OWASP ZAPのススメ #ssmjp

2014/03/28

亀田 勇歩
@YuhoKameda

OWASP
The Open Web Application Security Project

Agenda

OWASP
The Open Web Application Security Project

- 自己紹介
- ZAP機能紹介
- ZAPの使い方
- ZAPのコミュニティ紹介
- まとめ

自己紹介

Profile

- 亀田 勇歩 (Yuho Kameda)
  - Twitter : @YuhoKameda

- 活動
  - ZAP Evangelist
  - ZAPハンズオントレーニング in AppSec APAC
  - 『OWASP Zed Attack Proxy 運用マニュアル』執筆協力

ZAP Evangelist

OWASP
The Open Web Application Security Project

zaproxy
OWASP ZAP: An easy to use integrated penetration testing tool for finding vul

Project Home | Downloads | Wiki | Issues | Source

Search Current pages for Sear

Introduction
Screenshots
Tutorial Videos
Other Videos

ZapEvangelists

ZAP Evangelists

The following people are happy to give **free** ZAP ta

Name	Contacts	Locations *	Languages	Talks	Training	Notes / Specialities	Previous talks / training / other links
Yuho Kameda		Japan	English, Japanese	Y	Y		OWASP Japanese Manual

ZAPハンズオントレーニング in AppSec APAC

OWASP
The Open Web Application Security Project

Home › トレーニング/Training Days › 3月17日 OWASP ZAPを利用した脆弱性診断-ハンズオン

3月17日 OWASP ZAPを利用した脆弱性診断-ハンズオン

インストラクター：境稔 & 亀田勇歩

インストラクター・プロフィール：
境稔
公認情報システムセキュリティプロフェッショナル(CISSP)。
主にWebアプリケーション脆弱性診断、セキュリティトレーニング
講師などに従事する。
『OWASP Zed Attack Proxy 運用マニュアル』監修
亀田勇歩
各国で行われているCTF(Capture the Flag)競技に参加し、
広範な知識と経験を活かして総合的な問題解決能力を磨いている。

『OWASP Zed Attack Proxy 運用マニュアル』執筆協力

OWASP
The Open Web Application Security Project

- Ver 2.1.0版にて作成
- インストール手順から各種メニューまで

OWASP Zed Attack Proxy 運用マニュアル

1 OWASP Zed Attack Proxy 概要
1.1 OWASP Zed Attack Proxy とは

OWASP Zed Attack Pro
ためのフリーツールで、現

- 動的スキャン
  設定したスキャン
- Forced Browse
  設定したリストの
- スパイダー検索
  選択したサイトに
- Fuzzer
  設定したリストの文字列で、任意の文字列を置換してリクエストを送信します。
- ローカル・プロキシ
  Web ブラウザからのリクエストをキャプチャできます。また、リクエストやレスポンス
  改ざんすることができます。
- レポート出力
  簡易ですが、スキャン結果をレポート出力できます。
- HttpSessions

OWASP Japan

Welcome to the Japan chapte
Click here to join the l

Participation

Translations / OWASPドキュメント

Completed

1. OWASP モバイルセキュリティプロジェクト -
2. OWASP Top 10 2013 (日本語)(pdf)
3. OpenSAMM(日本語)
4. OWASP ZAP マニュアル Ver.2.1.0版

OWASP ZAP

- Paros version:3.2.13をフォークしたもの

- 簡単に使える、Webアプリケーションの脆弱性を発見するための統合ペネトレーションツール

- https://code.google.com/p/zaproxy/
- https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

IPAテクニカルウォッチ　「ウェブサイトにおける脆弱性検査手法の紹介」の公開

ウェブ改ざんに繋がる脆弱性等をコストをかけずに検査する、3種のツールの使い勝手を比較

2013年12月12日
独立行政法人情報処理推進機構

表1：ツールの特徴比較

ツール名	検査者のスキル	操作性	検知精度	効率性	本番環境への影響
OWASP ZAP	初級者向け	使い易い	○	非常に良い	あり
Paros	上級者向け	使い易い	対象外	手間がかかる	あり (検査内容による)
Ratproxy	中級者向け	手間がかかる	△	良い	なし

IPAテクニカルウォッチ 「ウェブサイトにおける脆弱性検査手法の紹介」の公開
https://www.ipa.go.jp/about/technicalwatch/20131212.html

OWASP
The Open Web Application Security Project

ZAP機能紹介(初心者向け)

Quick Start

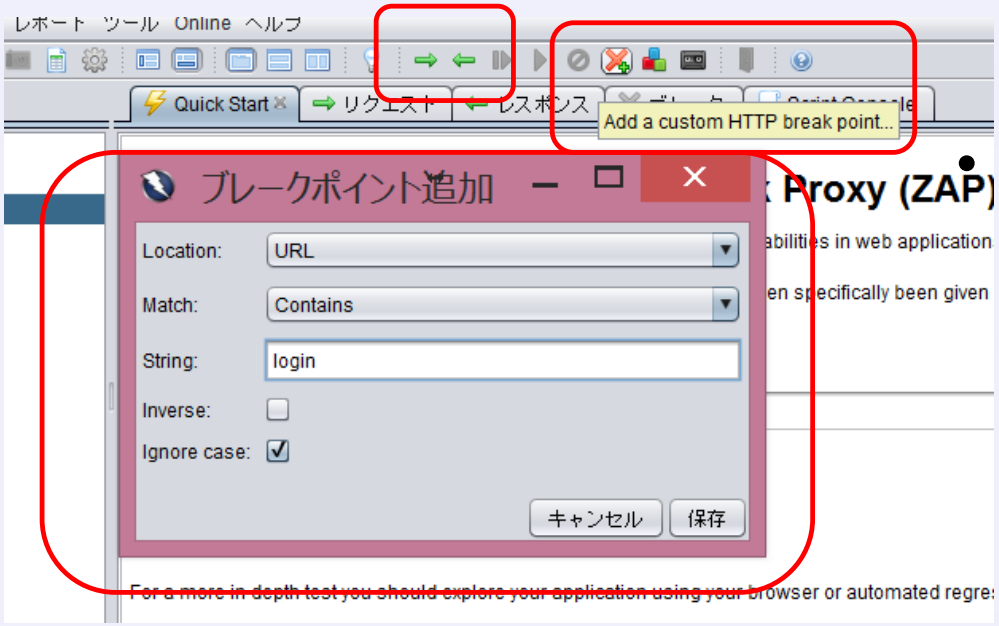
OWASP
The Open Web Application Security Project

- 開始URLを指定し検査を行う
- 操作が簡単

スパイダー検索

- 開始URLを選択し、スパイダー検索
- 簡単にサイトをクロールしてくれる

ブレーク機能

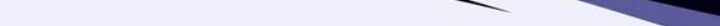


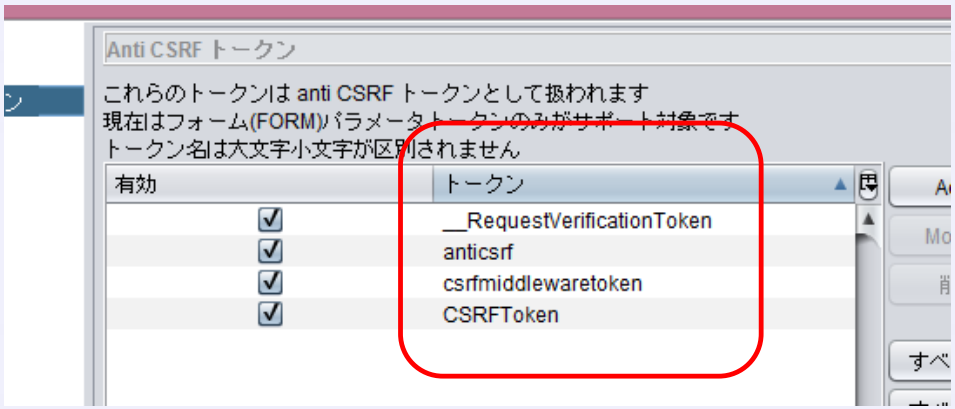
- 
  リクエストをブレーク
- 
  レスポンスをブレーク
- 
  特定条件(カスタム)の場合にブレーク

OWASP
The Open Web Application Security Project

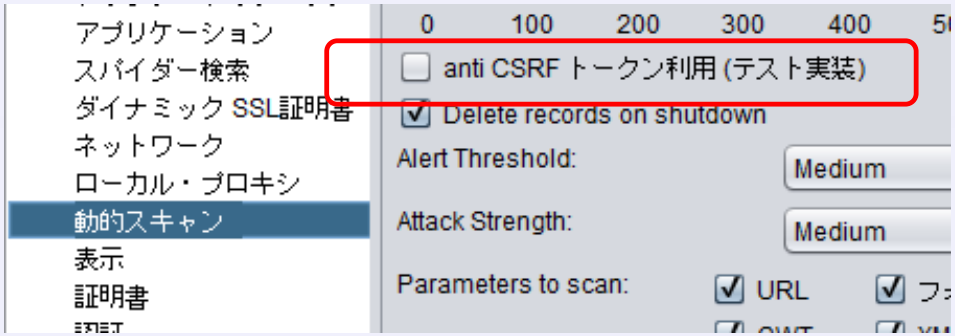
ZAP機能紹介(中級者向け)

CSRFトークン

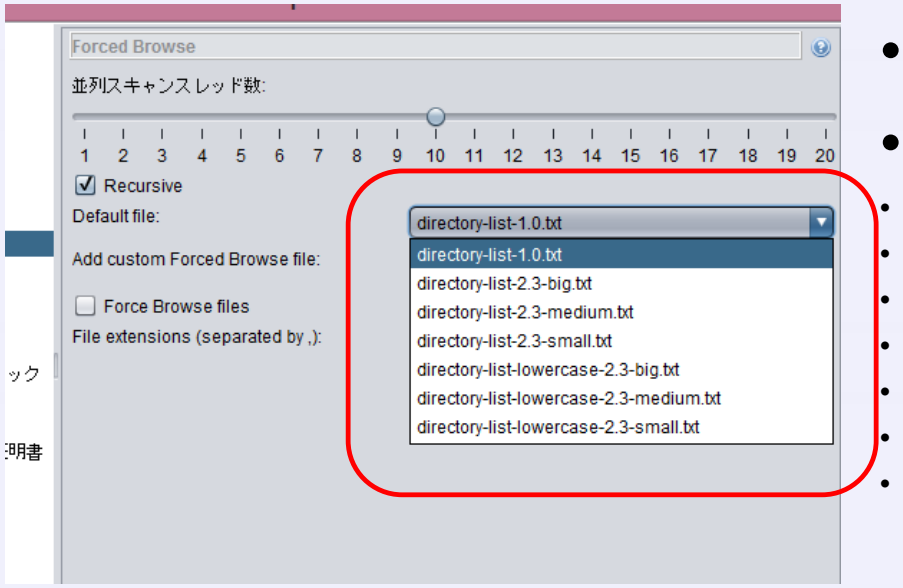




- トークンに用いられるパラメータを指定
- 使用する場合、オプションにて設定

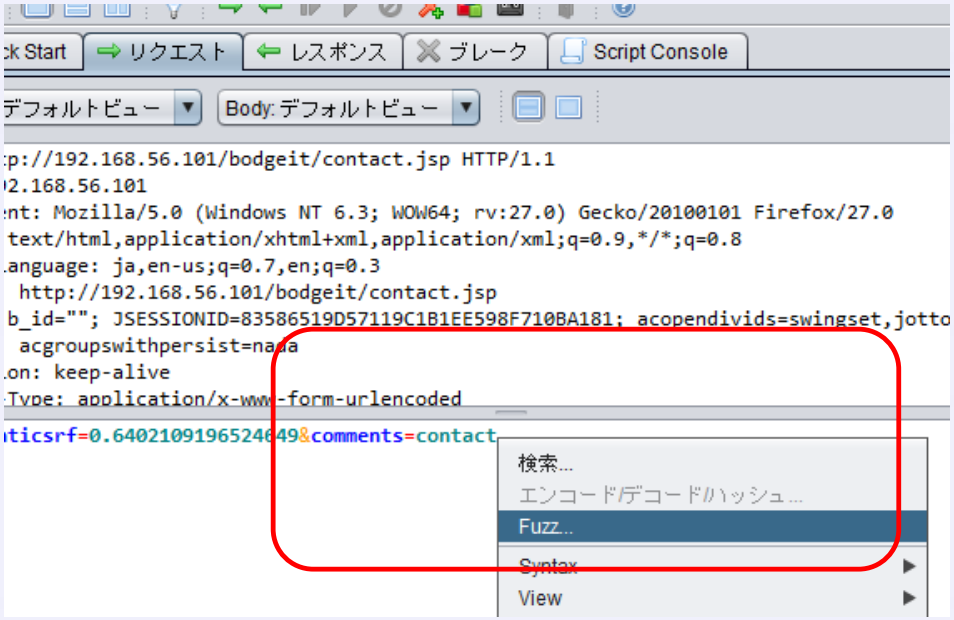


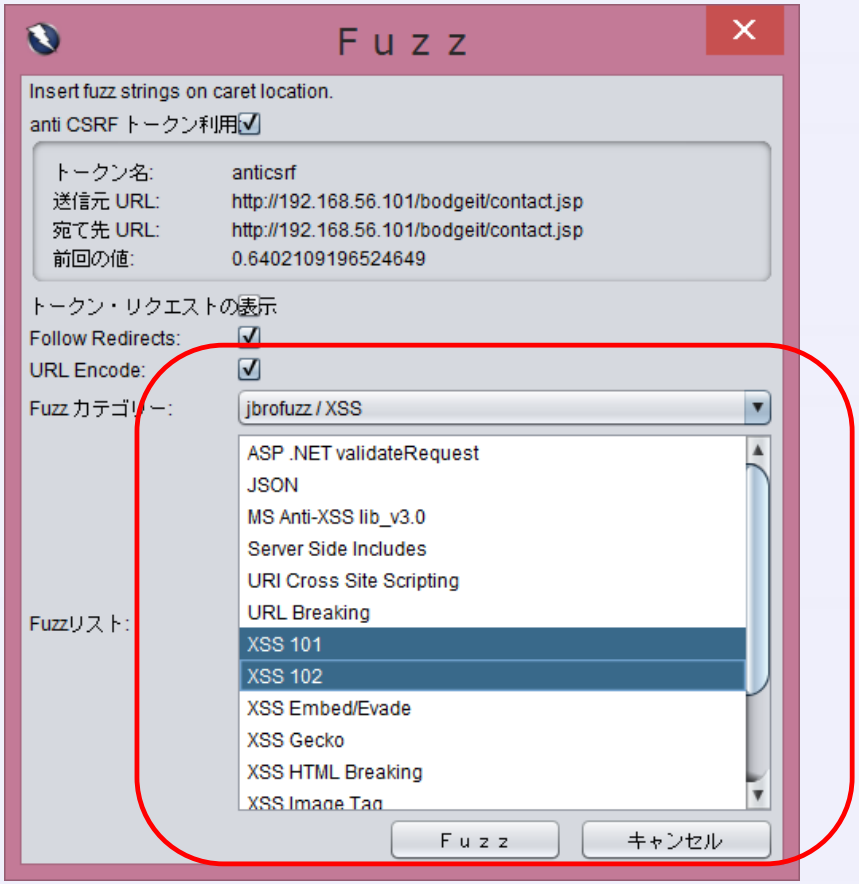
強制ブラウズ



- ディレクトリ調査
- カスタマイズも可能
  - directory-list-1.0.txt 141,694件 収録
  - directory-list-2.3-big.txt 1,273,819件 収録
  - directory-list-2.3-medium.txt 220,546件 収録
  - directory-list-2.3-small.txt 87,650件 収録
  - directory-***2.3-big.txt 1,185,240件 収録
  - directory-***2.3-medium.txt 207,619件 収録
  - directory-***2.3-small.txt 81,643件 収録

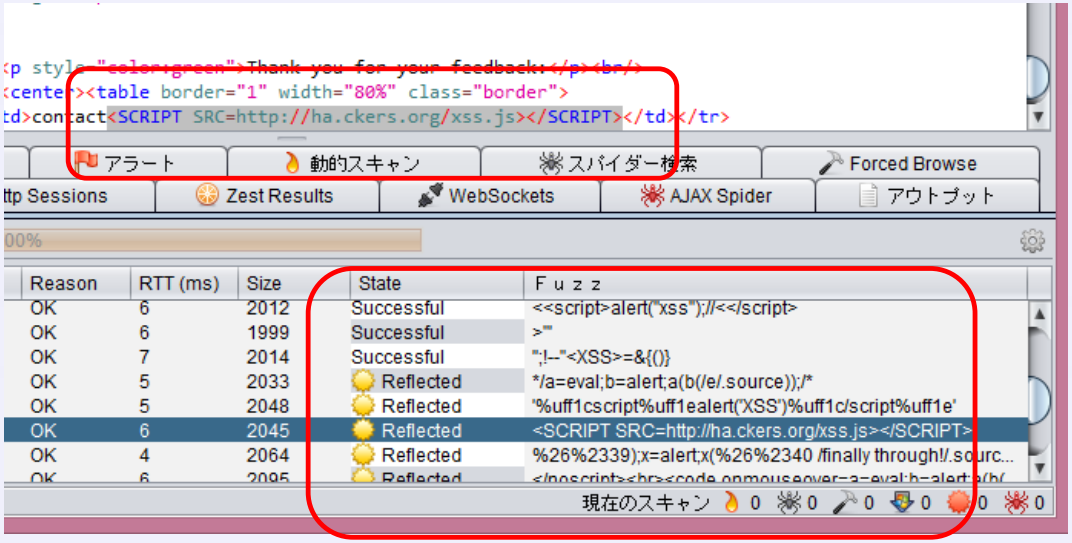
Fuzzer


ck Start
リクエスト
レスポンス
ブレーク
Script Console
デフォルトビュー
Body: デフォルトビュー
:p://192.168.56.101/bodgeit/contact.jsp HTTP/1.1
2.168.56.101
ent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
.anguage: ja,en-us;q=0.7,en;q=0.3
http://192.168.56.101/bodgeit/contact.jsp
b_id=""; JSESSIONID=83586519D57119C1B1EE598F710BA181; acopendivids=swingset,jotto
acgroupswithpersist=nada
.on: keep-alive
-Type: application/x-www-form-urlencoded
ticsrf=0.6402109196524649&comments=contact
検索...
エンコード/デコード/ハッシュ...
Fuzz...
Syntax
View


Fuzz
Insert fuzz strings on caret location.
anti CSRF トークン利用
トークン名: anticsrf
送信元 URL: http://192.168.56.101/bodgeit/contact.jsp
宛て先 URL: http://192.168.56.101/bodgeit/contact.jsp
前回の値: 0.6402109196524649
トークン・リクエストの表示
Follow Redirects:
URL Encode:
Fuzz カテゴリー: jbrofuzz / XSS
Fuzzリスト:
ASP .NET validateRequest
JSON
MS Anti-XSS lib_v3.0
Server Side Includes
URI Cross Site Scripting
URL Breaking
XSS 101
XSS 102
XSS Embed/Evade
XSS Gecko
XSS HTML Breaking
XSS Image Tag
Fuzz
キャンセル

Fuzzer

OWASP
The Open Web Application Security Project

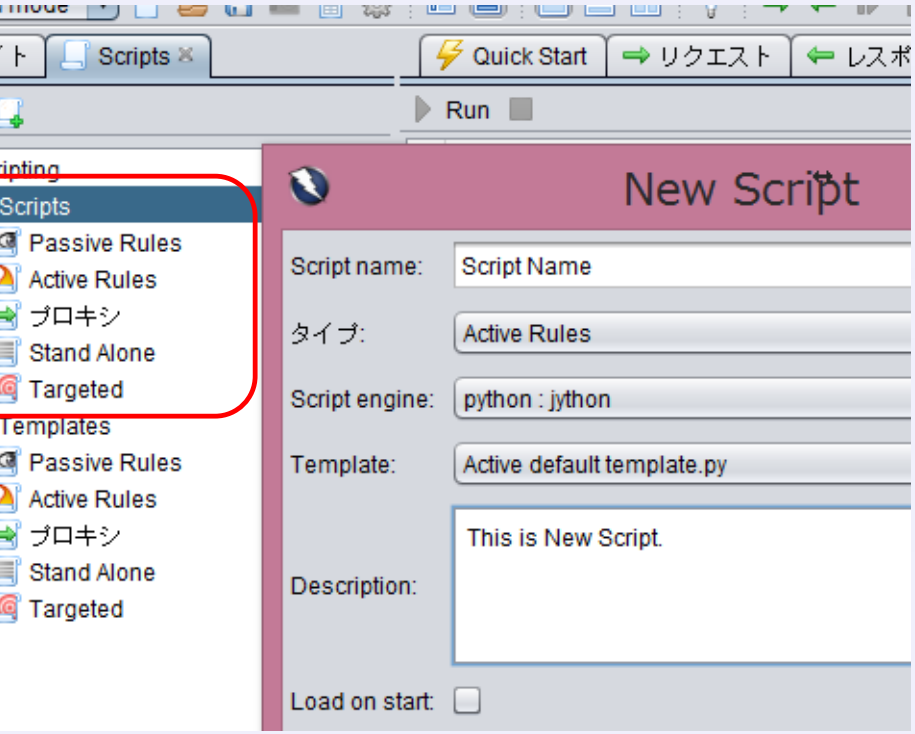


- 攻撃文字列を連続試行
- 「Reflected」で簡単判別
- レスポンスで、すぐ確認可能
- 試行パターンが豊富
  - Format String Payloads
  - SQL Injection
  - Cross Site Scripting
  - など

OWASP
The Open Web Application Security Project

ZAP機能紹介(上級者向け)

ZAP Script



- 様々な状況下でスクリプトを実行
  - Passive Rules
    - パッシブスキャン実行時に実行
  - Active Rules
    - 動的スキャン実行時に実行
  - プロキシ
    - ZAPをプロキシとして使用する時に実行
  - Stand Alone
    - 手動で実行
  - Targeted
    - 指定したURLに対して実行

Plug-n-Hack

- Firefoxのアドオン
- 有効にした後、Shift+F2で起動
- コマンドでZAP操作
  - zap http-session
  - zap record
  - zap scan
  - zap session
  - zap spider
  - …

Plug-n-Hack

OWASP
The Open Web Application Security Project

zap

概要: » zap

詳細:

OWASP ZAP Commands

サブコマンド:

- **zap brk**: Break on all new requests and/or responses » help zap brk
- **zap http-session**: Manipulate HTTP sessions » help zap http-session
- **zap http-session new**: Start a new HTTP session » help zap http-session new
- **zap http-session rename**: Rename an HTTP session » help zap http-session rename
- **zap http-session switch**: Switch to another HTTP session » help zap http-session switch
- **zap record**: Record all requests » help zap record
- **zap scan**: Control the ZAP active scanner » help zap scan
- **zap scan start**: Start actively scanning a site » help zap scan start
- **zap scan status**: Scan progress out of 100 » help zap scan status
- **zap session**: Manipulate ZAP sessions » help zap session
- **zap session clear**: Clear the ZAP session (not saved to disk) » help zap session clear
- **zap session new**: Create a new ZAP session (saved to disk) » help zap session new
- **zap spider**: Control the ZAP spider » help zap spider
- **zap spider start**: Start spidering a site » help zap spider start
- **zap spider status**: Spider progress out of 100 » help zap spider status
- **zap spider stop**: Stop spidering a site » help zap spider stop
- **zap version**: Returns the ZAP version » help zap version

»

ZAP API

OWASP
The Open Web Application Security Project

localhost:8880/UI/spider/

ZAP API ユーザインターフェース

コンポーネント: spider

ビュー

status ()
results ()
excludedFromScan ()
optionScope ()
optionRequestWaitTime ()
optionSkipURLString ()
optionMaxDepth ()
optionHandleODataParametersVisited ()
optionParseComments ()
optionHandleParameters ()

Ajax Spider

OWASP
The Open Web Application Security Project

Scripts
Quick Start
リクエスト
レスポンス
ブレーク
bodgeit
GET:home.jsp
GET:ab
GET:co
GET:log
GET:ba
GET:se
GET:pro
GET:pro
GET:sty
GET:ad
POST:c
POST:b
GET:ad
images
js
GET:sc
GET:reg
POST:lo
GET:se

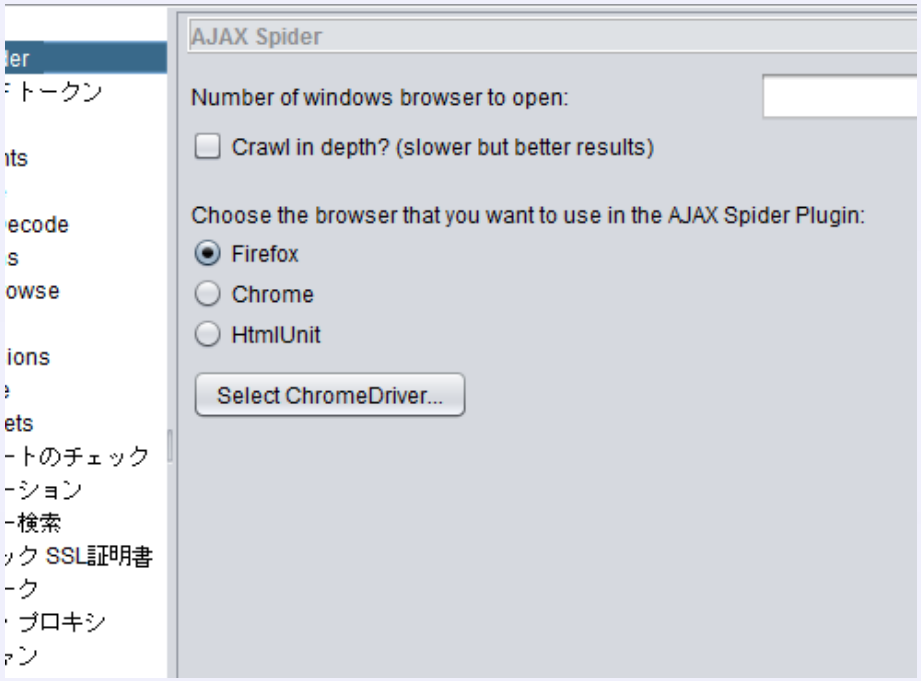
攻撃
データベースから削除
Include in Context
Flag as Context
アプリケーションの実行
Exclude from Context
以下の処理から除外する:
ブレーク...
Alerts for this node
再送信...
新しいアラート...
Show in History tab
ブラウザで表示
Copy URLs to clipboard
Generate anti CSRF test FORM
Invoke with script...
Add to Zest Script
Compare 2 requests
Compare 2 responses
Refresh Sites tree

Active Scan all in Scope
サイトの動的スキャン
Active Scan subtree
Active Scan single URL
Spider Context...
Spider all in Scope
サイトをスパイダー検索
Spider Subtree
Spider URL
Forced Browse site
Forced Browse directory
Forced Browse directory (and children)
AJAX Spider in Scope
AJAX Spider Site

Welcome to the OWASP Zed Attac
for finding vulne
that you have b
ess 'Attack'.
tab for details
ion using your b
ou are using Firefox 24.0 or later you can use 'Plug-n-Hack' to configur
nfigure your browser:
Plug-n-Hack
point your browser at:
http://localhost:8880/pnh/

スパイダー検索
Fuzzer
パラメータ
Http Sessions

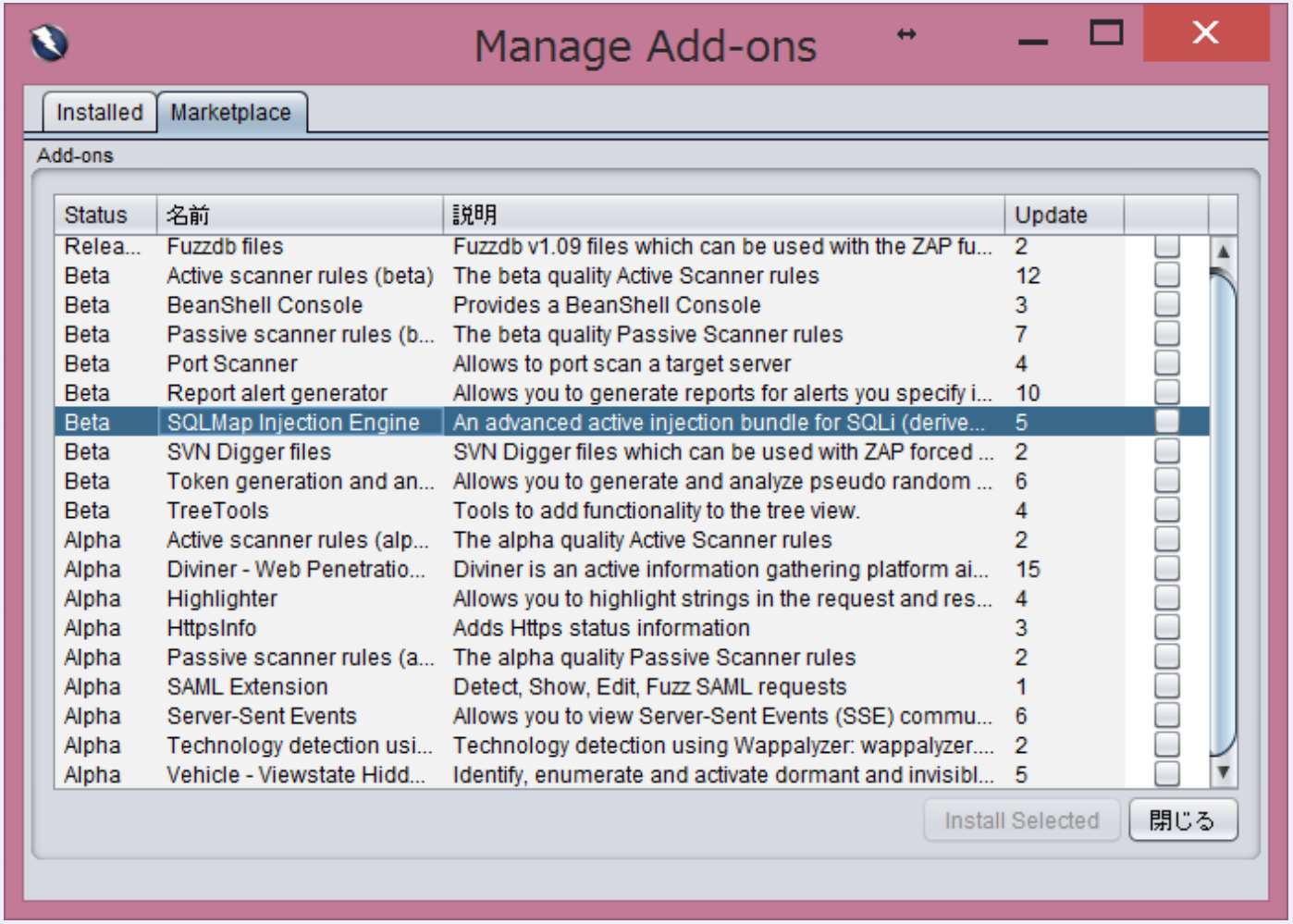
Ajax Spider



- Ajaxベースの動的解析ツール
- Crawljax (http://crawljax.com/)

Manage Add-ons

OWASP
The Open Web Application Security Project

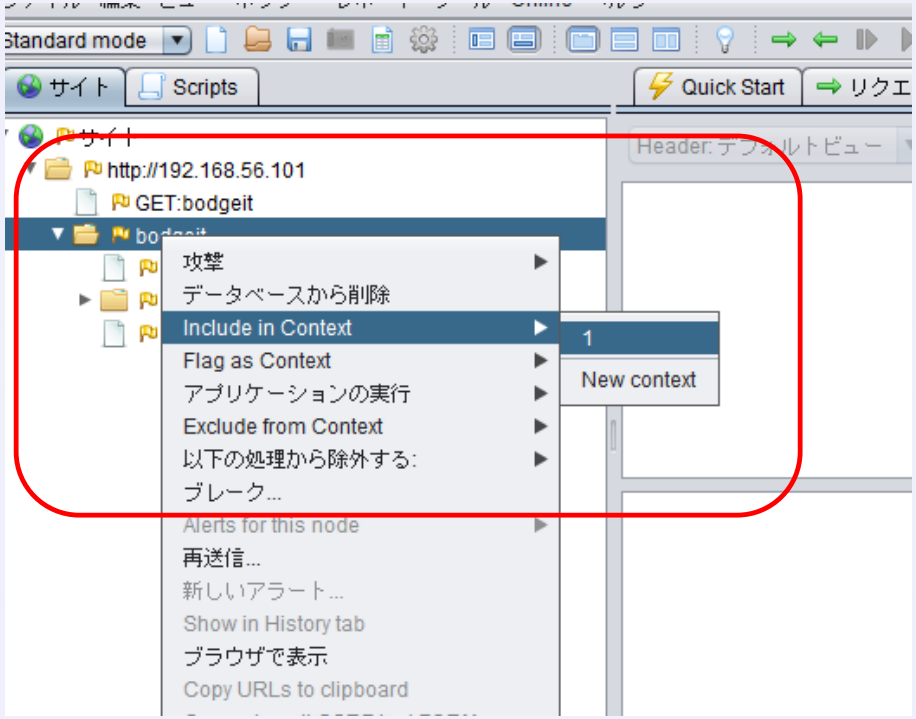


Status	名前	説明	Update
Relea...	Fuzzdb files	Fuzzdb v1.09 files which can be used with the ZAP fu...	2
Beta	Active scanner rules (beta)	The beta quality Active Scanner rules	12
Beta	BeanShell Console	Provides a BeanShell Console	3
Beta	Passive scanner rules (b...	The beta quality Passive Scanner rules	7
Beta	Port Scanner	Allows to port scan a target server	4
Beta	Report alert generator	Allows you to generate reports for alerts you specify i...	10
Beta	SQLMap Injection Engine	An advanced active injection bundle for SQLi (derive...	5
Beta	SVN Digger files	SVN Digger files which can be used with ZAP forced ...	2
Beta	Token generation and an...	Allows you to generate and analyze pseudo random ...	6
Beta	TreeTools	Tools to add functionality to the tree view.	4
Alpha	Active scanner rules (alp...	The alpha quality Active Scanner rules	2
Alpha	Diviner - Web Penetratio...	Diviner is an active information gathering platform ai...	15
Alpha	Highlighter	Allows you to highlight strings in the request and res...	4
Alpha	HttpsInfo	Adds Https status information	3
Alpha	Passive scanner rules (a...	The alpha quality Passive Scanner rules	2
Alpha	SAML Extension	Detect, Show, Edit, Fuzz SAML requests	1
Alpha	Server-Sent Events	Allows you to view Server-Sent Events (SSE) commu...	6
Alpha	Technology detection usi...	Technology detection using Wappalyzer: wappalyzer....	2
Alpha	Vehicle - Viewstate Hidd...	Identify, enumerate and activate dormant and invisibl...	5

OWASP
The Open Web Application Security Project

ZAPの基本的な使い方

Context設定

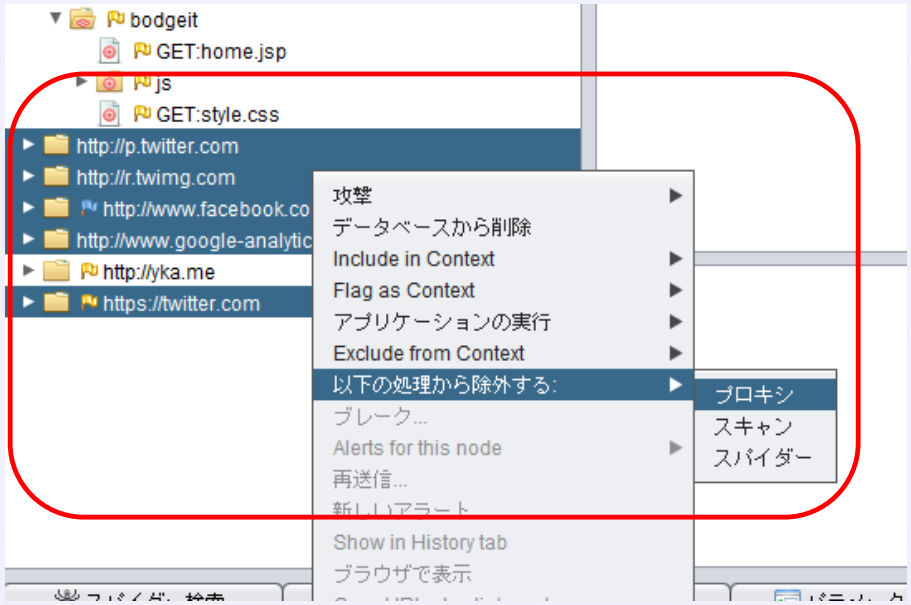


- スコープを指定
  - 検査対象を明示

除外設定

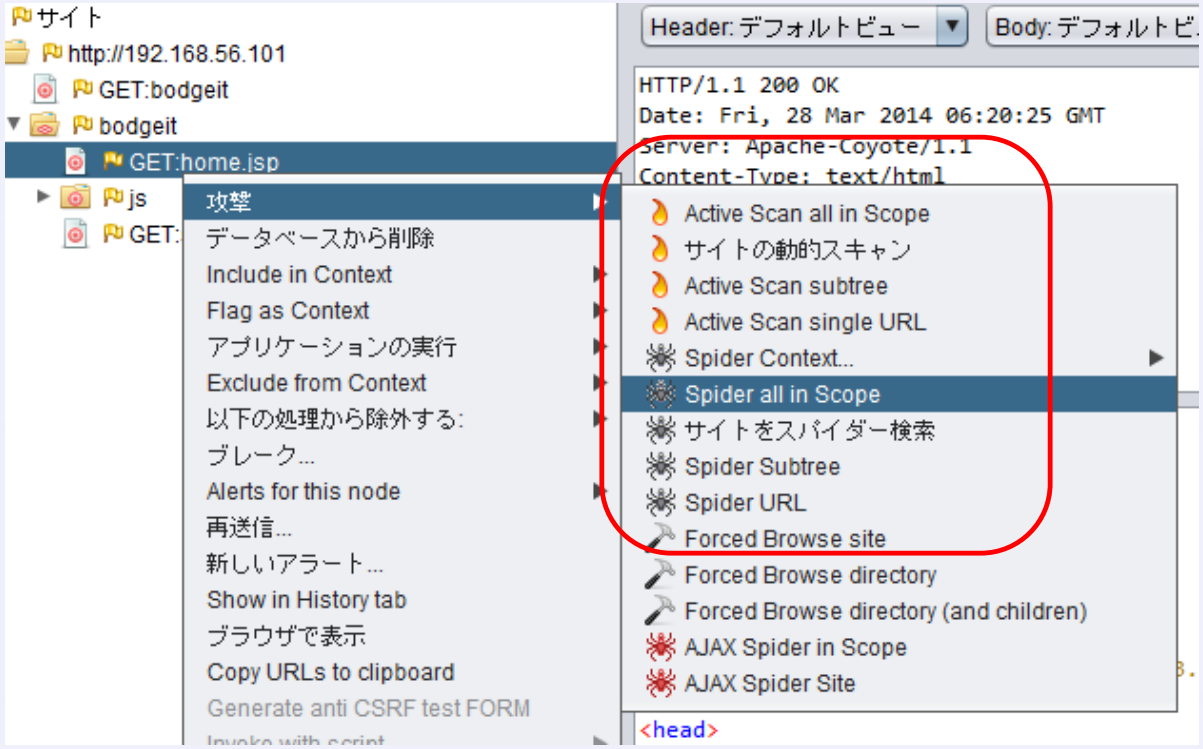
OWASP
The Open Web Application Security Project

- (必要がある場合、)検査に不要なリクエストを除外



Spider検索

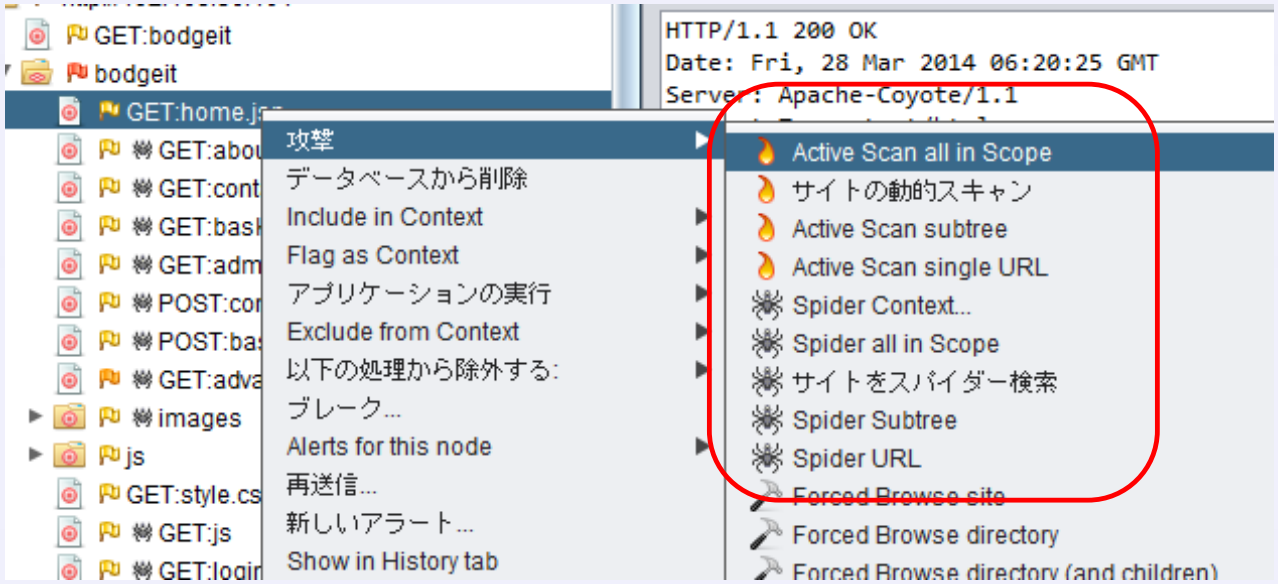
- スコープ内をSpider検索



動的スキャン

OWASP
The Open Web Application Security Project

- スコープ内を動的スキャン
  - All In Scope
  - Site Scan
  - Subtree
  - Single URL Scan



OWASP
The Open Web Application Security Project

ZAP SCRIPTの使い方

言語スクリプトのアドオン追加

1. 各言語スクリプトのアドオン追加
   i. 「Manage Add-ons」の「Marketplace」にアクセスする。
   ii. 使用したい言語のアドオンをチェック
   iii. 「Install Selected」を押下する。

≪選択できるアドオン≫

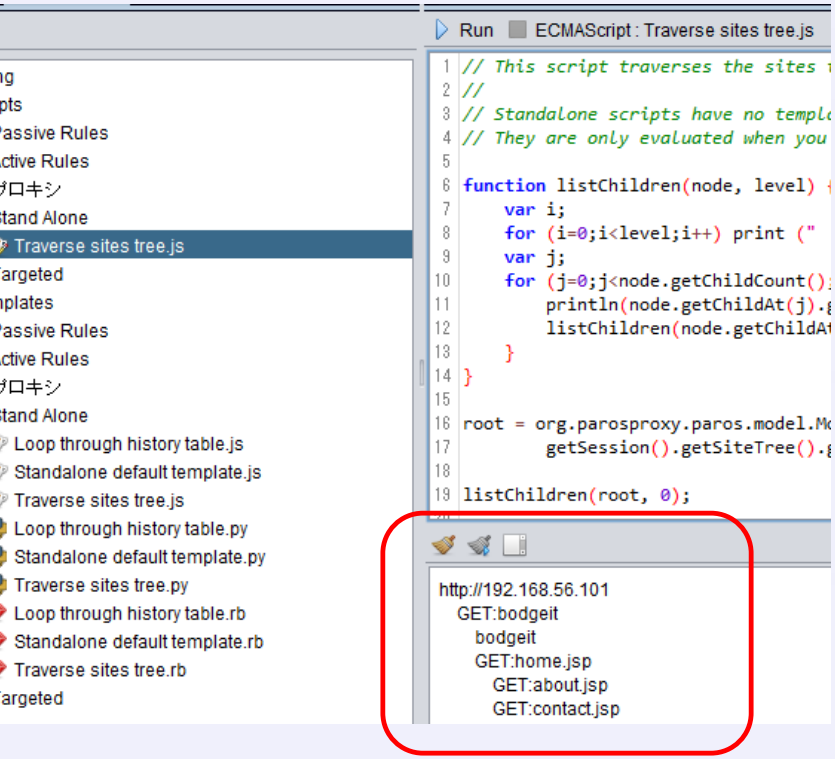
- Zest - Scripting Security Tests
- Python Scripting
- Ruby scripting
- など

スクリプトの作成

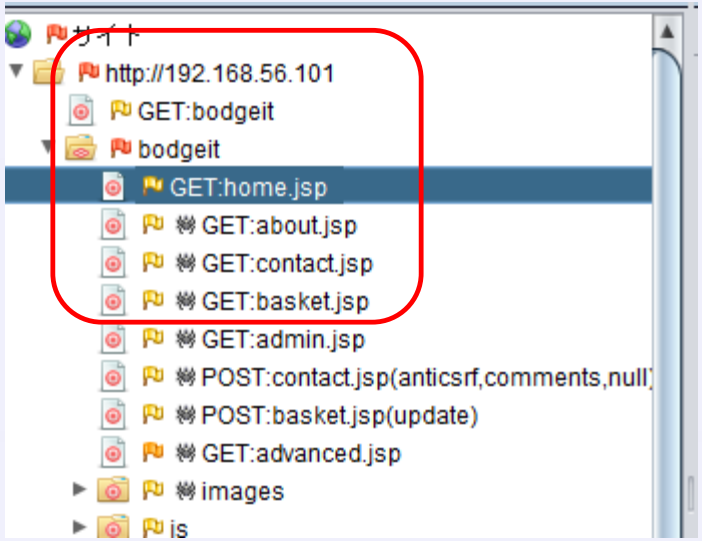
2. スクリプトの作成
   i. 「Scripts」タブを選択
   ii. 「New Script」を選択、もしくは「Templates」内のスクリプトを右クリックし「New Script」を選択
   iii. 入力欄を選択し、「保存」を押下しスクリプトを作成
   iv. 「Script Console」の結果出力部分に結果が表示される

スクリプト実行方法	
Passive Rules/Active Rules/プロキシ	「Enable Script」を選択し有効にする
Stand Alone	「Script Console」タブにある「Run」を押下し実行する
Targeted	「履歴」内か「サイト」タブ内のURLを右クリックし、「Invoke with script」を選択し実行する

スクリプト実行例



- Traverse sites tree.js
  - ページ一覧抽出
- Find HTML comments.js
  - HTMLコメント抽出



ZESTスクリプト例

OWASP
The Open Web Application Security Project

- 一連の遷移をレコードし、マクロ化
  - トークンやパラメータの引き渡しも可能

OWASP
The Open Web Application Security Project

ZAPコミュニティの紹介

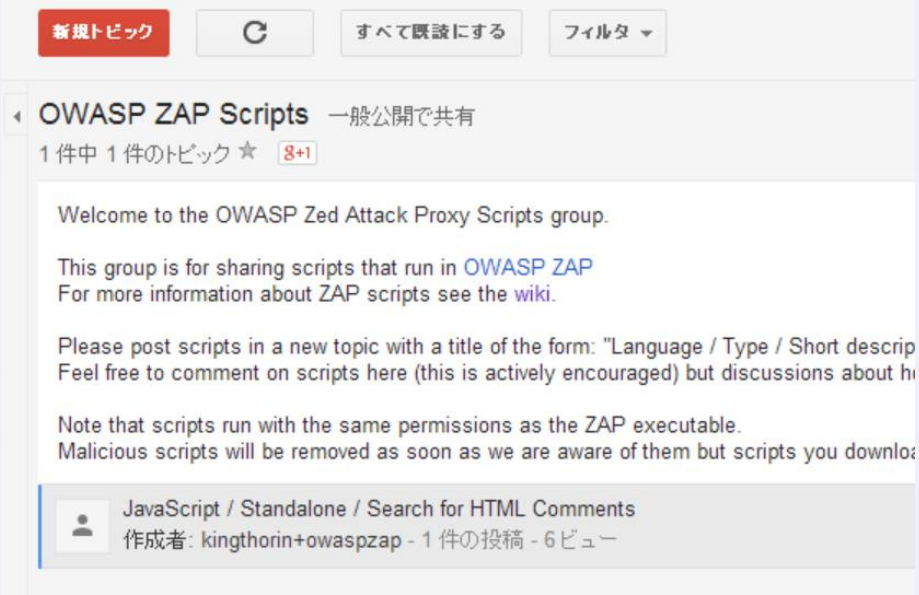
Google Group

- OWASP ZAP Developer Group
  - メンバー数：314人
  - 開始日：2010/08/17
  - 主な内容
    - ZAP開発に関すること
    - Extensionの開発
    - バグ修正
- OWASP ZAP User Group
  - メンバー数：214人
  - 開始日：2012/05/22
  - 主な内容
    - 使い方の質問
    - 実装してほしいリクエスト

Google Group (NEW!)

OWASP
The Open Web Application Security Project

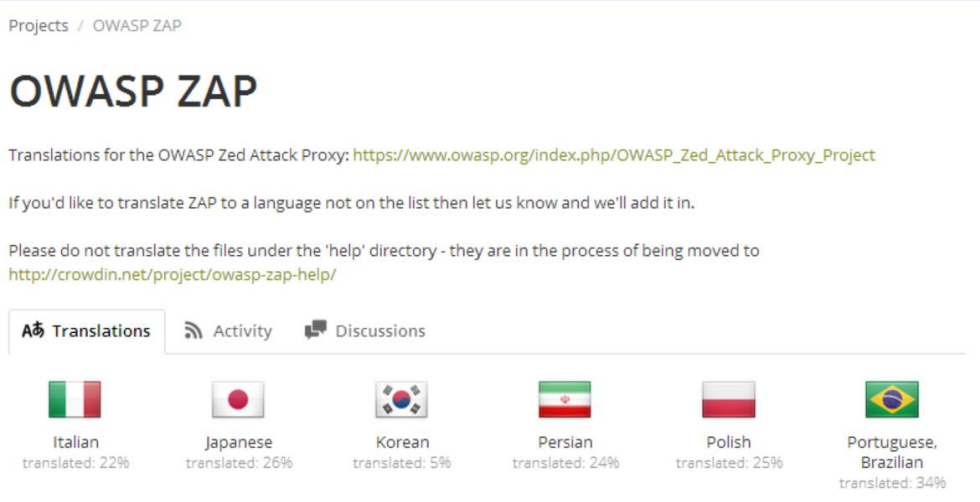
- OWASP ZAP Scripts
  - メンバー数：11人
  - 開始日：2014/03/26
  - 主な内容
    - ZAPスクリプトを共有するためのグループ



Translations for the OWASP ZAP
(https://crowdin.net/project/owasp-zap)

OWASP
The Open Web Application Security Project

- ZAP翻訳プロジェクト
- 日本語翻訳度は26%
(2014/3/28現在)
- だれでも参加可能



OWASP
The Open Web Application Security Project

まとめ

まとめ

- ZAPは、初心者には使いやすい、上級者には拘りを実現できる検査ツール
- 直感的に使いづらい部分は、使い方のコツを広めていく
- ターゲットを絞ったハンズオン(デモ形式)による教育機会は非常に有効
- 幅広い層の方にZAPを使ってほしい！

(Web開発/ 情シス/診断業務など)

Any Question?

OWASP
The Open Web Application Security Project

- Social Account
  - Twitter : @YuhoKameda
- E-mail
  - tyoisu@gmail.com
- OWASP
  - yuho.kameda@owasp.org
  - https://www.owasp.org/index.php/User:Yuho_Kameda