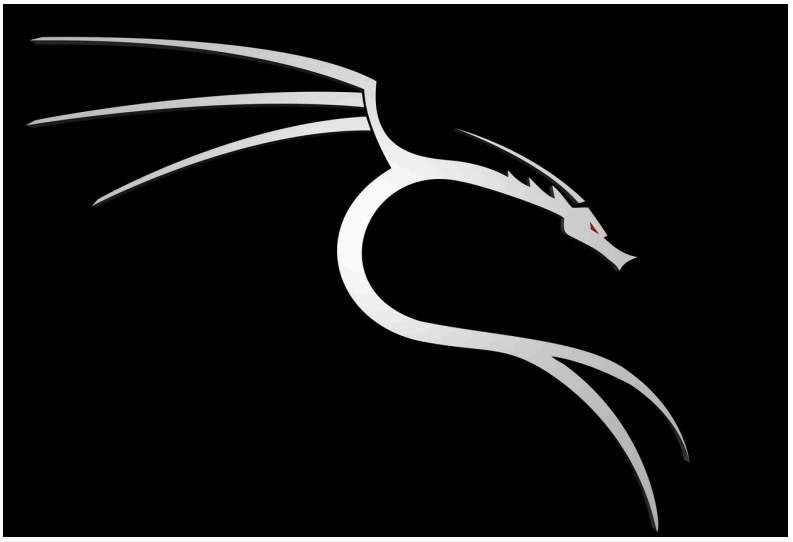
Pentester Report.

——----------

Client: Machine / UltraTech.



TeamWork:

- **Sh3llr1ck0.**

Content.

Executive Report.

Subject.

Follow pentester methodology, searching and exploiting as well as exploiting vulnerabilities found within the machine "UltraTech". Aiming to present this report in order to search further upgrades and fixes available for the website safety and its customers.
Such penetration testing was performed under the perspective known as "Grey box" or "Grey Hat Hacker", representing the acquisition of some information about client "UltraTech".

Scope.

- Directories: All.
- Domain / subdomains: All.
- Ip: 10.10.227.163

Findings.

Client or machine "UltraTech" was considerado vulnerable as there was such cybersecurity holes that allow an attacker to generate connections from the client (UltraTech) to the attacker (hacker), most commonly known as revshell (reverse shell) making possible to get full remote access on the server by taking advantage of the vulnerability known as "Command Injections". Command Injection is commonly considered risky, that's why it should not be skipped.

In the hosting system was possible to elevate privileges from a normal user to a fully administrator user with enough permissions to perform any kind of action from as simple as deleting some configurations to making the server totally unusable by applying the method docker breakout.

Score	Total	Vulnerability	Description
8.6 High	1	Command Injection	High risk meaning the impact that a command injection may cause.
7.9 High	1	Docker Breakout	High risk meaning the impact that a user migration may cause.

Recommendations.

- Input validation: Method specifically designed to deny any other extra data introduced right after what's supposed to be introduced.
- Docker Breakout: Right file permissions management.

Vulnerabilities Report.

Command Injection.

Information.

known as shell injection. It's a vulnerability where a hacker is allowed to execute commands directly in the operating system (server) where the website is located, further compromising the information stored.

Details.

The work team found the presence of Command Injection vulnerability specifically within the parameter "?ip=".

Using the burp suite tool, it was possible to intercept the request before it is sent to the backend where data is processed. So, adjusting a little bit the parameter value as such ' localhost;echo+"";`id` ' we got the ability to make command execution possible:

Figure 1: Common Injection requested.

Getting a response showing "groups=1002(www)" as proof of the vulnerability's existence.

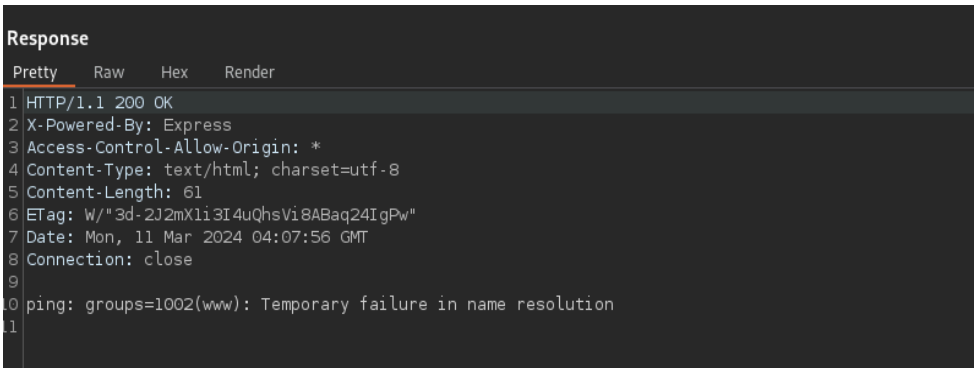


Figure 2: Injection response.

Performing further enumeration on resources inside the web server, we could locate and obtain the database file “utech.db.sqlite” content.

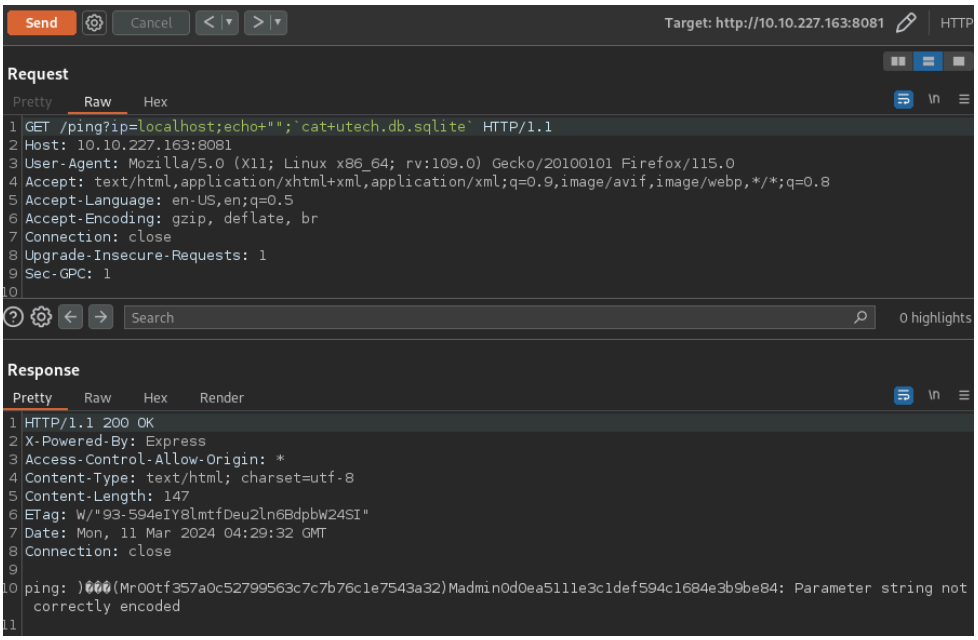


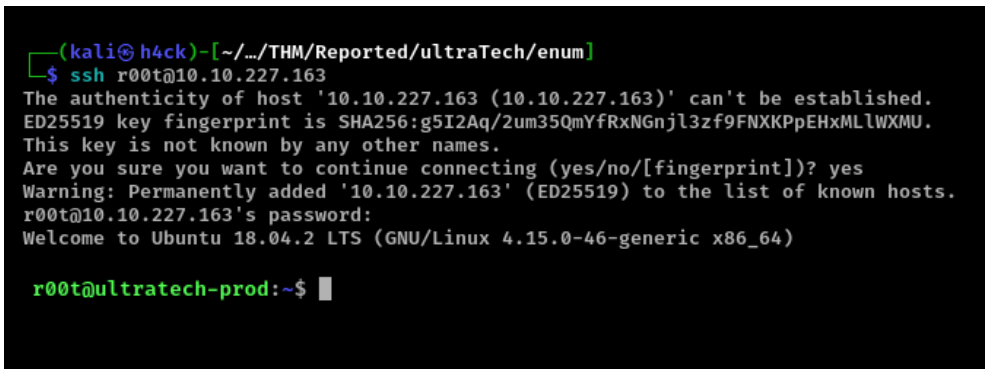
Figure 3: Credential encrypted request.

Going to the website “crack station” (page address in link section) we were able to decrypt the hash and obtain password in plain txt:

r00t:f357a0c52799563c7c7b76c1e7543a32:n100906
admin:0d0ea5111e3c1def594c1684e3b9be84:mrsheafy

Figure 4: passwords decrypted.

Password re-utilization is, in a way, another high risk vector for users and systems as well which may result in remote access, most commonly and in our case, through ssh.



Affected resource.

http://10.10.227.163/ping**?ip=**

Links.

https://portswigger.net/web-security/os-command-injection
https://crackstation.net/

Recommendations.

Keep in mind a few consideration at the fixing process time as the following:

- Strong input validation method implementation on the backend side, making sure only data hoped is an ip.

Docker Breakout.

Information.

Docker is an open source for application developers within a sandbox (testing box), its light virtualization is known as container. Docker Breakout is considered as a technique focused in getting out from the container, obtaining another session within the same session, usually as root.

Details.

As a fundamental part of penetration testing performed, there is another step known as privilege escalation; several steps taken to search any possible vector to migrate from a user with less or normal privileges to another user with higher privileges than those we already have; usually such migration is focused to an administrator user (windows) or root (linux / mac).

Steps to follow may vary depending the system we are dealing with and technologies in use. Being the company / machine “UltraTech” case, privilege escalation was possible through the same docker mounting to the server.

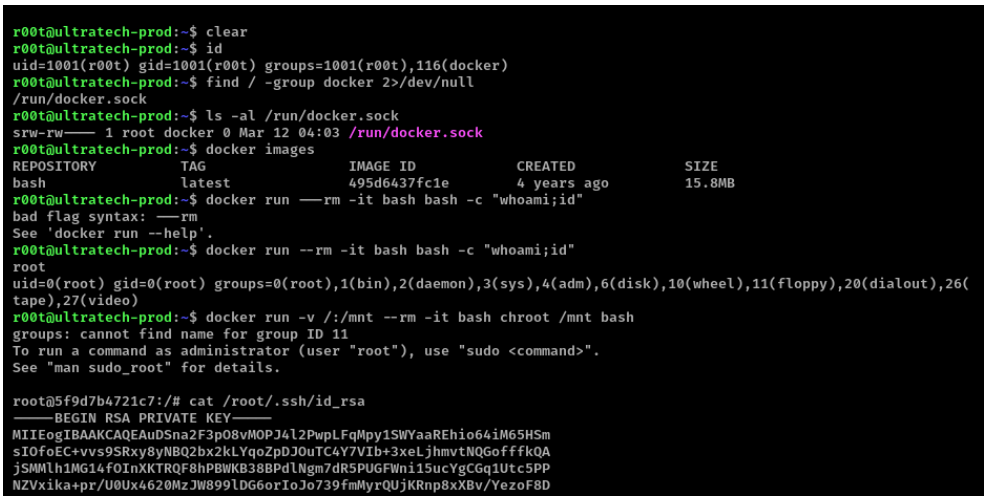


Figure 1: User root migration.

Affected sources.

groups=1001(r00t),**116(docker)**.

Links.

https://juggernaut-sec.com/docker-breakout-lpe/
https://juggernaut-sec.com/docker-breakout-lpe/#Hunting_for_a_Docker_Privileges

Recomendations.

Keep in mind:

- Remove r00t user from docker group.

Scale.

Rating	CVSS Score
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0