'hunter' logo, a link to 'See results on hunter.io', a search count '3/25 searches', an 'Upgrade' button, and a user profile icon 'AR'. Below the header, it displays '29 results for hackthissite.org' and the email pattern '{f}{last}@hackthissite.org'. A filter bar contains 'Type', 'Departments', and 'Find by name' dropdowns. Three email results are visible: 'sam@hackthissite.org' with a 92% confidence score and '20+ sources', 'scram@hackthissite.org' with an 89% confidence score and '8 sources', and 'kage@hackthissite.org' with '4 sources'.

HackTools

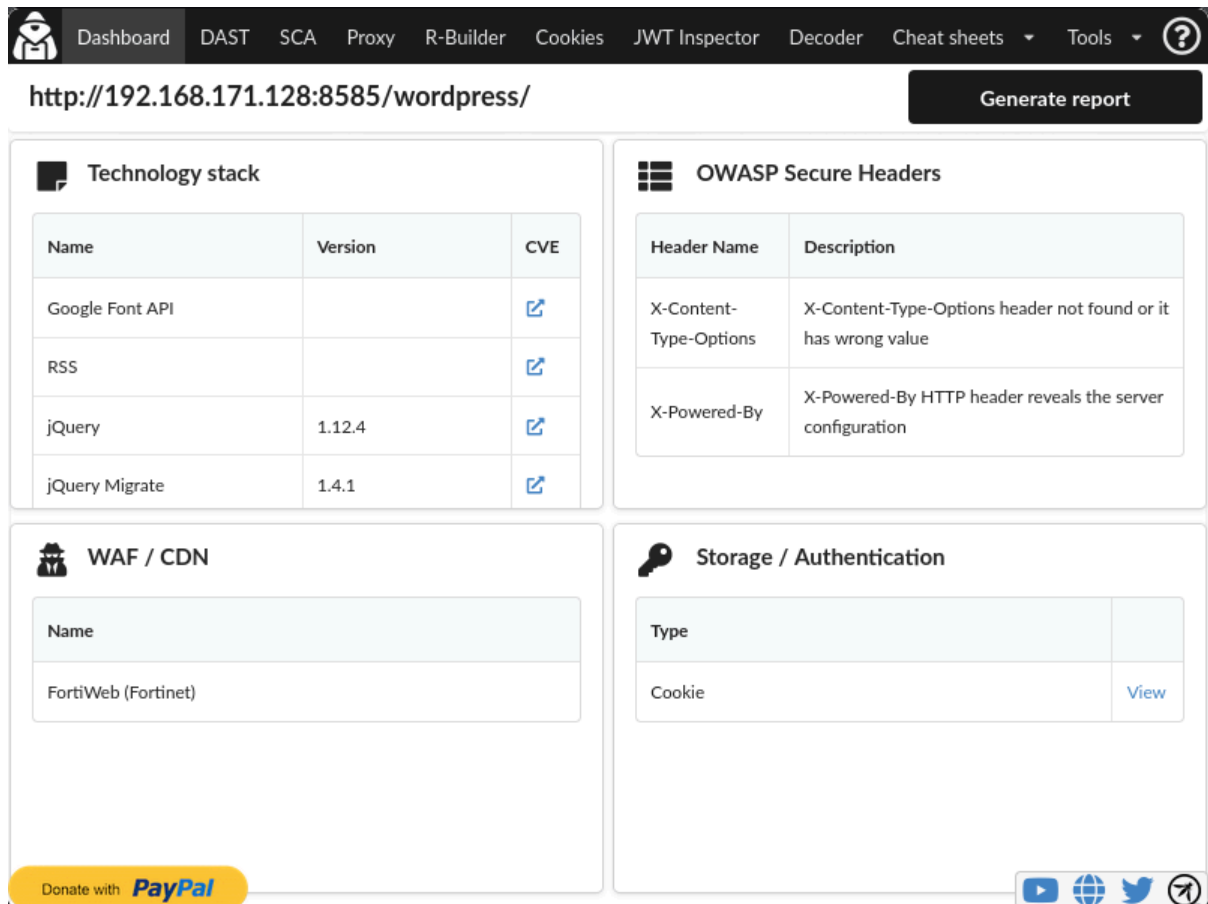
HackTools is a powerful all-in-one extension for pentesters that provides quick access to frequently used commands and payloads in security testing, such as **XSS**, **SQLi**, **LFI**, etc. In addition to useful commands for Linux, Windows, PowerShell, reverse shells, post-exploitation commands, and much more.



The screenshot shows the HackTools extension interface. On the left is a dark sidebar with various tool icons, including a hat icon at the top, and a 'SQL' button at the bottom. The main content area is titled 'SQL Injection' and contains a definition: 'SQL injection (SQLi) is an application security weakness that allows attackers to control an application's database letting them access or delete data, change an application's data-driven behavior, and do other undesirable things by tricking the application into sending unexpected SQL commands.' Below this, there's a section titled 'Number of column' with a link 'MySQL/MSSQL/PGSQL'. At the bottom, a text box contains the SQL payload: 'UNION SELECT NULL,NULL,NULL -- --' followed by a copy icon.

OWASP Penetration Testing Kit

The **OWASP Penetration Testing Kit** is an extension developed by the OWASP community to facilitate penetration testing directly from the browser. It is designed to offer a modular set of integrated tools such as **basic vulnerability scanning** (XSS, SQLi, LFI, etc.) directly from the interface, **identification of technologies** and **potential vulnerabilities**, **automatic injection of payloads** into detected parameters, logging and modification of requests (similar to Burp but lighter), and more.



The screenshot shows the OWASP Penetration Testing Kit interface. At the top is a navigation bar with links: Dashboard, DAST, SCA, Proxy, R-Builder, Cookies, JWT Inspector, Decoder, Cheat sheets, Tools, and a help icon. Below the navigation bar, the current URL is `http://192.168.171.128:8585/wordpress/` and there is a "Generate report" button. The main content area is divided into four panels:

- Technology stack**: A table listing detected technologies.
- OWASP Secure Headers**: A table listing security headers and their status.
- WAF / CDN**: A table listing Web Application Firewall or Content Delivery Network services.
- Storage / Authentication**: A table listing storage or authentication mechanisms.

At the bottom left, there is a "Donate with PayPal" button. At the bottom right, there are social media icons for YouTube, a globe, Twitter, and a share icon.

Name	Version	CVE
Google Font API		🔗
RSS		🔗
jQuery	1.12.4	🔗
jQuery Migrate	1.4.1	🔗

Header Name	Description
X-Content-Type-Options	X-Content-Type-Options header not found or it has wrong value
X-Powered-By	X-Powered-By HTTP header reveals the server configuration

Name
FortiWeb (Fortinet)

Type	
Cookie	View

Although it does not replace tools like Burp Suite or ZAP, it is a very useful option for quick analysis or environments where you cannot install heavy tools.