Cybersecurity Daily Dairy

Day 17: Website Auditing & Burp Suite in Windows

Date: July 6, 2025

Topics Covered:

- Burp Suite installation on Windows
- Website auditing concepts
- Search engine rules & SEO types
- Business logic and server-side vulnerabilities
- HTTPS, SSL/TLS, and data transfer methods
- Common hacking terms: bots, MITM, sniffing

Burp Suite Installation on Windows

Burp Suite is a widely used web vulnerability scanner and penetration testing tool for websites.
Downloaded from the PortSwigger website and installed the Community Edition or Professional Trial on Windows using the EXE installer.
Configured HTTP proxy to capture and modify traffic between browser and web servers.

Website Auditing Fundamentals

Website auditing includes:

- Crawling and analyzing site structure
- Finding broken links, insecure endpoints
- Identifying hidden files and folders (e.g., robots.txt)
- Testing forms, authentication, sessions
- robots.txt is a file used to instruct search engine bots on what to crawl or avoid.
- SERP (Search Engine Result Page) refers to the pages that a search engine displays in response to a user query.

SEO Types

Type	**Description**
On-Page SEO	Optimizing website content, titles, tags, speed
Off-Page SEO	Backlinking and external promotion
Local SEO	Optimizing for location-specific search (e.g., "restaurants near me")

Website Vulnerabilities

- Business Logic Vulnerabilities: Flaws in application behavior (e.g., price manipulation)
- Server-side Vulnerabilities: API flaws, logic errors
- Client-side Vulnerabilities: Cross-site scripting (XSS), DOM-based issues
- Request/Response manipulation through tools like Burp Suite

Secure Protocols

SSL (Secure Socket Layer) and TLS (Transport Layer Security) are used in HTTPS to encrypt data during transmission.

GET and POST Methods:

Method	**Purpose**	**Use for**
GET	Retrieve data	Normal parameters
POST	Submit data securely	Sensitive info

Popular Platforms & Bug Bounties

- PortSwigger – creator of Burp Suite
- BugCrowd, HackerOne – platforms for ethical hackers to find and report bugs

Other Cyber Terms

Term	**Description**
Bots	Infected systems used in attacks without user knowledge
MITM	Man-in-the-middle attack: intercepting communications
VOIP	Voice over IP – can be abused if unencrypted
ARP Poisoning	Redirecting LAN traffic by spoofing ARP table
Ettercap/Bettercap	Tools for MITM, sniffing, spoofing
Sniffing/Snooping	Intercepting network traffic to collect sensitive data
JDK (.jar)	Java Development Kit; .jar files are compiled Java programs used in applications

Key Learnings

- Website auditing helps detect security issues in structure and behavior
- Burp Suite is essential for web penetration testing
- Understanding SEO and search engine directives improves cyber recon
- Use SSL/TLS and secure code practices to defend against threats
- Awareness of cyber terms enhances understanding of network-level attacks