



Vulnerability Scan Report

 **Date & Time of Scan:**
Tuesday, June 17, 2025, 16:11:44

 **Target Scanned:**
demo.owasp-juice.shop (81.169.145.156)

 **Nmap Command Used:**

```
bash
CopyEdit
nmap -sV -sC --script vuln -oN juice_scan.txt demo.owasp-juice.shop
```

Open Ports and Services

Port	State	Service	Version
21	Open	FTP	ftpd.bin round-robin file server 3.4.0r16
25	Filtered	SMTP	--
80	Open	HTTP Proxy	F5 BIG-IP load balancer http proxy

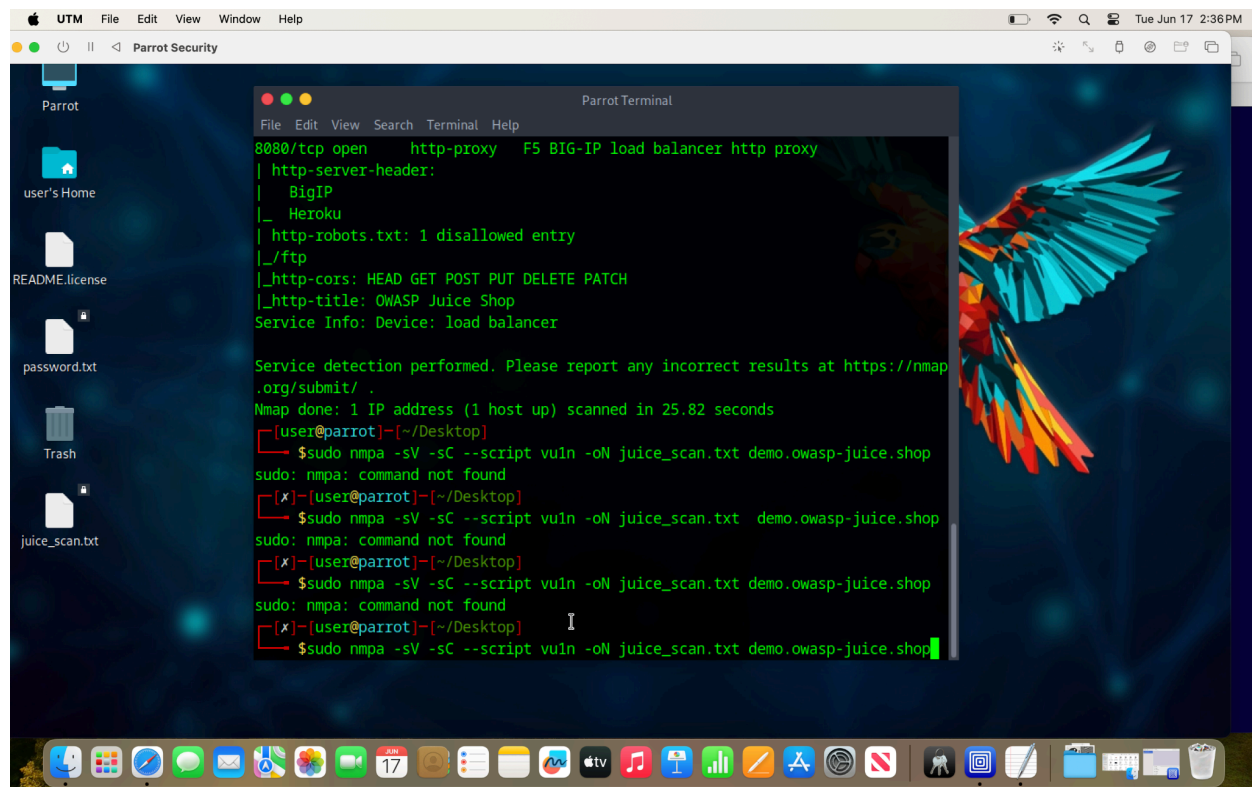
Vulnerabilities Detected

CVE ID	Description
CVE-2011-3192	Apache ByteRange Filter DoS: This vulnerability allows attackers to send overlapping byte range requests, consuming server resources and potentially crashing the Apache server. [17] Disclosure: 2011-08-19]
CVE-2009-750	Slowloris DoS: A tool that keeps many HTTP connections open to exhaust server resources by sending partial requests. [17] Disclosure: 2009-09-17]
CVE-2005-299	phpMyAdmin LFI: A file inclusion flaw in grab_globals.lib.php can allow attackers to read sensitive files like /etc/passwd by exploiting the subform parameter. [17] Disclosure: ~2005]

● **Note:** Several scripts like `http-vuln-cve2017-1001000` and `http-majordomo2-dir-traversal1` failed to execute, which may indicate issues or limitations during the scan.

Summary & Analysis

This scan on **OWASP Juice Shop**, a deliberately vulnerable web application for security testing, uncovered several significant issues. Most notably, **CVE-2011-3192** and **CVE-2007-6750** present serious **Denial-of-Service risks**, where an attacker could degrade or crash services by exhausting server resources. Additionally, the possible **Local File Inclusion (LFI)** vulnerability in **phpMyAdmin (CVE-2005-3299)** could allow attackers to read critical system files, posing a serious confidentiality risk. While this is a known intentionally vulnerable environment, these findings represent real-world risks often found in poorly secured web applications.



The screenshot displays a Parrot OS desktop environment. A terminal window titled "Parrot Terminal" is open, showing the output of an Nmap scan. The scan results indicate that the target is a load balancer with several open ports (80, 443, 8080, 8443, 9090, 9443) and various headers. The terminal also shows several failed attempts to run the command `sudo nmap -sV -sC --script vuln -oN juice_scan.txt demo.owasp-juice.shop` due to "command not found".

```
8080/tcp open  http-proxy  F5 BIG-IP load balancer http proxy
| http-server-header:
|   BigIP
|_  Heroku
| http-robots.txt: 1 disallowed entry
|_ /ftp
|_ http-cors: HEAD GET POST PUT DELETE PATCH
|_ http-title: OWASP Juice Shop
Service Info: Device: load balancer

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.82 seconds
[user@parrot]~/Desktop
$ sudo nmap -sV -sC --script vuln -oN juice_scan.txt demo.owasp-juice.shop
sudo: nmap: command not found
[x]-[user@parrot]~/Desktop
$ sudo nmap -sV -sC --script vuln -oN juice_scan.txt demo.owasp-juice.shop
sudo: nmap: command not found
[x]-[user@parrot]~/Desktop
$ sudo nmap -sV -sC --script vuln -oN juice_scan.txt demo.owasp-juice.shop
sudo: nmap: command not found
[x]-[user@parrot]~/Desktop
$ sudo nmap -sV -sC --script vuln -oN juice_scan.txt demo.owasp-juice.shop
```