****

**### Web Application 1: \*Your Wish is My Command Injection\***

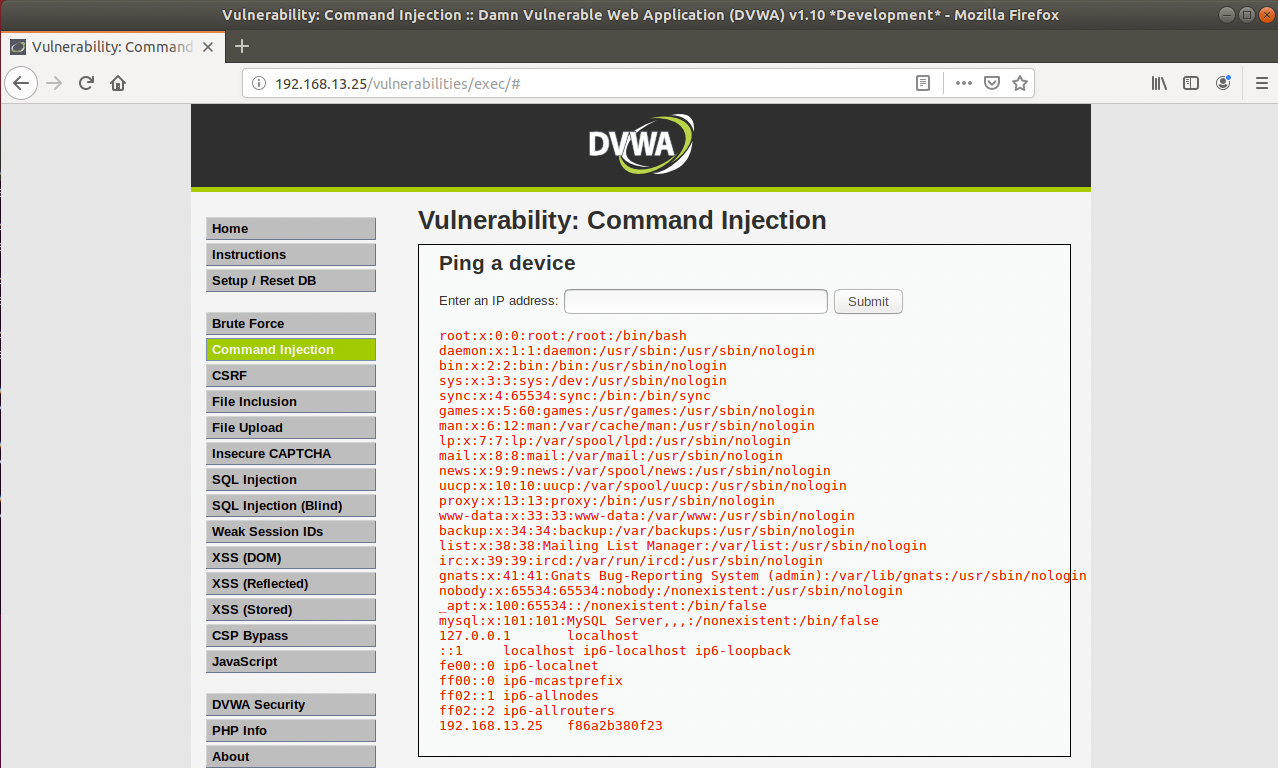
\*\*Deliverable\*\*: Take a screen shot confirming that this exploit was successfully executed and provide 2-3 sentences outlining mitigation strategies.

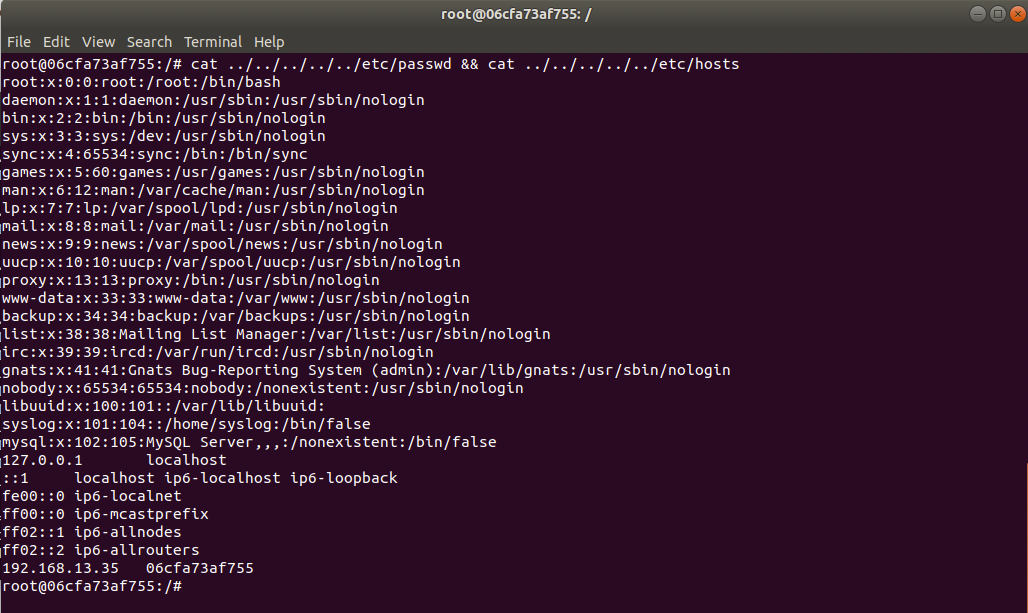
**Answer: -** Below are several recommended mitigation strategies for an operating system command injection attack.

* A Server-side validation to only allow numerical single values as inputs and parameterized database queries that restrict input from the user.
* Avoid system calls and user input to prevent threat actors from inserting characters into the operating system command.
* Set up input validation to prevent attacks like XSS and SQL Injection.
* Create a white list of possible inputs to ensure the system accepts only preapproved inputs.
* Use only secure APIs when executing system commands such as execFile()
* Use execFile() securely to prevent users from gaining control over the name of the program and also map user input to command arguments in a way that ensures user input does not pass as is into program execution.

**Command: - ; cat ../../../../../etc/passwd && cat ../../../../../etc/hosts**

Screenshots: -





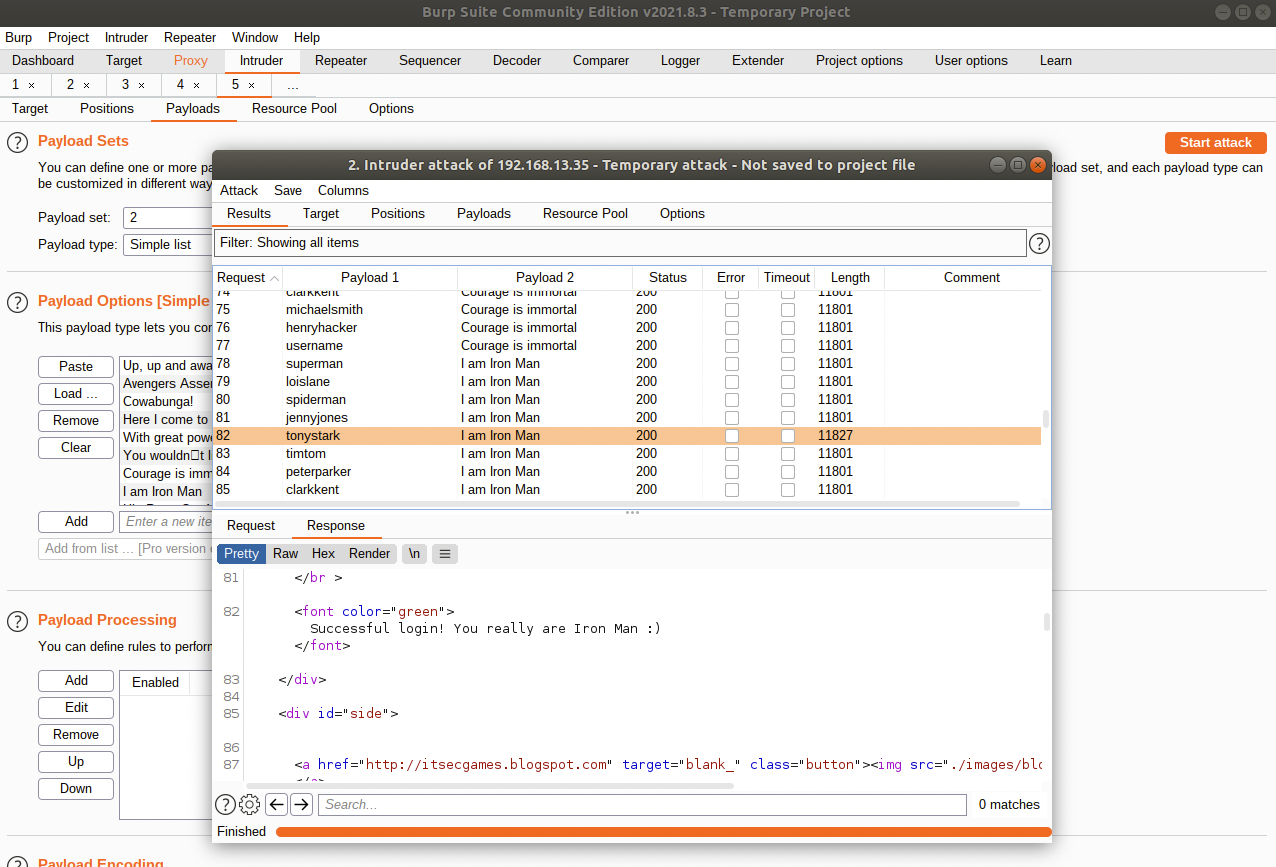
****

**### Web Application 2: \*A Brute Force to Be Reckoned With\***

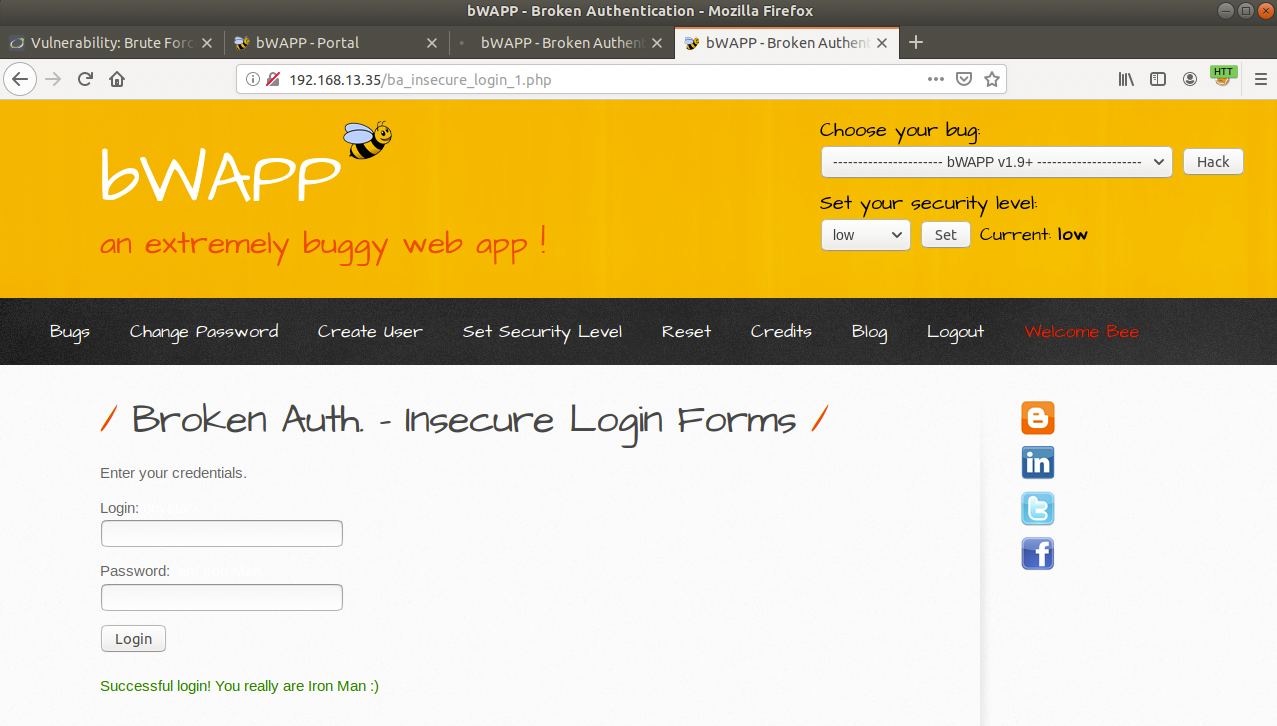
\*\*Deliverable\*\*: Take a screen shot confirming that this exploit was successfully executed and provide 2-3 sentences outlining mitigation strategies.

**Answer: -** Below are mitigation strategies for a Brute Force attack on compromised passwords.

* Setup complex usernames and passwords and regularly change your passwords.
* Using multi-factored authentication.
* Enabling a lockout after a certain amount of failed login attempts.
* Send an alert email to the user about new login from different IP address or failed login attempts or change password.
* Monitor your accounts, there are paid services that will monitor online identities, but you can also use free services like haveIbeenpwned.com to check whether your email address is connected to any recent leaks.
* Use a password manager.
* Run a virus scan, use a reputable antivirus software to scan computer on a regular basis and antivirus companies keep records of the most common malware keyloggers and will flag them as dangerous.
* Set up biometrics’ login to account, a malicious actor will find it very difficult to replicate fingerprint or facial shape, enabling biometric authentication turns password into only one of several points of trust that a hacker needs to overcome.



****



****

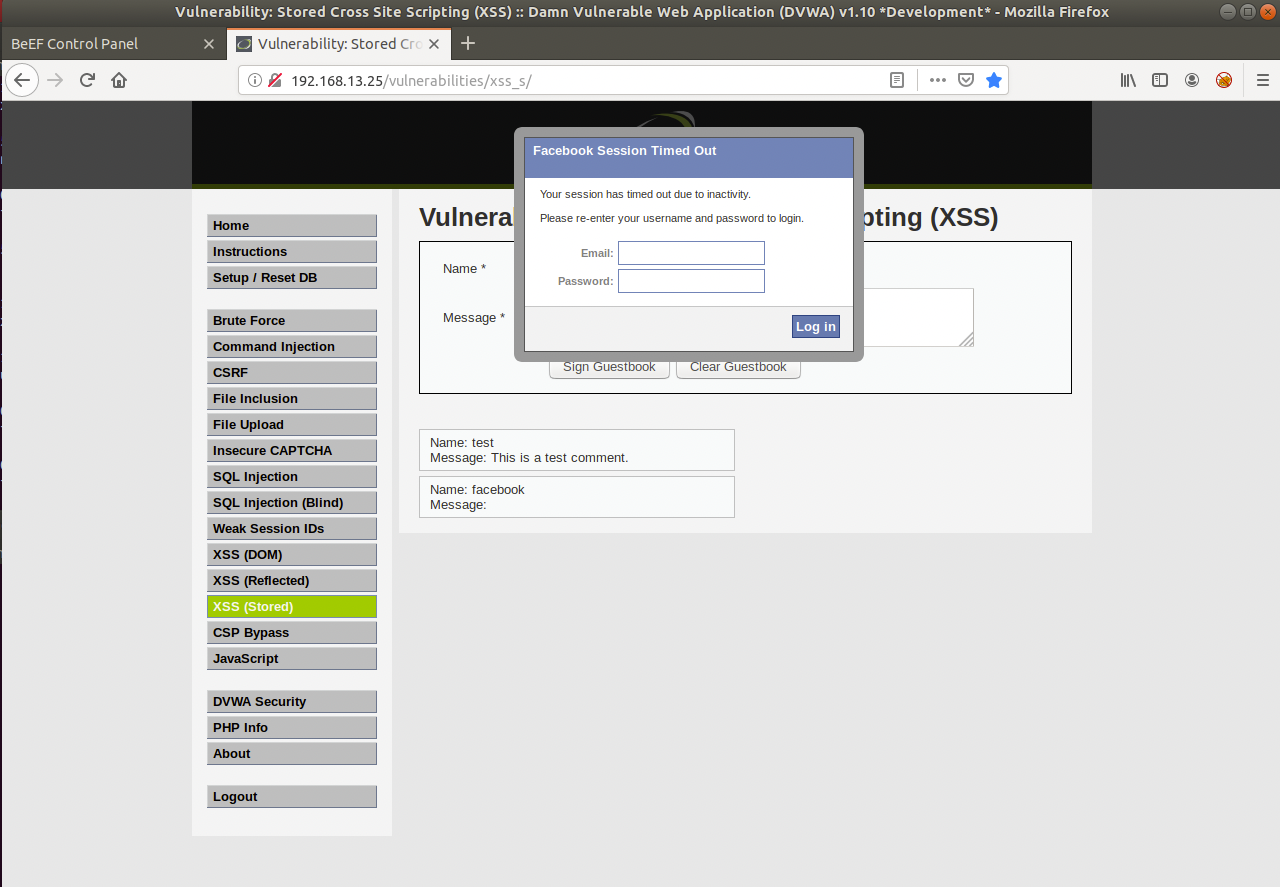
**### Web Application 3: \*Where's the BeEF?\***

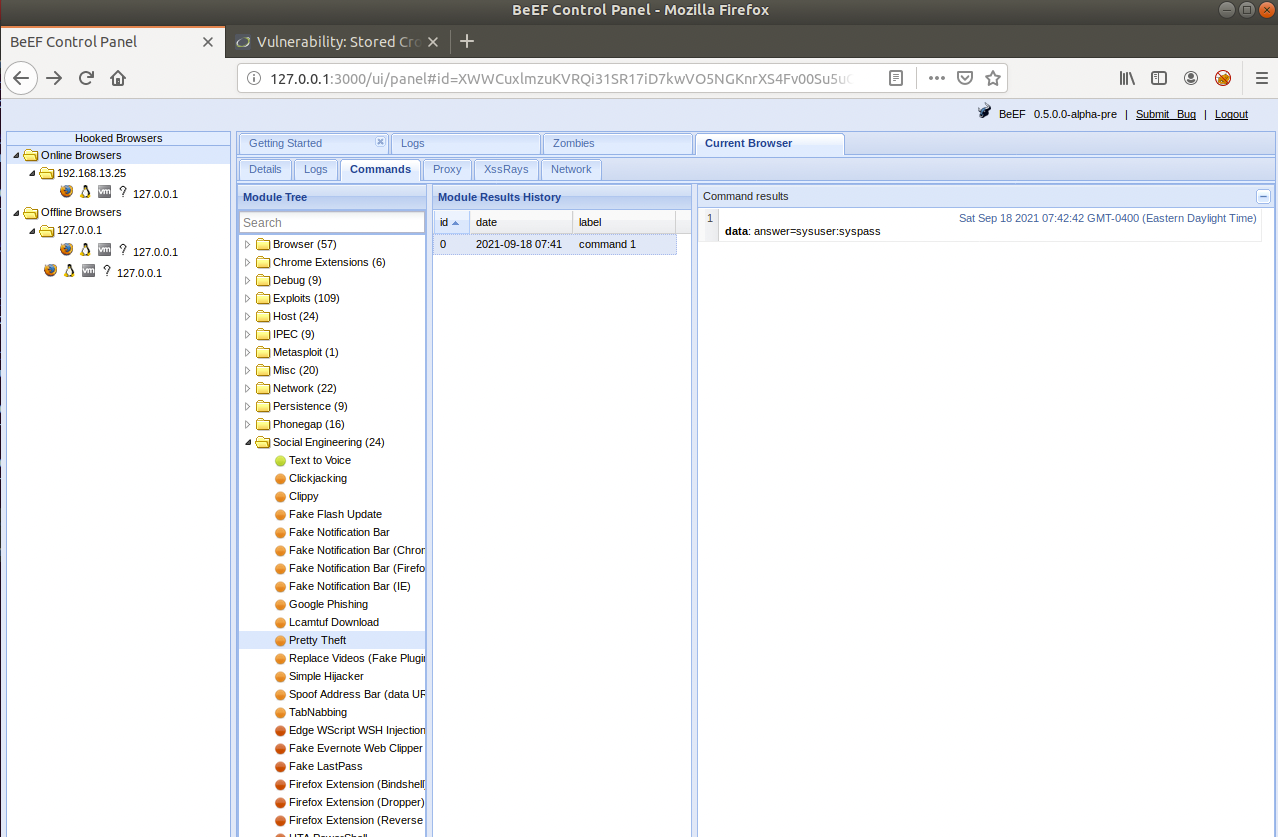
\*\*Deliverable\*\*: Take a screen shot confirming that this exploit was successfully executed and provide 2-3 sentences outlining mitigation strategies.

**Answer: -** Below are few mitigation strategies for xxx vulnerability.

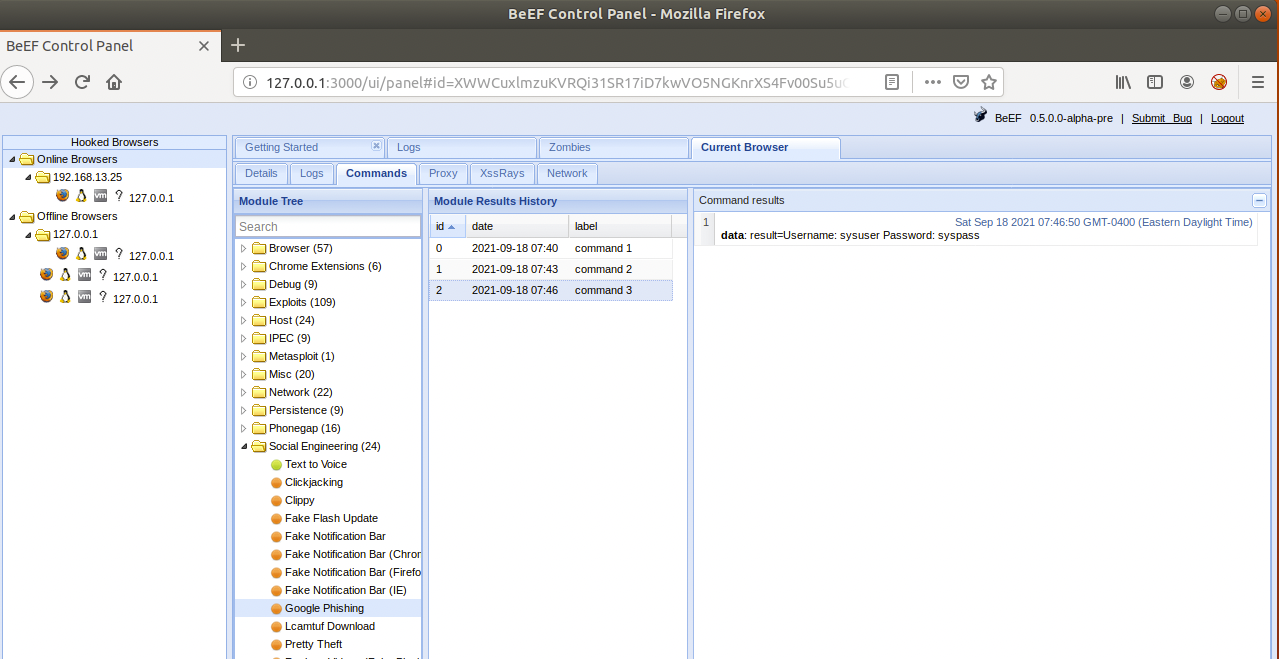
* xxs vulnerability could be mitigate in adding form validation, this would validate that the user is not trying to enter an xss script and include any other unintended responses.
* Prohibit HTML code in inputs and preventing users from posting HTML code into form inputs is a straightforward and effective measure.
* Validate inputs - If accepting form inputs validate the data to ensure it meets specific criteria will be helpful.
* Secure your cookies and set rules in web applications defining how cookies are handled can prevent xss and even block javascript from accessing cookies.
* Sanitize data in similar to validation, for example sanitizing occurs after data has been posted but before it is executed, always use trusted online tools like HTML sanitizer to sanitize code online for xss vulnerabilities.
* Use a web application firewall (WAF) and set rules can be created on a WAF to specifically address xxx by blocking abnormal server requests.

- Social Engineering >> Pretty Theft



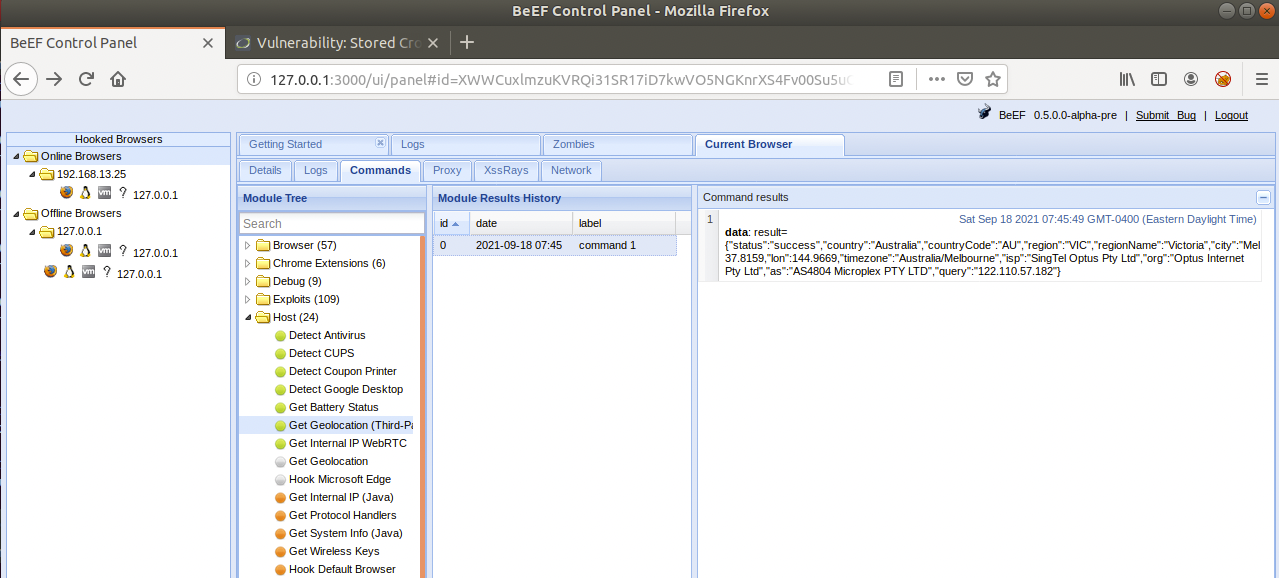


- Social Engineering >> Google Phishing

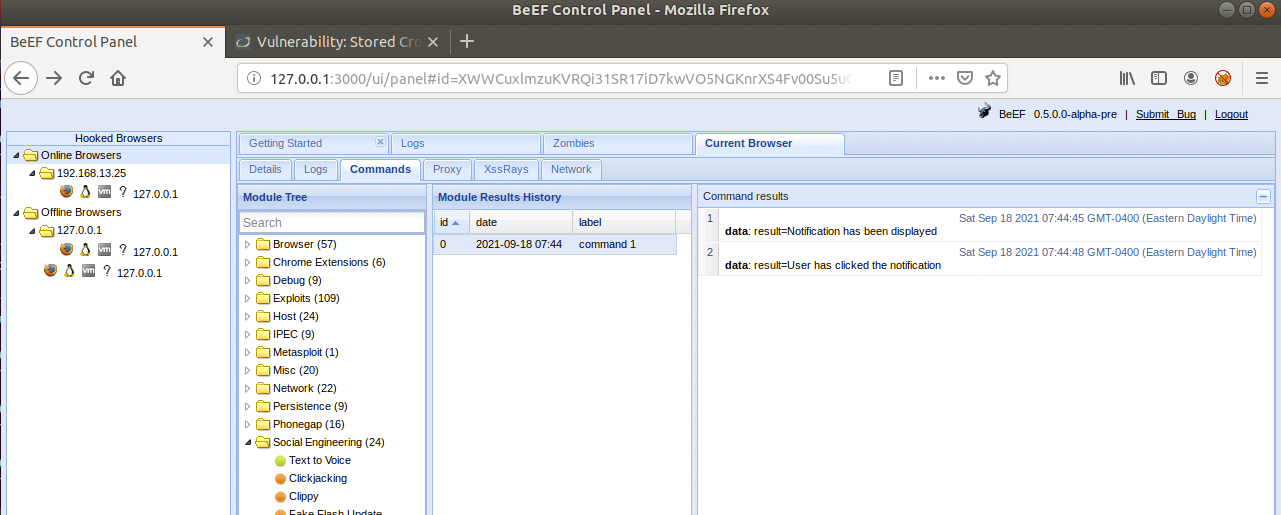


****

- Host >> Get Geolocation (Third Party)



- Social Engineering >> Fake Notification Bar



Thank you,

Aziz Somani