

# Burp Suite Startup マニュアル

Burp Suite Japan User Group Project



version 1.0

## 目的

本ドキュメントは Burp Suite をふれたことがない方や使い始めの方向けに Burp Suite の基本的な使用方法を理解するためのドキュメントです。各機能の説明および使用方法を記載しますが、Web アプリケーションの検査手法については本ドキュメントの対象外となっています。Burp Suite Japan User Group でマニュアルなどの日本語化を行う活動により本ドキュメントは作成されました。本ドキュメントにより言語の違いによるハードルが少しでも低くなることを期待しています。

## 目次

Burp Suite Startup マニュアル .....	1
目的 .....	2
目次 .....	3
1 Burp Suite 概要 .....	4
1.1 Burp Suite とは .....	4
1.2 特徴 .....	4
1.3 診断プロセス .....	6
2 インストール手順 .....	8
2.1 Windows 版インストール手順 .....	8
3 初回起動、使用準備 .....	11
3.1 初回起動 .....	11
3.1.3 Burp Suite のアップデート .....	13
3.2 起動ウィザード .....	14
3.3 Burp Suite の設定 .....	16
4 診断方法について .....	23
4.1 Proxy 機能 .....	23
4.2 Burp Suite による通信のキャプチャ .....	24
4.3 その他 .....	31

# 1 Burp Suite 概要

## 1.1 Burp Suite とは

Burp Suite は PortSwigger 社が Java で作成した、ローカル Proxy を中心に構成された Web アプリケーションのセキュリティ診断に特化したツールです。ローカル Proxy は、会社や学校などで使用されている Proxy とは異なり、Web アプリケーションのセキュリティ診断やデバッグなどに活用されます。同様のツールとして Burp Suite 以外にも OWASP ZAP や Fiddler などが存在しています。

Burp Suite <http://portswigger.net/>



## 1.2 特徴

Burp Suite は、プロフェッショナル版（Professional Edition）とフリー版（Free Edition）の 2 種類あります。最新バージョンは、フリー版 v1.7.03 で、プロフェッショナル版 v1.7.03 です（2016 年 7 月 19 日時点）。

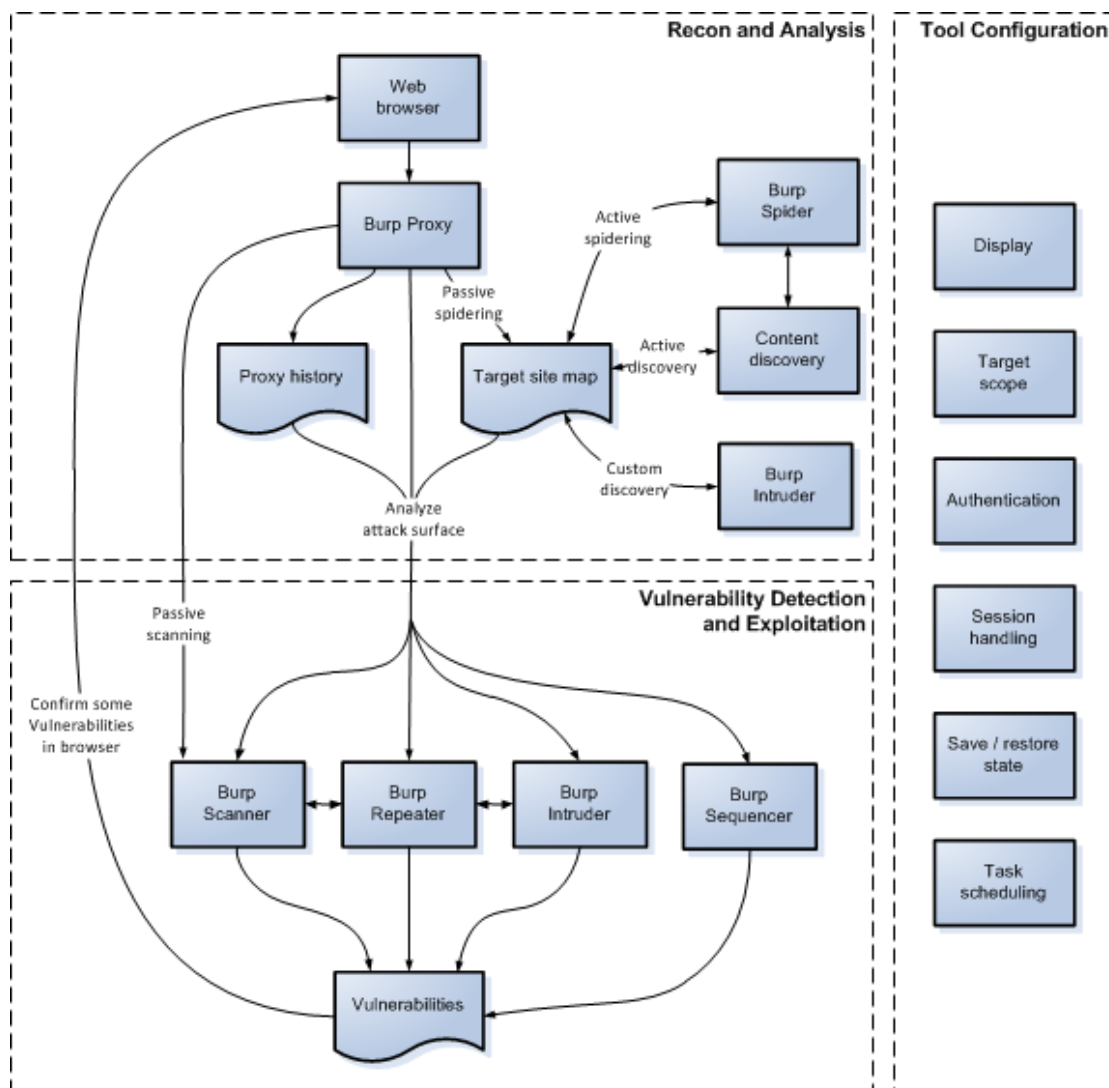
Burp Suite は以下の機能で構成されており、プロフェッショナル版でしか利用できない機能もあります。

機能	概要
Target	対象サイトの詳細情報を収集する site map の作成やターゲットと

	なるスコープを設定します。
Proxy	ブラウザと Web サーバの間でリクエストやレスポンスを仲介し、内容変更などの制御を行います。
Spider	事前に設定されたスコープ内で自動巡回し、コンテンツの洗い出しを行います。
Scanner	プロフェッショナル版の機能で、アクティブスキャン(動的解析)およびパッシブスキャン(静的解析)による脆弱性スキャンを行います。
Intruder	定型化されたパターンによる自動的なスキャンを行います。 Scanner とは異なり、結果の分析は行いません。
Repeater	リクエストを手動で修正し再送付します。
Sequencer	トークンなどのランダム性を解析します。
Decoder	BASE64 などのエンコード・デコードや hash 算出を行います。
Comparer	リクエスト、レスポンスの差分を表示します。
Extender	BApp Store や独自の拡張プログラムを制御します。
User Options	UI など Burp Suite の実行環境に関するオプションを設定します。
Project Options	Project に関するオプションを設定します。
Alerts	エラーメッセージなどを出力します。
その他	User オプション、Project オプションの保存や読み込みなどを行います。

## 1.3 診断プロセス

Burp Suite を使って効果的に診断するには、手動と自動による診断を組み合わせる必要があります。ブラウザを用いて対象となるアプリケーションへアクセスし、情報を収集します。収集した情報を分析し、必要に応じて Burp Suite の設定を変更します。設定後、脆弱性スキャンを行います。



- 対象アプリケーションの調査(Recon and Analysis)
- 各機能の設定(Tool Configuration)
- 脆弱性スキャン(Vulnerability Detection and Exploitation)

## 対象アプリケーションの調査(Recon and Analysis)

このフェーズでは、手動でブラウザを操作し、対象アプリケーションをマッピングします。Proxy history と Target の site map にブラウザでアクセス下すべてのリクエストが登録されていきます。site map は、レスポンスのリンクやフォームなどからコンテンツの存在を予測します。存在しているがまだアクセスしていないコンテンツを見つけ、ブラウザでアクセスしていきます。

## 各機能の設定(Tool Configuration)

対象となるアプリケーションで Burp Suite が動作するように、Burp Suite の設定を確認、変更します。以下の設定がポイントです。

### ディスプレイ

HTTP ログを表示するためのフォントや文字コードを変更します。日本語に対応していないフォントの場合、日本語が正常に表示されないため、対応したフォントなどを選択してください。

### スコープ

対象とする範囲(スコープ)を設定します。設定すると Proxy history や Target site map での表示内容のフィルタや、インターセプトするリクエスト・レスポンスの実行範囲を制限できます。この設定により、誤ってほかの環境へアクセスするミスを抑制します。

## 認証

BASIC 認証などの認証を設定します。

## ログの保存

Logging または extension などの拡張機能を用いてログを保存します。フリー版の場合、state ファイルおよび Project ファイルの作成ができないため、特に重要です。

## 脆弱性スキャン(Vulnerability Detection and Exploitation)

対象アプリケーションを調査し必要な設定を実施後、脆弱性スキャンを実施します。フリー版では Proxy でインターセプトしたリクエストを変更するか、Intruder や Repeater を利用します。プロフェッショナル版では Scanner も利用できます。

## 2 インストール手順

### 2.1 Windows 版インストール手順

Burp Suite は実行可能な JAR ファイルとなっており、フリー版は PortSwigger 社のサイトよりダウンロードが可能です。JAR を実行するために Java の実行環境を用意する必要があります。



### 2.1.1 Java 実行環境の準備

Burp の JAR ファイルは Java Runtime Enviroment(JRE)で実行可能です。また、JAR ファイル自体を解凍する必要はありません。まず最初に Java がインストールされているか確認します。

1. コマンドプロンプトで"java -version"を実行します。
2. Java がインストールされている場合、java version "1.8.0\_91"のようなメッセージが表示されます。また、Burp は v1.6 以降の Java が必要となります。ただし、Java v1.6 などのすでにサポートがされていないバージョンをご利用の場合、サポートされたバージョンへの移行を強く推奨します。
3. Java がインストールされていない場合や v1.5 などの古いバージョンの場合、Oracle 社のサイト  
( <http://www.oracle.com/technetwork/java/javase/downloads/index.html> )より JRE をダウンロードし、インストールします。



JRE のインストールが完了したら手順 2 を実施し、正常にインストールができているか確認してください。

### 2.1.2 Burp Suite のダウンロード

JRE のインストールが完了したら、Burp Suite のフリー版を  
<https://portswigger.net/burp/download.html> からダウンロードします。

## Download Burp Suite

Please choose the edition of Burp Suite that is right for you. [Help me choose >](#)

	Free Edition	Professional Edition \$349 per user per year
Burp Proxy	✓	✓
Burp Spider	✓	✓
Burp Repeater	✓	✓
Burp Sequencer	✓	✓
Burp Decoder	✓	✓
Burp Comparer	✓	✓
Burp Intruder	Time-throttled demo	✓
Burp Scanner		✓
Save and Restore		✓
Search		✓
Target Analyzer		✓
Content Discovery		✓
Task Scheduler		✓
Release Schedule	Major point releases	Frequent updates, earlier releases, beta versions
	<b>Download now</b> 	<b>Buy now</b> 



### Testimonials

"Burp Suite Pro is an unbelievably powerful tool. The scanner is amazingly fast and accurate. I use Burp extensively and it has never let me down."

**Alex Lauerman, FishNet Security**

"If you test the security of web applications for a living, Burp Suite Pro is an essential weapon you must have in your arsenal."

**Jack Mannino, CEO, nVisium Security Inc.**

[Read more Success Stories >](#)



### Blog

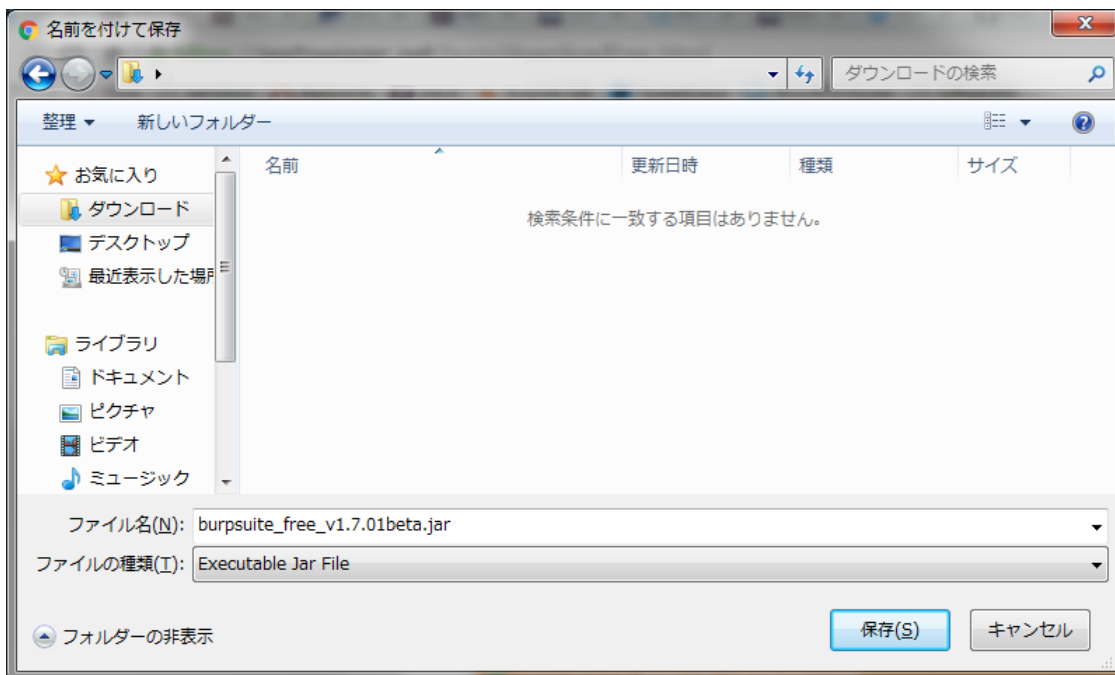
Friday, April 8, 2016

#### Introducing Burp projects

The latest major release of Burp introduces some great new capabilities for handling Burp's data and configuration. This blog post covers the following areas:

- Burp project files
- Changes to Burp's configuration options

任意のフォルダにダウンロードします。



## 3 初回起動、使用準備

### 3.1 初回起動

Burp Suite は、Java 実行可能ファイル（拡張子 .jar）として配布されています。この JAR ファイルをダブルクリックするだけでも起動できますが、メモリサイズなどを指定するため、次のようにコマンドラインからの起動をお勧めします。

```
java -Xmx1024m -jar /path/to/burp.jar
```

これは、1024MB のメモリを Burp に割り当てて Burp を起動する例です。

### 3.1.1 コマンドライン引数

Burp Suite には、いくつかのコマンドライン引数があります。

- `--config-file`

指定したファイルから設定を読み込みます。ユーザ設定とプロジェクト設定（後述）など、複数のファイルに設定が分かれている場合、このオプションを複数指定して読み込みができます。

- `--disable-extensions`

起動時に拡張機能を読み込まないようにするオプションです。Burp Suite は起動時に拡張機能を自動的に読み込みます。何らかの拡張機能の不具合で Burp Suite が起動しなくなってしまった場合、このオプションを使用して拡張機能の自動読み込みを抑止できます。

- `--project-file`

プロフェッショナル版専用のオプションです。保存してあるプロジェクトファイルを読み込みます。

その他全てのコマンドライン引数を確認するには、次のように `--help` を付けて実行してください。

```
java -jar /path/to/burp.jar -help
```

### 3.1.2 起動バッチファイル

これらのコマンドライン引数を、起動のたびに毎回指定するのは面倒です。よく使うコマンドラインオプションを指定したバッチファイルを作り、ダブルクリッ

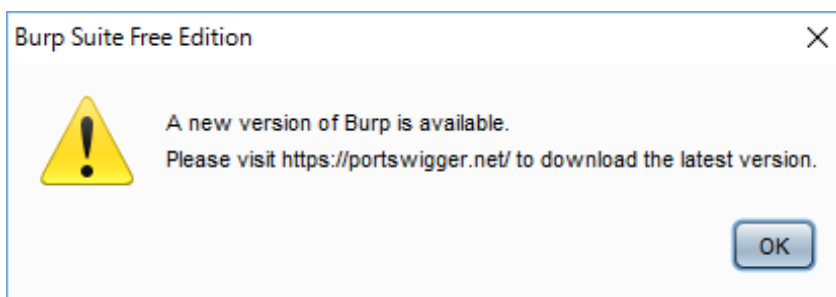
クだけで起動したいところです。ただし、Burp Suite がバージョンアップすると jar ファイルのファイル名が変わるため、アップデートのたびにバッチの修正またはファイル名の変更が必要になってしまいます。

はせがわようすけ氏が、最新バージョンの jar ファイルを自動的に探して起動するスクリプトを公開しています。jar ファイルの保存先フォルダと、コマンドライン引数を適宜書き換えて利用してください。

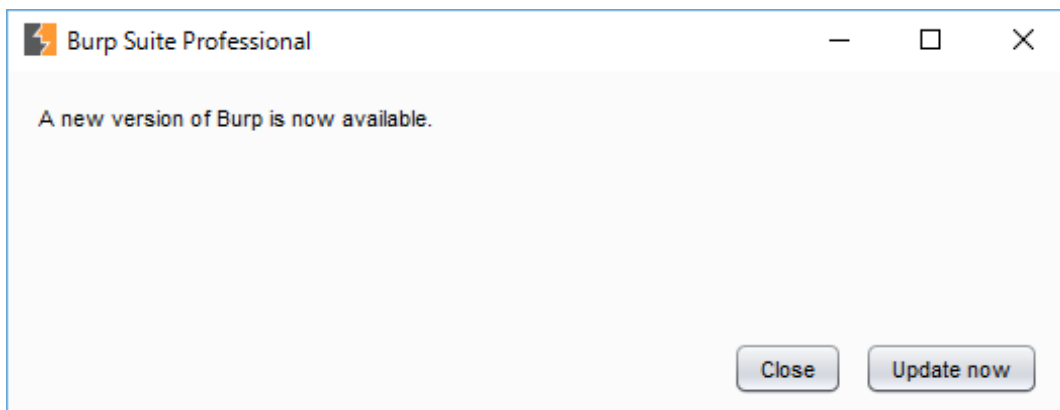
<https://gist.github.com/hasegawayosuke/71729d508f903a7dd42e>

### 3.1.3 Burp Suite のアップデート

Burp Suite を起動すると、自動的に最新バージョンのチェックが行われます。もし、現在起動しているバージョンより新しいバージョンがリリースされていると、Burp Suite はそれを通知します。フリー版では、最新の Burp Suite をダウンロードするための URL が表示されますので、そのページにアクセスしダウンロードしてください。

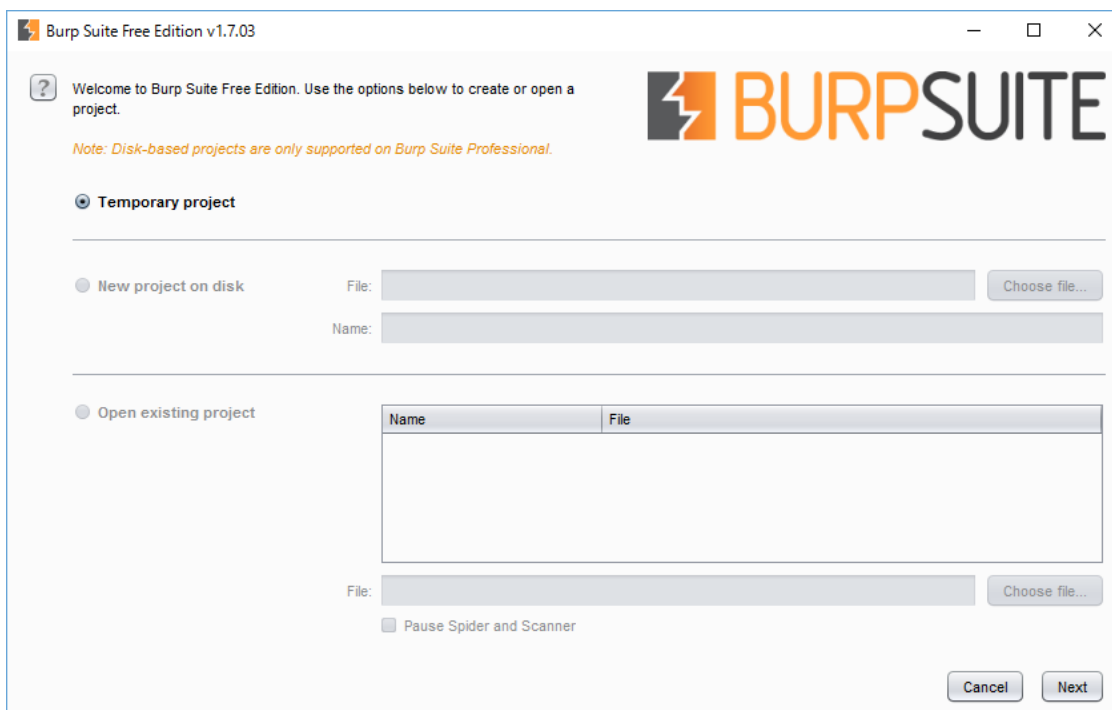


プロフェッショナル版では、UI から最新版のダウンロードと、最新版での再起動が可能です。



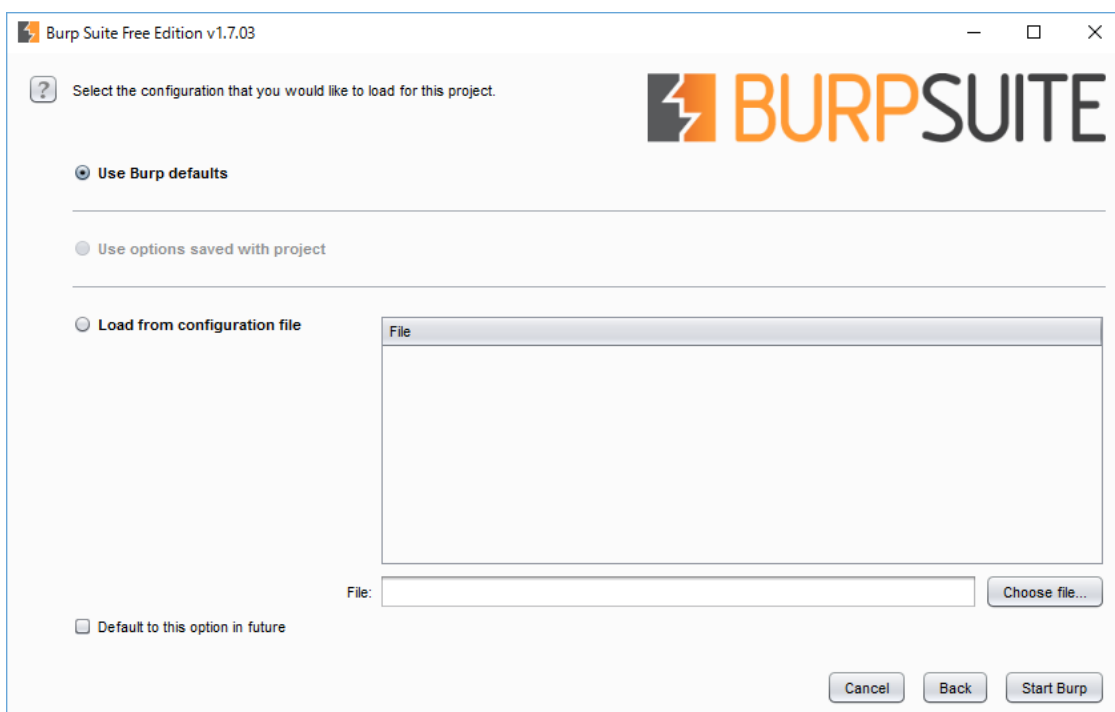
## 3.2 起動ウィザード

Burp Suite を起動すると、数秒間スプラッシュスクリーンが表示され、その後起動ウィザードが開きます。



最初にプロジェクトの種類を選ぶ画面が表示されますが、フリー版では Temporary project しか選択できませんので、そのまま次へ進みます。プロフェッショナル版では、Burp Suite のログなどをディスクに保存するディスクベースのプロジェクト機能があり、その新規作成、または既存のプロジェクトファイルの読み込みができます。

次に、設定ファイルを指定する画面が表示されます。



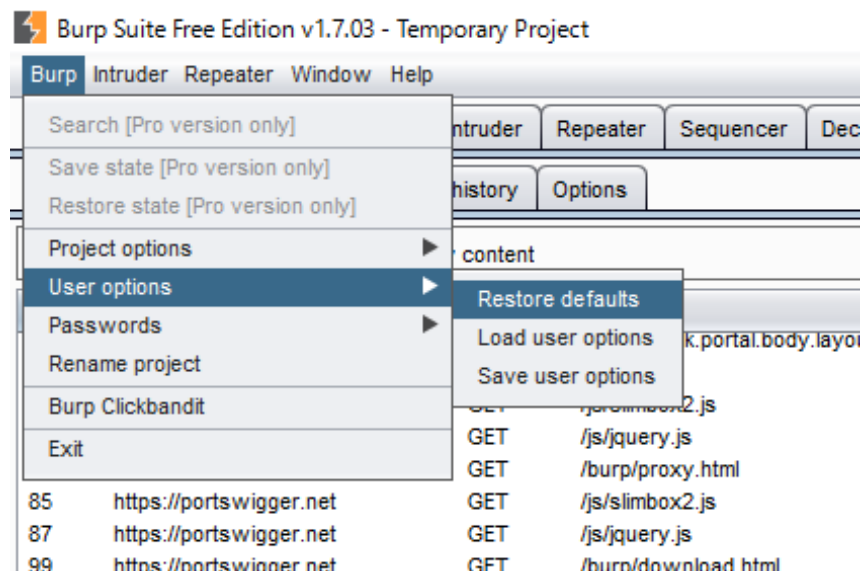
初めて Burp Suite を起動する場合は、[Use Burp defaults]を選択した状態で、[Start Burp]ボタンをクリックします。

Burp Suite の設定ファイルを保存（後述）していて、その設定ファイルを読み込む場合は、[Choose file]ボタンから設定ファイルを選択してください。設定ファ

イルは、複数のファイルが指定できます。コマンドライン引数で設定ファイルを指定している場合は、この設定選択ウィザード画面は表示されません。

本マニュアルでは、デフォルト設定の状態を前提に解説を進めますので、設定を変更している場合は適宜読み替えてください。設定をデフォルトに戻すには、起動ウィザードで[Use Burp defaults]を選択して起動する、または次のようにメニューから設定のリセットが行えます。

- [Burp]メニュー-[Project options]-[Restore defaults]-[All]
- [Burp]メニュー-[User options]-[Restore defaults]

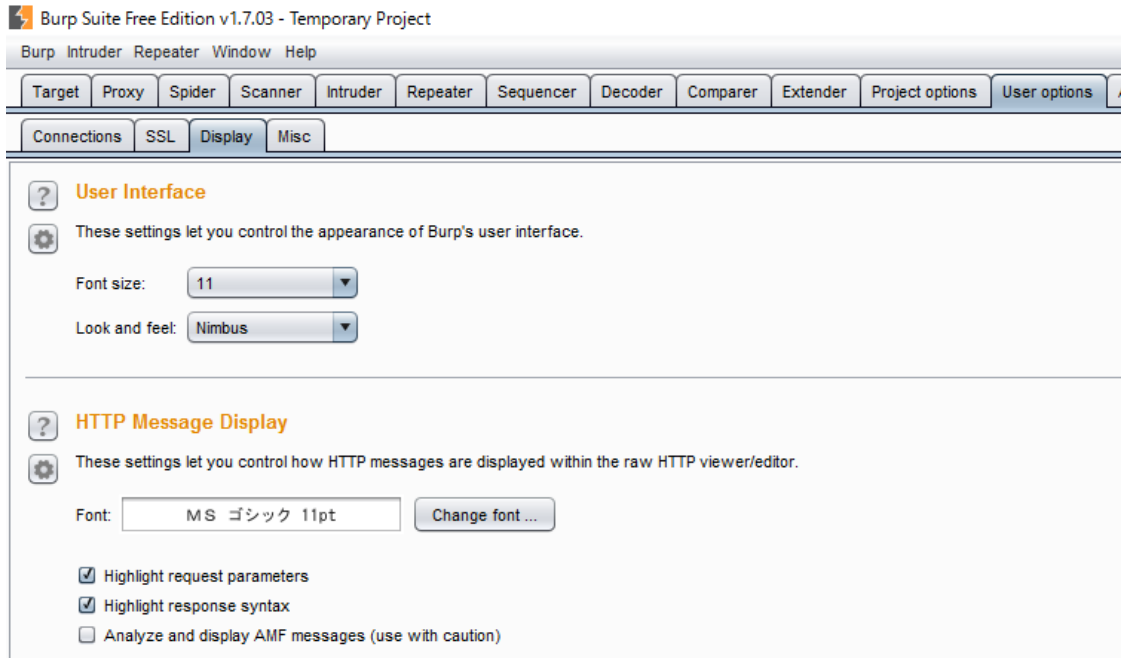


## 3.3 Burp Suite の設定

### 3.3.1 表示設定

Burp Suite を本格的に使い始める前に、表示設定を見直しておくことを推奨します。表示設定は、[User options]-[Display]で行います。





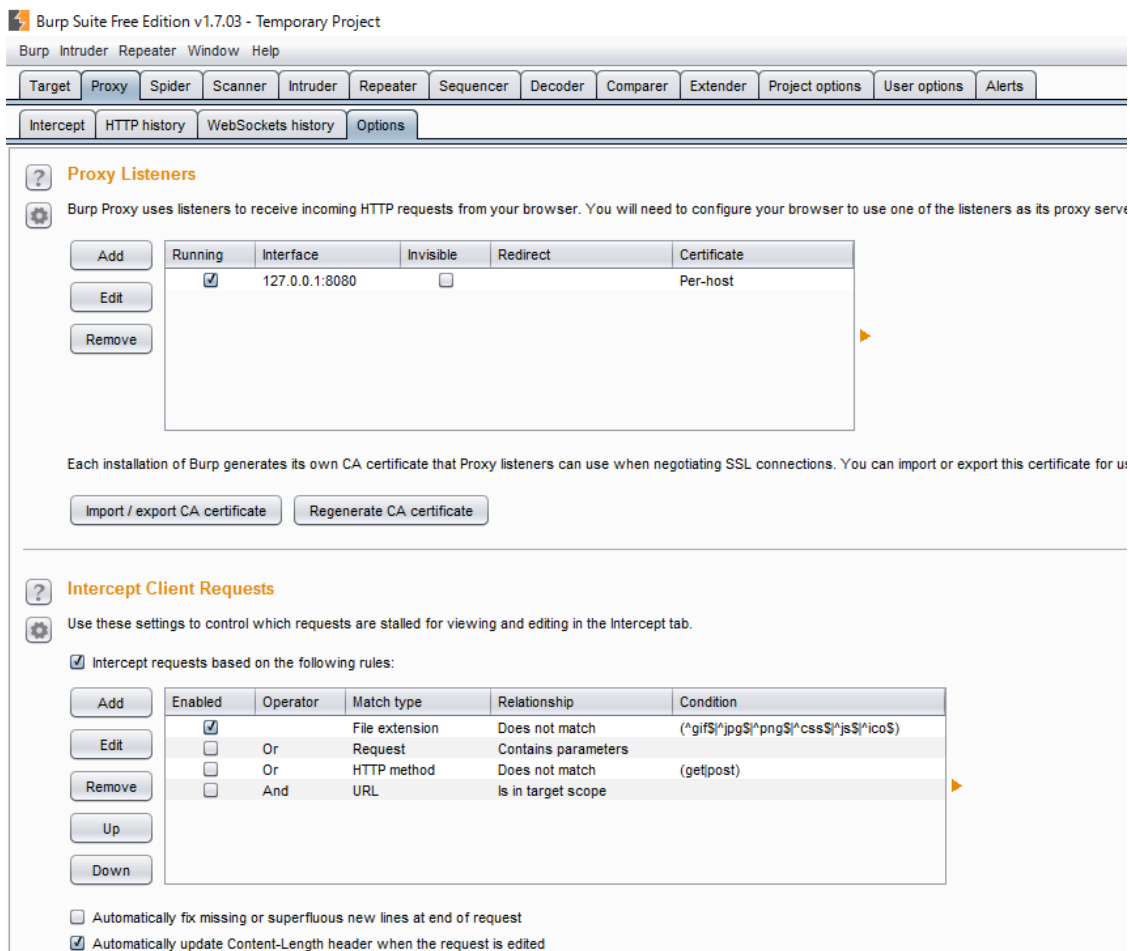
[User Interface]で、Burp Suite 全体の UI の見た目を設定できます。ここで、好みのフォントサイズと、ルック・アンド・フィールを選択してください。設定を反映させるには、Burp Suite の再起動が必要です。

[HTTP Message Display]では、HTTP メッセージエディタで表示される HTTP リクエストやレスポンスのフォントなどが指定できます。こちらも、好みのフォントやフォントサイズを指定してください。設定を変更するとすぐにメッセージエディタに反映されます。デフォルトで指定されている Courier New フォントは英字フォントのため、日本語文字が表示できません。"Arial Unicode MS"や"MS ゴシック"などの日本語フォントを推奨します。

### 3.3.2 Proxy 設定

Burp Suite の心臓部である、Proxy の設定を行います。

[Proxy]-[Options]を確認してください。



[Proxy Listeners]にはデフォルトのプロキシリスナーが設定されています。

Interface が"127.0.0.1:8080"となった行が 1 つあり、問題なければ Running 列にチェックが付いているはずです。もしチェックが付いていない場合はチェックボックスをクリックしてみて、それでもチェックが付かない場合は、8080 ポート

が他のアプリケーションで使われてしまっている可能性があります。左側の Edit ボタンをクリックし、バインドするポート番号を他のポート番号に変えて、チェックボックスがオンになるか確認してください。

この状態で[Proxy]-[Intercept]に移動し、インターセプト状態を一旦オフにします。UI 上のボタンが[Intercept is off]となっていることを確認してください。[Intercept is on]になっている場合はボタンをクリックし、[Intercept is off]に変更します。

次に、ブラウザのプロキシ設定を行います。ブラウザのプロキシ設定で、HTTP と HTTPS 両方のプロトコルの設定についてアドレス（デフォルトは 127.0.0.1）とポート（デフォルトは 8080）を指定し、例外設定は空にします。

インターネット接続

インターネット接続に使用するプロキシの設定

☐ プロキシを使用しない(Y)

☐ このネットワークのプロキシ設定を自動検出する(W)

☐ システムのプロキシ設定を利用する(U)

☒ 手でプロキシを設定する(M):

HTTP プロキシ(X): 127.0.0.1 ポート(P): 8080

☒ すべてのプロトコルでこのプロキシを使用する(S)

SSL プロキシ(L): 127.0.0.1 ポート(O): 8080

FTP プロキシ(F): 127.0.0.1 ポート(R): 8080

SOCKS ホスト(C): 127.0.0.1 ポート(T): 8080

☐ SOCKS v4(K) ☒ SOCKS v5(V) ☐ リモート DNS(D)

プロキシなしで接続(N):

例: .mozilla.org, .net.nz, 192.168.1.0/24

☐ 自動プロキシ設定スクリプト URL(A):

再読み込み(E)

☐ パスワードを保存してある場合は認証を確認しない(I)

OK キャンセル ヘルプ(H)

この状態で、ブラウザで適当なページアクセスしてみてください。もし設定がうまくいっていれば、[Proxy]-[HTTP history]にアクセスしたページに関するログが、どんどんと追加されているはずです。

Burp Suite Free Edition v1.7.03 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	M
57	https://cdn.desk.com	GET	/portal/desk.portal.body.layout_footer.js	<input type="checkbox"/>	<input type="checkbox"/>	200	7386	H
63	https://portswigger.net	GET	/burp/	<input type="checkbox"/>	<input type="checkbox"/>	200	4624	H
65	https://portswigger.net	GET	/js/slimbox2.js	<input type="checkbox"/>	<input type="checkbox"/>	200	72816	H
66	https://portswigger.net	GET	/js/jquery.js	<input type="checkbox"/>	<input type="checkbox"/>	200	6818	H
82	https://portswigger.net	GET	/burp/proxy.html	<input type="checkbox"/>	<input type="checkbox"/>	200	4624	H
85	https://portswigger.net	GET	/js/slimbox2.js	<input type="checkbox"/>	<input type="checkbox"/>	200	72816	H
87	https://portswigger.net	GET	/js/jquery.js	<input type="checkbox"/>	<input type="checkbox"/>	200	10309	H
99	https://portswigger.net	GET	/burp/download.html	<input type="checkbox"/>	<input type="checkbox"/>	200	6818	H
114	https://portswigger.net	GET	/burp/proxy.html	<input type="checkbox"/>	<input type="checkbox"/>	200	72816	H
123	https://portswigger.net	GET	/js/jquery.js	<input type="checkbox"/>	<input type="checkbox"/>	200	4624	H
125	https://portswigger.net	GET	/js/slimbox2.js	<input type="checkbox"/>	<input type="checkbox"/>	200	10790	H
143	https://portswigger.net	GET	/burp/successstories.html	<input type="checkbox"/>	<input type="checkbox"/>	200	6707	H
155	https://portswigger.net	GET	/burp/editions.html	<input type="checkbox"/>	<input type="checkbox"/>	200		

Request

Raw Headers Hex

```
GET /assets/tracking/settings/production-158454f93db4467614c0b03dd247b5b0.js HTTP/1.1
Host: cdn.desk.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0
Accept: */*
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate, br
Referer: https://support.portswigger.net/customer/portal/questions/16352823-settings-not-saved-in-project
Connection: close
```

### 3.3.3 設定の保存

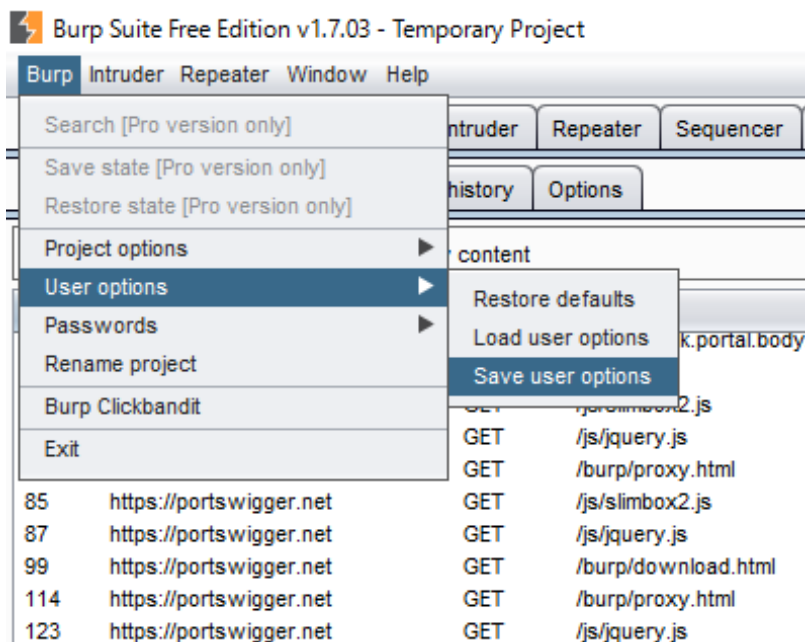
Burp Suite には、ユーザ設定とプロジェクト設定の 2 種類の設定があります。

ユーザ設定には、フォントなど UI の見た目、ホットキーなど操作に関する設定、上位プロキシ設定、拡張機能などユーザ固有の設定が含まれます。プロジェクト設定には、ターゲットスコープ、プロキシリスナー、リダイレクトやヘッダなど詳細な HTTP オプション、SSL 設定など、診断対象に関する設定が含まれます。

各設定はファイルに保存ができます。好みの設定を起動時に指定する場合や、設定を他人と共有する場合に便利です。

設定を全ての保存するには、Burp メニューから保存操作を行ってください。

- [Burp]メニュー-[User options]-[Save]
- [Burp]メニュー-[Project options]-[Save]



特定の設定だけ指定した保存または読み込みが可能です。保存したい設定項目にある、左側のオプションボタンをクリックし、[Save]または[Load]を選択してください。またこのオプションボタンから、個別設定項目のリセットも可能です。

## 4 診断方法について

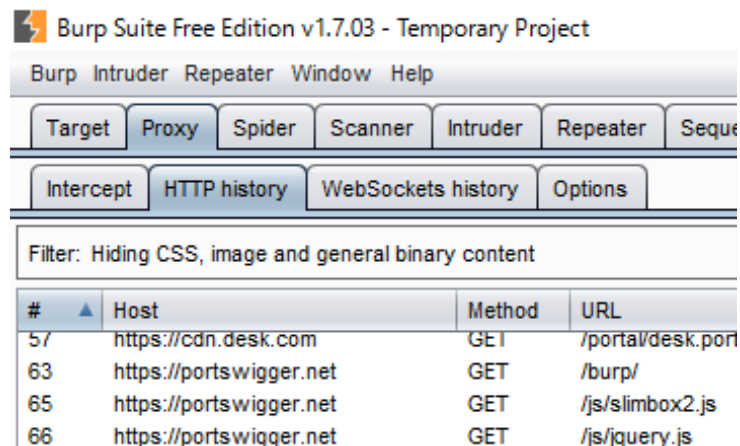
### 4.1 Proxy 機能

#### 4.1.1 Proxy を利用した通信キャプチャ

Burp Suite は、HTTP や HTTPS をブラウザと Web サーバの間で仲介し、通信内容の参照や書き換えができます。

#### 4.1.2 Proxy タブの構成

Proxy タブは複数のタブから構成されており、HTTP ログの履歴参照や Proxy 設定などが行えます。



#### タブ

#### 機能概要

Intercept	HTTP や WebSocket のリクエストやレスポンスをインターセプトし、内容の確認や変更が可能
-----------	--

HTTP history	Proxy を経由したすべての HTTP ログを参照可能
WebSockets history	Proxy を経由したすべての WebSockets ログを参照可能
Options	Proxy の稼働 IP アドレスやポートの設定、インターセプトの条件設定、HTTP ログの置換設定など

## 4.2 Burp Suite による通信のキャプチャ

### 4.2.1 通信をキャプチャしてみよう！

Burp Suite が稼働する IP アドレスおよびポートをブラウザで Proxy として適切に設定すると、Burp Suite はブラウザのリクエスト・レスポンスを仲介できます。3.3.2 の Proxy 設定が済んでいれば、ブラウザから任意の HTTP ページにアクセスしてみてください（HTTPS ページの場合は警告が出る場合があるので後述します）。

インターセプトがオンの場合、ブラウザからサーバへのリクエストは Burp Suite に止められてしまうため、レスポンスがなく、ブラウザは何も表示されません。[Forward]をクリックするか、[Intercept is On]をクリックして[Intercept is Off]にするとインターセプトされていたリクエストがサーバに送信され、ブラウザに Web ページが表示されます。

[Proxy]-[HTTP history]には、Burp Proxy が Proxy した HTTP ログが一覧で表示されます。以下の項目が表示されます。

- Host
- Method



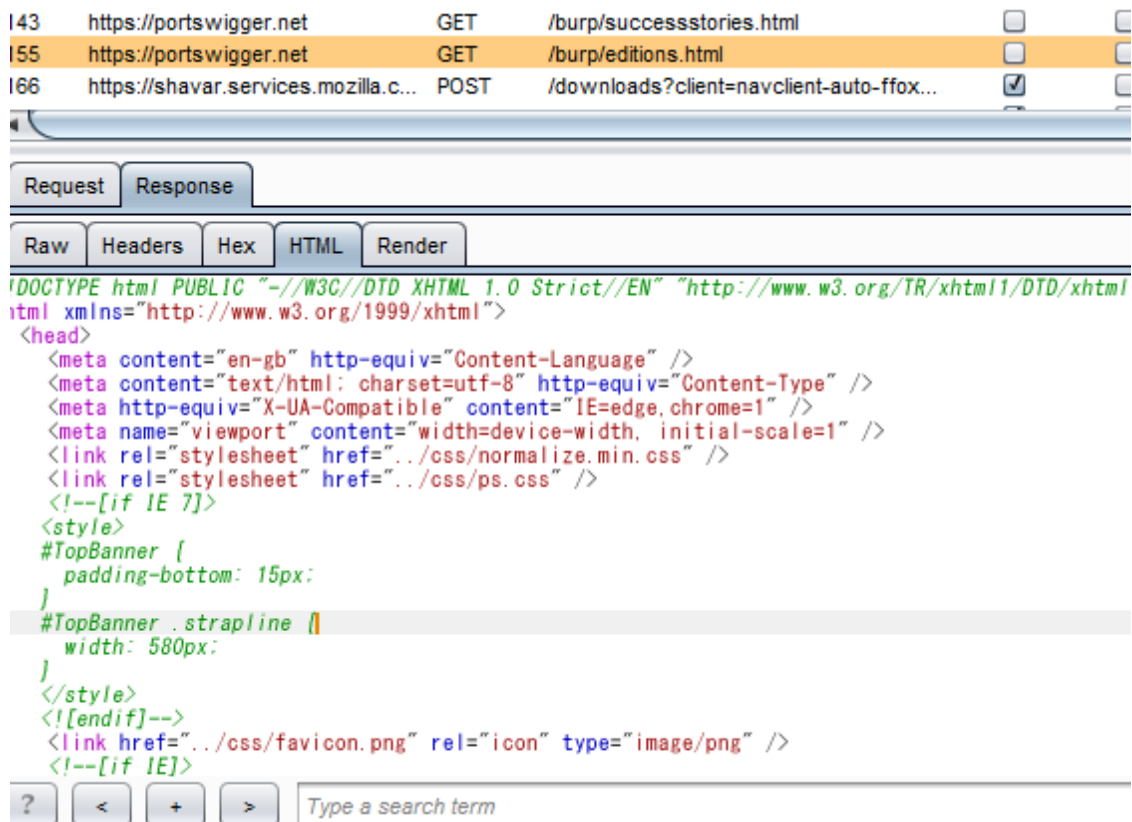
- URL
- Params
- Edited
- Status
- Length
- MIME type
- Extension
- title
- Comment
- SSL
- IP
- Cookies
- Time
- Listener port

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	P	Cookies
65	https://portswigger.net	GET	/js/limbox2.js		<input type="checkbox"/>	200	4624	script	js			<input checked="" type="checkbox"/>	54.246.133.196	
66	https://portswigger.net	GET	/js/jquery.js		<input type="checkbox"/>	200	72816	script	js			<input checked="" type="checkbox"/>	54.246.133.196	
82	https://portswigger.net	GET	/burp/proxy.html		<input type="checkbox"/>	200	6810	HTML	html	Burp Proxy		<input checked="" type="checkbox"/>	54.246.133.196	
85	https://portswigger.net	GET	/js/limbox2.js		<input type="checkbox"/>	200	4624	script	js			<input checked="" type="checkbox"/>	54.246.133.196	
87	https://portswigger.net	GET	/js/jquery.js		<input type="checkbox"/>	200	72816	script	js			<input checked="" type="checkbox"/>	54.246.133.196	
99	https://portswigger.net	GET	/burp/download.html		<input type="checkbox"/>	200	10309	HTML	html	Download Burp Suite		<input checked="" type="checkbox"/>	54.246.133.196	
114	https://portswigger.net	GET	/burp/proxy.html		<input type="checkbox"/>	200	6810	HTML	html	Burp Proxy		<input checked="" type="checkbox"/>	54.246.133.196	
123	https://portswigger.net	GET	/js/jquery.js		<input type="checkbox"/>	200	72816	script	js			<input checked="" type="checkbox"/>	54.246.133.196	
125	https://portswigger.net	GET	/js/limbox2.js		<input type="checkbox"/>	200	4624	script	js			<input checked="" type="checkbox"/>	54.246.133.196	
143	https://portswigger.net	GET	/burp/successstories.html		<input type="checkbox"/>	200	10790	HTML	html	Burp Suite Success Stori...		<input checked="" type="checkbox"/>	54.246.133.196	
155	https://portswigger.net	GET	/burp/editions.html		<input type="checkbox"/>	200	6707	HTML	html	Burp Suite Editions		<input checked="" type="checkbox"/>	54.246.133.196	
166	https://shavar.services.mozilla.c...	POST	/downloads?client=navclent-auto-ffox...		<input checked="" type="checkbox"/>	200	141	text				<input checked="" type="checkbox"/>	52.34.183.103	

また、各 HTTP ログを選択すると選択した HTTP ログのリクエストおよびレスポンスが下部に表示されます。Request タブおよび Response タブそれぞれに以下

のタブがあり、表示形式を変更して内容が確認できます。※1 は Request タブのみ、※2 は Response タブでのみ表示されます。

- Raw
- Params ※1
- Headers
- Hex
- HTML ※2
- Render ※2



[HTTP history]の一覧の各カラムをクリックすると降順または昇順での並び替えができます。例えば[Params]をクリックすると HTTP ログの中でパラメータが存在する HTTP ログが上部に表示されます。Filter をクリックし条件を設定すると、それに応じて表示する HTTP ログをフィルタできます。正規表現でのフィルタ機能はプロフェッショナル版でのみ利用可能です。

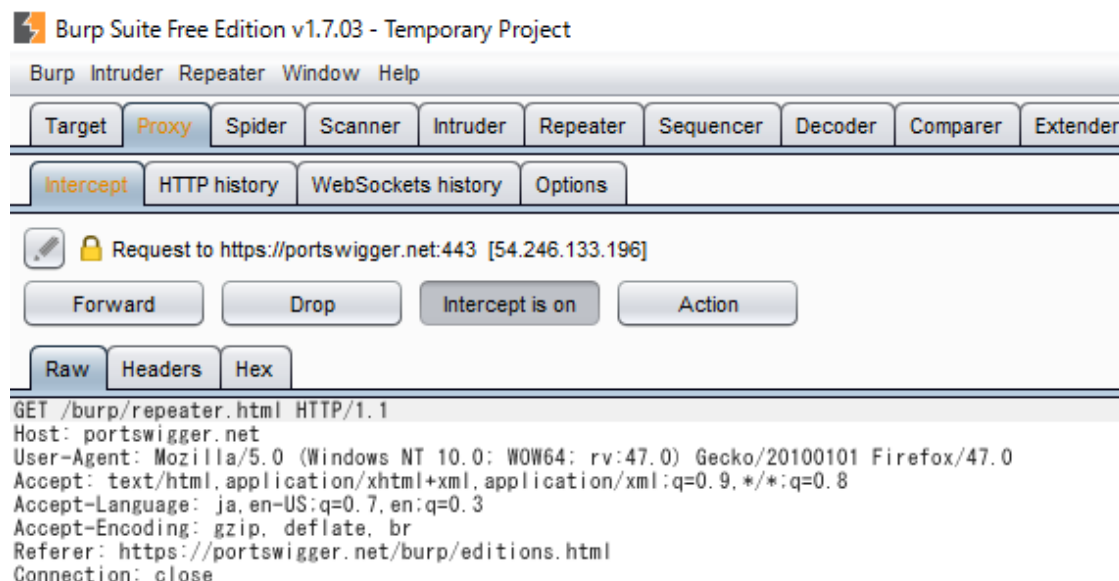
設定	設定内容
Filter by request type	スコープ内のログ、パラメータが存在するリクエストなどが指定できます。
Filter by MIME type	HTML・CSS・Script などの MIME タイプを指定できます。
Filter by status code	レスポンスのステータスコードを指定できます。
Filter by file extension	URL の拡張子が指定できます。
Filter by annotation	HTTP ログにコメントまたは色づけしたもののみ表示できます。

#### 4.2.2 値を書き換えて送信してみよう！

リクエスト・レスポンスの内容を変更する場合はインターセプトする必要があります。リクエストを改変する場合は[Intercept is On]でインターセプトしたリクエストの内容を変更します。POST データを変更した場合 Content-Length ヘッ

ダの値と不整合が起こる場合がありますが、Burp Suite が変更後の内容をもとに Content-Length を再計算しセットするため、意識する必要はありません。

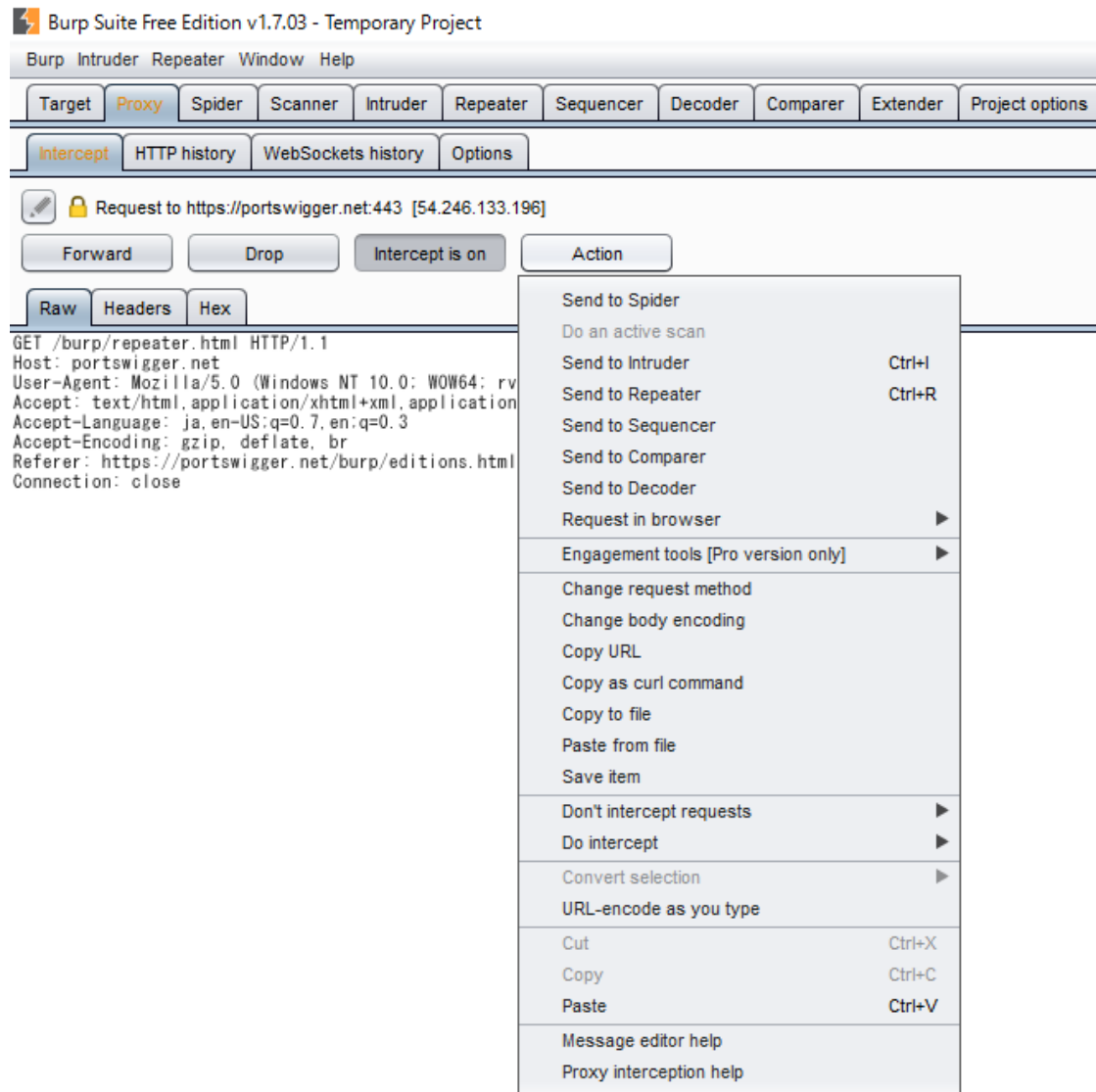
[Forward]はインターセプトしたリクエストをサーバへ送信します。複数のリクエストがインターセプトされている場合、1 リクエストごとに[Forward]をクリックする必要があります。



[Drop]はインターセプトしたリクエストを破棄します。サーバへは送信されません。


[Intercept is On]/[Intercept is Off]でインターセプトをするかどうかを設定します。ステータスを[Intercept is Off]に変更するとインターセプトされているすべてのリクエストがサーバに送信されます。

[Actions]では、特定の条件のリクエストをインターセプトしない設定やレスポンスを設定するなど、インターセプトしたリクエストに対するアクションが設定できます。



インターセプトしてリクエストの内容を変更した場合、[Proxy]-[HTTP history]の該当ログで[Edited]がチェックされます。また、下部のタブに[Original

request]と[Edited request]が表示され、変更前と変更後のリクエストの内容が確認できます。レスポンスを変更した場合は[Original response]と[Edited response]が表示され、変更前と変更後のレスポンスが確認できます。

 Burp Suite Free Edition v1.7.03 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Ed
85	https://portswigger.net	GET	/js/slimbox2.js	<input type="checkbox"/>	
87	https://portswigger.net	GET	/js/jquery.js	<input type="checkbox"/>	
99	https://portswigger.net	GET	/burp/download.html	<input type="checkbox"/>	
114	https://portswigger.net	GET	/burp/proxy.html	<input type="checkbox"/>	
123	https://portswigger.net	GET	/js/jquery.js	<input type="checkbox"/>	
125	https://portswigger.net	GET	/js/slimbox2.js	<input type="checkbox"/>	
143	https://portswigger.net	GET	/burp/successstories.html	<input type="checkbox"/>	
155	https://portswigger.net	GET	/burp/editions.html	<input type="checkbox"/>	
166	https://shavar.services.mozilla.c...	POST	/downloads?client=navclient-auto-ffox...	<input checked="" type="checkbox"/>	
167	https://shavar.services.mozilla.c...	POST	/downloads?client=navclient-auto-ffox...	<input checked="" type="checkbox"/>	
168	https://portswigger.net	GET	/burp/repeater.html	<input type="checkbox"/>	
170	https://portswigger.net	GET	/js/slimbox2.js	<input type="checkbox"/>	
172	https://portswigger.net	GET	/js/jquery.js	<input type="checkbox"/>	

Original request Edited request Response

Raw Headers Hex

GET /burp/repeater.html HTTP/1.1  
Host: portswigger.net  
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0  
Connection: close

## 4.3 その他

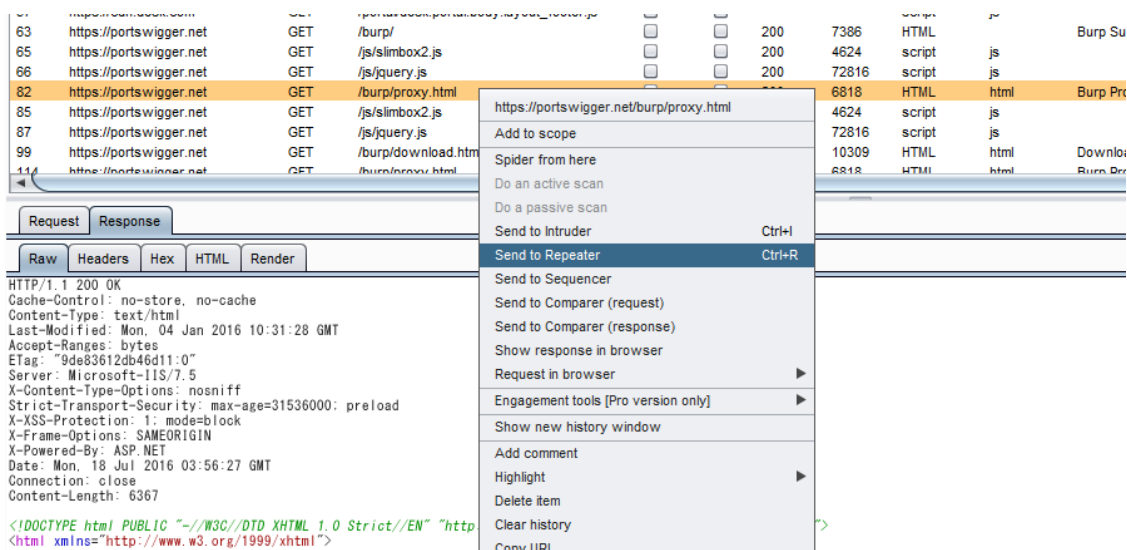
### 4.3.1 リクエストの再送信

診断では、リクエストを多数送信します。Repeater を使用すると、HTTP History に記録されているリクエストの再送信や、新規に作成したリクエストの送信ができます。

#### 4.3.1.1 History からリクエストの送信

History に記録されている既存のリクエストを Repeater で使用するには、次のように操作してください。

1. Repeater に送信したいリクエストを[HTTP History]で選択します。
2. 右クリックしコンテキストメニューから[Send To Repeater]を選択し、Repeater にリクエストを送信します。
3. Repeater を開きます。



#### 4.3.1.2 リクエストの新規作成

既存のリクエストは元にせず、新規にリクエストを指定するには、次のように操作してください。

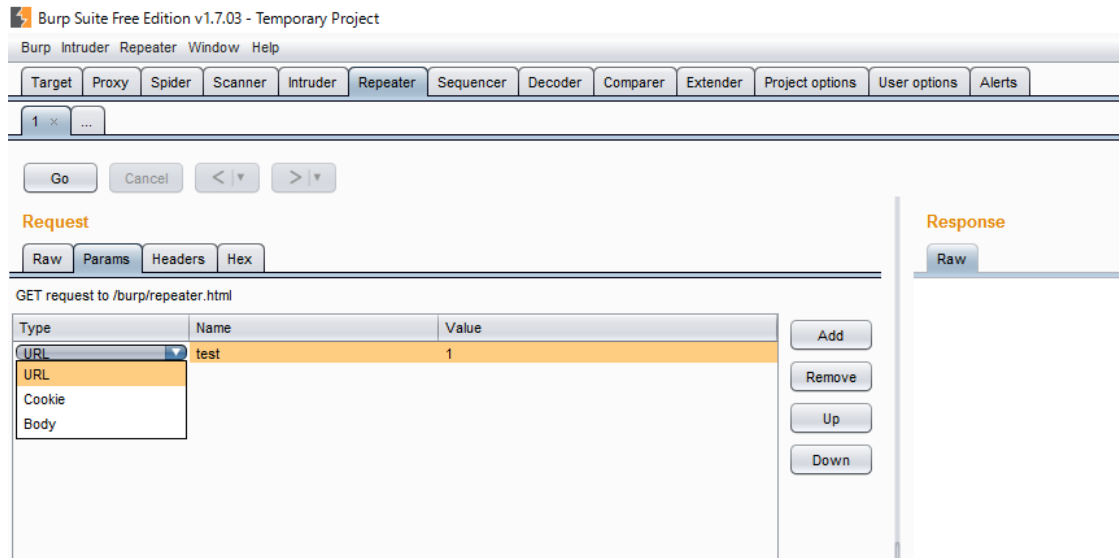
1. Repeater の[...]タブを選択します。
2. 右上にある[Target]をクリックします。
3. 接続先を入力する画面が表示されたら、[Host]と[Port]を入力し、[OK]ボタンを押します。HTTPS での接続を行う場合は、[Use HTTPS]にチェックを入れます。

#### 4.3.1.3 リクエストの編集、送信

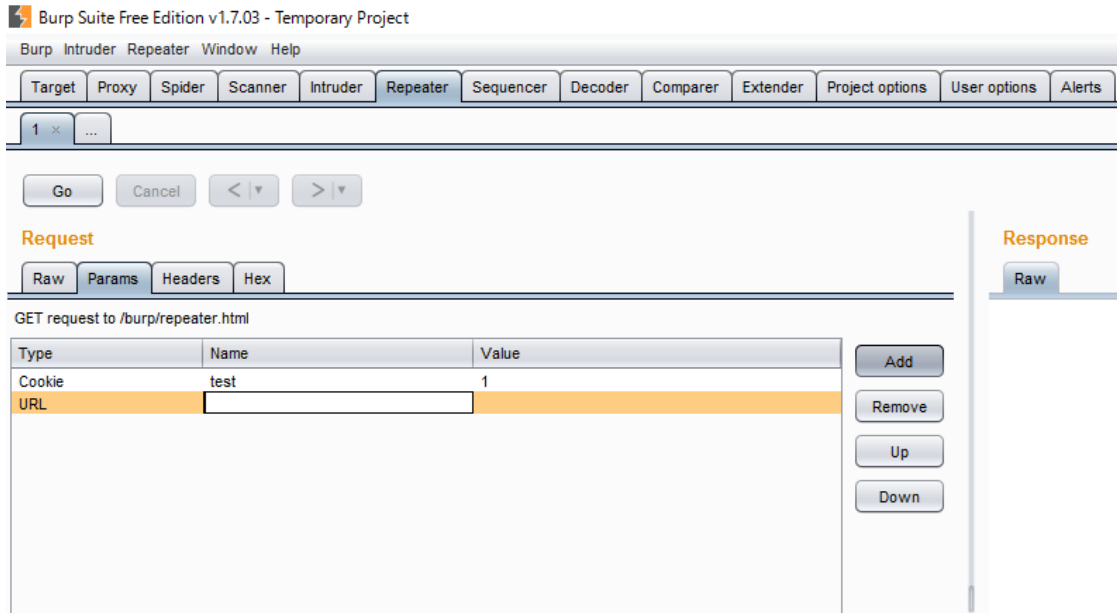
1. 編集したいリクエストのタブを選択します。
2. [Request]の[RAW]タブでは HTTP リクエストを直接編集できます。



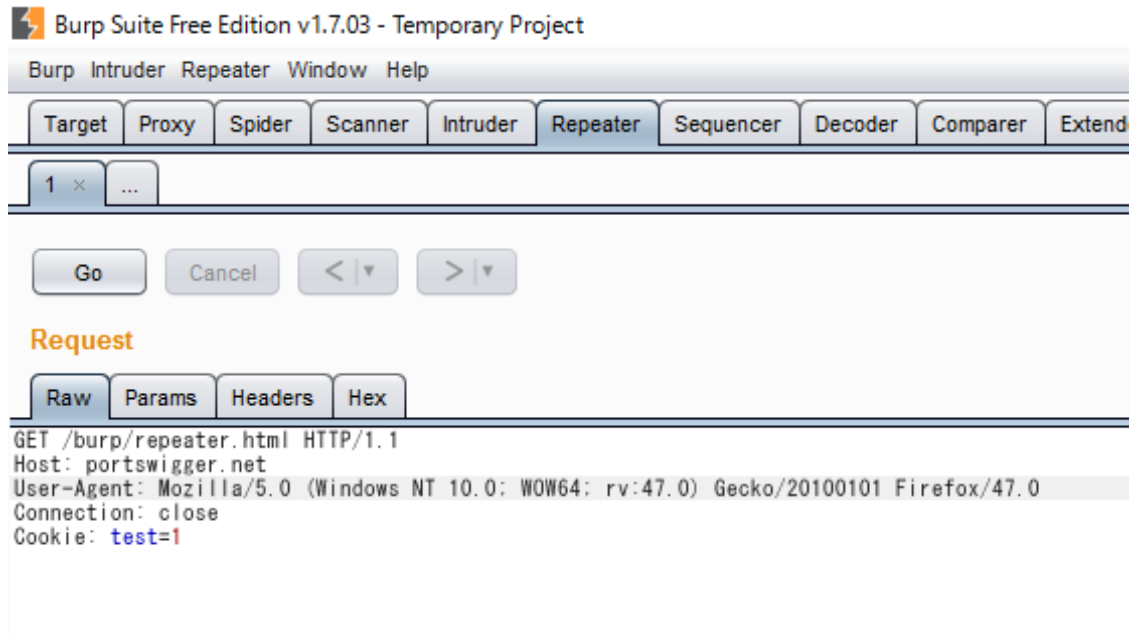
[Request]-[Params]タブではパラメータを表形式で表示し、変更できます。  
[Type]を変更すると、パラメータの位置を変更できます。例えば、[Type]を  
[Body]から[Cookie]に変更すると、ボディパラメータを Cookie に移動できます。



[Add]ボタンを押すとパラメーターを追加できます。[Remove]ボタンを押すと選  
択しているパラメーターを削除できます。[Up]ボタン、[Down]ボタンを押すと  
パラメーターを送信する順番を変更できます。

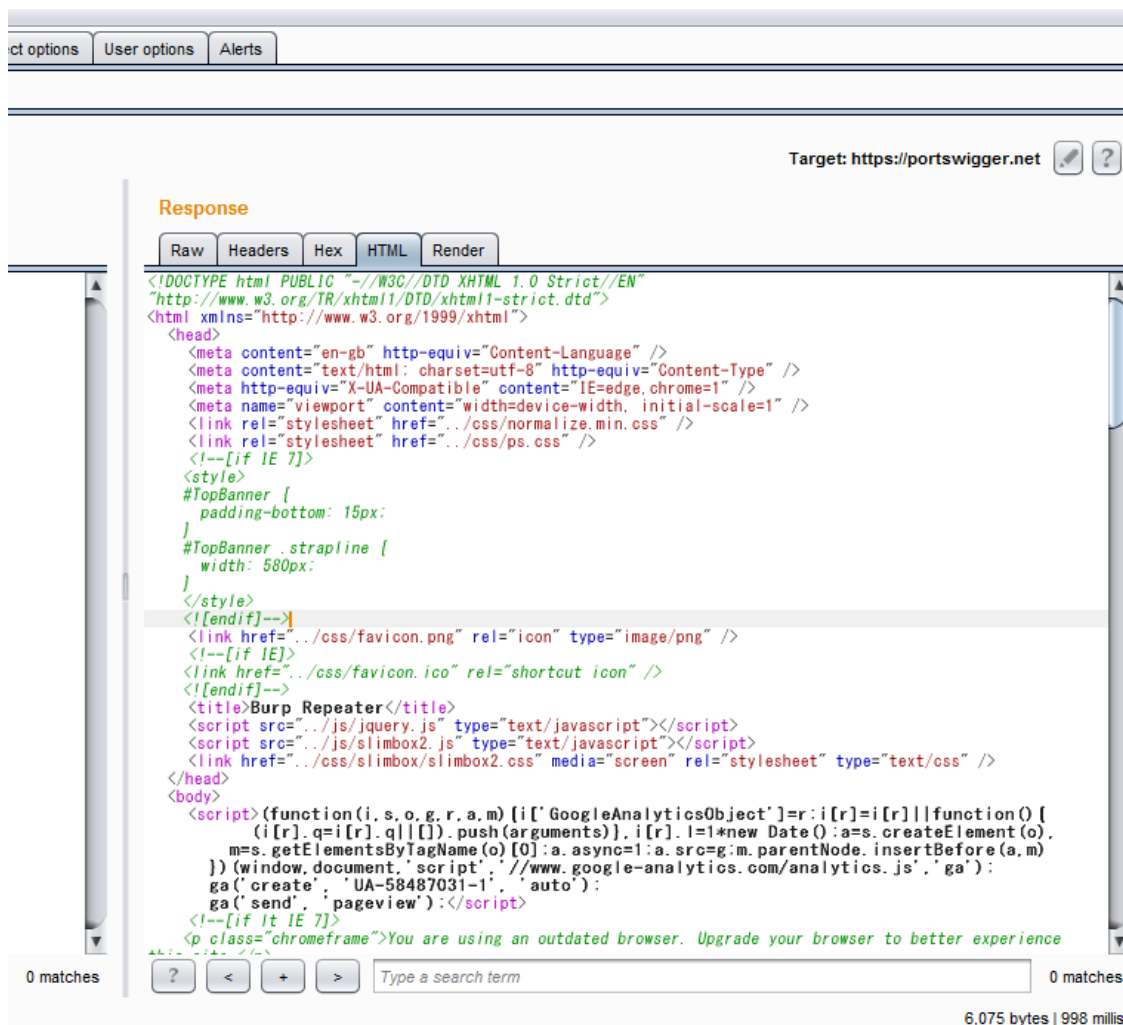


[Request]-[Headers]タブではヘッダーを表形式で表示し、変更できます。  
[Add]ボタンを押すとヘッダーを追加できます。[Remove]ボタンを押すと選択しているヘッダーを削除できます。[Up]ボタン、[Down]ボタンを押すとヘッダーを送信する順番を変更できます。 [Request]-[Hex]タブではリクエストを Hex で確認、編集できます。 3. 右上にある「Target」をクリックすると、接続先を変更できます。 4. [Go]ボタンを押し、リクエストを送信します。



#### 4.3.1.4 レスポンスの確認

1. 「Response」の「Raw」タブでは生の HTTP レスポンスを確認できます。
2. 「Response」の「Headers」タブではヘッダーを表形式で表示します。  
[Response]-[Hex]タブではレスポンスを Hex で表示します。 [Response]-[Render]タブでは Response が HTML の場合、レスポンスをレンダリングし表示します。



### 4.3.2 Scope 設定

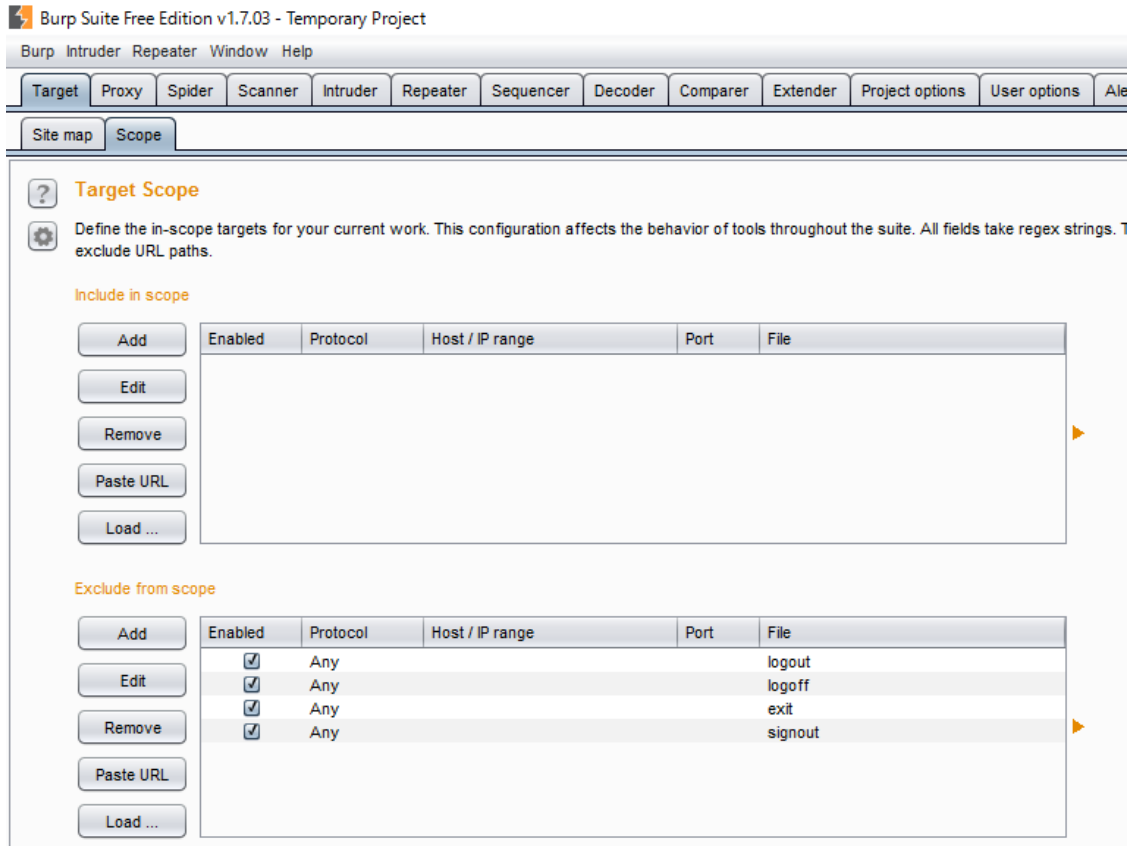
診断対象外のアプリケーションに対して診断を実施してはいけません。誤って診断対象外のサーバーや URL を診断しないように Scope を設定します。Scope を設定すると、Burp Suite の動作に以下のような制限がかかります。

- Scope で設定した条件を満たすリクエストのみを Proxy History に表示するようフィルタを設定できます。

- Scope で設定した条件を満たすリクエストのみを Intercept して、リクエストの改ざんができます
- Scope で設定した条件を満たさないリクエストを Spider の開始 URL としてしようとすると、Scope に追加するか確認するポップアップが表示されます。

対象	動作
Include in scope	記述された条件はスコープ内として認識されます。
Exclude from scan	記述された条件を満たすリクエストはスコープ外として認識されます。

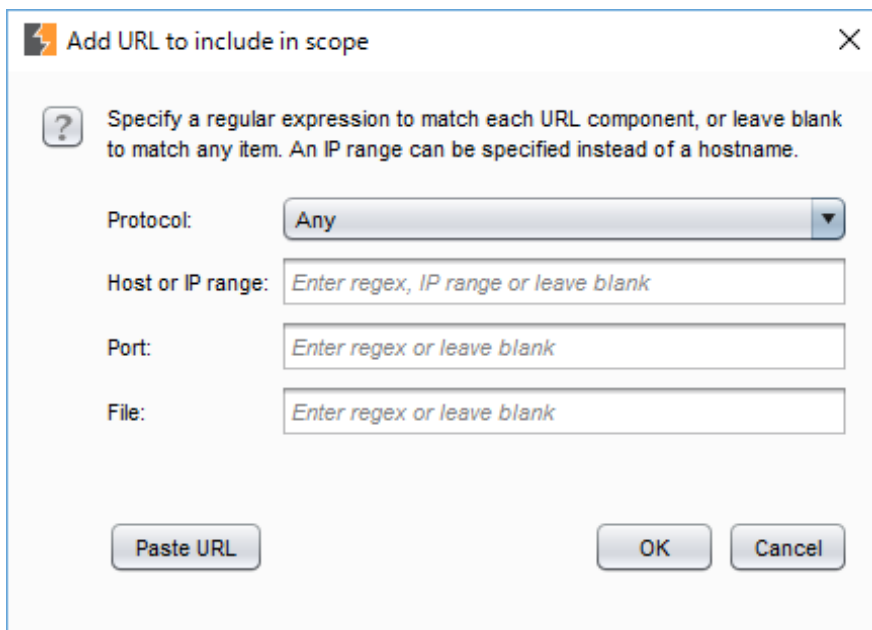
デフォルトで、[Exclude from scan]に 4 つ設定されています。これは、Spider(自動巡回する機能)を実行した際に、ログアウトしてセッションが無効化されないようにログアウト機能と推測される文字列を含む URL にはアクセスしようようにしているためです。



#### 4.3.2.1 Scope への追加

Scope の追加は 3 つ方法があります。 1. [Add]ボタンを使用する 2. [Paste URL]ボタンを使用する 3. HTTP history などから[Add to scope]を使用する

[Add]ボタンを使用する 1. [Add]ボタンを押します。 2. [Host or IP range]、[Port]、[File]を正規表現で記述します。 3. [OK]ボタンを押します。



**Add URL to include in scope**

? Specify a regular expression to match each URL component, or leave blank to match any item. An IP range can be specified instead of a hostname.

Protocol: Any

Host or IP range: Enter regex, IP range or leave blank

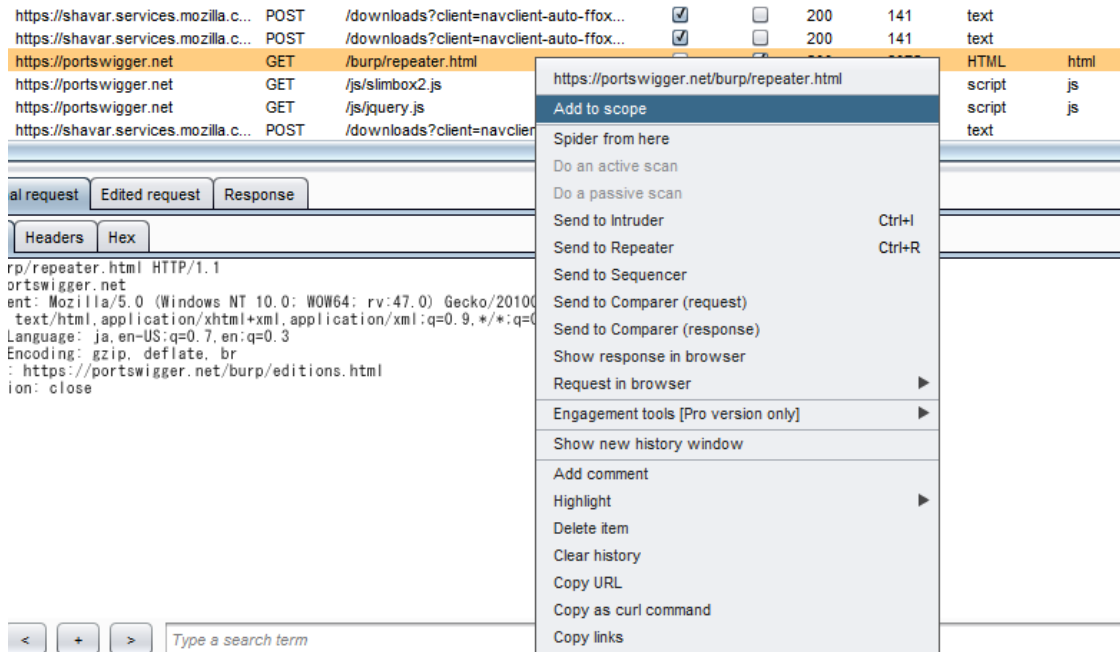
Port: Enter regex or leave blank

File: Enter regex or leave blank

Paste URL OK Cancel

[Paste URL]ボタンを使用する 1. Scope に追加したい URL を、クリップボードにコピーします。 1. [Paste URL]ボタンを押します。

「Add to scope」ボタンを使用する 1. スコープに含めたい HTTP ログを選択します。 2. 右クリックしコンテキストメニューから、[Add to scope]をクリックします。



## パターン

## 設定内容

診断対象が

www.example.com で URL  
やプロトコルが事前に分から  
ない場合

[Include in scope]で[Host or IP range]に  
^www.example.com\$と設定します。[Port]や  
[File]などの他の項目を設定しない場合、  
www.example.com に対するリクエストはすべ  
て許可されます。

診断対象が 192.0.2.1 で

/sample/以下のパスに対して  
実施する場合

[Include in scope]で[Host or IP range]に  
192.0.2.1\$を、[File]に/sample/を設定しま  
す。http、https の/sample/配下にあるコンテ  
ンツすべてがスコープ内になります。

診断対象が

www.example.com で  
/sample/以下のパスで

[Include in scope]で[Host or IP range]に  
www.example.com\$を、[File]に/sample/を設定します。[Exclude in  
scope]で[File]に/sample/exclude/を設定します。



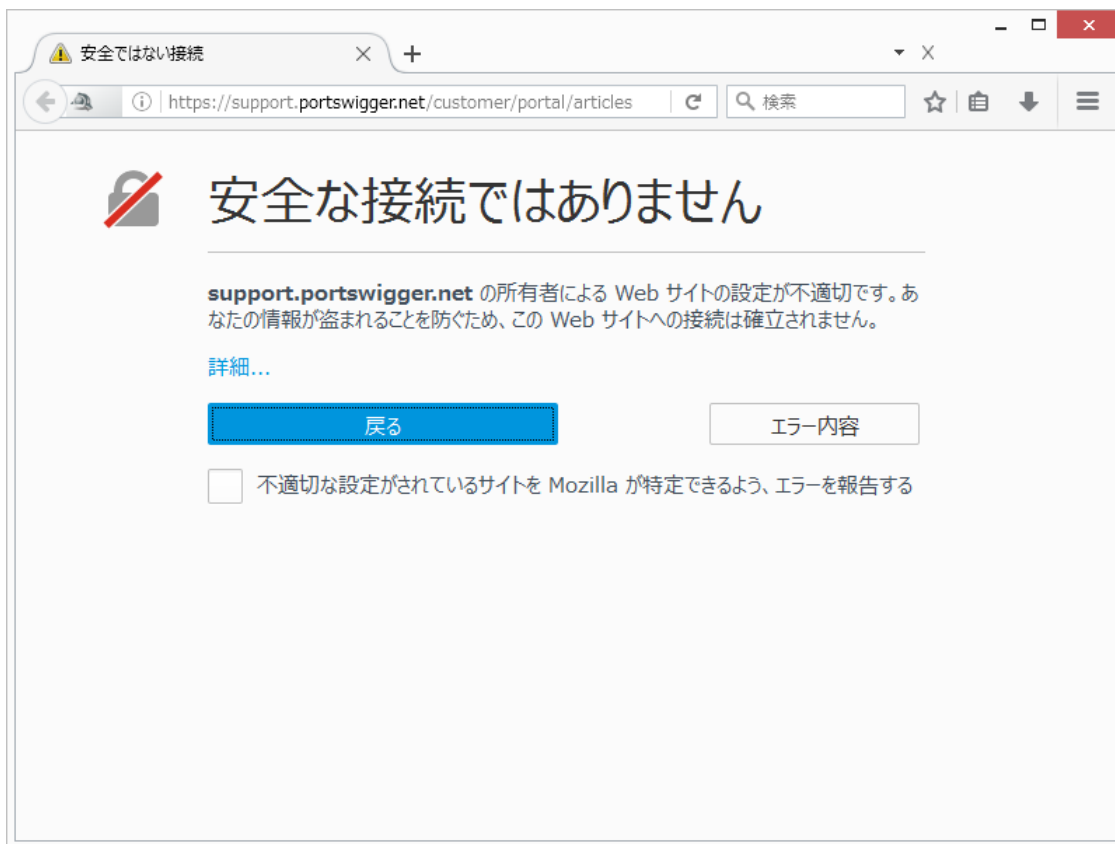
/sample/exclude/を除いて実施する場合

#### 4.3.2.1 Scope からの削除

1. 削除したい条件を選択します。
2. 「Remove」ボタンを押します。

#### 4.3.3 サーバ証明書設定

暗号化通信（https://～）が必要な Web アプリケーションに、デフォルト設定の Burp Suite でアクセスすると、ブラウザは不正であることを伝えるセキュリティ警告画面を表示します。



セキュリティ警告画面が表示される原因は、Burp Suite が起動時に独自に生成した CA 証明書により署名された自己署名証明書を接続に使用しているためです。

一時的に例外として Burp Suite 独自の証明書を受け入れると、Burp Suite 上で暗号化されている通信内容を平文で確認することが可能になります。しかし、警告のたびに操作をするのは煩わしいうえに、Web アプリケーションの設定によっては、自己署名証明書を使用して接続できない場合があります。

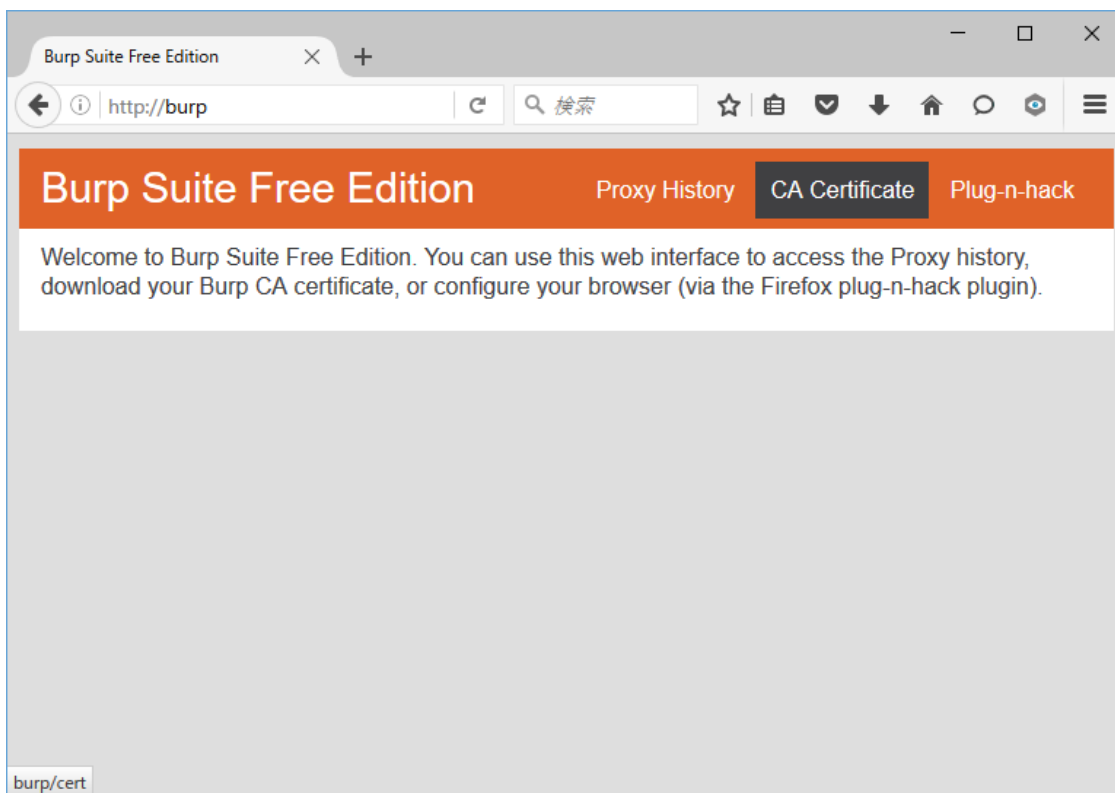
そのため、暗号化通信を効率よく取り扱うために、Burp Suite の独自 CA 証明書を OS あるいはブラウザにインポートする必要があります。

なお、Firefox は CA 証明書を独自に管理しています。そのため、Windows と OS X および Firefox の 3 パターンについて解説します。

### 独自 CA 証明書の保存

すべてのパターンで共通する操作は Burp Suite が生成した独自 CA 証明書の保存です。

1. ブラウザのプロキシ設定が Burp Suite に接続するようになっていることを確認
2. <http://burp/> にアクセスして「CA certificate」リンクをクリック
3. 任意の名前で CA 証明書を保存



## Windows

1. Windows の「インターネットオプション」 (inetcpl.cpl) → 「コンテンツ」 → 「証明書」 ボタンをクリック
2. 「インポート...」 をクリックして証明書ファイルを選択し、証明書ストアから「信頼されたルート証明機関」を選択してインポート
3. 「セキュリティ警告」ダイアログで「はい」をクリック

## OS X

OS X の場合は「キーチェーンアクセス」アプリにより設定します。

1. 「Launchpad」 → 「その他」 から「キーチェーンアクセス」アプリを起動
2. 左上の南京錠が閉じている場合はクリックしてパスワードを入力してロックを解除
3. 「キーチェーン」で「ログイン」を選択し、「分類」で「証明書」を選択
4. 「ファイル」 → 「読み込む...」で保存した CA 証明書を読み込み
5. 読み込んだ「PortSwigger CA」をダブルクリック
6. 「▶信頼」を展開し、「この証明書を使用するとき」プルダウンリストで「常に信頼」を選択
7. パスワードを入力して「設定をアップデート」ボタンをクリック

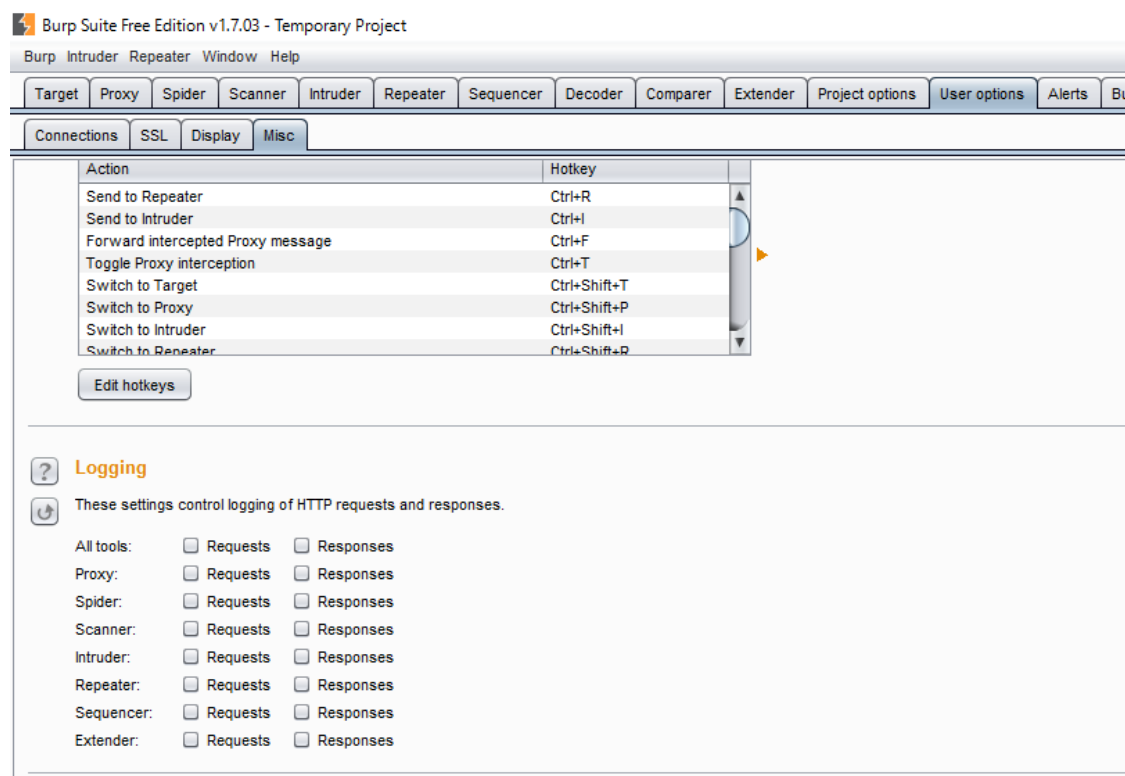
## Firefox

1. ブラウザの設定「オプション」 → 「詳細」 → 「証明書」 → 「証明書を表示...」をクリックで「証明書マネージャ」を表示
2. 「インポート...」 ボタンをクリックして保存した証明書を「開く」
3. 「証明書のインポート」ダイアログで「この認証局による Web サイトの識別を信頼する」にチェックを入れて「OK」ボタンをクリック

### 4.3.4 ログ保存設定

フリー版でログを保存するには、[User Options]-[Misc]-[Logging]で[All tools]の[Request]と[Response]をチェックします。するとリクエストおよびレスポンスが、指定されたファイルにテキスト形式で保存されます。[All tools]は一部の例外を除き Burp Suite を用いてアクセスしたログがすべて保存されます。

なおプロフェッショナル版ではこれに加え、Project ファイル(v1.6 以前は state ファイル)で HTTP ログなどの保存や復元が可能です。



ヘッダとしてアクセス時刻・プロトコル・ドメインなどが出力されます。リクエストとレスポンスは===で分離して出力されます。

```
=====
=====
22:32:54 https://portswigger.net:443 [54.246.133.196]
=====
=====
GET / HTTP/1.1
Host: portswigger.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:47.0) Gecko/20100101
Firefox/47.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate, br
Connection: close

=====
=====
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache
Content-Type: text/html
Last-Modified: Thu, 12 May 2016 14:38:34 GMT
Accept-Ranges: bytes
ETag: "0515f65bacd11:0"
Vary: Accept-Encoding
Server: Microsoft-IIS/7.5
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; preload
X-XSS-Protection: 1; mode=block
```

X-Frame-Options: SAMEORIGIN

X-Powered-By: ASP.NET

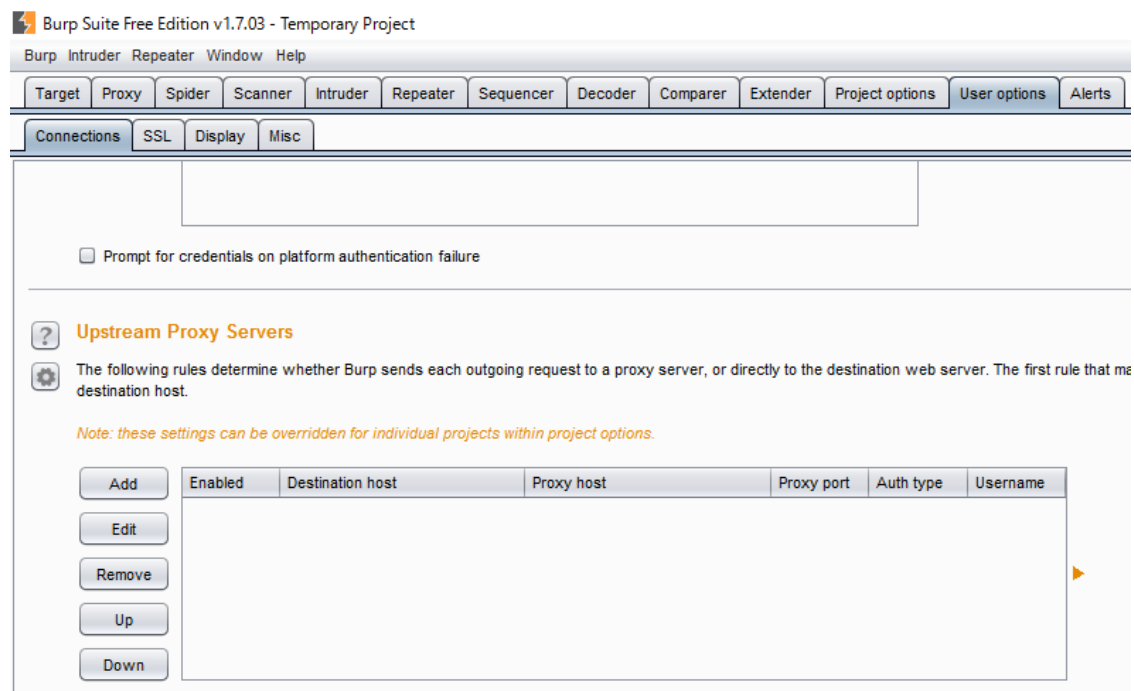
Date: Sun, 03 Jul 2016 13:32:54 GMT

Connection: close

Content-Length: 7012

### 4.3.5 アップストリーム Proxy 設定

Burp Suite は、アップストリーム Proxy(上位にある Proxy)の指定をする機能を持っています。企業などのネットワークでインターネット接続のため Proxy を経由する必要がある場合には、これを設定する必要があります。また、Burp Suite のフリー版ではログの保存機能が十分ではないため、ZAP や Fiddler などの別のローカル Proxy を指定して、ログを保存するなどの活用方法があります。



*Upstream Proxy* の設定

[User Options]-[Connections]-[Upstream Proxy Server]で[Add]をクリックすると[Add upstream proxy rule]が表示されます。アップストリーム Proxy は複数設定することができますが、[Destination host]の条件に最初に合致したアップストリーム Proxy を利用します。

設定内容	
Destination host	Proxy する対象に応じてアップストリーム Proxy を変更する場合にドメイン名などを設定します。Proxy するすべてのリクエストを特定のアップストリーム Proxyで行う場合は*(アスタリスク)を設定します。
Proxy host	アップストリーム Proxy が稼働する Host の IP アドレスなどを設定します。
Proxy port	アップストリーム Proxy が稼働するポート番号を設定します。
Authentication type	アップストリーム Proxy へのアクセスに認証が必要な場合に認証方法に応じて選択します。選択可能な認証方法は、Basic・NTLMv1・NTLMv2・Digest です。
Username	認証のユーザ名を設定します。
Password	認証のパスワードを設定します。
Domain	NTLM 認証のドメイン名を設定します。
Domain hostname	NTLM 認証のドメインコントローラのホストを設定します。



**Add upstream proxy rule**

Enter the details of the upstream proxy rule. You can use wildcards to specify destination hosts (\* matches zero or more characters, ? matches any character except a dot). Leave the proxy host blank to connect directly for the specified destination host.

Destination host:

Proxy host:

Proxy port:

Authentication type:

Username:

Password:

Domain:

Domain hostname:

### 4.3.6 Intruder

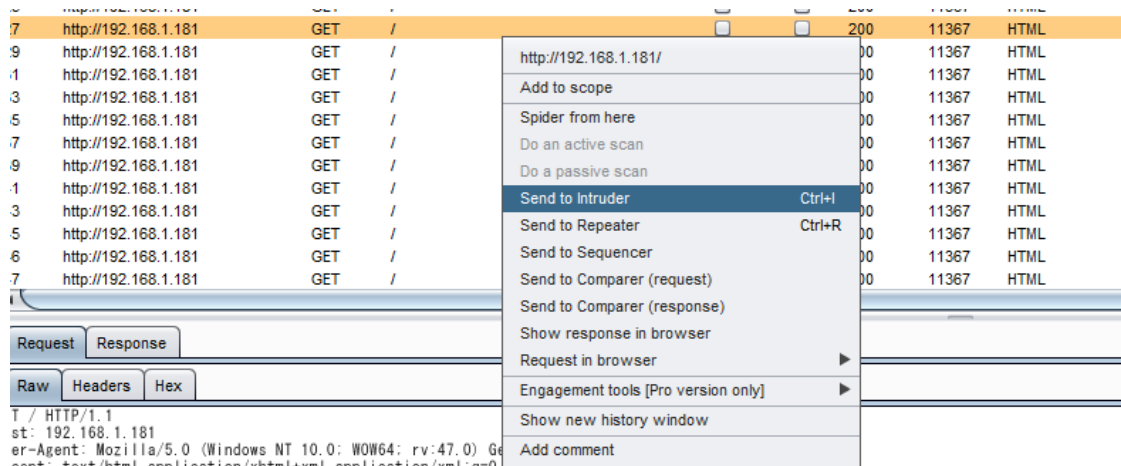
Intruder は、任意のリクエストを元に、SQL インジェクションや XSSなどを診断するためのパターンなど事前に設定されたパターンに沿ってリクエストを生成・送信することで、自動的に診断を行う機能です。設定されたパターンを自動的に送信するため、入力ミスがなく診断を確実に実施できます。

パターンを挿入するパラメータの指定や、脆弱性有無の確認は、人間がリクエストやレスポンス内容を確認して判断する必要があります。プロフェッショナル版

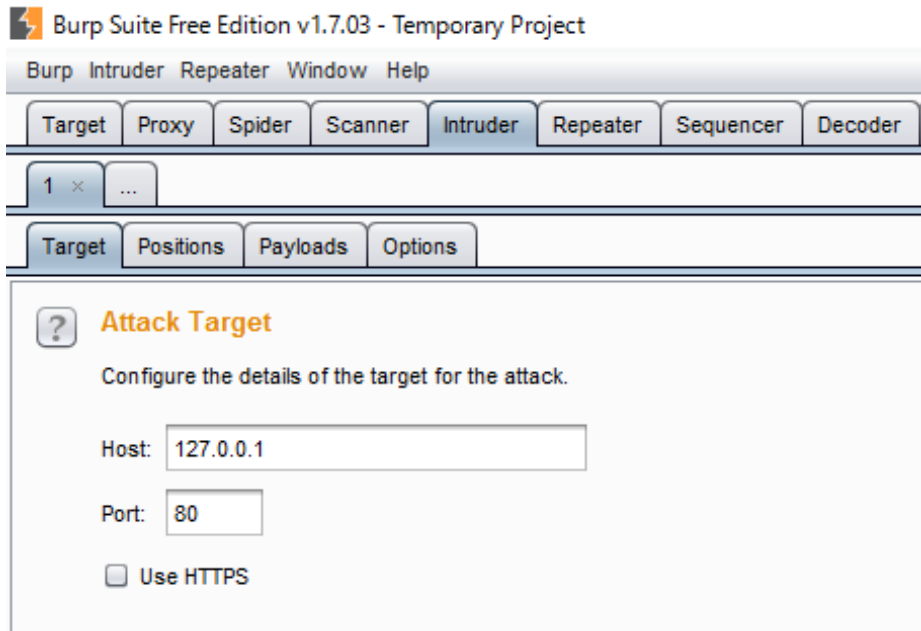
で利用可能な Scanner はパラメータの自動認識、結果判定を自動的に行うため、Intruder とはこの点において差があります。

#### 4.3.6.1 診断のやり方

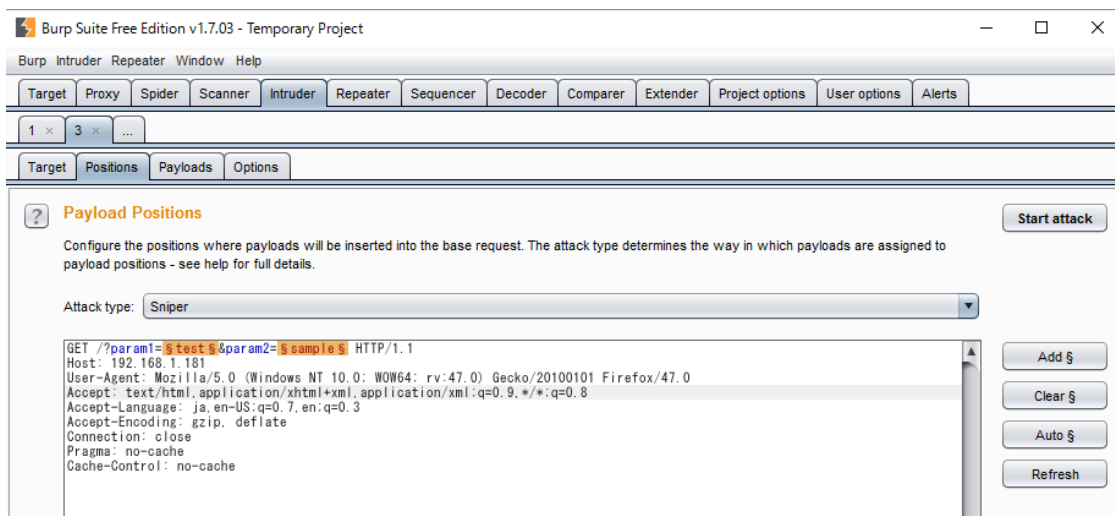
Intruder で送信する元となるリクエストを[Proxy]-[HTTP History]タブで選択します。右クリックしコンテキストメニューから[Send To Intruder]を選択し、Intruder にリクエストを送信します。



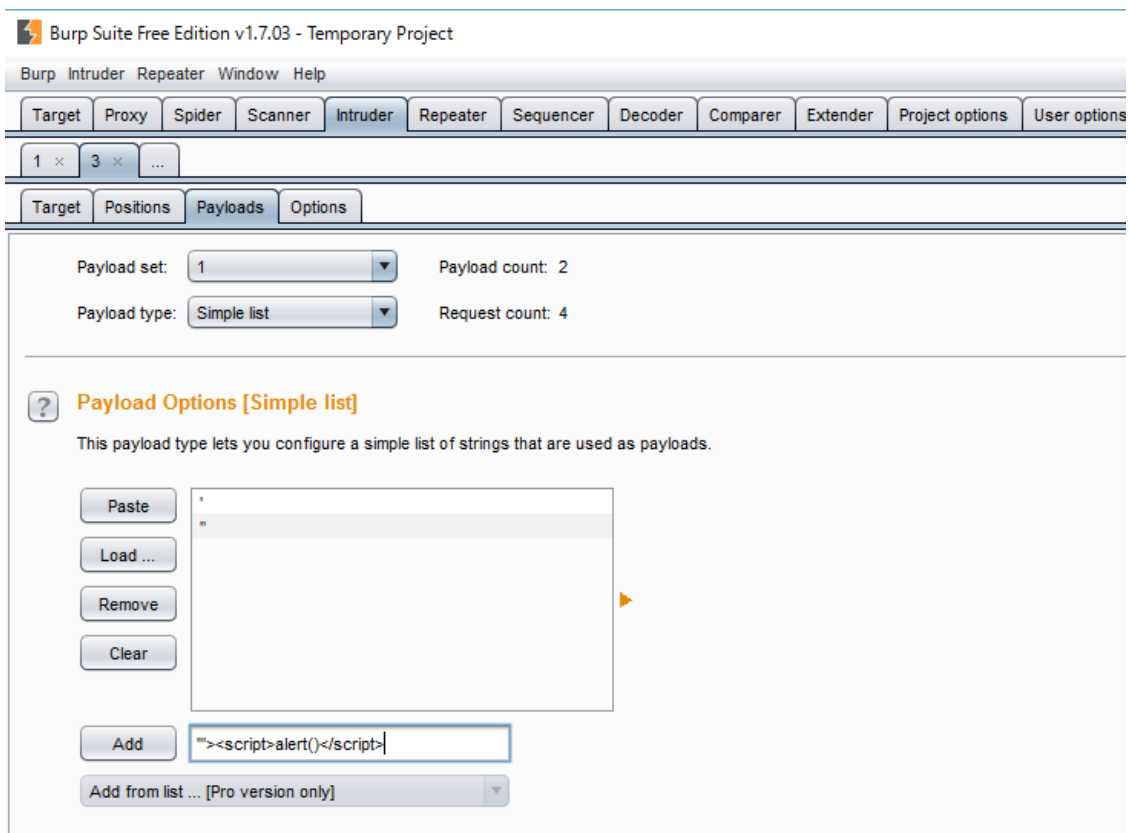
対象とするホストなどを変更する場合、[Intruder]-[Target]タブで[Host]や[Port]を変更します。HTTPS での接続を行う場合は、[Use HTTPS]にチェックを入れます。



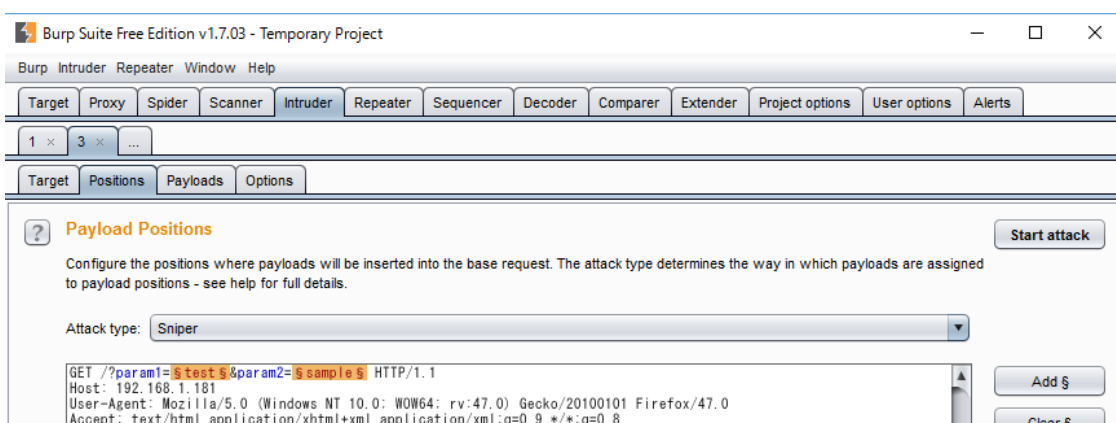
[Intruder]-[Positions]タブをクリックします。[Send To Intruder]で対象リクエストを入力した場合、診断箇所は自動的に[§]が囲まれます。追加したい場合、診断したい箇所を選択し、[Add §]をクリックします。診断箇所は複数選択することが可能です。[Auto §]で自動的に診断箇所の設定が可能で、URL クエリー・リクエストボディ・Cookie・マルチパートのパラメータ・XML データやエレメント、JSON を自動的に認識します。



[Intruder]-[Payloads]タブをクリックします。[Payload Options]で診断したいパターンを設定します。改行区切りのテキストの読み込みやパターンを1つずつ入力することも可能です。また、[Payload Encoding]でURL エンコードする文字を設定できます。

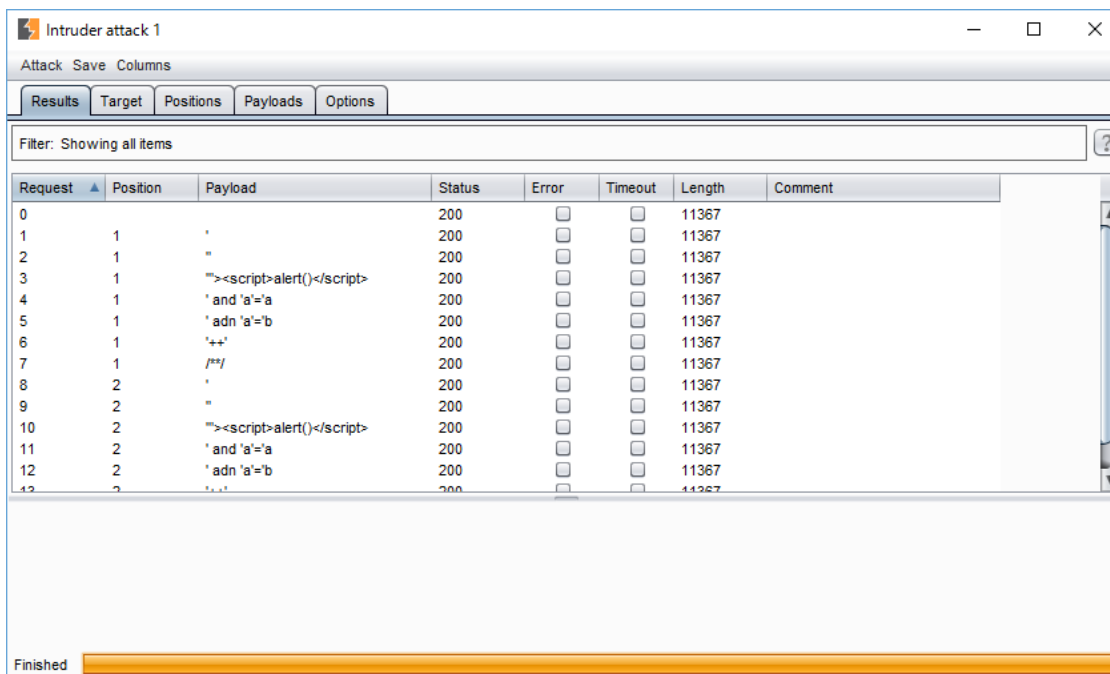


右上にある[Start attack]をクリックします。



### 4.3.6.2 結果の確認方法

Intruder が実行されると実行ウィンドウが表示されます。診断箇所へ診断パターンを送信した結果が[Results]に一覧で表示されます。各カラム名をクリックしてソートが可能です。



カラム	内容
-----	----

Request	診断したリクエストの番号。0 は Intruder にセットした元のリクエスト。
---------	--

Position	診断箇所の番号
----------	---------

Payload	診断パターン
---------	--------

Status	レスポンのステータスコード
--------	---------------

Error	リクエスト時のエラー有無
-------	--------------

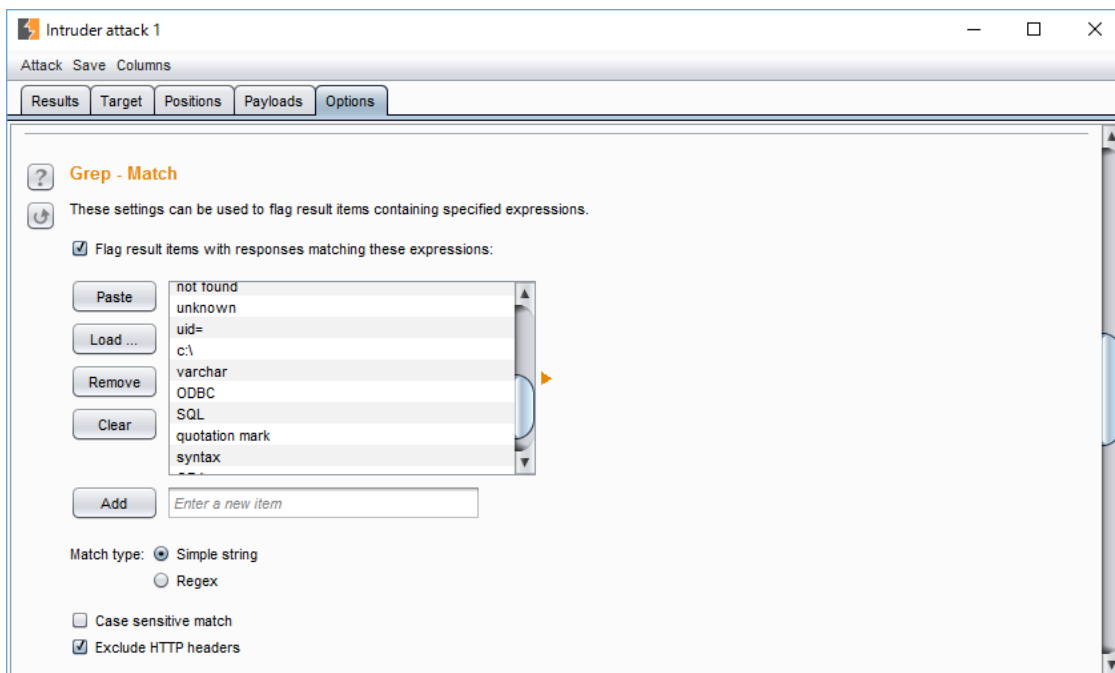
Timeout レスポンスのタイムアウト有無

Length レスポンスの byte 数

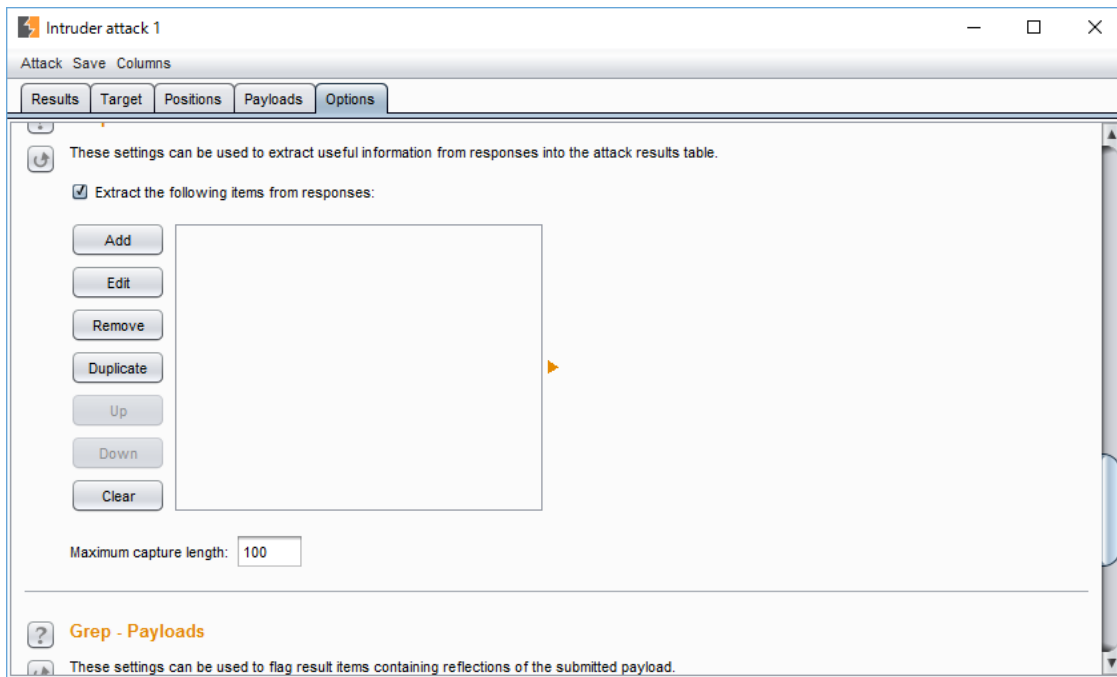
Comment コメントの記載

一覧で任意のログを選択するとウィンドウ下部の[Request]、[Response]タブにそれぞれの結果が表示されます。また、結果分析の補助機能として[Options]に[Grep - Match]と[Grep - Extract]があります。

[Grep - Match]は特定の文字列を指定し、レスポンス中に該当の文字列が含まれているかを確認するための機能です。[Flag result items with response matching these expressions]をチェックすると[Grep - Match]が有効化されます。設定を有効化すると[Go attack]実行後でも、該当の文字列が含まれるか確認できます。

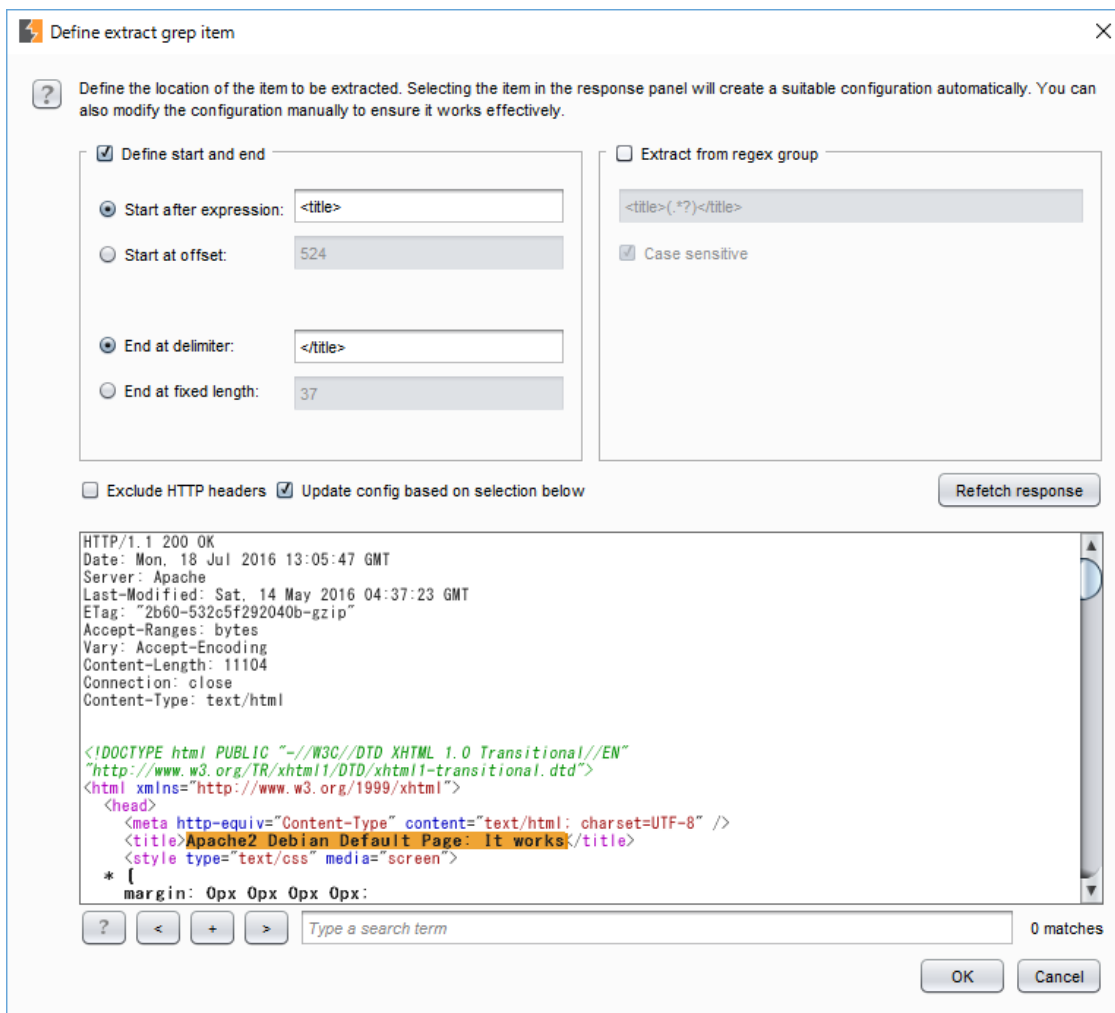


[Grep - Extract]は元のリクエストから正規表現により該当する箇所のログを出力するための機能です。[Grep - Match]同様に、[Extract the following items from responses]をチェックすると有効化されます。



[Add]で正規表現のルールが設定できます。元となるレスポンスから範囲選択することで[Start after expression]と[End at delimiter]が自動的設定されます。設定された該当する箇所が一覧で表示されます。





### 4.3.7 Extender

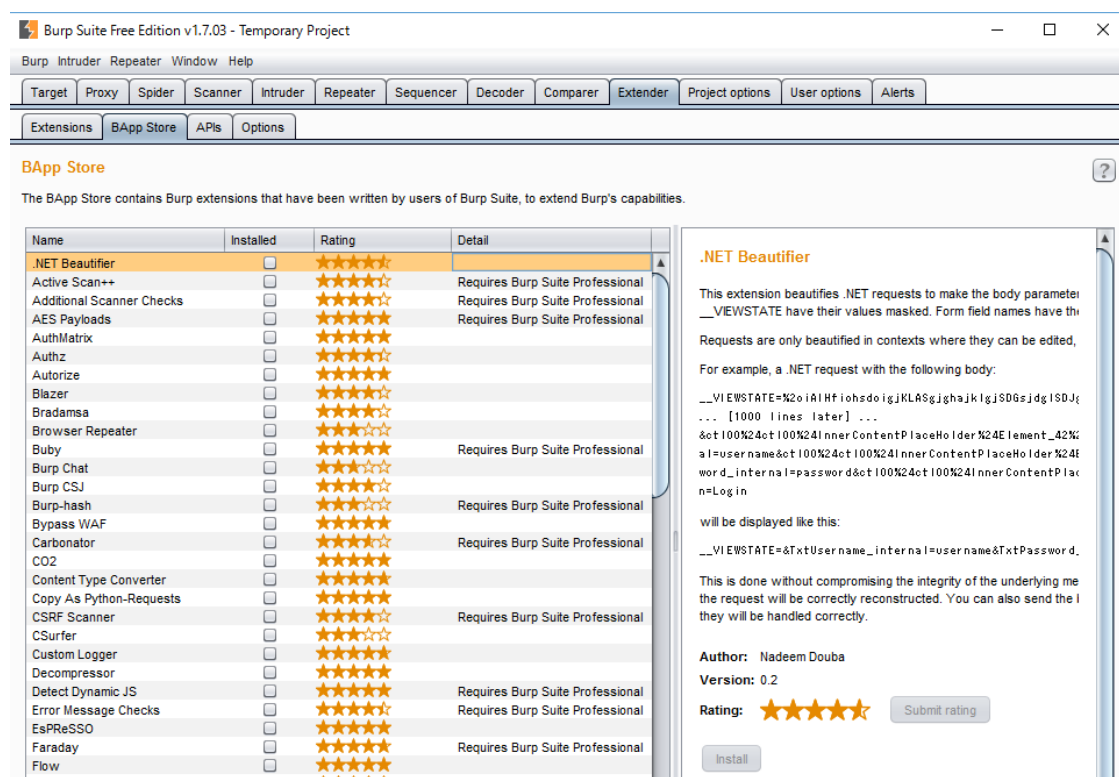
Burp Suite は、ユーザ自身、または第三者が独自に開発した拡張機能を取り込み、様々な機能の拡張ができます。例えば、HTTP リクエストやレスポンスの修正、UI のカスタマイズ、外部ツールとの連携、Intruder の独自ペイロードの作成、Scanner のシグネチャ追加（プロフェッショナル版専用）などです。これらの拡張機能の取り込みや管理をするためのツールが、Extender です。

Burp Suite で拡張機能を利用するには、2つの方法があります。拡張機能のファイルを用意し登録する方法と、BApp Store を利用する方法です。まずは、BApp Store を利用する方法を説明します。

## BApp Store を利用する

BApp Store は、Burp Suite のユーザが開発した拡張機能を登録し公開できるサービスです。2016/06 時点で、約 80 個の拡張機能が公開されています。

BApp Store で公開されている拡張機能は、Burp Suite の UI 上から簡単に取り込めるようになっています。「Extender」の「BApp Store」タブを開きます。



The screenshot shows the Burp Suite Free Edition v1.7.03 interface. The 'Extender' tab is selected, and the 'BApp Store' sub-tab is active. The main area displays a list of extensions with columns for Name, Installed, Rating, and Detail. The '.NET Beautifier' extension is highlighted. To the right, a detailed view of the '.NET Beautifier' extension is shown, including its description, author (Nadeem Douba), version (0.2), and a rating of 5 stars.

Name	Installed	Rating	Detail
.NET Beautifier	<input type="checkbox"/>	★★★★★	
Active Scan++	<input type="checkbox"/>	★★★★★	Requires Burp Suite Professional
Additional Scanner Checks	<input type="checkbox"/>	★★★★★	Requires Burp Suite Professional
AES Payloads	<input type="checkbox"/>	★★★★★	Requires Burp Suite Professional
AuthMatrix	<input type="checkbox"/>	★★★★★	
Authz	<input type="checkbox"/>	★★★★★	
Authorize	<input type="checkbox"/>	★★★★★	
Blazer	<input type="checkbox"/>	★★★★★	
Bradamsa	<input type="checkbox"/>	★★★★★	
Browser Repeater	<input type="checkbox"/>	★★★★★	
Buby	<input type="checkbox"/>	★★★★★	Requires Burp Suite Professional
Burp Chat	<input type="checkbox"/>	★★★★★	
Burp CSJ	<input type="checkbox"/>	★★★★★	
Burp-hash	<input type="checkbox"/>	★★★★★	Requires Burp Suite Professional
Bypass WAF	<input type="checkbox"/>	★★★★★	
Carbonator	<input type="checkbox"/>	★★★★★	Requires Burp Suite Professional
CO2	<input type="checkbox"/>	★★★★★	
Content Type Converter	<input type="checkbox"/>	★★★★★	
Copy As Python-Requests	<input type="checkbox"/>	★★★★★	
CSRF Scanner	<input type="checkbox"/>	★★★★★	Requires Burp Suite Professional
CSurfer	<input type="checkbox"/>	★★★★★	
Custom Logger	<input type="checkbox"/>	★★★★★	
Decompressor	<input type="checkbox"/>	★★★★★	
Detect Dynamic JS	<input type="checkbox"/>	★★★★★	Requires Burp Suite Professional
Error Message Checks	<input type="checkbox"/>	★★★★★	Requires Burp Suite Professional
EsPreSSO	<input type="checkbox"/>	★★★★★	
Faraday	<input type="checkbox"/>	★★★★★	Requires Burp Suite Professional
Flow	<input type="checkbox"/>	★★★★★	

**.NET Beautifier**

This extension beautifies .NET requests to make the body parameter \_\_VIEWSTATE have their values masked. Form field names have their values masked.

Requests are only beautified in contexts where they can be edited.

For example, a .NET request with the following body:

```
__VIEWSTATE=2oiAIHfiohsdoigjKLASgighajkljSD6sjdgISDj... [1000 lines later] ...&ot100%24ot100%24InnerContentPlaceholder%24Element_42%aI=username&ot100%24ot100%24InnerContentPlaceholder%24word_internal=password&ot100%24ot100%24InnerContentPlaceholder=Login
```

will be displayed like this:

```
__VIEWSTATE=&TxtUsername_internal=username&TxtPassword,
```

This is done without compromising the integrity of the underlying message. The request will be correctly reconstructed. You can also send the original request and they will be handled correctly.

Author: Nadeem Douba  
Version: 0.2  
Rating: ★★★★★ [Submit rating](#)

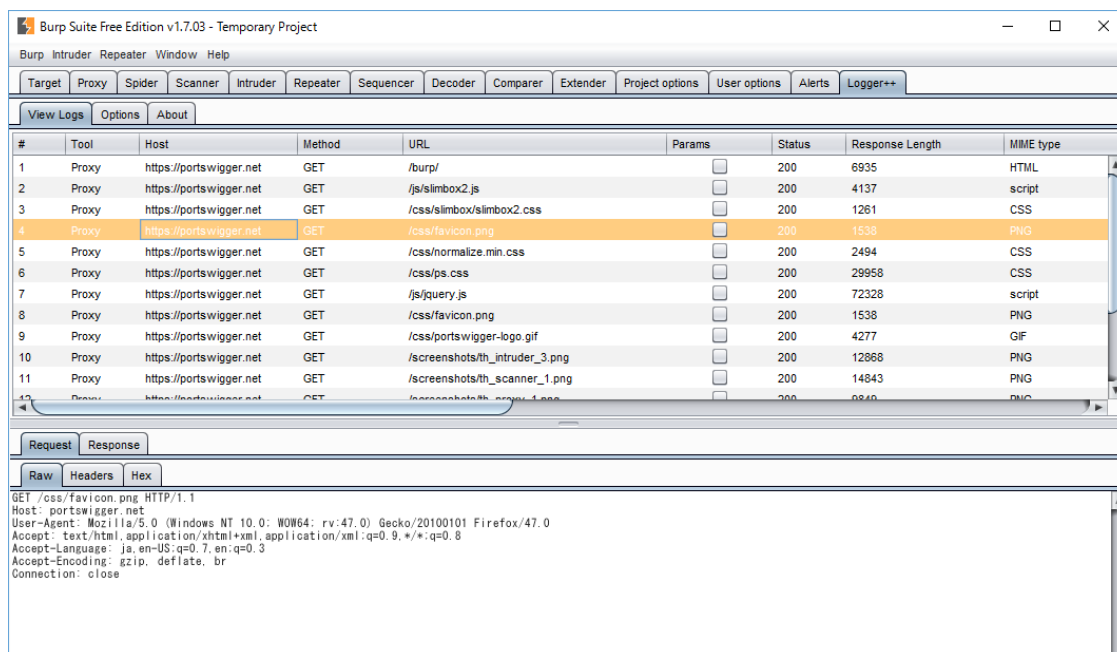
[Install](#)

この画面で、拡張機能名と詳細情報が確認できます。一部の拡張機能は、プロフェッショナル版でのみ利用可能で、Detail 列にその旨記載があります。

それでは、Logger++という拡張機能をインストールしてみましょう。この拡張機能は、Burp Suite の様々なツールが送受信した HTTP メッセージを、Proxy の HTTP history のようなインタフェースで表示できる拡張機能です。

左側の一覧表から、[Logger++]を選択します。すると右側のペインに Logger++の詳細情報が表示されます。一番下の[Install]ボタンをクリックしてください。インストールが進み、ボタンが[Reinstall]に変われば、インストールは完了です。

拡張機能によって Burp Suite のどこを拡張するかは様々です。カスタムタブの追加、コンテキストメニューへのアイテム追加、メッセージエディターへのタブ追加など、UI に反映される箇所は異なり、また UI 上では変化が分からないものもありますので、拡張機能の詳細情報で確認してください。Logger++の場合は、カスタムタブが追加されています。Logger++の詳細には触れませんので、様々なサイトにアクセスしてどのようなログが取れるか確認してください。



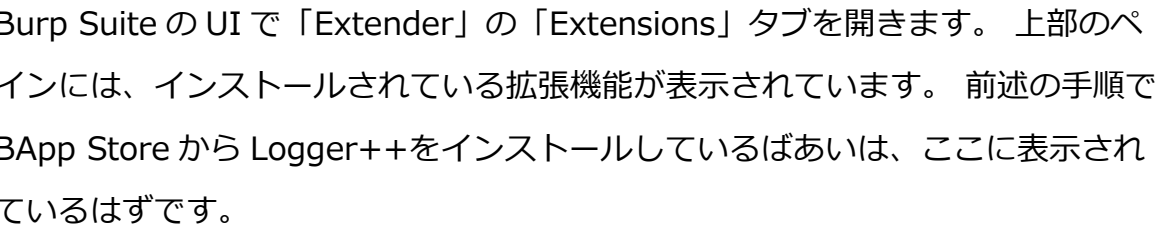
## 拡張機能ファイルを登録する

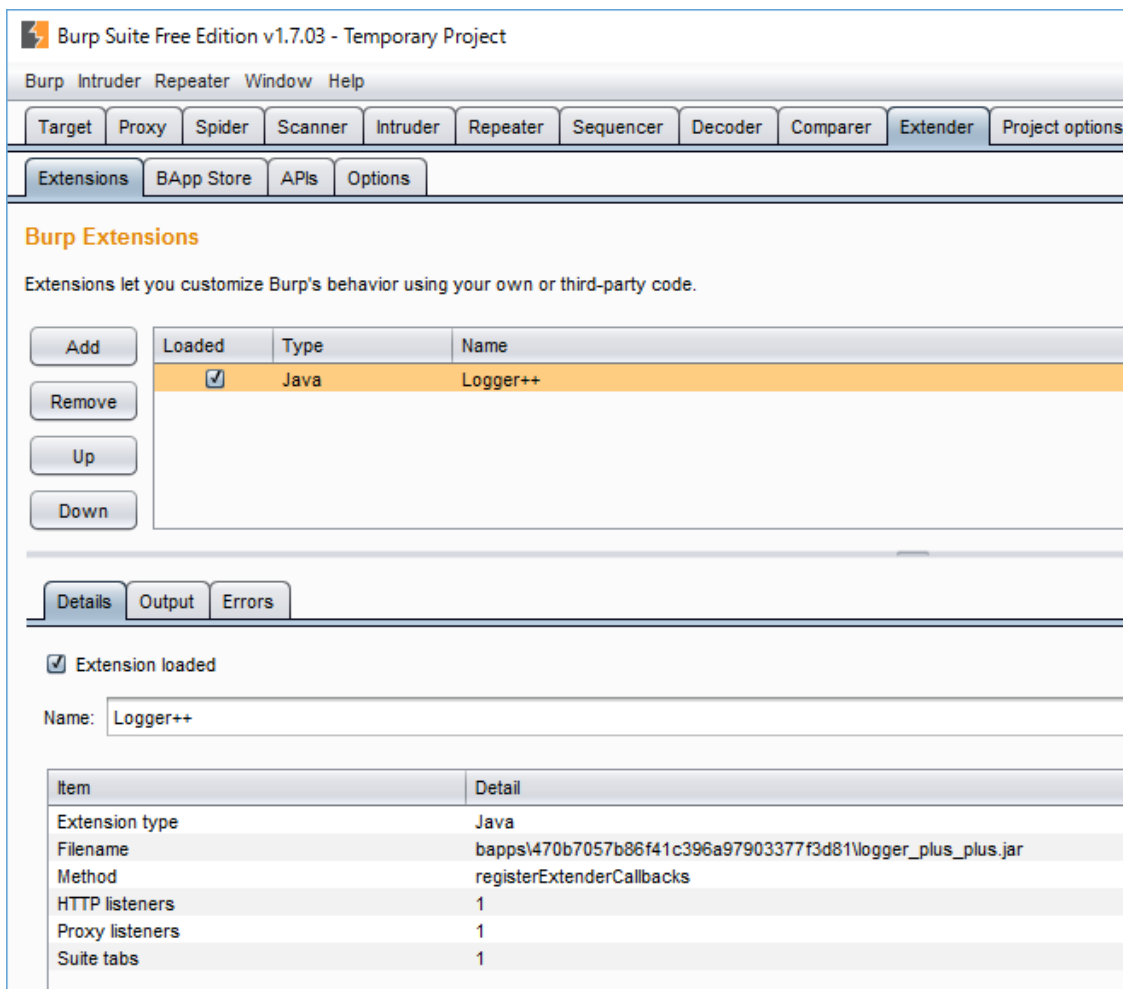
拡張機能は、BApp Store 以外からも入手できます。自身で拡張機能を開発した場合も、この手順で取り込むことになります。

今回は「OgaCopy」という拡張機能をインストールしてみましょう。Burp Suite はマルチバイト文字の取扱いが不得意で、メッセージエディターなどで日本語を含むテキストをコピーしてペーストすると、文字化けをしてしまいます。OgaCopy はこれを補正して、文字化けせずコピーができる拡張機能です。

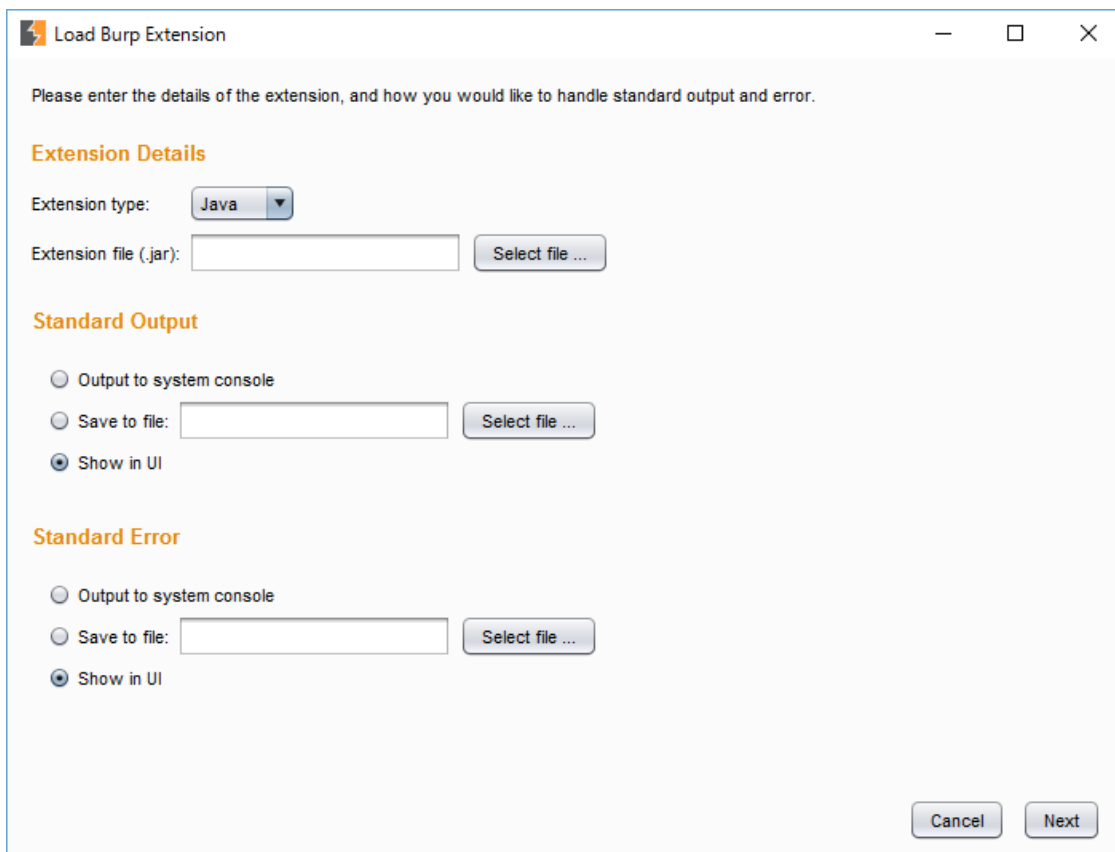
OgaCopy (<http://www.geocities.jp/burplogviewer/burpextender.html>)

まず上記のサイトにアクセスし、JAR ファイルをダウンロードします（2016/06 時点で最新は v1.1）。保存場所は任意の場所でもかまいません。





左側から「Add」ボタンをクリックすると、「Load Burp Extension」ダイアログボックスが開きます。



Extension type に「Java」が選択されていることを確認し、「Select file...」ボタンをクリックします。ここで、先程ダウンロードしておいた、OgaCopy\_v1.1.jar を選択します。

「Next」ボタンをクリックすると、拡張機能が読み込まれます。「Output」と「Errors」というタブがあり。ここには拡張機能が出力するログが表示されます。OgaCopy の場合は、Output タブに、"OgaCopy v1.1 Load OK!"と表示されているはずです。右下の「Close」ボタンをクリックして、このダイアログボックスを閉じてしまってもかまいません。すべてうまくいっていれば、拡張機能一覧テーブルに OgaCopy v1.1 が追加され、Loaded 列にチェックボックスがついているはずです。

OgaCopy は、コンテキストメニューに項目が追加されるタイプの拡張機能です。Proxy の履歴などで日本語を含むレスポンスを探してメッセージエディターで開いてください。コンテキストメニューを表示させると、OgaCopy の項目が 3 つ追加されています。今まで通りテキストを選択して「Ctrl+C」でコピーした場合と、OgaCopy でコピーした場合と、ペーストした結果を見比べてみてください。

### 拡張機能の管理

「Extender」の「Extensions」タブで、インストールされている拡張機能の管理ができます。

拡張機能が無効化するには、「Loaded」列のチェックボタンをオフにしてください。無効化すると Burp Suite を再起動しても自動的に有効になりませんので、再度使いたい場合はチェックボックスをオンにしてください。

拡張機能を Burp Suite から完全に削除するには、削除する拡張機能を選択して、左側から「Remove」ボタンをクリックしてください。

### Python や Ruby で開発された拡張機能

拡張機能は、Java だけではなく Python や Ruby で開発もできます。BApp Store で公開されている拡張機能にも、Python や Ruby で開発されたものがあります。これらの拡張機能を利用するには、Jython・JRuby をインストールしておく必要があります。

- Python

[Jython ダウンロードサイト](#) から、Standalone Jar（2016/06 時点で最新は 2.7.0）をダウンロードします。



Burp Suite の UI で「Extender」の「Options」タブを開きます。「Python Environment」セクションの「Location of Jython standalone JAR file:」で、ダウンロードした jython-standalone-2.7.0.jar を選択します。

- Ruby

[JRuby ダウンロードサイト](#) から、JRuby Complete .jar (2016/06 時点で最新は 9.1.2.0) をダウンロードします。

Burp Suite の UI で「Extender」の「Options」タブを開きます。「Ruby Environment」セクションの「Location of JRuby JAR file:」で、ダウンロードした jruby-complete-9.1.2.0.jar を選択します。

### 拡張機能の開発

Burp Suite や様々な拡張機能を使い込んでいくと、自分でも拡張機能を作ってみたくなることでしょう。「Extender」の「APIs」では、拡張機能の開発で使う Java インタフェースのソースコードが確認できます。また、以下のドキュメントが参考になりますので、拡張機能を開発する際は参照してください。

- Burp Extender <https://portswigger.net/burp/extender/>
- Burp API Javadoc <https://portswigger.net/burp/extender/api/>