

操作手順書

倫理規定

許可なく他者のサーバーに使用しないでください。
違法行為となり、罰せられる可能性があります。
製作者一同は一切の責任を負いません。

推奨Webブラウザ

動作確認の出来ているWebブラウザは以下です。

- Google Chrome 96.0.4664.45
- Firefox 97.0.1
- Microsoft Edge 95.0.1020.53

機能の詳しい説明は省いています。機能説明書をご参照ください。
二回目以降の診断を行う際、注意事項があります。機能説明書5.5をご参照ください。

1. 起動

インストール手順書に従い、Himawariをインストールしてください。
インストール済の場合、以下のコマンドでHimawariを起動出来ます。

```
$ bash exec.sh
```

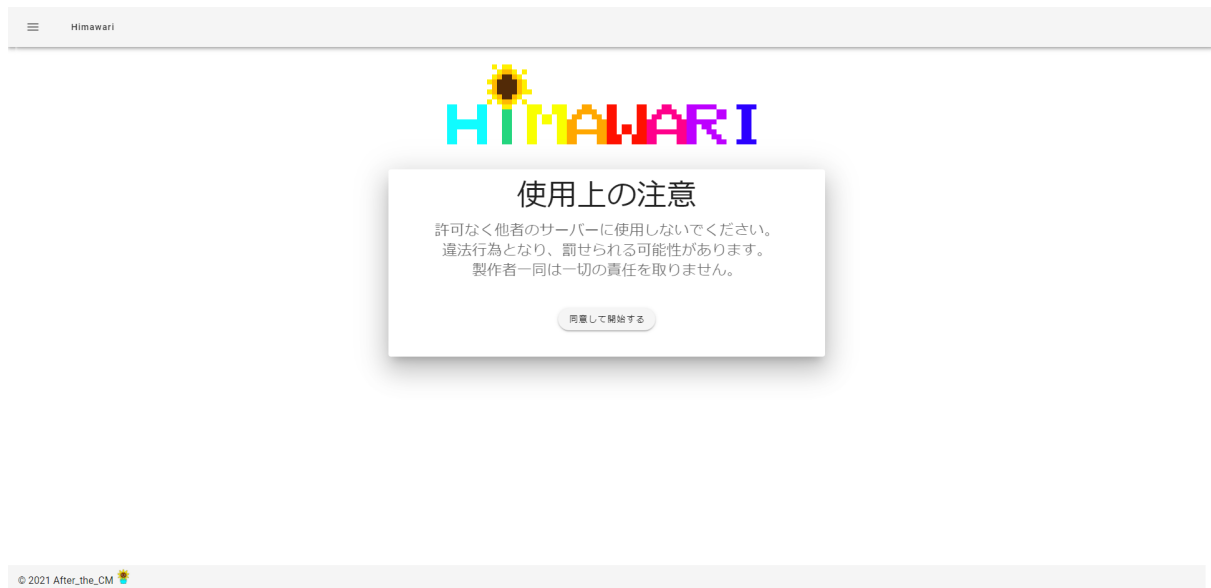
2. 診断を開始する

exec.shを実行すると、デフォルトのWebブラウザで `http://localhost:3000/` が開かれます。
※開かれない場合は手動で `http://localhost:3000/` にアクセスしてください。

このページにアクセスした時点でHimawari内の各種データをリセットしています。
構築済みのサイトマップ・実行中のScan・ダウンロードしていないレポート等が存在する場合はアクセスしないように注意してください。

使用上の注意を確認してください。

「同意して開始する」ボタンを押すことでHimawariの利用を開始できます。



3. サイトマップの構築

「同意して開始する」ボタンを押すと <http://localhost:3000/crawl> に遷移します。

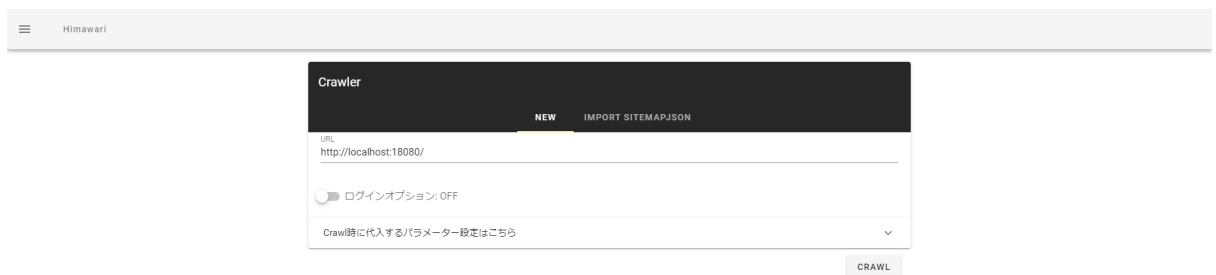
Scanを行う準備として、存在するページをリストアップする必要があります。
リストアップは、以下の二つの方法から選ぶことができます。

1. 自動でクローリングする
→ [手順 3.1 Crawl](#) へ
2. ダウンロード・編集したJSONファイルをアップロードする
→ [手順 3.2 Upload](#) へ

3.1 Crawl

診断対象サイトを自動でクローリングします。

1. 「URL」に診断対象サイトのURLを入力します。
※http又はhttpsから始まる完全なURLを入力してください。



The screenshot shows a web application interface for a crawler. At the top, there's a header with a hamburger menu icon and the text 'Himawari'. Below this is a dark-themed modal window titled 'Crawler'. Inside the modal, there are two tabs: 'NEW' (which is active) and 'IMPORT SITEMAPJSON'. Under the 'NEW' tab, there's a text input field labeled 'URL' containing the text 'http://localhost:18080/'. Below the input field is a toggle switch labeled 'ログインオプション: OFF'. At the bottom of the modal, there's a small text link that says 'Crawl時に代入する/パラメーター設定はこちら' with a downward arrow. To the right of the modal, there's a 'CRAWL' button.

© 2021 After_the_CM 🌻

2. 「ログインオプション」は対象にログイン機能が存在する場合に必要な設定です。
ログイン機能が存在しない場合はスキップしてください。

ログインオプションを有効にして、必要な情報を入力します。
少し複雑なため、入力例を用意しています。ご参照ください。

- a. 「**Login**フォームがあるURL」はログイン画面のURLです。
は、ログイン画面のURLの入力欄です。
リクエストのRefererの部分にあたります。
※http又はhttpsから始まる完全なURLを入力してください。
- b. 「**Login**リクエストの送信先」はログイン時に送信するリクエストのURLの入力欄
です。
※http又はhttpsから始まる完全なURLを入力してください。

- c. 「メソッド」ではパラメータが追加される箇所を選びます。
 - ・ GET → URLのクエリパラメータ
 - ・ POST → POSTボディ※リクエスト自体のメソッドとは異なる点に注意してください。
- d. 「**LoginKey**」はinputタグのname属性等です。
ログインリクエストのパラメータのnameを入力してください。
- e. 「**LoginValue**」はinputタグのvalue属性等です。
ログインリクエストのパラメータのvalueを入力してください。
- f. ログインパラメータが3個以上ある場合は「ログインパラメータ追加」から入力欄を増やすことができます。
- g. 不要になった入力欄は「削除」ボタンを押して削除してください。

example.

http://localhost:18080/login.php に存在するログインフォーム

```
<form action="auth.php" method="post">  
  <input type="text" name="name">  
  <input type="text" name="pass">  
  <input type="submit">  
</form>
```

上記のログインフォームがある場合の入力例

The screenshot shows the 'Crawler' application interface. At the top, there's a header with a menu icon and the name 'Himawari'. Below it, a dark bar contains 'NEW' and 'IMPORT SITEMAPJSON' buttons. The main area is divided into sections: 'URL' with a text input 'http://localhost:18080/', a 'ログインオプション' (Login Options) section with a toggle for 'ON', and a 'ログイン情報入力' (Login Information Input) section. This section contains two rows of configuration for login requests. The first row is for 'POST' method, with 'LoginKey' set to 'name' and 'LoginValue' set to 'yoden'. The second row is also for 'POST' method, with 'LoginKey' set to 'pass' and 'LoginValue' set to 'password'. Each row has a '削除' (Delete) button. At the bottom, there's a 'ログインパラメータ追加' (Add Login Parameters) button and a note 'Crawl時に代入するパラメーター設定はこちら' (Set parameters to be substituted at crawl time here).

3. 「**Crawl**時に代入するパラメータ」では、入力を必要とするページをCrawlする際にリクエストに入れる「key」と「value」を設定することができます。
入力値の検証等が存在する場合に必要な設定です。
- a. 「パラメータ追加」を押すことによりパラメータを追加できます。
 - b. 不要なパラメータは「削除」ボタンで削除をしてください。
 - c. keyが「*」の欄には、ここで指定されていないすべてのkeyのvalueを指定することができます。
 - d. もしkeyが「*」の欄が存在しない場合、ここで入力されていないkeyに対応するvalueはすべて空の状態でリクエストを送信します。

≡

Himawari

Crawler

NEWIMPORT SITEMAPJSON

URL

http://localhost:18080/

ログインオプション: OFF

Crawl時に代入するパラメータ設定はこちら

key	value	
*	Himawari	削除
key	hello	削除
email	Himawari@example.com	削除
url	http://example.com	削除
tel	00012345678	削除
date	2020-12-16	削除
text	Himawari	削除
textarea	Himawari	削除
input	I am Himawari	削除

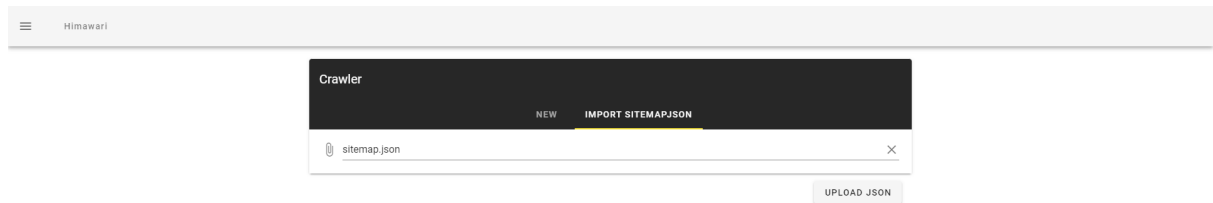
パラメーター追加

CRAWL

3.2 Upload

Crawlした結果であるsitemap.json(後述)をアップロードしてサイトマップを構築できます。
これにより、診断対象となるページの追加・削除を行うことができます。

1. 「クリップボタン」をクリックしてください。
2. JSONファイルを選択し、「**UPLOAD JSON**」ボタンをクリックしてください。



4. Scanの設定

Scan前にサイトマップの確認・Scanのオプション設定等を行います。

1. Sitemap

- a. サイトマップがツリー表示になっています。
クローリングが不十分だったり、Scanを行いたくないページがある場合は、以下の手順でサイトマップの構築をやり直すことができます。
 1. b からsitemap.jsonをダウンロード
 2. sitemap.jsonを編集
 3. 「3.2 Upload」からサイトマップをアップロード
- b. 「**DOWNLOAD SITEMAP**」ボタンを押すとsitemap.jsonとしてサイトマップをダウンロードできます。

2. Out of Scope

Crawlした際に発見したScope外のURLを表示します。
ここで表示されているURLにはCrawlもScanも実行されません。

ここに診断したいオリジンが含まれていた場合は 3. サイトマップの構築 から別途診断してください。

3. Scan Option

- a. 「**Full Scan**」「**Quick Scan**」のラジオボタンでは、「持続型クロスサイト・スクリプティング」のScanの有無を設定できます。
(※詳しくは機能説明書5.4をご参照ください)
- b. Crawlと同じように、「ログインオプション」を用意しています。
Crawlの際に入力した情報が自動入力されるようになっています。必要に応じて変更してください。(詳しい操作は 3.1 Crawl を参照してください。)
- c. 「**Start Scan**」を押すことによりScanを実行することができます。

Scanner

Sitemap

1. /[]
1. osc[]-[]
1. 404
2. OSCIQP.php
3. OSCIQV.php
4. OSCiUA.php
5. OSCiReferer.php
6. OSCiBP.php
7. OSCiBV.php
8. OSCiCookie.php
9. form.php
10. 301.php
11. OSCi301.php
12. 307.php
13. OSCi307.php
14. OSCiML.php
15. login.php

Download Sitemap

ScanOption

☒ Full Scan
☐ Quick Scan

☐ ログインオプション: OFF

Start Scan

Out-Of-Scope

Find in http://localhost:18080/

1 http://example.com

5. レポート

Scan開始後、<http://localhost:3000/report> に遷移します。
この画面では、以下を表示します。

- ・検出した脆弱性のCWE番号
- ・検出した脆弱性の名前
- ・脆弱性の重要度(severity)
- ・発見した脆弱性の件数
- ・脆弱性の説明
- ・脆弱性による被害を防ぐための必須対策
- ・脆弱性による被害を軽減するための保険的対策
- ・脆弱性を検出したParameter
- ・脆弱性を検出した際に利用したPayload
- ・脆弱性が存在すると判断をした証拠となるEvidence
- ・脆弱性を検出した際のHimawariからWebサーバへのリクエスト
- ・脆弱性を検出した際のWebサーバからHimawariへのレスポンス

1. 見つかった脆弱性一覧は動的に更新されていきます。
2. Scanが終了すると「**Download Report(Markdown)**」ボタンが表示され、Reportのダウンロードが行えます。

CWE-78	OSコマンド・インジェクション	High	13	^
<div>脆弱性の説明</div> <p>OSコマンド・インジェクションは、シェルの不適切な呼び出し方をしている場合に意図しないOSコマンドの実行が可能になる脆弱性です。</p> <p>OSコマンド・インジェクションの脆弱性が存在すると、攻撃者によって情報漏洩、任意のOSコマンドの実行、不正なシステム操作、他システムへの攻撃の踏み台などの攻撃を受ける可能性があります。</p> <div>必須対策</div> <p>可能な限り、シェルを呼び出す機能のある関数の利用は避けましょう。</p> <p>ライブラリを使った実装に切り替えることができないかを検討してください。</p> <p>シェルを呼び出す機能のある関数を利用する場合は、外部からのパラメータを渡さないように実装しましょう。</p> <div>保険的対策</div> <p>シェルを呼び出す機能のある関数を利用する場合は、その引数を構成する変数を調べ、許可した処理のみ実行するように実装しましょう。</p>				
1	http://localhost:18080/osc/	Parameter: Path		▼
2	http://localhost:18080/osc/404	Parameter: Added by Himawari		▼
3	http://localhost:18080/osc/OSCIQP.php	Parameter: Added by Himawari		▲
<div><div><div>Parameter</div><div>Added by Himawari</div></div><div><div>Payload</div><div> sleep 3 </div></div><div><div>Evidence</div><div>Response delay: 3.0036282s</div></div></div> <div><div>Request</div><div>GET /osc/OSCIQP.php?%7C+sleep+3+%7C=1 HTTP/1.1 Host: localhost:18080 User-Agent: Himawari Cookie: input=aaa Referer: http://localhost:18080/osc/ Accept-Encoding: gzip</div></div> <div><div>Response</div><div>HTTP/1.1 200 OK Transfer-Encoding: chunked Connection: keep-alive Content-Type: text/html; charset=UTF-8 Date: Fri, 19 Nov 2021 09:15:49 GMT Server: nginx/1.21.4 X-Powered-By: PHP/7.4.26 c9 <p>plz redirect to ?sleep 5;-a</p> <form method="get"> <input type="text" name="input"> <input type="submit"> </form> <p>current url RawQuery: sleep 3 =1</p> 0</div></div>				
4	http://localhost:18080/osc/OSCIQP.php	Parameter: input		▼
5	http://localhost:18080/osc/OSCIQV.php	Parameter: input		▼
6	http://localhost:18080/osc/OSCIUA.php	Parameter: User-Agent		▼
7	http://localhost:18080/osc/OSCIReferer.php	Parameter: Referer		▼
8	http://localhost:18080/osc/OSCIBP.php	Parameter: Added by Himawari		▼
9	http://localhost:18080/osc/OSCIBP.php	Parameter: hoge		▼
10	http://localhost:18080/osc/OSCI@V.php	Parameter: input		▼
11	http://localhost:18080/osc/OSCICookie.php	Parameter: input		▼
12	http://localhost:18080/osc/301.php	Parameter: input		▼
13	http://localhost:18080/osc/OSCI307.php	Parameter: input		▼
CWE-79	反射型クロスサイト・スクリプティング	High	12	▼
CWE-352	クロスサイト・リクエスト・フォージェリ	Medium	6	▼

Download Report(Markdown)

Scan completed

×

CWE-89	SQL インジェクション	High	1	▼
CWE-78	OSコマンド・インジェクション	High	13	▼
CWE-79	反射型クロスサイト・スクリプティング	High	11	▼

Download Report(Markdown)

6. 停止

Himawariはexec.shを実行したターミナルで「**Ctrl + C**」を入力することで停止できます。