

Inscreva-se em nossa Newsletter!

Fique sabendo de todas as novidades semanalmente.



Nome *

Email *

ENVIAR

[Não quero me manter atualizado](#)

Suas aplicações são seguras?

[CONHEÇA A CONVISO!](#)

Github Hacking for fun and... sensitive data search!

19 de junho de 2013 / Conviso / Segurança de Aplicação / 0 comments


Conviso Research and Development Team is usually reading thousands and thousands of information daily and we make some filters and pay attention to some special words. We saw a very interesting post at Full Disclosure about advanced [GitHub Search](#).

Right after reading what we shared in our internal list, this information and a little bit of Github Hacking proved that GitHub is a Disneyland of information leakage. We tried a lot of different searches and some interesting or I could say, VERY INTERESTING, as you see below.

Private Key

extension:pem private

We've found 134,204 code results



android-test-key-ecdsa.pem

Last indexed on Feb 6

1

-----BEGIN EC PARAMETERS-----

2

BggqhkJOPQMBBw==

3

-----END EC PARAMETERS-----

4

-----BEGIN EC PRIVATE KEY-----

5

MHcCAQEEIFb6/5kje8LB6bKDjQbfr2d4wfvLjy+SNs7j4J1eEF+FoAoGCCqGSM49

6

AwEHoUQDQgAEJH4uX5l3CYLPIQ7tXxBjtPZN7HVf14uyPAs6VCPitxLjEcKq3w/w

7

wnPAhbhXN7bnC6lq1Yro/5v1pa1RGB46yQ==

8

-----END EC PRIVATE KEY-----

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

```
extension:xls mail
```

We've found 445 code results

 - User List.xls

Last indexed on Jul 29, 2013

	"Username"	"Full Name"	"E-Mail"	"Enabled"
1	"admin"	"Matt Raible"	"matt@raibledesigns.com"	"true"
2	"user"	"Tomcat User"	"matt_raible@yahoo.com"	"true"

 - mfd_files_dwgrevform.xls

Last indexed on May 15

```
1 mfd input form a b c d e f g h i j k l m n o p q r 1 mechanical fabrication de
```

MySQL Password / History

```
extension:sql mysql dump
```

We've found 46,715 code results

 - mtr_check.sql

Last indexed 9 days ago

```
88 WHERE table_schema='mysql' AND table_name != 'ndb_apply_status'
89 ORDER BY columns_in_mysql;
90
91 -- Dump all events, there should be none
...
59 CALL check_testcase_perfschema();
60
61 -- Dump all global variables except those that may change.
62 -- timestamp changes if time passes, server_uuid changes if server restarts.
```

 - archivista_user.sql

Last indexed on Aug 6, 2013

```
1 -- MySQL dump 9.11
2 --
3 -- Host: localhost Database: archivista
4 --
```

How about finding some possible 0days? Backdoors? Hell yeah! It's possible too.

Check out this GitHub "Dork":

```
stars:>1000 forks:>100 extension:php "eval(preg_replace(""
```

We searched for big projects who have more than 1000 stars, 100 forks, files with PHP extension and a possible flaw that allows Remote Code Execution.

```
stars:>1000 forks:>100 extension:php "eval(preg_replace("

Showing 604 available code results ⓘ Sort: E

FWRouter.class.php
Last indexed on Aug 4, 2013
420     if($m_requirements)
421         $requirements = eval(preg_replace('|^r{(.*)}$|', 'return array($1);', $m_requi
...
425     $defaults = array('controller' => $controller, 'action' => $action);
426     if($m_defaults)
427         $defaults = array_merge(eval(preg_replace('|^d{(.*)}$|', 'return array($1);',

...

codeigniter - jslogger.php
Last indexed on Jan 29
188     if ($jsFormat && (is_array($data) || is_object($data))) {
189         $data = 'eval(' . preg_replace('#[\\s\\r\\n\\t\\0\\x0B]+#', '', json
```

Check out other prefixes that might help you keeping your search improved [GitHub Search Cheat Sheet](#). Lots of FUN isn't ? We could probably find just about anything, the sky is the limit!

So to make our lives easier we developed a tool to grab those information in a more automated way:

```
myhost:research_github_hack c00f3r$ perl github_hack.pl
Searching to:
save file:
Pattern to search:

githubhack

-----
Coded By Cooler_
-----
Version 0.02 Beta

contact: acosta[at]conviso[dot]com[dot]br
c00f3r[at]gmail[dot]com
Please follow the example ./programm str_2_search_on_git find_0
n_source_codes file_log.txt number_of_pages_2_search
```

You can check the code and download it from [here](#) (but keep in mind that it is still in beta version).

Take care about what information you share. Lots of sensitive information could probably be over there. Search for information about your company before the bad guys do.

Originalmente postado no Blog da Conviso Application Security – Siga-nos no Twitter [@conviso](#) Google+

Like 0

G+1

TAGS

Ferramentas



Autor: Conviso

POSTAGENS RELACIONADAS



4 erros de segurança de dados para evitar



Segurança de aplicações: investimento ou custo?