Student:	Email:
Truc Huynh	huyntl02@pfw.edu

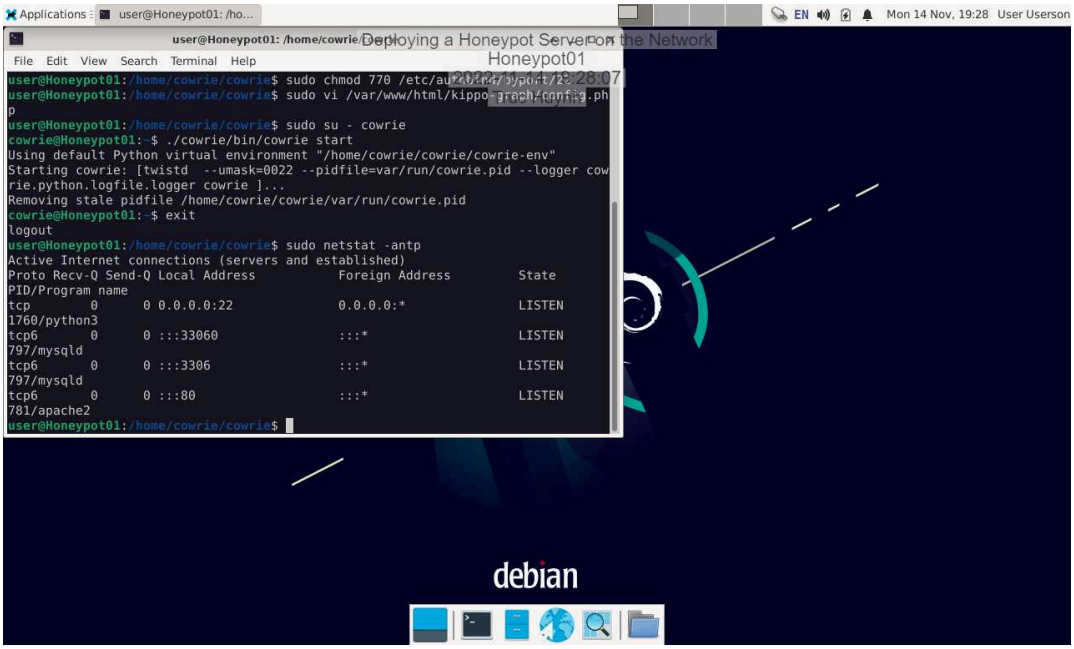
Time on Task:	Progress:
1 hour, 46 minutes	100%

Report Generated: Monday, November 14, 2022 at 8:46 PM

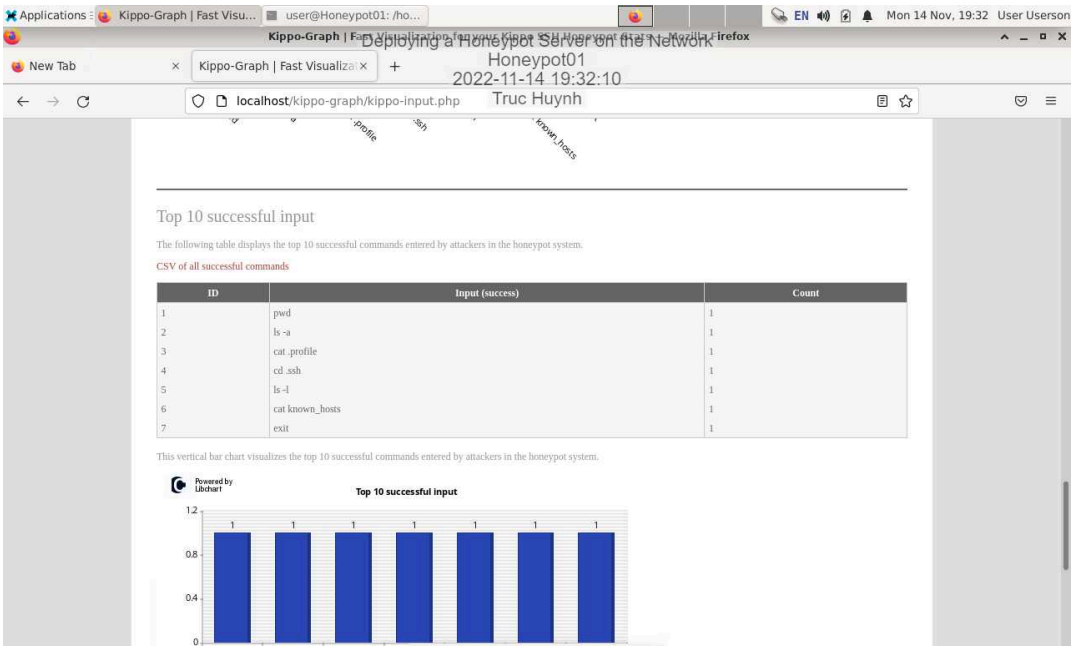
Hands-On Demonstration

Part 1: Configure an SSH Honeypot

37. **Make a screen capture** showing all three services listening on their default ports.

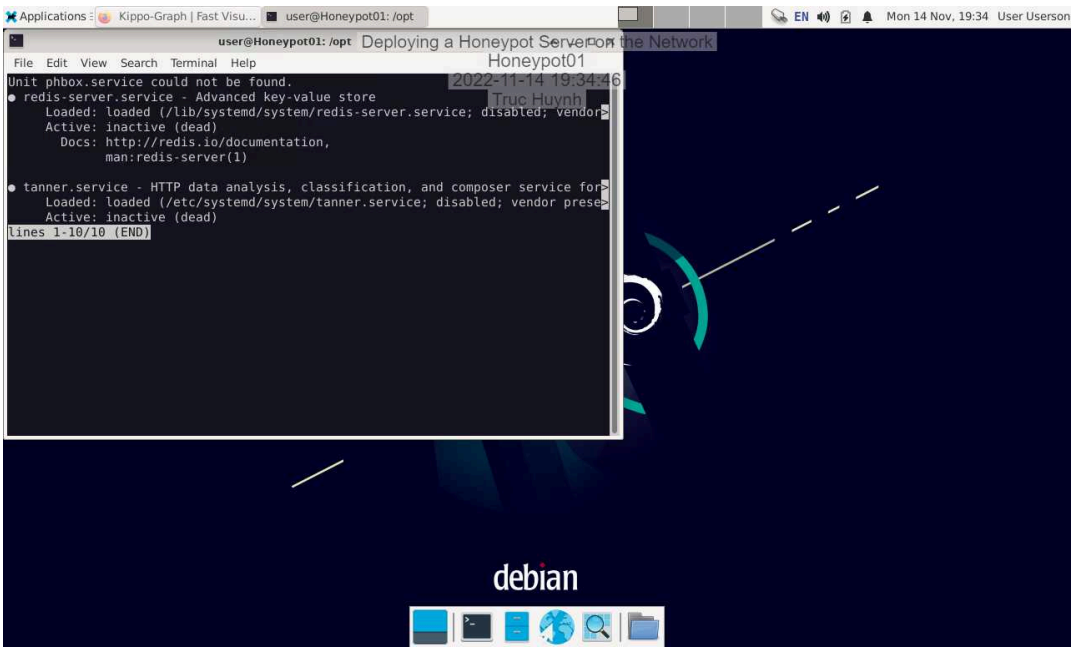


51. **Make a screen capture** showing the commands used per the accompanying table.

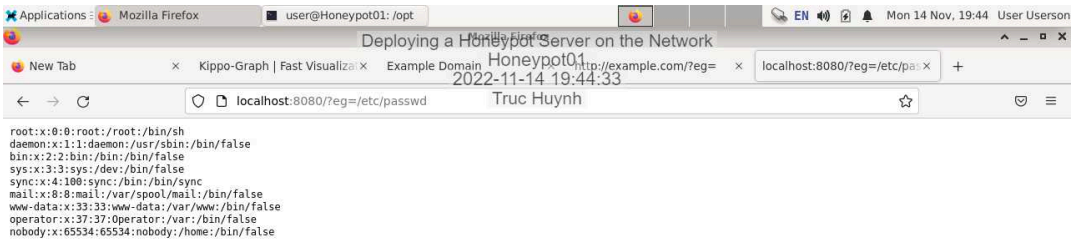


Part 2: Configure an HTTP Honeypot

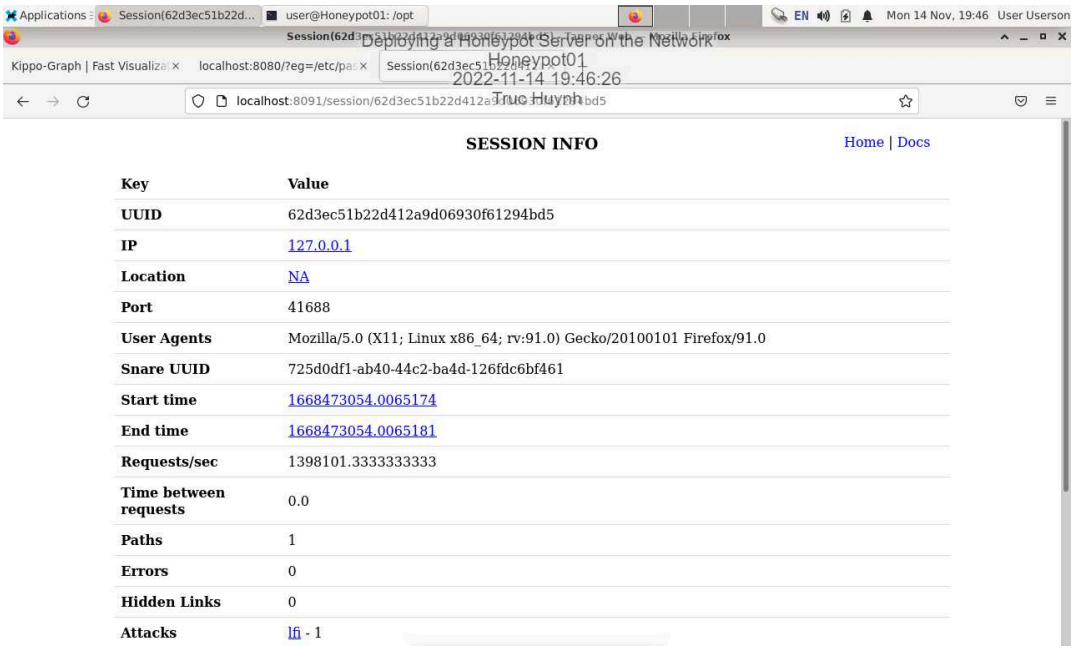
6. **Make a screen capture** showing the current status of the Tanner, PHP sandbox, and Redis services.



34. **Make a screen capture** showing output from the successful LFI attack.

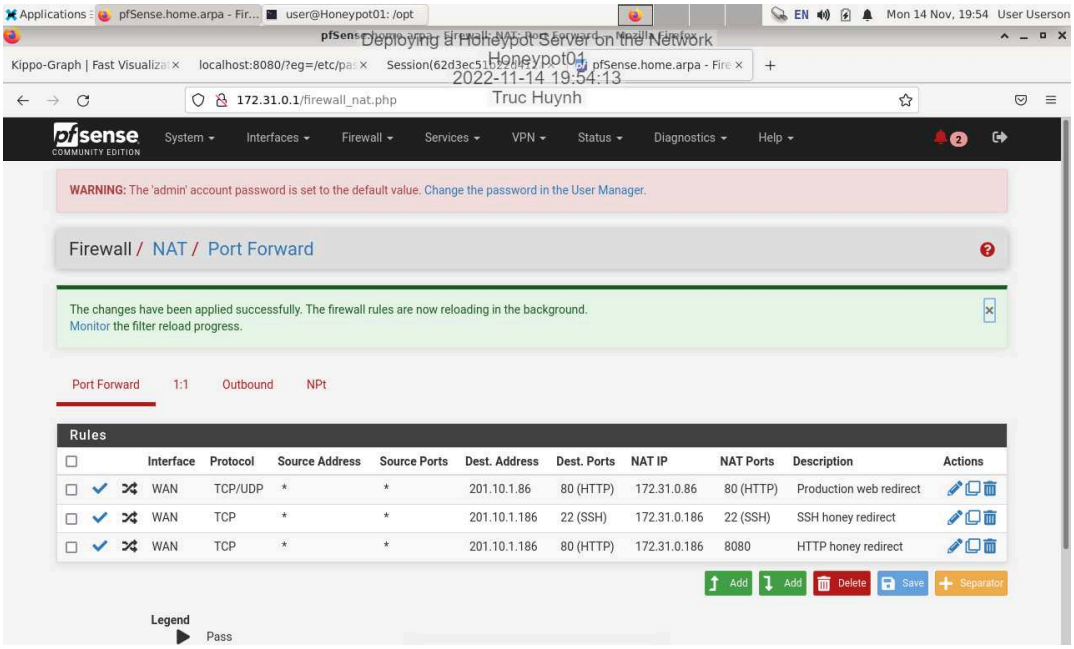


42. **Make a screen capture** showing your LFI payload threat actor session in Tannerweb.

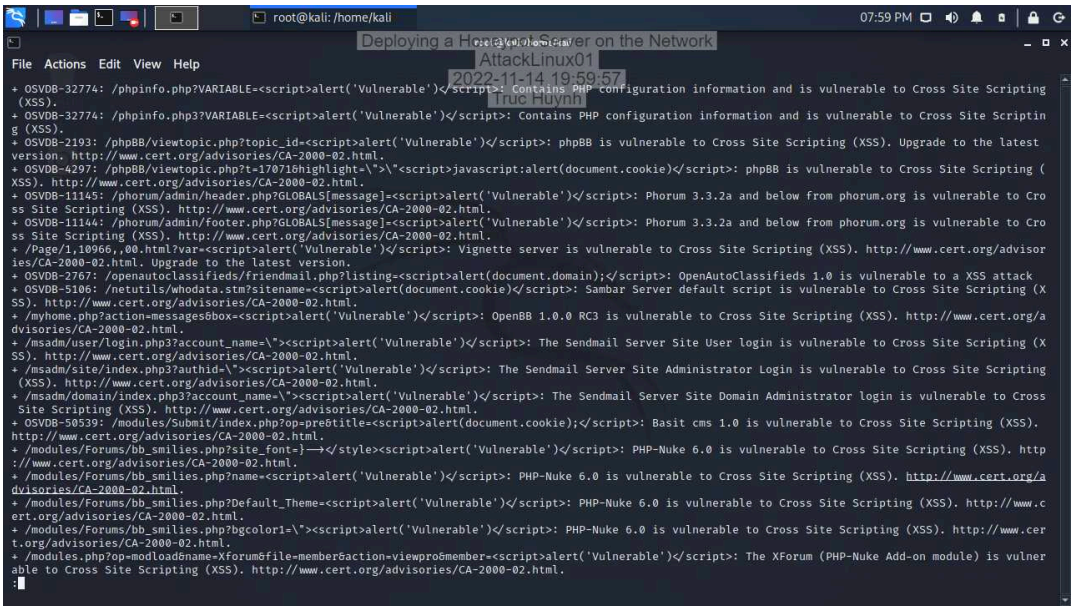


Part 3: Simulate Attacks and Evaluate Threat Intelligence

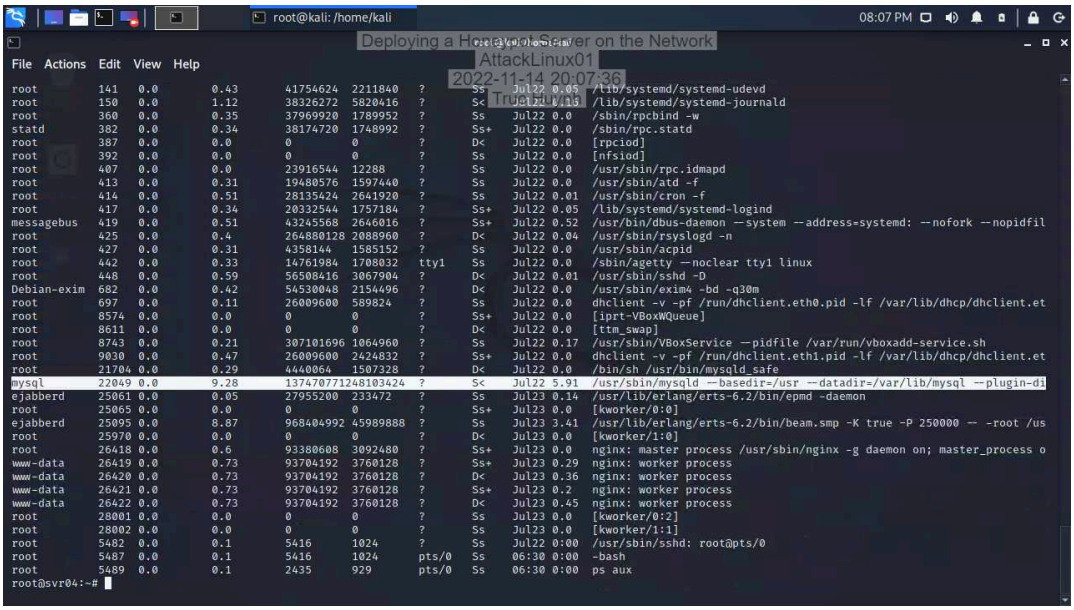
15. **Make a screen capture** showing the updated Firewall / NAT / Port Forward rules table and the feedback indicating their successful application.



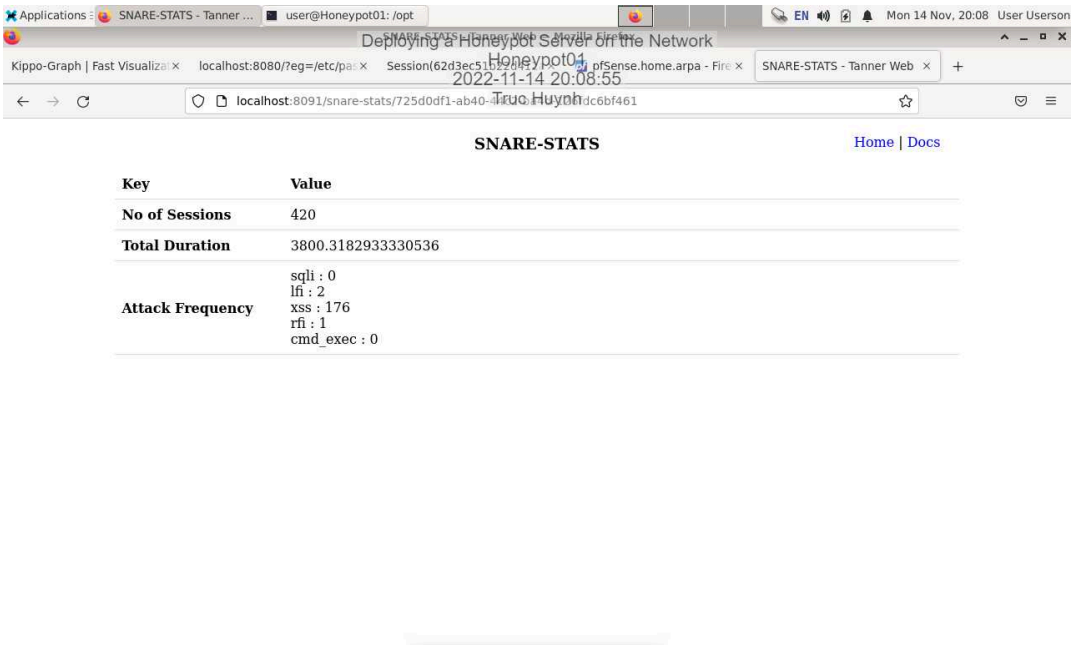
22. **Make a screen capture** showing the Server banner changed message in your Nikto output.



32. **Make a screen capture** showing MySQL, erlang, and NGINX processes in the output.



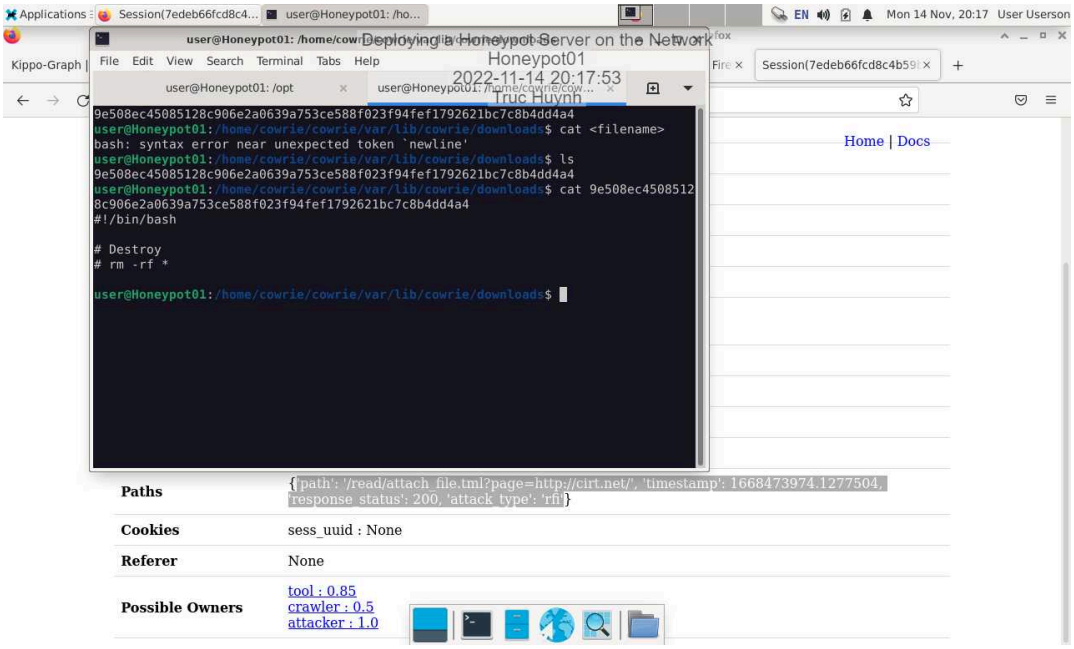
40. **Make a screen capture** showing the overall Snare-Stats.



46. **Record** the **website** the Red Team threat actor attempted to include in the path.

/read/attach_file.tml?page=http://cirt.net/

53. **Make a screen capture** showing the contents of the file that the Red Team member uploaded to the SSH honeypot.



58. **Record** the most popular username/password combination.

root/passwordroot/hackthegibson

root/secret

root/angel

root/love

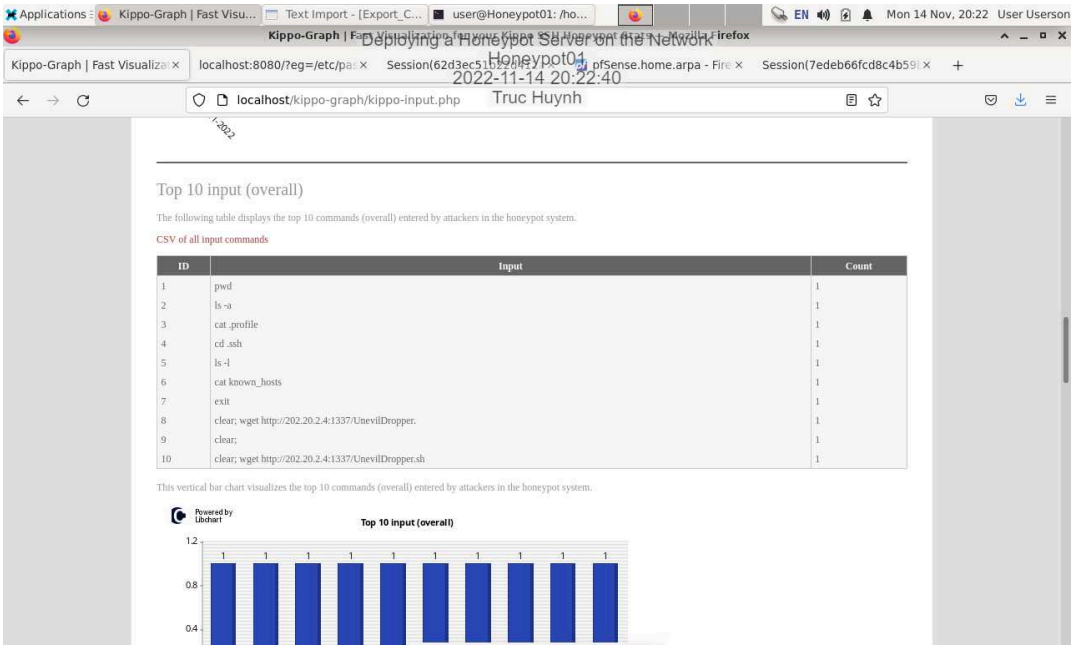
root/secrectsecretsecret
root/tigger

root/sunshine

root/chocolate

root/jennifer

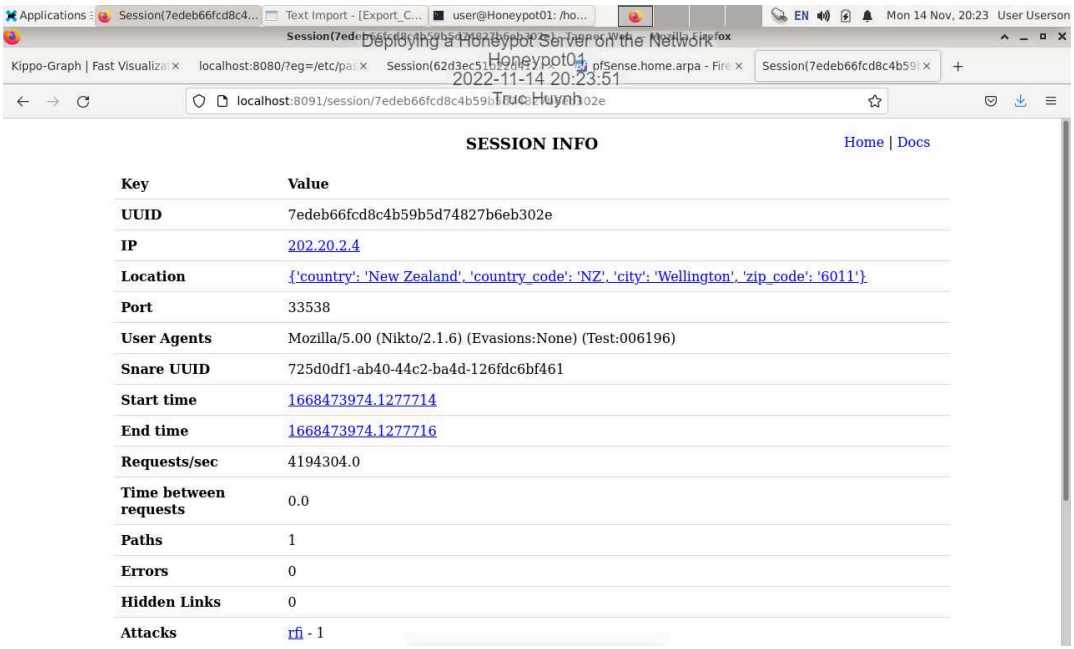
61. **Make a screen capture** showing the Top 10 successful input commands.



Challenge and Analysis

Part 1: Identify XSS Attacks in Tannerweb

Make a screen capture showing the details of one cross-site scripting event.



Part 2: Change SNARE's Web Server Header

Document the **additional option(s) and argument(s) used to change the SNARE Web Server Header to Apache.**

sudo snare -host-ip 0.0.0.0 -port 8080 -no-dorks true -auto-update false -page-dir example.com -tanner 127.0.0.1 -server-header apache

Make a screen capture showing that **the SNARE Web Server Header is set to Apache (using output from Nikto)**.