Mercury

Black Box Penetration Test

Performed by Shane Kell

July 15th – July 29th 2021

Text

Description automatically generated

Table of Contents

[Executive Summary: 3](#_Toc76491466)

[Summary of Results: 4](#_Toc76491467)

[Remediation Recommendations: 5](#_Toc76491468)

[Test Details: 6](#_Toc76491469)

[Scans: 11](#_Toc76491470)

# Executive Summary:

A contract was opened with ABC Corp to conduct a black box security analysis of the Mercury server located at IP address 10.0.0.55 from within the server’s network. This engagement included identification of vulnerabilities, documentation of any credentials discovered, demonstration of remote access, and elevation of privileges. Remediation recommendations are being provided to help harden the security posture of the Mercury server.

This analysis was conducted in a manner that simulated a malicious actor engaged in a targeted attack on the server, with the goals of:

* Identifying if a remote attacker could penetrate the defenses of the Mercury server
* Determining the impact of a security breach on:
  + Confidentiality and Integrity of private data stored on the server
  + Availability of services on Mercury

The testing window was two weeks, starting on July 15th, 2021 and ending on July 29th . This report being due on the final day of the engagement window.

# Summary of Results:

The initial foothold on the server came from an Structured Query Language Injection (SQLI) that was found because the debug mode was enabled for the Django based server, allowing for significant information leakage of system data, leading to the formation of a UNION SELECT query that dumped the usernames and passwords from the user table of the underlying SQL database.

The next target of the test was the SSH server. Using the credentials that were obtained, access was granted because of username and password reuse with the ‘webmaster’ account. The username ‘linuxmaster’ was saved in a file in the home folder, along with a base64 encoded password.

After moving laterally into the ‘linuxmaster’ account, check\_syslog.sh was identified as running with root permissions with ‘sudo -l’ and was using the ‘tail’ command without using the full path to the installed binary. A binary was created with the same name to set the uid to 0, and create a bash shell. The /tmp path was added to the $PATH variable ahead of the path to the correct tail binary, and sudo –preserve-env=PATH was used to preserve the environment variable. This caused the bash shell that was created to inherit elevated privileges, allowing root shell access.

# Remediation Recommendations:

Debug Mode: It is advised to either set Debug = false to have the server return a 404 error when a resource isn’t found. The information that is returned when it’s set to true is very useful to an attacker.

Sanitize Inputs to Queries: All input from users should be sanitized for malicious queries.

Password Reuse: Passwords being reused between accounts is not advised. Once compromised, an attacker will use the credentials to access as many resources as possible to expand their access and maintain persistence.

Implicit Binary Path: The script ‘/usr/bin/check\_syslog.sh’ is run as root and runs the ‘tail’ command on syslog. Including the full path to the binary (/usr/bin/tail) would prevent an attacker from replacing the binary used with one of their own, which then allows them to run their own commands with elevated privileges.

Banners: Any banners should be prevented from being displayed, i.g. ‘WSGIServer/0.2 CPython/3.8.2’. This provides an attacker information that they can then use to research known exploits.

# Test Details:

An Nmap scan was run with the following command:

**nmap -Pn -A -p- 10.0.0.55**

Two ports were found to be open, detailed as:

Port 22: OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)

Port 8080: http-proxy WSGIServer/0.2 CPython/3.8.2

Navigating to the page hosted on port 8080 showed the following page:

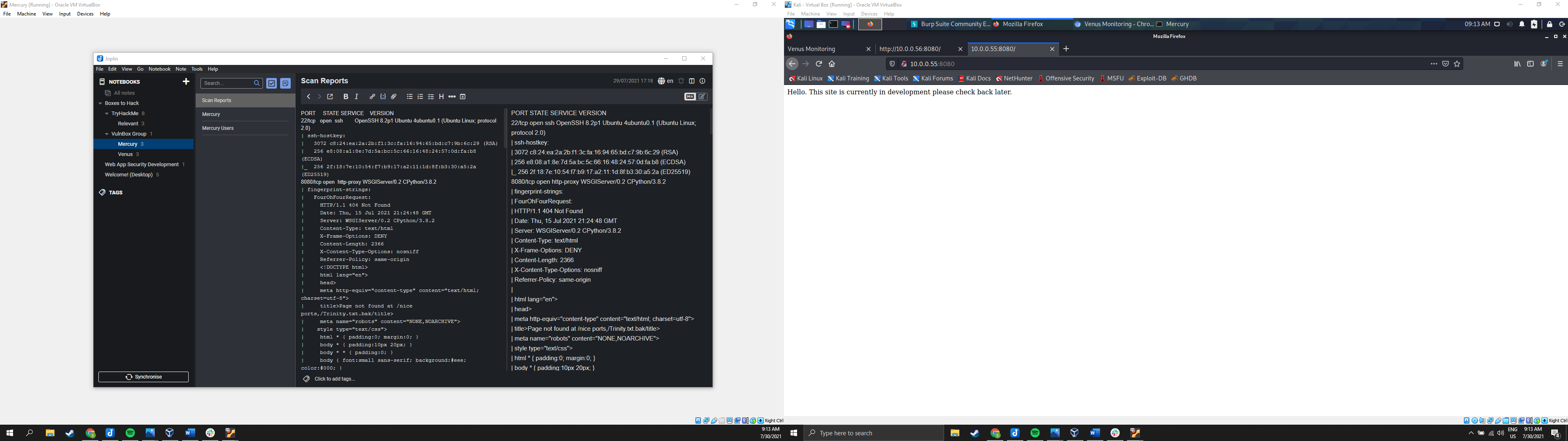


Figure 1: Message displayed for page at 10.0.0.55:8080

Viewing the page source did not reveal anything interesting.

A Nikto scan was run with the following command.

**Nikto -host http://10.0.0.55:8080**

This revealed that a directory titled ‘/SilverStream’ allowed for directory listing. Navigating to http://10.0.0.55:8080/SilverStream produced a detailed error, revealing that debugging mode was enabled for the web server.

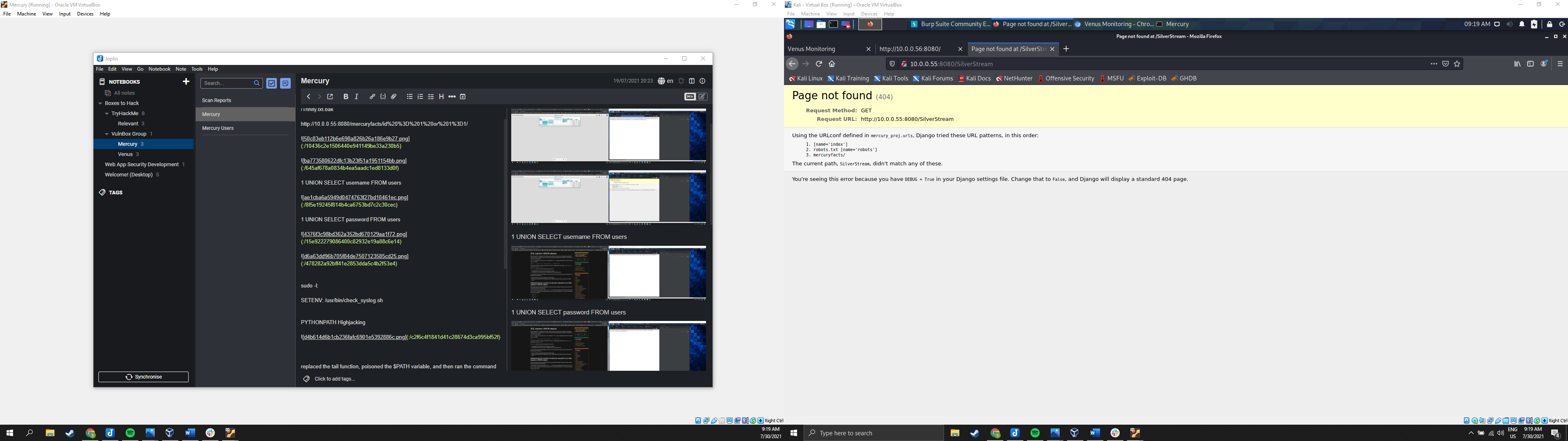


Figure 2: Detailed error screen instead of 404 not found error

The information dump revealed the mercuryfacts/ directory. Here is a screenshot of that page, the ‘todo’ list, and the ‘Load a fact’ page:



Figure 3: /mercuryfacts/ web page

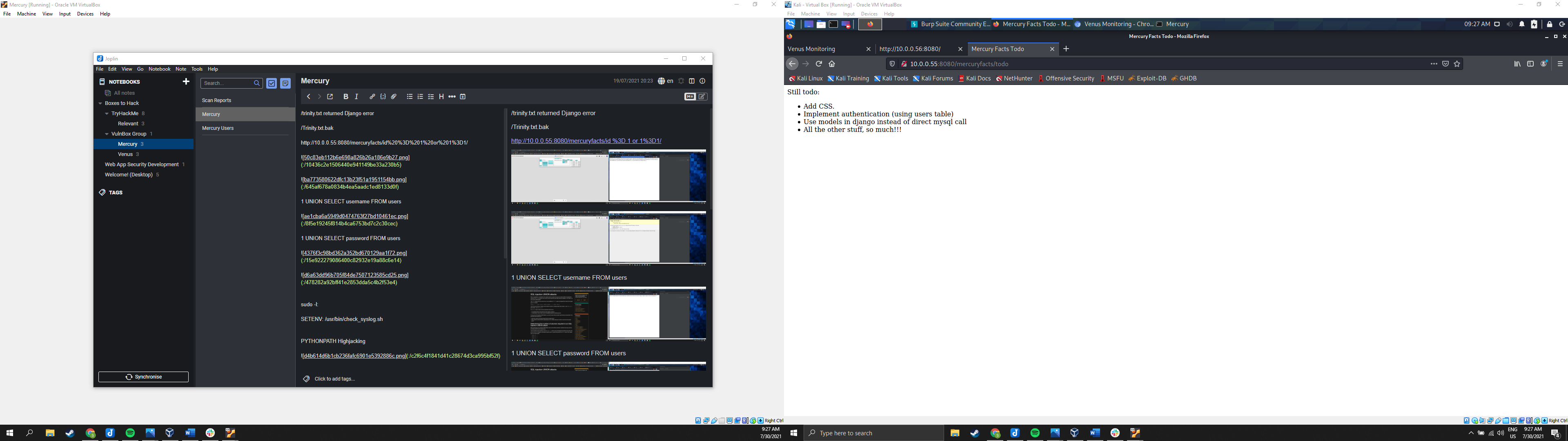


Figure 4: ToDo list, giving information on the users table, and using direct MySQL calls

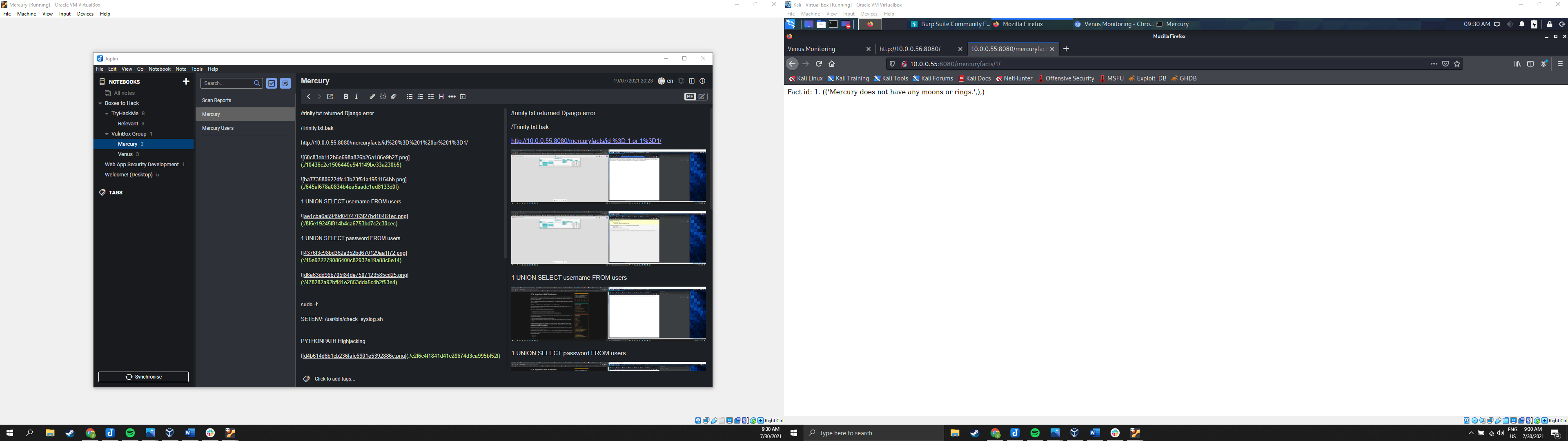


Figure 5: 'Load a fact' page

Note the ‘1’ in the URL. Changing this number, it was possible to navigate through the list of facts. At page ‘9’, a page was returned with no fact listed. Changing this value to ‘user’ generated an SQL WHERE clause error.

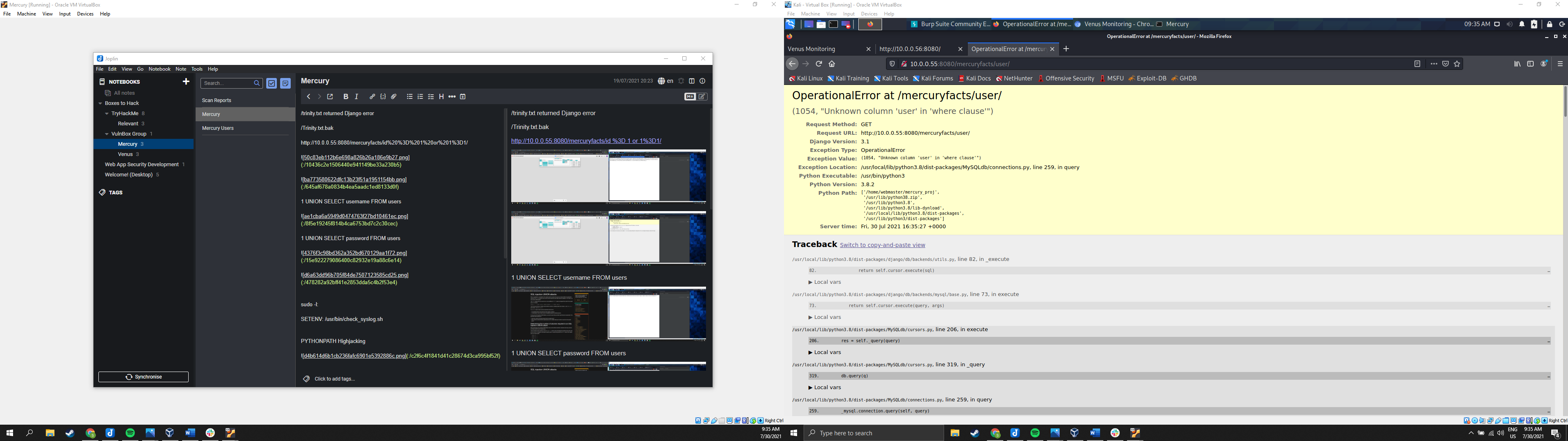


Figure : SQL WHERE clause error generated with /mercuryfacts/user URL

Changing the URL to /mercuryfacts/id = 1 OR 1=1 dumped all of the facts at once.

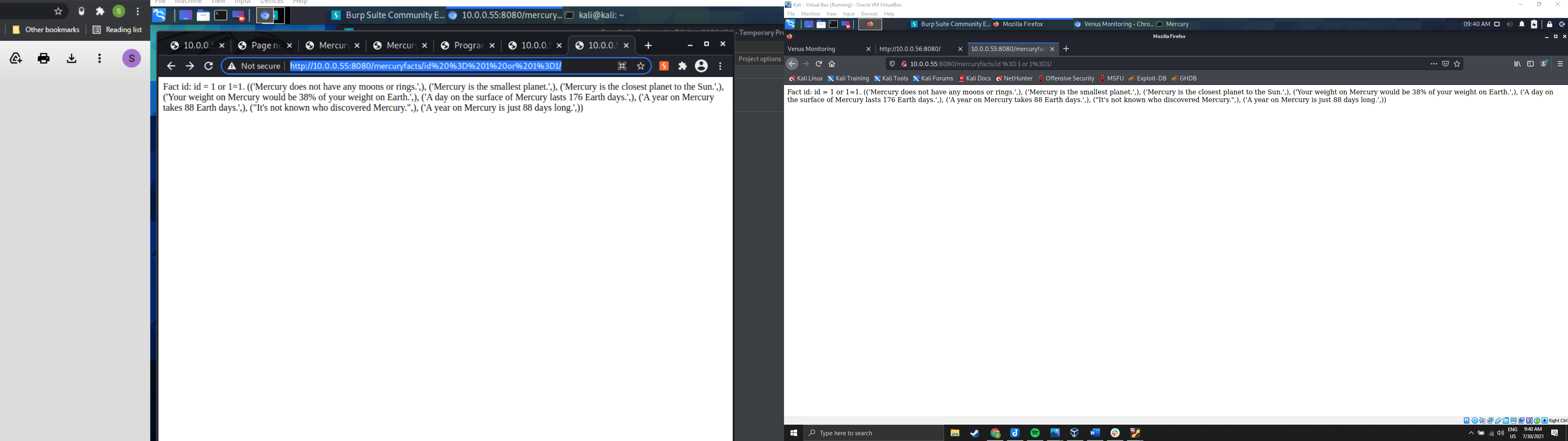


Figure : Facts dumped at once using /mercuryfacts/id =1 OR 1=1

Using a UNION SELECT statement it was possible to dump the users and passwords in two separate queries.

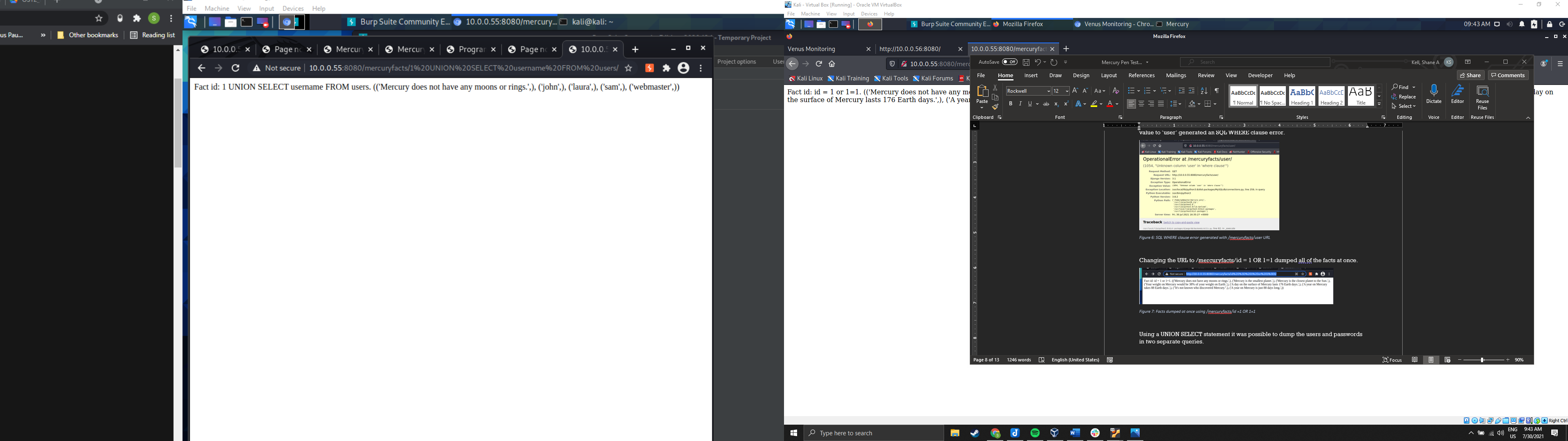


Figure : Result from ‘/mercuryfacts/1 UNION SELECT username FROM users’

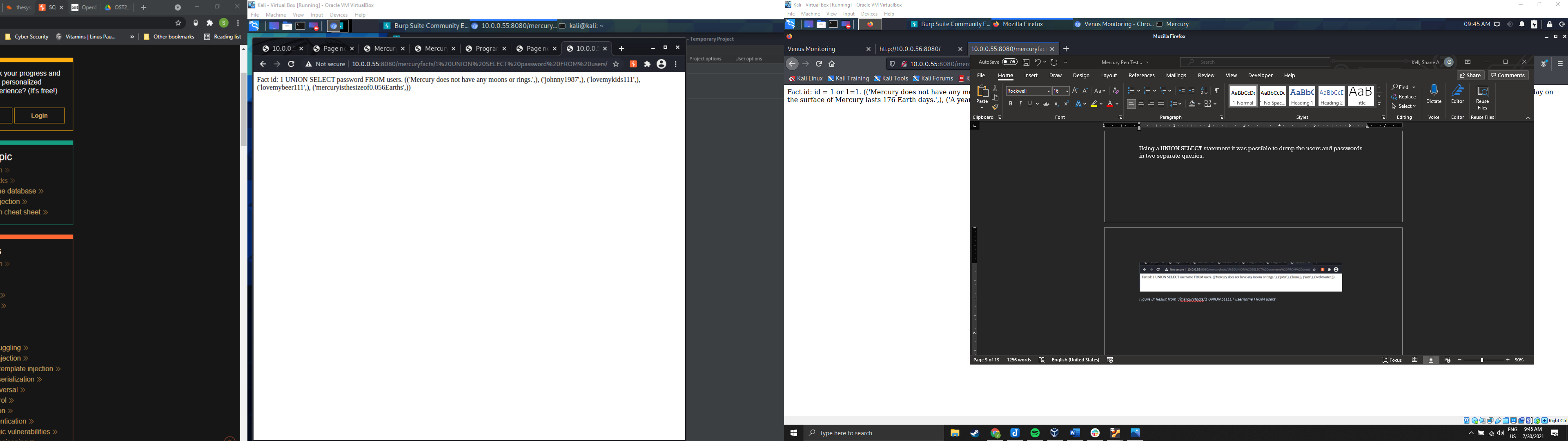


Figure : Result from '/mercuryfacts/1 UNION SELECT password FROM users'

Using the username and password combination webmaster:mercuryisthesizeof0.056Earths it was possible to login into the SSH port of the server.

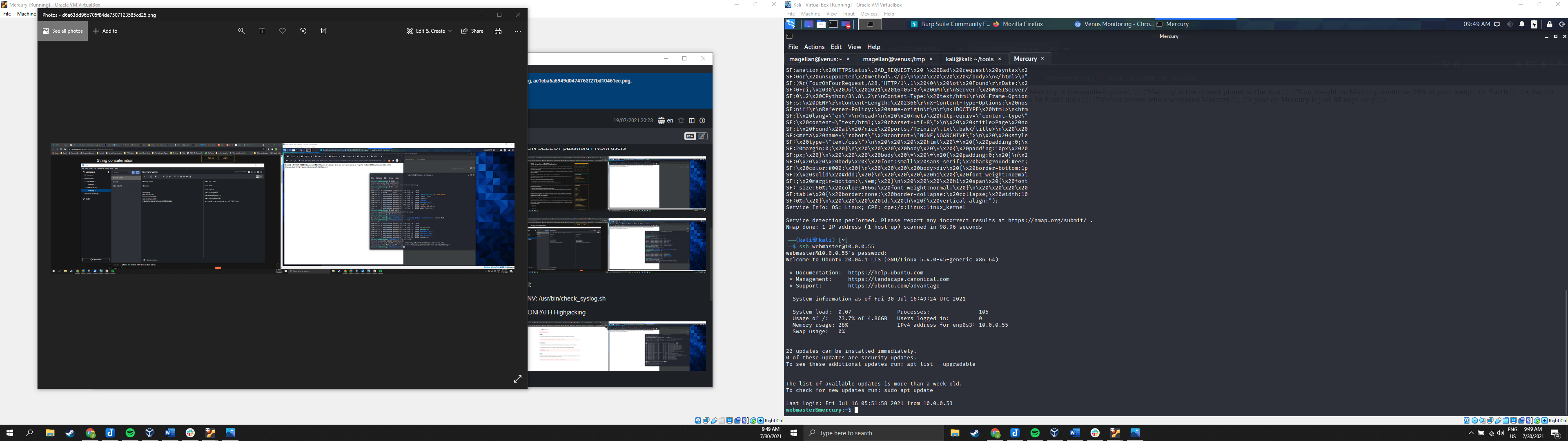


Figure : SSH access obtained with webmaster credentials recovered from SQLI query

Searching through the ~/mercury\_proj/ directory, the username linuxmaster and their base64 encoded password was saved in a text file titled ‘notes.txt’. This was used to move laterally into the linuxmaster user account.

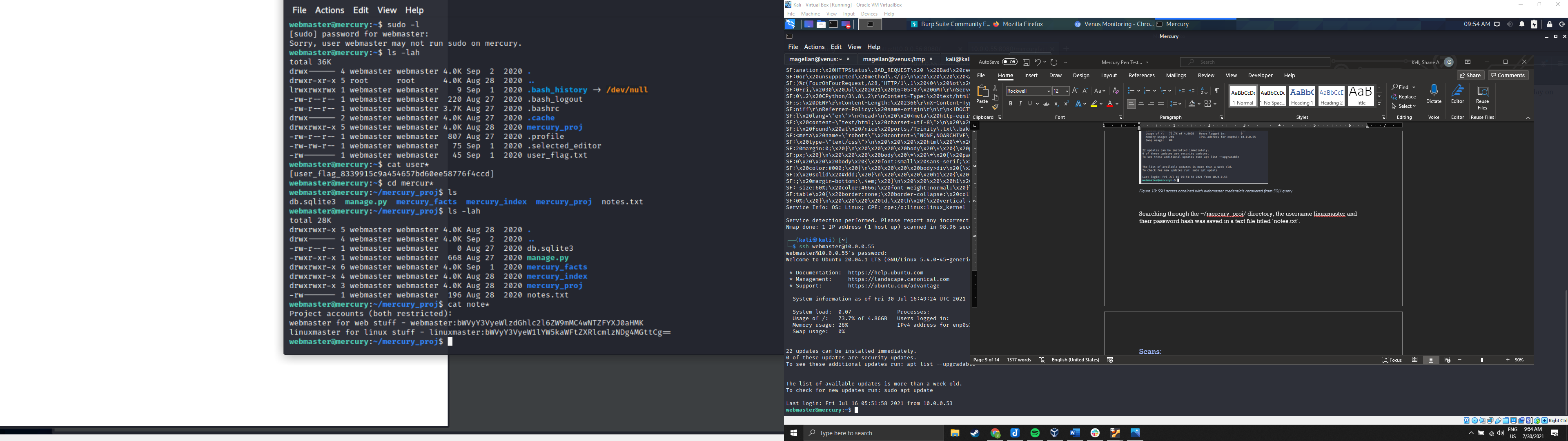


Figure : linuxmaster password decoded is 'mercurymeandiameteris4880km'

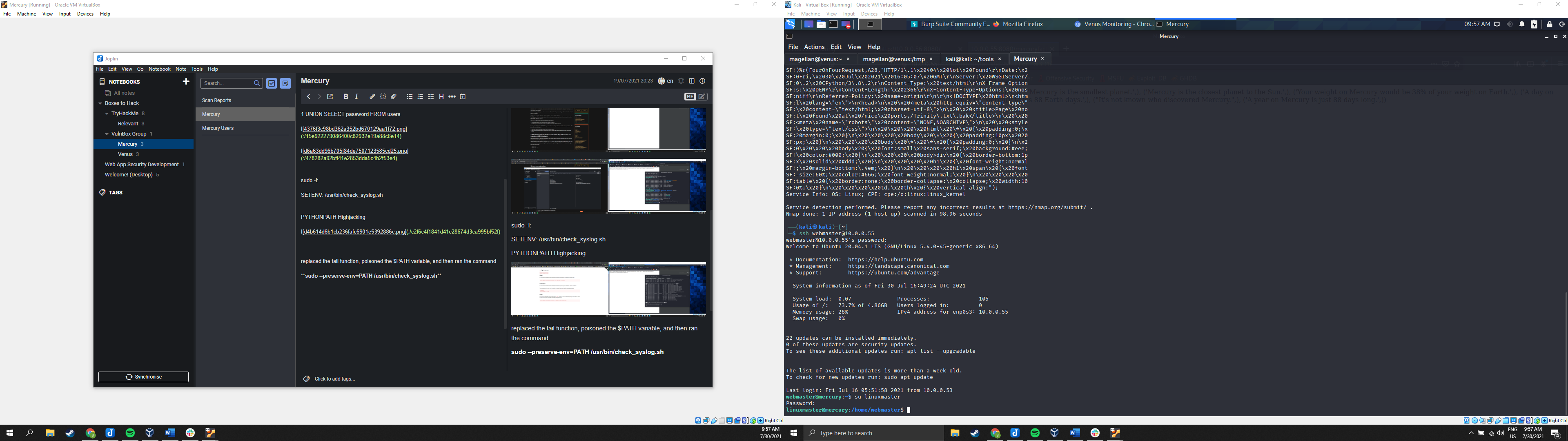


Figure : Lateral move into the linuxmaster user account

When the ‘sudo -l’ command was executed, this is what was reported.

**User linuxmaster may run the following commands on mercury:**

**(root : root) SETENV: /usr/bin/check\_syslog.sh**

When the contents of /usr/bin/check\_syslog.sh was output to the screen, it was found that a call to tail was used with the implicit path from the $PATH variable being used in a script that was being run as root.

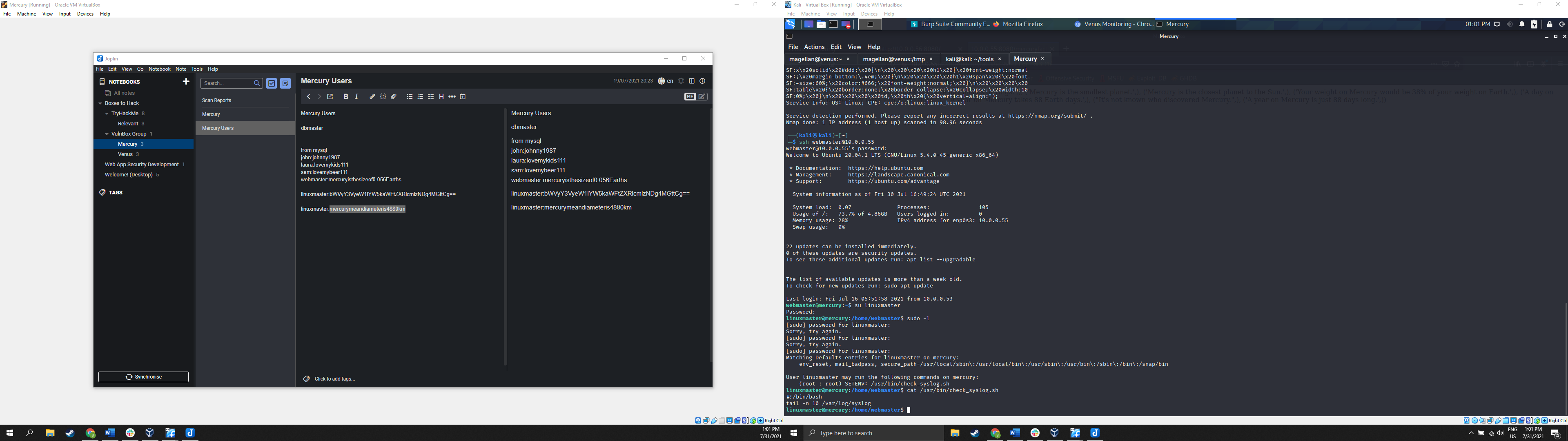


Figure 13: Output from sudo -l and displaying contents of check\_syslog.sh

A binary in C was written called ‘tail’ that set the uid to root and called a bash shell, and /tmp was added to the head of the $PATH variable. Then, check\_syslog.sh was executed with the following command to preserve the PATH variable and elevate the shell to root privileges.

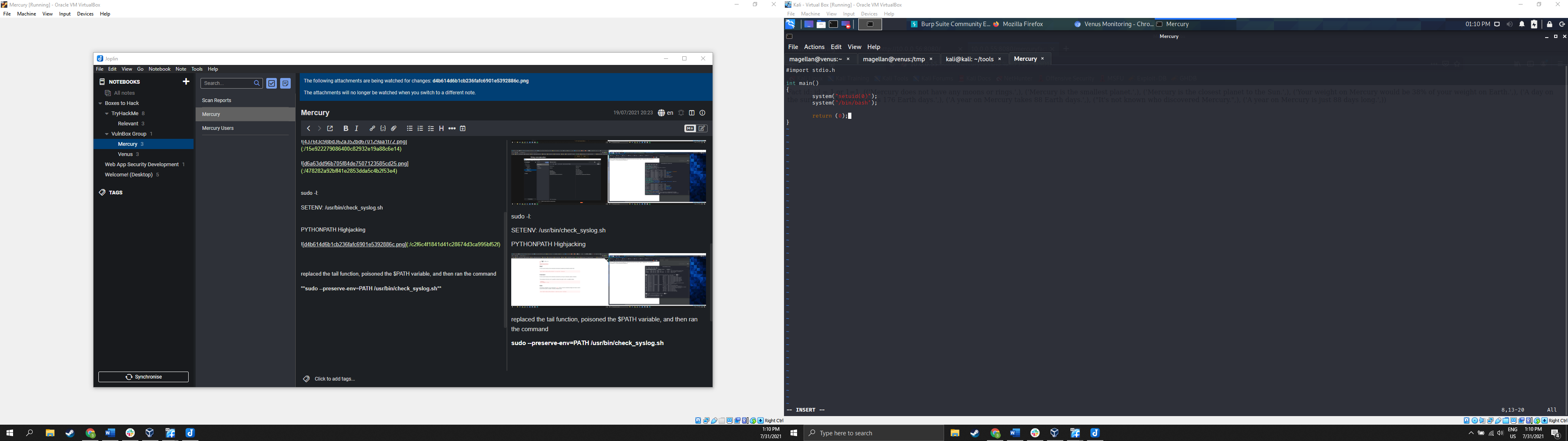


Figure : Contents of duplicate tail binary

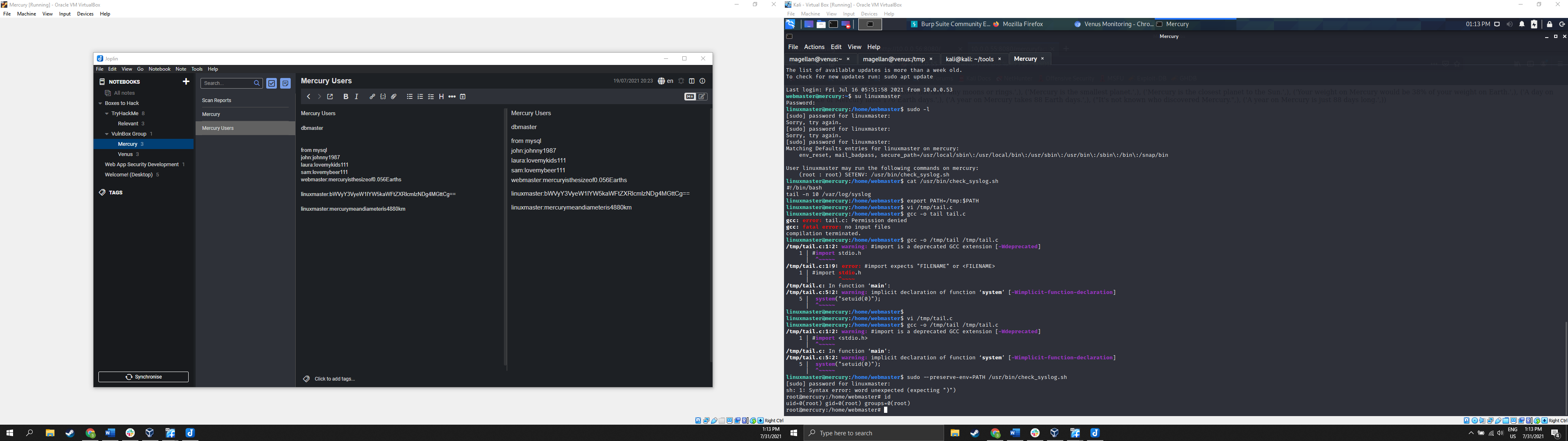


Figure Executing the shell after duplicating the tail binary and preserving the $PATH variable.

# Scans:

**NMAP:**

nmap -Pn -A -p- 10.0.0.55

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.

Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-30 09:04 PDT

mass\_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers

Nmap scan report for 10.0.0.55

Host is up (0.00041s latency).

Not shown: 65533 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 3072 c8:24:ea:2a:2b:f1:3c:fa:16:94:65:bd:c7:9b:6c:29 (RSA)

| 256 e8:08:a1:8e:7d:5a:bc:5c:66:16:48:24:57:0d:fa:b8 (ECDSA)

|\_ 256 2f:18:7e:10:54:f7:b9:17:a2:11:1d:8f:b3:30:a5:2a (ED25519)

8080/tcp open http-proxy WSGIServer/0.2 CPython/3.8.2

| fingerprint-strings:

| FourOhFourRequest:

| HTTP/1.1 404 Not Found

| Date: Fri, 30 Jul 2021 16:05:07 GMT

| Server: WSGIServer/0.2 CPython/3.8.2

| Content-Type: text/html

| X-Frame-Options: DENY

| Content-Length: 2366

| X-Content-Type-Options: nosniff

| Referrer-Policy: same-origin

| <!DOCTYPE html>

| <html lang="en">

| <head>

| <meta http-equiv="content-type" content="text/html; charset=utf-8">

| <title>Page not found at /nice ports,/Trinity.txt.bak</title>

| <meta name="robots" content="NONE,NOARCHIVE">

| <style type="text/css">

| html \* { padding:0; margin:0; }

| body \* { padding:10px 20px; }

| body \* \* { padding:0; }

| body { font:small sans-serif; background:#eee; color:#000; }

| body>div { border-bottom:1px solid #ddd; }

| font-weight:normal; margin-bottom:.4em; }

| span { font-size:60%; color:#666; font-weight:normal; }

| table { border:none; border-collapse: collapse; width:100%; }

| vertical-align:

| GetRequest, HTTPOptions:

| HTTP/1.1 200 OK

| Date: Fri, 30 Jul 2021 16:05:07 GMT

| Server: WSGIServer/0.2 CPython/3.8.2

| Content-Type: text/html; charset=utf-8

| X-Frame-Options: DENY

| Content-Length: 69

| X-Content-Type-Options: nosniff

| Referrer-Policy: same-origin

| Hello. This site is currently in development please check back later.

| RTSPRequest:

| <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"

| "http://www.w3.org/TR/html4/strict.dtd">

| <html>

| <head>

| <meta http-equiv="Content-Type" content="text/html;charset=utf-8">

| <title>Error response</title>

| </head>

| <body>

| <h1>Error response</h1>

| <p>Error code: 400</p>

| <p>Message: Bad request version ('RTSP/1.0').</p>

| <p>Error code explanation: HTTPStatus.BAD\_REQUEST - Bad request syntax or unsupported method.</p>

| </body>

|\_ </html>

| http-robots.txt: 1 disallowed entry

|\_/

|\_http-server-header: WSGIServer/0.2 CPython/3.8.2

|\_http-title: Site doesn't have a title (text/html; charset=utf-8).

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :

SF-Port8080-TCP:V=7.91%I=7%D=7/30%Time=61042335%P=x86\_64-pc-linux-gnu%r(Ge

SF:tRequest,135,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Fri,\x2030\x20Jul\x202

SF:021\x2016:05:07\x20GMT\r\nServer:\x20WSGIServer/0\.2\x20CPython/3\.8\.2

SF:\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nX-Frame-Options:\x2

SF:0DENY\r\nContent-Length:\x2069\r\nX-Content-Type-Options:\x20nosniff\r\

SF:nReferrer-Policy:\x20same-origin\r\n\r\nHello\.\x20This\x20site\x20is\x

SF:20currently\x20in\x20development\x20please\x20check\x20back\x20later\."

SF:)%r(HTTPOptions,135,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Fri,\x2030\x20J

SF:ul\x202021\x2016:05:07\x20GMT\r\nServer:\x20WSGIServer/0\.2\x20CPython/

SF:3\.8\.2\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nX-Frame-Opti

SF:ons:\x20DENY\r\nContent-Length:\x2069\r\nX-Content-Type-Options:\x20nos

SF:niff\r\nReferrer-Policy:\x20same-origin\r\n\r\nHello\.\x20This\x20site\

SF:x20is\x20currently\x20in\x20development\x20please\x20check\x20back\x20l

SF:ater\.")%r(RTSPRequest,1F4,"<!DOCTYPE\x20HTML\x20PUBLIC\x20\"-//W3C//DT

SF:D\x20HTML\x204\.01//EN\"\n\x20\x20\x20\x20\x20\x20\x20\x20\"http://www\

SF:.w3\.org/TR/html4/strict\.dtd\">\n<html>\n\x20\x20\x20\x20<head>\n\x20\

SF:x20\x20\x20\x20\x20\x20\x20<meta\x20http-equiv=\"Content-Type\"\x20cont

SF:ent=\"text/html;charset=utf-8\">\n\x20\x20\x20\x20\x20\x20\x20\x20<titl

SF:e>Error\x20response</title>\n\x20\x20\x20\x20</head>\n\x20\x20\x20\x20<

SF:body>\n\x20\x20\x20\x20\x20\x20\x20\x20<h1>Error\x20response</h1>\n\x20

SF:\x20\x20\x20\x20\x20\x20\x20<p>Error\x20code:\x20400</p>\n\x20\x20\x20\

SF:x20\x20\x20\x20\x20<p>Message:\x20Bad\x20request\x20version\x20\('RTSP/

SF:1\.0'\)\.</p>\n\x20\x20\x20\x20\x20\x20\x20\x20<p>Error\x20code\x20expl

SF:anation:\x20HTTPStatus\.BAD\_REQUEST\x20-\x20Bad\x20request\x20syntax\x2

SF:0or\x20unsupported\x20method\.</p>\n\x20\x20\x20\x20</body>\n</html>\n"

SF:)%r(FourOhFourRequest,A28,"HTTP/1\.1\x20404\x20Not\x20Found\r\nDate:\x2

SF:0Fri,\x2030\x20Jul\x202021\x2016:05:07\x20GMT\r\nServer:\x20WSGIServer/

SF:0\.2\x20CPython/3\.8\.2\r\nContent-Type:\x20text/html\r\nX-Frame-Option

SF:s:\x20DENY\r\nContent-Length:\x202366\r\nX-Content-Type-Options:\x20nos

SF:niff\r\nReferrer-Policy:\x20same-origin\r\n\r\n<!DOCTYPE\x20html>\n<htm

SF:l\x20lang=\"en\">\n<head>\n\x20\x20<meta\x20http-equiv=\"content-type\"

SF:\x20content=\"text/html;\x20charset=utf-8\">\n\x20\x20<title>Page\x20no

SF:t\x20found\x20at\x20/nice\x20ports,/Trinity\.txt\.bak</title>\n\x20\x20

SF:<meta\x20name=\"robots\"\x20content=\"NONE,NOARCHIVE\">\n\x20\x20<style

SF:\x20type=\"text/css\">\n\x20\x20\x20\x20html\x20\\*\x20{\x20padding:0;\x

SF:20margin:0;\x20}\n\x20\x20\x20\x20body\x20\\*\x20{\x20padding:10px\x2020

SF:px;\x20}\n\x20\x20\x20\x20body\x20\\*\x20\\*\x20{\x20padding:0;\x20}\n\x2

SF:0\x20\x20\x20body\x20{\x20font:small\x20sans-serif;\x20background:#eee;

SF:\x20color:#000;\x20}\n\x20\x20\x20\x20body>div\x20{\x20border-bottom:1p

SF:x\x20solid\x20#ddd;\x20}\n\x20\x20\x20\x20h1\x20{\x20font-weight:normal

SF:;\x20margin-bottom:\.4em;\x20}\n\x20\x20\x20\x20h1\x20span\x20{\x20font

SF:-size:60%;\x20color:#666;\x20font-weight:normal;\x20}\n\x20\x20\x20\x20

SF:table\x20{\x20border:none;\x20border-collapse:\x20collapse;\x20width:10

SF:0%;\x20}\n\x20\x20\x20\x20td,\x20th\x20{\x20vertical-align:");

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 98.96 seconds

# References:

SQLI: <https://portswigger.net/web-security/sql-injection>

<https://portswigger.net/web-security/sql-injection/union-attacks>

<https://css-tricks.com/snippets/php/sanitize-database-inputs/>

Password: <https://www.hypr.com/password-reuse/>

<https://gizmodo.com/the-5-best-ways-to-store-passwords-safely-1782047318>

$PATH: <https://betterprogramming.pub/becoming-root-via-a-misconfigured-path-720a52981c93>