

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取りません。

推奨ブラウザ

動作確認の出来ている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

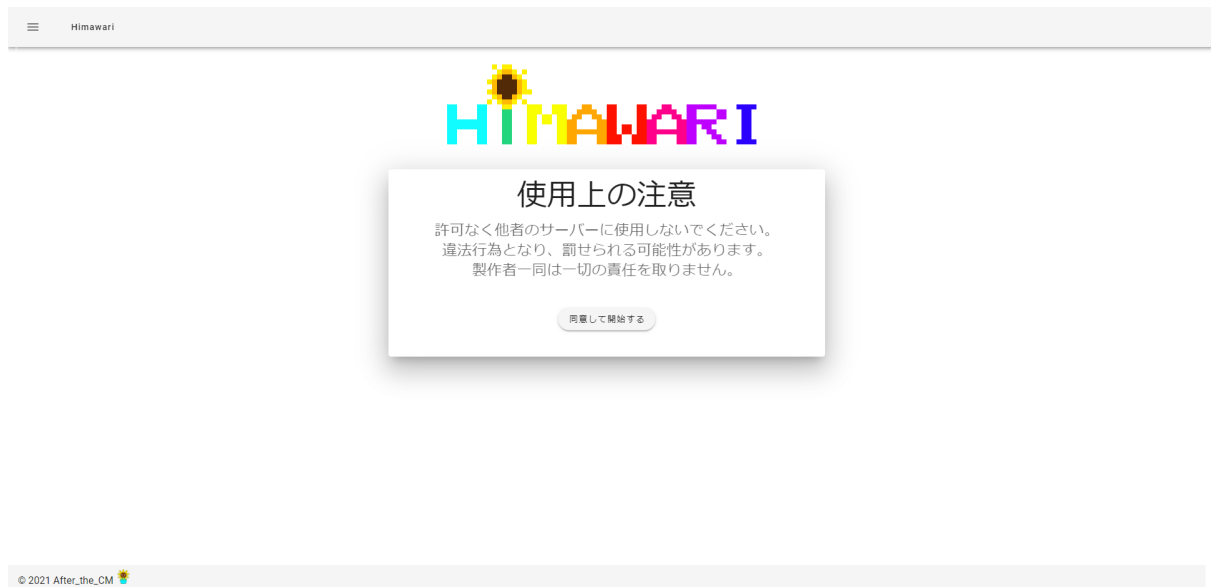
インストール手順書に従い、Himawariをインストールしてください。
インストール済の場合、以下のコマンドでHimawariを起動出来ます。

```
$ bash exec.sh
```

2. 倫理規定

デフォルトのブラウザで <http://localhost:3000/> が開かれるはずです。
(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。)

使用上の注意を確認してください。
「同意して開始する」を押下することでHimawariの利用を開始できます。



3. サイトマップの構築

開始ボタンを押下すると `http://localhost:3000/crawl` に遷移します。

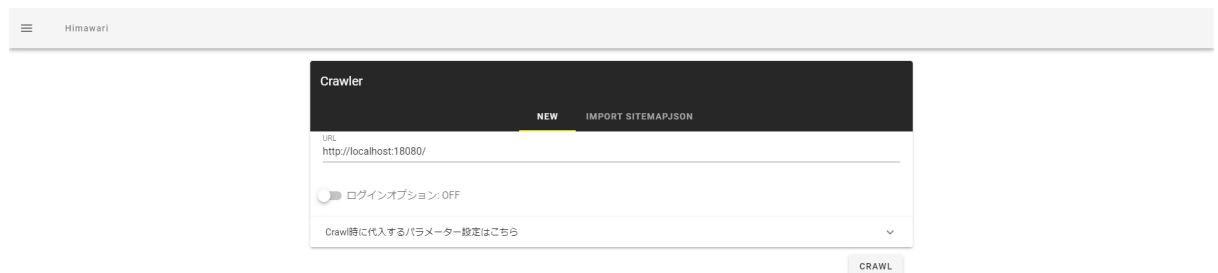
Scanを行う準備として、存在するページをリストアップする必要があります。
リストアップは、以下の二つの方法から選ぶことができます。

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

対象サイトを自動でクローリングします。

1. 「URL」に診断対象のURLを入力します。



The screenshot shows a web application interface for a crawler. At the top, there is a header with a hamburger menu icon and the text 'Himawari'. Below the header, there is a dark-themed modal window titled 'Crawler'. Inside the modal, there are two tabs: 'NEW' (which is highlighted) and 'IMPORT SITEMAPJSON'. Under the 'NEW' tab, there is a text input field labeled 'URL' containing the text 'http://localhost:18080/'. Below the input field, there is a toggle switch for 'ログインオプション' (Login Option) which is currently turned off. At the bottom of the modal, there is a link that says 'Crawl時に代入するパラメーター設定はこちら' (Click here for parameter settings to be substituted during crawling). To the right of the modal, there is 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、必要な情報を入力してください。

- a. 「**Login**フォームがある**URL**」はログイン画面のURLです。
リクエストのRefererの部分にあたります。
- b. 「**Login**リクエストの送信先」はログイン画面のformタグのaction属性です。
リクエストの送信先にあたります。
- 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。

The screenshot shows the 'Crawler' application interface. At the top, there's a header with a menu icon and the text 'Hitmawari'. Below the header, there's a dark bar with 'Crawler' and two tabs: 'NEW' (selected) and 'IMPORT SITE MAP JSON'. The main area has a URL input field with 'http://localhost:18080/'. Below that, a toggle switch for 'ログインオプション ON' is turned on. The 'ログイン情報入力' section contains two text fields for 'LoginフォームがあるURL (url)' and 'Login/クエスリの読取り' (both set to 'http://localhost:18080/robots/login.php'). Below these are two rows of parameter configuration. Each row has a 'メソッド' dropdown set to 'POST', a 'Loginkey' field, and a 'Loginvalue' field. The first row has 'name' as the key and 'yoden' as the value. The second row has 'pass' as the key and 'pass' as the value. Each row has a '削除' button. At the bottom, there's a 'ログインパラメータ追加' button and a link 'Crawlerに代入するパラメータ設定はこちら'. A 'Crawl' button is at the bottom right.

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。
入力値の検証等がある場合に必要になる設定です。
- 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はすべて空の状態の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

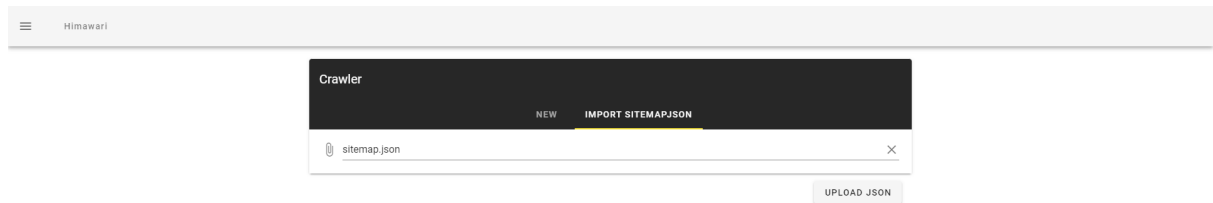
パラメーター追加

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. 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. スキャンの設定

スキャン前にサイトマップの確認・スキャン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、スキャン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。

ここにも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をご覧ください)
- 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の際に入力した時の情報が自動入力されるようになっていますが、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. osel[-]
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。

- ・脆弱性が存在するページのURL
- ・パラメータ
- ・見つかった件数
- ・ペイロード
- ・エビデンス
- ・リクエスト
- ・レスポンス
- ・その脆弱性の説明
- ・必須対策
- ・保険的対策

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。

Himawari

CWE-78OSコマンド・インジェクションHigh5

脆弱性の説明

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悪用しないOSコマンドの実行が可能になる脆弱性です。
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。

必須対策

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。
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。
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。

保険的対策

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、許可した範囲のみ実行するように実装しましょう。

1http://localhost:18080/osc/ParameterPathPayload/osc/ sleep 3EvidenceResponse delay: 3.0082947s

リクエスト

GET /osc/%7c%20sleep%203 HTTP/1.1
Host: localhost:18080
User-Agent: Himawari
Referer: http://localhost:18080/
Accept-Encoding: gzip

レスポンス

HTTP/1.1 200 OK
Transfer-Encoding: chunked
Connection: keep-alive
Content-Type: text/html; charset=UTF-8
Date: Thu, 18 Nov 2021 14:10:05 GMT
Server: nghttp/1.21.3
X-Powered-By: PHP/7.4.25

0b
<p>git redirect to /a/sleep 5</p>
<p>current url: Path: /osc/ sleep 3</p>
0

2http://localhost:18080/osc/404Parameter: Added by Himawari

3http://localhost:18080/osc/OSCIQP.phpParameter: Added by Himawari

4http://localhost:18080/osc/OSCIQP.phpParameter: input

5http://localhost:18080/osc/OSCIQP.phpParameter: input

CWE-79反射型クロスサイト・スクリプティングHigh3

脆弱性の説明

反射型クロスサイト・スクリプティング(XSS)は、攻撃者によって仕掛けられた悪意のあるスクリプトをサイトに貼られたユーザのブラウザ上で実行させることができる脆弱性です。
XSSの攻撃を受けたユーザは、ユーザ自身のアカウントでWebアプリケーションの機能を悪用されたり、Cookieの値を盗まれて成りすましの被害に合う可能性があります。

必須対策

悪意内容・属性値の文字をエスケープして、属性値はダブルクォーテーションでくくります。
(例: < を < にする等、HTML特殊文字はHTMLエンティティに置き換えます。)
HTTPレスポンスヘッダのContent-Typeフィールドに文字コードを指定しましょう。文字コードの指定を省略している場合、Webアプリケーションとブラウザとの文字エンコーディングの差異でXSSの原因になります。

保険的対策

XSS Protectionレスポンスヘッダを利用することでブラウザ機能により反射型XSSを無害な出力に変換できます。XSS Protectionレスポンスヘッダを利用しては利用者が悪用化している場合でも上書きして有効にすることができ、CSP(Content Security Policy)を設定することでevalを禁止、インラインスクリプトを禁止にする等、スクリプトに対してより強い制約を設けることができます。入力値の検証は行ったほうがよいです。この対策は設定ですが、郵便番号など文字の範囲や入力値の長さを知ることができる型所に要求していない入力された場合はエラーを表示し、再入力を求めるようにすることでスクリプトを注入できないようにすることができます。上記の検証はサーバ側で行いましょう。クライアント上で入力値の検証を行ったとしても、プロキシツールなどの使用により攻撃者は要求を満たしていない種の送信が可能です。これを防ぐために、サーバ側で適切な検証を行いましょう。CookieにhttpOnly属性を付与するとCookieに保存されている情報へのアクセスを防ぐことができます。

1http://localhost:18080/osc/404Parameter: Added by Himawari

2http://localhost:18080/osc/OSCIQP.phpParameter: Added by Himawari

3http://localhost:18080/osc/OSCIQP.phpParameter: input

© 2021 After, the CM

☰

Himawari

Scan completed

CWE ID	脆弱性名	リスク	件数	
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)