# NATAS COMMANDS

OverTheWire natas Lab (Level 0 to Level 34)

### Level 0 → Level 1

* + No command used
  + Password got-0nzCigAq7t2iALyvU9xcHlYN4MlkIwlq

### Level 1 → Level 2

* + No command used
  + Password got- TguMNxKo1DSa1tujBLuZJnDUlCcUAPlI

### Level 2 → Level 3

* + NO command used
  + Password got-3gqisGdR0pjm6tpkDKdIWO2hSvchLeYH

### Level 3 → Level 4

* + curl -I [http://natas4.natas.labs.overthewire.org](http://natas4.natas.labs.overthewire.org/)
  + password got-0n35PkggAPm2zbEpOU802c0x0Msn1ToK

### Level 4 → Level 5

* + No command used
  + Password got-0RojwHdSKWFTYR5WuiAewauSuNaBXned

### Level 5 → Level 6

* + No command used
  + Password got- 0RoJwHdSKWFTYR5WuiAewauSuNaBXned

### Level 6 → Level 7

* + No command used
  + Password got- bmg8SvU1LizuWjx3y7xkNERkHxGre0GS

### Level 7 → Level 8

* + No command used
  + Password got- xcoXLmzMkoIP9D7hlgPlh9XD7OgLAe5Q

### Level 8 → Level

* + <http://natas7.natas.labs.overthewire.org/index.php?page=/etc/natas>

\_webpass/natas8

### Level 9 → Level 10

* + Decode and reverse the string (base64 decoding).
  + Password: nOpp1igQAkUzaI1GUUjzn1bFVj7xCNzu

### Level 10 → Level 11

* + No command used
  + Password got- t7I5VHvpa14sJTUGV0cbEsbYfFP2dmOu

### Level 11→ Level 12

* + Manipulated application cookies (decoded data, flipped bits)
  + Password: EDXp0pS26wLKHZy1rDBPUZk0RKfLGIR3

### Level 12→ Level 13

* + Created and uploaded .php file.
  + Password: jmLTY0qiPZBbaKc9341cqPQZBJv7MQbY

### Level 13→ Level 14

* + Created a fake .jpg file with PHP code inside.
  + Password: Lg96M10TdfaPyVBkJdjymbllQ5L6qdl1

### Level 14→ Level 15

* + SQL Injection: ' OR 1=1 –
  + Password: AwWj0w5cvxrZiONgZ9J5stNVkmxdk39J

### Level 15→ Level 16

* + Brute force password one character at a time using SQL injection
  + Password: W0mMhUcRRnG8dcghE4qvk3JA9lGt8nDl

### Level 16→ Level 17

* + $(expr substr $(cat /etc/natas\_webpass/natas17) 1 1)
  + Password: 8Ps3H0GWbn5rd9S7GmAdgQNdkhPkq9cw

### Level 17→ Level 18

* + " union select 1, if((select password from users where CHAR\_LENGTH(password)=32) like binary "%", sleep(2),1)
  + Password: xvKIqDjy4OPv7wCRgDlmj0pFsCsDjhdP

### Level 18→ Level 19

* + Burp Suite Intruder Attack on PHPSESSID (0 to 640).
  + Password: 4IwIrekcuZlA9OsjOkoUtwU6lhokCPYs

### Level 19→ Level 20

* + Burp Suite Intruder Attack hex encoded session IDs like 101-admin
  + Password: oZ0F1ZqXjkU7XnS7f2E3cFGJfSvq3s1F

### Level 20→ Level 21

* + Inject admin%0Aadmin 1 as username (manipulate session file).
  + Password: NvEihvjQyvqBVwtJcIuZgKkEU9clYwuU

### Level 21→ Level 22

* + Manipulate session ID to set admin=1 using Burp Suite.
  + Password: IFekPyrQXftziDEsUr3x21sYuahypdgJ

### Level 22→ Level 23

* + Added parameter ?revelio in URL.
  + Password: aGoY4q2Dc6MgDq4oL4YtoKtyAg9PeHa1

### Level 23→ Level 24

* + Input a password like iloveyou123456
  + Password: TzbeZfemC8XmqAHEBuSHhzn4WdrdogHK

### Level 24→ Level 25

* + Input array as password to break strcmp()
  + Password: UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ

### Level 25→ Level 26

* + ?lang=....//....//....// ... //etc/natas\_webpass/natas26
  + Password: 5iwkcmiGCx6ag9G8JrAp7v7j9JUFi5ev

### Level 26→ Level 27

* + Use PHP object injection (malicious serialized object)
  + Crafted a payload that sets exit() as a destructor
  + Password: oGgWAJ7zcGTlMSfZ87iUhzazj7mkgchr

### Level 27→ Level 28

* + Bypass file upload restriction (Uploaded .php with fake extension)
  + Password: 55TBjpPZUUJgVP5b3BnbG6ONQbP8L6kg

### Level 28→ Level 29

* + Local File Inclusion (LFI) vulnerability exploitation
  + Password: JWwR438wkgTsNKBbcJoowyysdM82YjeF

### Level 29→ Level 30

* + SQL injection bypass (like using wildcard % characters)
  + Password: b4TaoukWUrc6e4Gh63hLkE2oMUDsE6aC

### Level 30→ Level 31

* + GET parameter (; separator)
  + &dir=;cat /etc/natas\_webpass/natas31
  + Password: mIwhBf6TyiQjhxCN91uqrKkId8rw2dwq

### Level 31→ Level 32

* + Used tricks like $(cat /etc/natas\_webpass/natas32)
  + Password: meGz9cN7EYgoyuzwG9uoppyv7BSk1gGR

### Level 32→ Level 33

* + WAF (Web Application Firewall) evasion
  + Used HTTP Parameter Pollution (HPP) technique
  + Password: N9pVwGgsjV8eTI4B5iXYkMDtUPYEAfIk

### Level 33→ Level 34

* + Used Unicode/hex encoding tricks to inject payload
  + Password: SSh1ZT9vF8uP0v6k7hh7yKy2U6jtyIRh