Web アプリケーション・レポート

このレポートには、Web アプリケーションに関する重要なセキュリティー情報が含まれています。

セキュリティー・レポート

このレポートは IBM Security AppScan Standard によって作成されました 9.0.3.7 iFix004, ルール: 12676
スキャン開始時刻: 2018/06/12 17:47:07

目次

はじめに

概要

問題のタイプ別にソートされた問題

推奨される修正

- 有害な文字のインジェクションに対して考えられる解決策を確認します
- ディレクトリーの一覧表示を拒否するようにサーバーの設定を変更し、使用できる最新のセキュリティー・パッチをインストールします
- Content-Security-Policy ヘッダーを使用するようにサーバーを構成してください
- Web サーバーの HTTP TRACE サポートを無効にします
- Web サイトから内部 IP アドレスを削除します
- X-Content-Type-Options ヘッダーを使用するようにサーバーを構成してください
- X-XSS-Protection ヘッダーを使用するようにサーバーを構成してください
- クエリー・ストリングで送信されるボディー・パラメーターを受け入れる受け入れません
- すべてのセッション Cookie に HttpOnly 属性を追加してください。
- パラメーター値が期待される範囲とタイプであることを確認します。デバッグ・エラー・メッセージおよび例外を出力しないようにします。
- ビジネスおよびセキュリティー・ロジックをクライアント側から削除します
- 仮想ディレクトリーから古いバージョンのファイルを削除します
- 禁止されているリソースについて「404 - Not Found」レスポンス・ステータス・コードを送出するか、完全に削除します
- 秘密のセッション情報をパーマネント Cookie に保存しないようにします

アドバイザリー

- クロスサイト・スクリプティング
- ディレクトリーの一覧作成
- フレームからのフィッシング
- Content-Security-Policy ヘッダーが欠落しています
- TRACE および TRACK HTTP メソッドが有効
- X-Content-Type-Options ヘッダーが欠落しています
- X-XSS-Protection ヘッダーが欠落しています
- セッション Cookie に HttpOnly 属性がありません
- ボディー・パラメーターをクエリーで送信
- 一時ファイルのダウンロード
- 秘密セッション情報を含むパーマネント Cookie
- 非表示のディレクトリーを検出
- アプリケーション・エラー
- クライアント側 (JavaScript) Cookie 参照
- 内部 IP の開示パターンを発見

アプリケーション・データ

- Cookie
- JavaScript
- パラメーター
- コメント
- 認識された URL
- 失敗した要求
- フィルタリングされた URL

はじめに

このレポートには、IBM Security AppScan Standard が実行した Web アプリケーション・セキュリティー・スキャンの結果が含まれています。

重大度の高い問題:	1
中重大度の問題:	5
低重大度の問題:	25
情報として示された問題:	16
レポートに含まれているセキュリティー問題の合計:	47
スキャンで発見されたセキュリティー問題の合計:	47

全般情報

スキャン・ファイル名: org

スキャン開始時刻: 2018/06/12 17:47:07

テスト・ポリシー: Default

ホスト	10.228.148.130
ポート	0
オペレーティング・システム:	Unix
Web サーバー:	Oracle Web Listener
アプリケーション・サーバー:	PHP

ログイン設定

ログイン方法: なし

概要

問題のタイプ 15

TOC

	問題のタイプ	問題の数
高	クロスサイト・スクリプティング	1
中	ディレクトリーの一覧作成	4
中	フレームからのフィッシング	1
低	Content-Security-Policy ヘッダーが欠落しています	4
低	TRACE および TRACK HTTP メソッドが有効	1
低	X-Content-Type-Options ヘッダーが欠落しています	4
低	X-XSS-Protection ヘッダーが欠落しています	4
低	セッション Cookie に HttpOnly 属性がありません	2
低	ボディ・パラメーターをクエリーで送信	1
低	一時ファイルのダウンロード	1
低	秘密セッション情報を含むパーマネント Cookie	2
低	非表示のディレクトリーを検出	6
情	アプリケーション・エラー	9
情	クライアント側 (JavaScript) Cookie 参照	2
情	内部 IP の開示パターンを発見	5

脆弱性のある URL 17

TOC

	URL	問題の数
高	http://10.228.148.130/app/org	13
中	http://10.228.148.130/	1
中	http://10.228.148.130/app/org/	10
中	http://10.228.148.130/icons/	1
中	http://10.228.148.130/icons/small/	1
低	http://10.228.148.130/app/org/detail/130102044	5
低	http://10.228.148.130/app/org/list	5

低	http://10.228.148.130/app/css/	1
低	http://10.228.148.130/app/images/	1
低	http://10.228.148.130/app/js/	1
低	http://10.228.148.130/app/uploads/	1
低	http://10.228.148.130/cgi-bin/	1
低	http://10.228.148.130/mrtg/	1
情	http://10.228.148.130/app/home/trackLog	2
情	http://10.228.148.130/app/js/functionCommon.js	1
情	http://10.228.148.130/app/js/jquery.cookie.js	1
情	http://10.228.148.130/app/org/detail/130100001	1

推奨される修正 14

TOC

	修復タスク	問題の数
高	有害な文字のインジェクションに対して考えられる解決策を確認します	2
中	ディレクトリーの一覧表示を拒否するようにサーバーの設定を変更し、使用できる最新のセキュリティー・パッチをインストールします	4
低	Content-Security-Policy ヘッダーを使用するようにサーバーを構成してください	4
低	Web サーバーの HTTP TRACE サポートを無効にします	1
低	Web サイトから内部 IP アドレスを削除します	5
低	X-Content-Type-Options ヘッダーを使用するようにサーバーを構成してください	4
低	X-XSS-Protection ヘッダーを使用するようにサーバーを構成してください	4
低	クエリー・ストリングで送信されるボディー・パラメーターを受け入れる受け入れません	1
低	すべてのセッション Cookie に HttpOnly 属性を追加してください。	2
低	パラメーター値が期待される範囲とタイプであることを確認します。デバッグ・エラー・メッセージおよび例外を出力しないようにします。	9
低	ビジネスおよびセキュリティー・ロジックをクライアント側から削除します	2
低	仮想ディレクトリーから古いバージョンのファイルを削除します	1
低	禁止されているリソースについて「404 - Not Found」レスポンス・ステータス・コードを送出するか、完全に削除します	6
低	秘密のセッション情報をパーマネント Cookie に保存しないようにします	2

セキュリティー・リスク 9

TOC

	リスク	問題の数

高	ハッカーが正規のユーザーになりすまし、ユーザーのレコードを表示または改変したり、ユーザーとしてトランザクションを実行するのに使用することができる、カスタマー・セッションおよび Cookie を盗み出したり操作することができる可能性があります	4
中	制限のかけられたファイルを含む可能性のある Web アプリケーションの仮想ディレクトリーの内容を、表示およびダウンロードすることができます	4
中	知識の乏しいユーザーに、ユーザー名、パスワード、クレジット・カード番号、社会保険番号などの秘密情報を提供するように求めることができます	14
低	ユーザー名、パスワード、マシン名などの Web アプリケーションに関する秘密情報や、秘密のファイルの場所などの情報を取得することができます	18
低	アプリケーション・ロジック、およびユーザー名やパスワードなどのその他の秘密情報を公開する可能性のある一時スクリプト・ファイルをダウンロードできます	1
低	パーマネント Cookie としてディスク上に保存されたセッション情報 (Cookie) を盗み出せる可能性があります	2
低	攻撃者が Web サイトをマップするのに利用できるサイトのファイル・システム構造についての情報を取得することができます	6
情	秘密のデバッグ情報を収集することができます	9
情	この攻撃による最悪のケースのシナリオは、コンテキストとクライアント側で作成された Cookie の役割によって異なります	2

原因 10

TOC

	原因	問題の数
高	ユーザーの入力内容に対する有害文字の除去が適切に行われませんでした	2
中	ディレクトリー・ブラウジングが有効になっています	4
低	セキュリティーで保護されていない Web アプリケーション・プログラムまたは設定	18
低	Web サーバーまたはアプリケーション・サーバーが安全でない方法で設定されています	7
低	Web アプリケーションが HttpOnly 属性のないセッション Cookie を設定しています	2
低	テンポラリー・ファイルが製作環境に残されています	1
低	Web アプリケーションがパーマネント Cookie に秘密のセッション情報を (ディスク上) を格納しています	2
情	受信したパラメーター値について、適切な境界チェックが行われませんでした	9
情	ユーザーの入力が必要なデータ型式に一致することを確認するための検証が行われませんでした	9
情	クライアント側に Cookie を作成します	2

WASC 脅威の分類

TOC

脅威	問題の数
クロスサイト・スクリプティング	1
コンテンツ・スプーフィング	1
ディレクトリー索引付け	4
機能の悪用	1
情報漏えい	37
不適切なセッション有効期限	2
予測可能なリソースの位置	1

問題のタイプ別にソートされた問題

高 クロスサイト・スクリプティング 1 TOC

問題 1 / 1 TOC

クロスサイト・スクリプティング

重大度:	高
CVSS スコア:	7.5
URL:	http://10.228.148.130/app/org
エンティティー:	kankei_kikan (Parameter)
リスク:	ハッカーが正規のユーザーになりすまし、ユーザーのレコードを表示または改変したり、ユーザーとしてトランザクションを実行するのに使用することができる、カスタマー・セッションおよび Cookie を盗み出したり操作することができる可能性があります
原因:	ユーザーの入力内容に対する有害文字の除去が適切に行われませんでした
修正:	有害な文字のインジェクションに対して考えられる解決策を確認します

差: **パラメーター** 操作元: 操作先: `'"</script><svg/onload=alert(1610) width=100/>`

論拠: Appscan によりスクリプト (ユーザーのブラウザーにページがロードされるときに実行される) が応答に正常に埋め込まれたため、テスト結果では脆弱性が示されていると考えられます。

テスト要求と応答:

```
POST /app/org HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.228.148.130/app/org
Cookie: soudanList=;
laravel_session=eyJpdiI6IlNyRlkyallKc2dKNGpGdWFFVDVLOXc9PSIsInZhbHVlIjoiWlFpUTkzUVphcHVBYnFIZzM5T
015bjgxVFBOUEllbXROY1Y0N1g0YmNydnI4RUZia0dZeGE3dlwvdXZCbGg5NnowQWdlVmhEQ0x4Y1c0YVJnUjJwS0RBPT0iLC
JtYWMiOiJjNGNiMzM5MTFmN2JhMGI5YmJmNmEwMTczMDhlNDE0MmNlMWI0NjYwNjJjNDM0YzdkZWYyNTYzZGEzNmU3MmM5In0
%3D; XSRF-
TOKEN=eyJpdiI6IjdlUWlKaHZ3NFZiS1F4ZDZrUld3dmc9PSIsInZhbHVlIjoiWVRaOE9wbVpOMDNpNzJPaW9Mak50cUxxVld
0OUdXZTVKbk5Sd1ZKVU5zd2RnWTFqcTNSbG1ucERIN1dJOFM4QVpsZnBCbHc3ZEx0NENORzQyUHI0Z3c9PSIsIm1hYyI6IjFl
YWQ5NDRkZThiOTFiZTM5OGNhMGJmMTVmZDAwNzdlNjdlNGE4OGE4ZWNmY2U1MDY5ODg1MzQ5NThiMGZmNjIifQ%3D%3D;
PHPSESSID=6ebsdplhncev03jjcb2lklcia0
Connection: Keep-Alive
Host: 10.228.148.130
Pragma: no-cache
Content-Length: 256
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
```

```
application/x-ms-xbap, */*
Accept-Language: ja-JP
Content-Type: application/x-www-form-urlencoded

_token=yuEor3ontYoqIVemgYB9Md6zAOEcgAoJnyhA89RA&key_pref=13&key_addr=&kankei_kikan='"</script>
<svg/onload=alert(1610)
width=100/>&key_keyword=&key_new=%E6%96%B0%E8%A6%8F&key_update=%E5%A4%89%E6%9B%B4&key_publish=%E5
%85%AC%E9%96%8B&submit=%E6%A4%9C%E7%B4%A2

HTTP/1.1 200 OK
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
default-style: IE=edge
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ikxhb0QwRXdtVUFSRE1wdlBtcWQ5SGc9PSIsInZhbHVlIjoiRTZseEdxd28yM0ZOR0IzV0ZwVmY1UEo4cHF
UUGt4Vkp5UldFNDliemJHWVlRb1FaWFQzQnFaXC9OaFdZUFR6U3MzbzZHUFZXTitBVFBiUmFnOGtNVEpRPT0iLCJtYWMiOiJm
YjhmZGZjYTQ5NGVjMTkyYjY3MTcxZGM3N2VmNmVkMjM4ODI0ZWU1OWNmNDlmZDcwZDVkNDM4ZDRmNzNiZTU1In0%3D;
expires=Tue, 12-Jun-2018 11:00:37 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6ImswSW43ck4rVG9cL2xQSXZieVJicXpBPT0iLCJ2YWx1ZSI6IjBEWWFxXC9GNER5SkF6WG9VR
mFXbU5PbWxRa0hPSDlTTFd6ZThPU1dyeTYzSXloXC9meit4Zmc1Z3dtcnA1N2xZZzlQUTNGUmswRWFMRlNpQzYzc08zRUE9PS
IsImlhYyI6ImE5Mzg5ODZmNTYyYjIzZDZiZWY0ZGNkYzc4YjI5ZDBiMjlhMDA4ZDFhNzUyYWFhZjM4ODJiMDFhYjVmYzE2NGY
ifQ%3D%3D; expires=Tue, 12-Jun-2018 11:00:37 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.30
Connection: Keep-Alive
Date: Tue, 12 Jun 2018 09:00:37 GMT
Keep-Alive: timeout=5, max=46
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-cache, private
Transfer-Encoding: chunked

<!DOCTYPE HTML>
<html lang="ja">
<head><meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<meta name="Author" content="Houterasu" />
<meta http-equiv="DEFAULT-STYLE" content="IE=edge" />
<meta name="viewport" content="width=device-width,initial-scale=1.0,shrink-to-fit=no" />
<link rel="shortcut icon" href="/app/images/100555157.gif" />
<title>相談窓口検索　法テラス</title>
<link rel="stylesheet" href="/app/css/bootstrap.min.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_layout.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_style.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_pc.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_print.css" type="text/css" media="print" />

</head>
<body id="base" class="container-fluid">
    <!-- scs_jyogai_start -->
<div id="basebg">
    <noscript>
        <p class="jsmessage">法テラス公式ホームページではJavaScriptを使用しています。
          <br/>JavaScriptの使用を有効にしていない場合は、一部の機能が正確に動作しない恐れがあります。
          <br/>お手数ですがJavaScriptの使用を有効にしてください。</p>
    </noscript>
    <div class="blockjump">
        <a id="PTOP"></a>
    </div>

    <div id="blockskip">
        <script src="/app/js/jquery-1.9.1.min.js"></script>
        <script>
          $(function () {
          $("#blockskip a").focus(function () {
          $(this)
          .parent()
          .animate({
          height: '1.5em'
          }, { duration: 'fast' })
          .addClass("show");
          });
          $("#blockskip a").blur(function () {
          $(this)
          .parent()
          .animate({
          height: '1px'
          }, {
```

```
            duration: 'fast',
            complete: function () {
            $(this).removeClass("show");
            }
            })
            });
            });
          </script>
          <a href="#">このページの本文へ移動</a>
      </div>
      <div id="b
...
...
...

            var valueRadio = '"</script><svg/onload=alert(1610) width=100/>';
            initCheckedRadio(valueRadio);
            disableLanguageDropdown();
            clearMessgeWhenBackBrowser('soudanList');
          });
...
...
...
```

テスト応答

中 ディレクトリーの一覧作成 4 TOC

問題 1 / 4 TOC

ディレクトリーの一覧作成

重大度:	中
CVSS スコア:	6.4
URL:	http://10.228.148.130/app/org/
エンティティー:	10.228.148.130 (Global)
リスク:	制限のかけられたファイルを含む可能性のある Web アプリケーションの仮想ディレクトリーの内容を、表示およびダウンロードすることができます
原因:	ディレクトリー・ブラウジングが有効になっています
修正:	ディレクトリーの一覧表示を拒否するようにサーバーの設定を変更し、使用できる最新のセキュリティー・パッチをインストールします

差: **パス** 操作元: `/app/org/` 操作先: `http://demo.testfire.net`
ヘッダー 操作元: `10.228.148.130` 操作先: `demo.testfire.net`
操作元: `HTTP/1.1` 操作先: `HTTP/1.0`

論拠: レスポンスがディレクトリーの内容 (ディレクトリー一覧) を含んでいます。これは、サーバーでディレクトリー内容の一覧表示が許可されていることを示しています。通常、このような設定は推奨されません。

テスト要求と応答:

```
GET http://demo.testfire.net HTTP/1.0
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Host: demo.testfire.net
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


HTTP/1.1 200 OK
Connection: Keep-Alive
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
Content-Length: 481
Keep-Alive: timeout=5, max=100
Date: Tue, 12 Jun 2018 08:48:02 GMT
Content-Type: text/html;charset=ISO-8859-1

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /</title>
 </head>
 <body>
<h1>Index of /</h1>
  <table>
```

```
   <tr><th valign="top"><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?
C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?
C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
   <tr><th colspan="5"><hr></th></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
</body></html>
```

テスト応答

問題 2 / 4

TOC

ディレクトリーの一覧作成

重大度:	中
CVSS スコア:	6.4
URL:	http://10.228.148.130/icons/
エンティティー:	icons/ (Page)
リスク:	制限のかけられたファイルを含む可能性のある Web アプリケーションの仮想ディレクトリーの内容を、表示およびダウンロードすることができます
原因:	ディレクトリー・ブラウジングが有効になっています
修正:	ディレクトリーの一覧表示を拒否するようにサーバーの設定を変更し、使用できる最新のセキュリティー・パッチをインストールします

差: **パス** 操作元: `/app/org/` 操作先: `/icons/`

論拠: レスポンスがディレクトリーの内容 (ディレクトリー一覧) を含んでいます。これは、サーバーでディレクトリー内容の一覧表示が許可されていることを示しています。通常、このような設定は推奨されません。

テスト要求と応答:

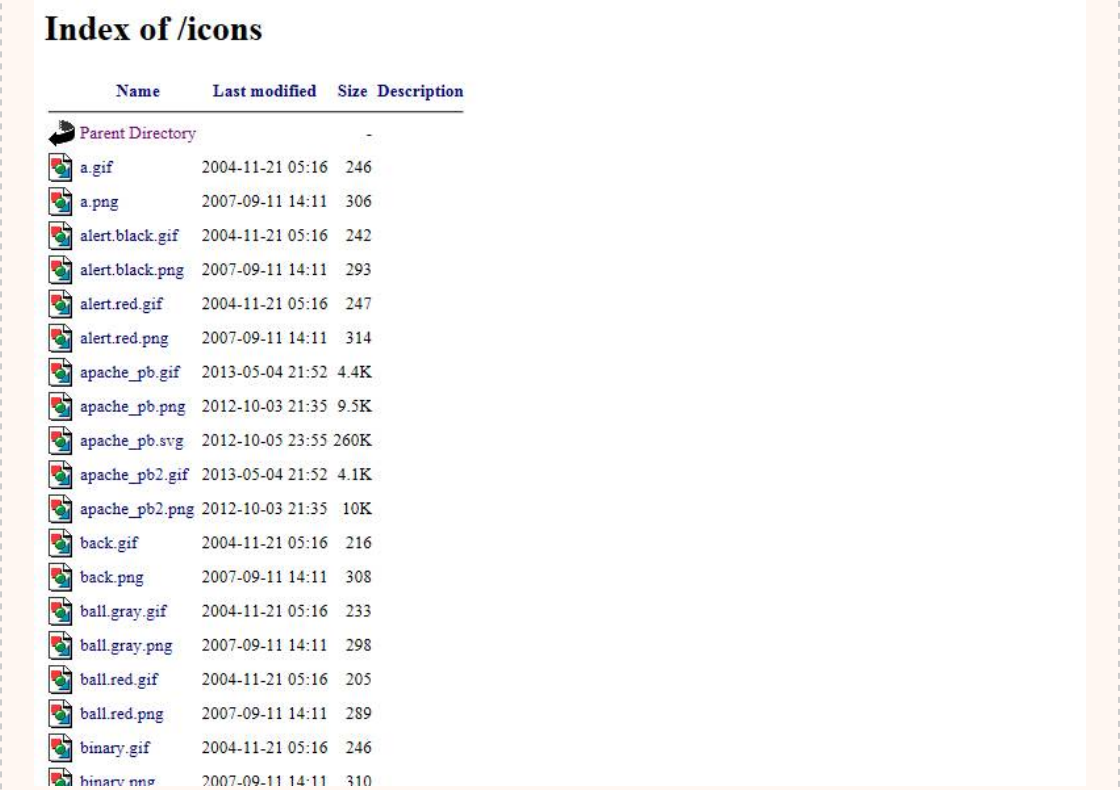
```
GET /icons/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


HTTP/1.1 200 OK
Transfer-Encoding: chunked
Connection: Keep-Alive
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
Keep-Alive: timeout=5, max=100
Date: Tue, 12 Jun 2018 09:11:03 GMT
Content-Type: text/html;charset=ISO-8859-1

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /icons</title>
 </head>
 <body>
<h1>Index of /icons</h1>
  <table>
   <tr><th valign="top"><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?
C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?
C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
   <tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[PARENTDIR]"></td><td><a href="/">Parent
Directory</a>       </td><td> </td><td align="right">  - </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a href="a.gif">a.gif</a>
</td><td align="right">2004-11-21 05:16  </td><td align="right">246 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a href="a.png">a.png</a>
</td><td align="right">2007-09-11 14:11  </td><td align="right">306 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="alert.black.gif">alert.black.gif</a>        </td><td align="right">2004-11-21 05:16  </td>
<td align="right">242 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="alert.black.png">alert.black.png</a>        </td><td align="right">2007-09-11 14:11  </td>
<td align="right">293 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="alert.red.gif">alert.red.gif</a>          </td><td align="right">2004-11-21 05:16  </td><td
align="right">247 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="alert.red.png">alert.red.png</a>          </td><td align="right">2007-09-11 14:11  </td><td
align="right">314 </td><td> </td></tr>
```

```
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="apache_pb.gif">apache_pb.gif</a>          </td><td align="right">2013-05-04 21:52  </td><td
align="right">4.4K</td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="apache_pb.png">apache_pb.png</a>          </td><td align="right">2012-10-03 21:35  </td><td
align="right">9.5K</td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="apache_pb.svg">apache_pb.svg</a>          </td><td align="right">2012-10-05 23:55  </td><td
align="right">260K</td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="apache_pb2.gif">apache_pb2.gif</a>         </td><td align="right">2013-05-04 21:52  </td>
<td align="right">4.1K</td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="apache_pb2.png">apache_pb2.png</a>         </td><td align="right">2012-10-03 21:35  </td>
<td align="right"> 10K</td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="back.gif">back.gif</a>          </td><td align="right">2004-11-21 05:16  </td><td
align="right">216 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="back.png">back.png</a>          </td><td align="right">2007-09-11 14:11  </td><td
align="right">308 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="ball.gray.gif">ball.gray.gif</a>          </td><td align="right">2004-11-21 05:16  </td><td
align="right">233 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="ball.gray.png">ball.gray.png</a>          </td><td align="right">2007-09-11 14:11  </td><td
align="right">298 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="ball.red.gif">ball.red.gif</a>          </td><td align="right">2004-11-21 05:16  </td><td
align="right">205 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="ball.red.png">ball.red.png</a>          </td><td align="right">2007-09-11 14:11  </td><td
align="right">289 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.g
...
...
...
```

テスト応答



Index of /icons

Name	Last modified	Size	Description
Parent Directory		-	
a.gif	2004-11-21 05:16	246	
a.png	2007-09-11 14:11	306	
alert.black.gif	2004-11-21 05:16	242	
alert.black.png	2007-09-11 14:11	293	
alert.red.gif	2004-11-21 05:16	247	
alert.red.png	2007-09-11 14:11	314	
apache_pb.gif	2013-05-04 21:52	4.4K	
apache_pb.png	2012-10-03 21:35	9.5K	
apache_pb.svg	2012-10-05 23:55	260K	
apache_pb2.gif	2013-05-04 21:52	4.1K	
apache_pb2.png	2012-10-03 21:35	10K	
back.gif	2004-11-21 05:16	216	
back.png	2007-09-11 14:11	308	
ball.gray.gif	2004-11-21 05:16	233	
ball.gray.png	2007-09-11 14:11	298	
ball.red.gif	2004-11-21 05:16	205	
ball.red.png	2007-09-11 14:11	289	
binary.gif	2004-11-21 05:16	246	
binary.png	2007-09-11 14:11	310	

問題 3 / 4

TOC

ディレクトリーの一覧作成

重大度:	中
CVSS スコア:	6.4
URL:	http://10.228.148.130/icons/small/
エンティティー:	small/ (Page)
リスク:	制限のかけられたファイルを含む可能性のある Web アプリケーションの仮想ディレクトリーの内容を、表示およびダウンロードすることができます
原因:	ディレクトリー・ブラウジングが有効になっています
修正:	ディレクトリーの一覧表示を拒否するようにサーバーの設定を変更し、使用できる最新のセキュリティー・パッチをインストールします

差: **パス** 操作元: `/app/org/` 操作先: `/icons/small/`

論拠: レスポンスがディレクトリーの内容 (ディレクトリー一覧) を含んでいます。これは、サーバーでディレクトリー内容の一覧表示が許可されていることを示しています。通常、このような設定は推奨されません。

テスト要求と応答:

```
GET /icons/small/ HTTP/1.1
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


HTTP/1.1 200 OK
Transfer-Encoding: chunked
Connection: Keep-Alive
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
Keep-Alive: timeout=5, max=100
Date: Tue, 12 Jun 2018 09:12:18 GMT
Content-Type: text/html;charset=ISO-8859-1

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /icons/small</title>
 </head>
 <body>
<h1>Index of /icons/small</h1>
  <table>
   <tr><th valign="top"><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?
C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?
C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
   <tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[PARENTDIR]"></td><td><a
href="/icons/">Parent Directory</a>       </td><td> </td><td align="right">  - </td>
<td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="back.gif">back.gif</a>          </td><td align="right">2004-11-21 05:16  </td><td
align="right">129 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="back.png">back.png</a>          </td><td align="right">2007-08-28 19:53  </td><td
align="right">181 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="binary.gif">binary.gif</a>          </td><td align="right">2004-11-21 05:16  </td><td
align="right">134 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="binary.png">binary.png</a>          </td><td align="right">2007-08-28 19:53  </td><td
align="right">172 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="binhex.gif">binhex.gif</a>          </td><td align="right">2004-11-21 05:16  </td><td
align="right">131 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="binhex.png">binhex.png</a>          </td><td align="right">2007-08-28 19:53  </td><td
align="right">178 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="blank.gif">blank.gif</a>          </td><td align="right">2004-11-21 05:16  </td><td
align="right"> 55 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="blank.png">blank.png</a>          </td><td align="right">2007-08-28 19:53  </td><td
align="right">100 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="broken.gif">broken.gif</a>          </td><td align="right">2004-11-21 05:16  </td><td
align="right">139 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="broken.png">broken.png</a>          </td><td align="right">2007-08-28 19:53  </td><td
align="right">184 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="burst.gif">burst.gif</a>          </td><td align="right">2004-11-21 05:16  </td><td
align="right">128 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="burst.png">burst.png</a>          </td><td align="right">2007-08-28 19:53  </td><td
align="right">210 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="comp1.gif">comp1.gif</a>          </td><td align="right">2004-11-21 05:16  </td><td
align="right">130 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="comp1.png">comp1.png</a>          </td><td align="right">2007-08-28 19:53  </td><td
align="right">216 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="comp2.gif">comp2.gif</a>          </td><td align="right">2004-11-21 05:16  </td><td
align="right">131 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="comp2.png">comp2.png</a>          </td><td align="right">2007-08-28 19:53  </td><td
```

```
align="right">215 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG]"></td><td><a
href="compressed.gif">compressed.gif</a>         </td><td align="right">2004-11-21 05:16  </td>
<td align="right">128 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/image2.gif" alt="[IMG
...
...
...
```

テスト応答

Index of /icons/small

Name	Last modified	Size	Description
Parent Directory		-	
back.gif	2004-11-21 05:16	129	
back.png	2007-08-28 19:53	181	
binary.gif	2004-11-21 05:16	134	
binary.png	2007-08-28 19:53	172	
binhex.gif	2004-11-21 05:16	131	
binhex.png	2007-08-28 19:53	178	
blank.gif	2004-11-21 05:16	55	
blank.png	2007-08-28 19:53	100	
broken.gif	2004-11-21 05:16	139	
broken.png	2007-08-28 19:53	184	
burst.gif	2004-11-21 05:16	128	
burst.png	2007-08-28 19:53	210	
comp1.gif	2004-11-21 05:16	130	
comp1.png	2007-08-28 19:53	216	
comp2.gif	2004-11-21 05:16	131	
comp2.png	2007-08-28 19:53	215	
compressed.gif	2004-11-21 05:16	128	
compressed.png	2007-08-28 19:53	212	
continued.gif	2004-11-21 05:16	114	

問題 4 / 4

TOC

ディレクトリーの一覧作成

重大度:	中
CVSS スコア:	6.4
URL:	http://10.228.148.130/
エンティティー:	/ (Global)
リスク:	制限のかけられたファイルを含む可能性のある Web アプリケーションの仮想ディレクトリーの内容を、表示およびダウンロードすることができます
原因:	ディレクトリー・ブラウジングが有効になっています
修正:	ディレクトリーの一覧表示を拒否するようにサーバーの設定を変更し、使用できる最新のセキュリティー・パッチをインストールします

差: **パス** 操作元: `/app/org/` 操作先: `/`
クエリー 操作元: – 操作先: `q=search&keys[]=AppScan`

論拠: レスポンスがディレクトリーの内容 (ディレクトリー一覧) を含んでいます。これは、サーバーでディレクトリー内容の一覧表示が許可されていることを示しています。通常、このような設定は推奨されません。

テスト要求と応答:

```
GET /?q=search&keys[]=AppScan HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


HTTP/1.1 200 OK
Connection: Keep-Alive
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
Content-Length: 481
Keep-Alive: timeout=5, max=100
Date: Tue, 12 Jun 2018 08:48:02 GMT
Content-Type: text/html;charset=ISO-8859-1

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /</title>
 </head>
 <body>
<h1>Index of /</h1>
  <table>
   <tr><th valign="top"><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?
C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?
C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
   <tr><th colspan="5"><hr></th></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
</body></html>
```

テスト応答

中 フレームからのフィッシング 1 TOC

問題 1 / 1 TOC

フレームからのフィッシング

重大度:	中
CVSS スコア:	6.4
URL:	http://10.228.148.130/app/org
エンティティー:	kankei_kikan (Parameter)
リスク:	知識の乏しいユーザーに、ユーザー名、パスワード、クレジット・カード番号、社会保険番号などの秘密情報を提供するように求めることができます
原因:	ユーザーの入力内容に対する有害文字の除去が適切に行われませんでした
修正:	有害な文字のインジェクションに対して考えられる解決策を確認します

差: **パラメーター** 操作元: 操作先:

```
%27%22%3E%3Ciframe+id%3D1511+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E
```

論拠: テスト応答に URL「http://demo.testfire.net/phishing.html」へのフレーム/I フレームが含まれていたため、テスト結果では脆弱性が示されていると考えられます。

テスト要求と応答:

```
POST /app/org HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.228.148.130/app/org
Cookie: soudanList=;
laravel_session=eyJpdiI6IlNyRlkyallKc2dKNGpGdWFFVDVLOXc9PSIsInZhbHVlIjoiWlFpUTkzUVphcHVBYnFIZzM5T
015bjgxVFBOUEllbXROY1Y0N1g0YmNydnI4RUZia0dZeGE3dlwvdXZCbGg5NnowQWdlVmhEQ0x4Y1c0YVJnUjJwS0RBPT0iLC
JtYWMiOiJjNGNiMzM5MTFmN2JhMGI5YmJmNmEwMTczMDhlNDE0MmNlMWI0NjYwNjJjNDM0YzdkZWYyNTYzZGEzNmU3MmM5In0
%3D; XSRF-
TOKEN=eyJpdiI6IjdlUWlKaHZ3NFZiS1F4ZDZrUld3dmc9PSIsInZhbHVlIjoiWVRaOE9wbVpOMDNpNzJPaW9Mak50cUxxVld
0OUdXZTVKbk5Sd1ZKVU5zd2RnWTFqcTNSbG1ucERIN1dJOFM4QVpsZnBCbHc3ZEx0NENORzQyUHI0Z3c9PSIsIm1hYyI6IjFl
YWQ5NDRkZThiOTFiZTM5OGNhMGJmMTVmZDAwNzdlNjdlNGE4OGE4ZWNmY2U1MDY5ODg1MzQ5NThiMGZmNjIifQ%3D%3D;
PHPSESSID=6ebsdplhncev03jjcb2lk1cia0
Connection: Keep-Alive
Host: 10.228.148.130
Pragma: no-cache
Content-Length: 294
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP
Content-Type: application/x-www-form-urlencoded

_token=yuEor3ontYoqIVemgYB9Md6zAOEcgAoJnyhA89RA&key_pref=13&key_addr=&kankei_kikan=%27%22%3E%3Cif
rame+id%3D1511+src%3Dhttp%3A%2F%2Fdemo.testfire.net%2Fphishing.html%3E&key_keyword=&key_new=%E6%9
6%B0%E8%A6%8F&key_update=%E5%A4%89%E6%9B%B4&key_publish=%E5%85%AC%E9%96%8B&submit=%E6%A4%9C%E7%B4
%A2

HTTP/1.1 200 OK
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
default-style: IE=edge
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ikdqbzc1a0dpZ2xpdWlhTDZEK0szQ2c9PSIsInZhbHVlIjoiRE5Vbk1EdkRDZG9UU0pxUStBYXdFY0ozWmI
3V0Rabmo1RFVvUWRjZ2pOQTVjbU9pMGRHY01MQ3daU2lna012TTNaTmFMaUl2UElDYmdlcStEMW84cEE9PSIsIm1hYyI6Ijhj
MmRkMmIzZDU4OTAxZjY3ZGUzMzdiZjc1N2I2YmFiZTk2MWE0NDgwOTkzZWUxYjJmZDU3MDIyOGZkZWIyY2QifQ%3D%3D;
expires=Tue, 12-Jun-2018 10:59:22 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6IlJLa1QxR1BIUXQwa3BFMUtNV1NUN1E9PSIsInZhbHVlIjoidnZqbm5wck5hdkMrMVJvVjhOV
XNBNGtMV2t5NmRyNDV3citIOWxPUDRnWk1PeWV5R3pSUFdEYnZcLzhEOTc5RXo2R1VyMkVcL2xjbVA5WVYrYW8rZGZHZz09Ii
wibWFjIjoiN2FiNDU2NzViZTE2ZmY4ZDQ4OTgwMDQyNzkxYjU4YmIxNmQwZTFkMTYwYzE5OGFlOWQ2OGI4OTI1YmU0MTdkNyJ
9; expires=Tue, 12-Jun-2018 10:59:22 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.30
Connection: Keep-Alive
Date: Tue, 12 Jun 2018 08:59:22 GMT
Keep-Alive: timeout=5, max=99
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-cache, private
Transfer-Encoding: chunked

<!DOCTYPE HTML>
<html lang="ja">
<head><meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<meta name="Author" content="Houterasu" />
<meta http-equiv="DEFAULT-STYLE" content="IE=edge" />
<meta name="viewport" content="width=device-width,initial-scale=1.0,shrink-to-fit=no" />
<link rel="shortcut icon" href="/app/images/100555157.gif" />
<title>相談窓口検索　法テラス</title>
<link rel="stylesheet" href="/app/css/bootstrap.min.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_layout.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_style.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_pc.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_print.css" type="text/css" media="print" />

</head>
<body id="base" class="container-fluid">
    <!-- scs_jyogai_start -->
<div id="basebg">
    <noscript>
        <p class="jsmessage">法テラス公式ホームページではJavaScriptを使用しています。
```

```
            <br/>JavaScriptの使用を有効にしていない場合は、一部の機能が正確に動作しない恐れがあります。
            <br/>お手数ですがJavaScriptの使用を有効にしてください。</p>
    </noscript>
    <div class="blockjump">
        <a id="PTOP"></a>
    </div>

    <div id="blockskip">
        <script src="/app/js/jquery-1.9.1.min.js"></script>
        <script>
          $(function () {
          $("#blockskip a").focus(function () {
          $(this)
          .parent()
          .animate({
          height: '1.5em'
          }, { duration: 'fast' })
          .addClass("show");
          });
          $("#blockskip a").blur(function () {
          $(this)
          .parent()
          .animate({
          height: '1px'
          }, {
          duration: 'fast',
          complete: function () {
          $(this).removeClass("show");
          }
          })
          });
          });
        </script>
        <a hr
...
...
...

          var valueRadio = ''"><iframe id=1511 src=http://demo.testfire.net/phishing.html>';
          initCheckedRadio(valueRadio);
          disableLanguageDropdown();
          clearMessgeWhenBackBrowser('soudanList');
        });
...
...
...
```

テスト応答


法テラス公式ホームページではJavaScriptを使用しています。
JavaScriptの使用を有効にしていない場合は、一部の機能が正確に動作しない恐れがあります。
お手数ですがJavaScriptの使用を有効にしてください。
法テラスは、国が設立した法的トラブル解決の総合案内所です。
音声読み上げ・文字拡大 | English | 携帯サイト | サイトマップ |
日本司法支援センター 法テラス
法的トラブルでお困りの方 法テラス・サポートダイヤル
0570-078374
平日9時～21時 土曜9時～17時
メールでのお問い合わせ
24時間受付中
トップページ ▸ 相談窓口検索
相談窓口検索
相談窓口を以下の項目から検索することができます。
お知りになりたい内容を入力または選択してください（※複数の選択も可能です）。
検索結果が見つかりませんでした。

低 Content-Security-Policy ヘッダーが欠落しています 4 TOC

問題 1 / 4 TOC

Content-Security-Policy ヘッダーが欠落しています

重大度:	低
CVSS スコア:	5.0
URL:	http://10.228.148.130/app/org/list
エンティティー:	list (Page)
リスク:	知識の乏しいユーザーに、ユーザー名、パスワード、クレジット・カード番号、社会保険番号などの秘密情報を提供するように求めることができます ユーザー名、パスワード、マシン名などの Web アプリケーションに関する秘密情報や、秘密のファイルの場所などの情報を取得することができます
原因:	セキュリティーで保護されていない Web アプリケーション・プログラムまたは設定
修正:	Content-Security-Policy ヘッダーを使用するようにサーバーを構成してください

差:

論拠: AppScan は Content-Security-Policy 応答ヘッダーが欠落していることを検出しました。そのため各種クロスサイト注入攻撃にさらされる可能性が高くなります。

テスト要求と応答:

```
GET /app/org/list?page=2 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.228.148.130/app/org/detail/130102044
Cookie: soudanList=1;
laravel_session=eyJpdiI6InlZbzJTVTNzaGRwb2JzQlQxcGtUaFE9PSIsInZhbHVlIjoieHZZUThKRkFaa2lqUkU3UEJWV
zhIMWVDbXI1MEx3aGptcjNHM3I1MzdraE5mdGZ6cFhCbzBma0xHck1BMG5zdEhPNlhNUDd0TjdBcDd5dVdueUVyNFE9PSIsIm
1hYyI6IjJlZjE5ZmFkNDY5YzU0YzcyMzc0Yzc3OTk4OTMwZmIyNTIxZWY4NzI2N2RhZjAxN2ViYTUzNmYxYmM5YzkxMmIifQ%
3D%3D; XSRF-
TOKEN=eyJpdiI6IjB5QnpHN2V6Yk5LcjhpNWlIdFwvZVVRPT0iLCJ2YWx1ZSI6Ims4c1VpTitqM2VwXC9xOFhZczF4cG5kTFp
aaE1uWHRRK29CR25VamhCeG5hRTJtSFNyaW5CdlZ1dEJkbTY3alZ3M04yQzA3V2gxWW9HVjI2VTNKQ1YwUT09IiwibWFjIjoi
M2VlZDIyNjc3YTBhMDZjZGZjNGVkZDM0MWM0MjU1OWI5ZDUxZWU3YjY2N2ZlZWFlOTdkNzNkYmVmODAzMDY0MyJ9;
PHPSESSID=6ebsdplhncev03jjcb2lk1cia0
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


HTTP/1.1 200 OK
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
default-style: IE=edge
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlQ2dGh4QmswRDRZRHRXYWdkVnByaHc9PSIsInZhbHVlIjoiOVdvTWZQSFhoY1hZd2JNMWpZOGJvcmNKSVh
2dUZUeU10aFNib1ZYbFlwU0NZV3VIZEwwbjNqSnJWbUNjOWh6ZEJjQTVlZUxwYnVYaGVnMm1nUzRiYVE9PSIsImlhYyI6Ijg4
OGE3ZDM1MTJiN2NmOTZjMzBiM2UzOTg3ZTFmNTBjNDBiN2VjZDE0ZjNhYWM1YmM3ZDE0YTZmZTE3ZDg3ZTQifQ%3D%3D;
expires=Tue, 12-Jun-2018 10:53:04 GMT; Max-Age=7200; path=/
```

```
Set-Cookie:
laravel_session=eyJpdiI6ImtxTWZYM0Fra0podlowRXJUS2JxNXc9PSIsInZhbHVlIjoiUEJVcHh4a1JqOWs4eDVEM0Z3c
zV5dG9lRitmWkc0R3BZYmZVR1hvY2JcL1lsSG9TZ0VDSDczZWZ5djZ4VFVpXC90bzlCQ3ppQUF2QXhFSGdDUVNzT2dWdz09Ii
wibWFjIjoiZDU1Y2NiNTU0MjU2NzBlN2E1NzY2YjcxNDhhNmYyMjA2ZmJmYzhlYWNlMTk3YzA0ZTdkNTNmNTVlZmY3ZDdhNSJ
9; expires=Tue, 12-Jun-2018 10:53:04 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.30
Connection: Keep-Alive
Date: Tue, 12 Jun 2018 08:53:04 GMT
Keep-Alive: timeout=5, max=98
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-cache, private
Transfer-Encoding: chunked

<!DOCTYPE HTML>
<html lang="ja">
<head><meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<meta name="Author" content="Houterasu" />
<meta http-equiv="DEFAULT-STYLE" content="IE=edge" />
<meta name="viewport" content="width=device-width,initial-scale=1.0,shrink-to-fit=no" />
<link rel="shortcut icon" href="/app/images/100555157.gif" />
<title>相談窓口一覧 法テラス</title>
<link rel="stylesheet" href="/app/css/bootstrap.min.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_layout.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_style.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_pc.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_print.css" type="text/css" media="print" />
    <link rel="stylesheet" href="/app/css/style.tableconverter.css"/>
</head>
<body id="base" class="container-fluid">
    <!-- scs_jyogai_start -->
<div id="basebg">
    <noscript>
        <p class="jsmessage">法テラス公式ホームページではJavaScriptを使用しています。
          <br/>JavaScriptの使用を有効にしていない場合は、一部の機能が正確に動作しない恐れがあります。
          <br/>お手数ですがJavaScriptの使用を有効にしてください。</p>
    </noscript>
    <div class="blockjump">
        <a id="PTOP"></a>
    </div>

    <div id="blockskip">
        <script src="/app/js/jquery-1.9.1.min.js"></script>
        <script>
          $(function () {
          $("#blockskip a").focus(function () {
          $(this)
          .parent()
          .animate({
          height: '1.5em'
          }, { duration: 'fast' })
          .addClass("show");
          });
          $("#blockskip a").blur(function () {
          $(this)
          .parent()
          .animate({
          height: '1px'
          }, {
          duration: 'fast',
          complete: function () {
          $(this).removeClass("show");
          }
          })
          });
          });
        </script>
        <a href="#">このページの本文へ移動</a>
    </div>
    <div id="baseall" class="no-sub">
        <div class="header_wp">
          <div class="header_wp_in clearfix">
          <div class="header_text_wp">
          <div class="header_text_in sp-none">
          <p>法テラスは、国が設立した法的トラブル解決の総合案内所です。</p>
          <ul class="headlist clearfix col-md-6 col-md-offset-6 col-sm-12 col-xs-12">
```

```
          <li>
          <a href="https://www.zoomsight-
sv2.jp/HTRS/controller/index.html#https://www.houterasu.or.jp">音声読み上げ・文字拡大</a>

...
...
...
```

問題 2 / 4

TOC

Content-Security-Policy ヘッダーが欠落しています

重大度:	低
CVSS スコア:	5.0
URL:	http://10.228.148.130/app/org/
エンティティー:	(Page)
リスク:	知識の乏しいユーザーに、ユーザー名、パスワード、クレジット・カード番号、社会保険番号などの秘密情報を提供するように求めることができます ユーザー名、パスワード、マシン名などの Web アプリケーションに関する秘密情報や、秘密のファイルの場所などの情報を取得することができます
原因:	セキュリティーで保護されていない Web アプリケーション・プログラムまたは設定
修正:	Content-Security-Policy ヘッダーを使用するようにサーバーを構成してください

差:

論拠: AppScan は Content-Security-Policy 応答ヘッダーが欠落していることを検出しました。そのため各種クロスサイト注入攻撃にさらされる可能性が高くなります。

テスト要求と応答:

```
GET /app/org/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


HTTP/1.1 200 OK
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
default-style: IE=edge
Set-Cookie: PHPSESSID=pb2b8dkcag87r9ic36s1d477a2; path=/
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjVRSHVVMEorZWdHUU1oK0EwemFOVlE9PSIsInZhbHVlIjoiVlVhcWVyZHRzRDZ5eFltSWx6S0V2YVpTa25
5Z094ZFVkSDJsZERZTlZyV0puUmxrY1FuVDJjZk5sSzRWZnkrUGNUOFYxalo3RmV4ejkwK3FrSmhyUnc9PSIsIm1hYyI6Ijlk
ZmI4OGZmYmNjMDE5NWFkMmZjZmVhMzY4NjU0YzU4OWYyMGU2OTFhMzk0NzEwNzc5ZTRjOWU3NGIwNWQ5MzAifQ%3D%3D;
expires=Tue, 12-Jun-2018 10:53:04 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6IkdMWWxpMFBSNXhxT0V5b0JjeDQzTlE9PSIsInZhbHVlIjoiR25wMWlkcjZtM3p0R24yRzd6Q
3YzdGtwMitGUjU1RlhTNjVsMG0wZlJ4bU1FUXhpYW5hc2Y5NnNwU2E2bnN2UUhuY3BkSXQ2ZTZHWUhadVNNNGRuRVE9PSIsIm
1hYyI6ImY2Y2RhY2NkNTQyZmI3N2UxNDBhN2I5ZGM4MzEzZjJjYWJmZGIyM2I0NTk0ZTc0NGVmNGVlMjA3OWZmZDI5MDAifQ%
3D%3D; expires=Tue, 12-Jun-2018 10:53:04 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.30
Connection: Keep-Alive
Date: Tue, 12 Jun 2018 08:53:04 GMT
Keep-Alive: timeout=5, max=100
Content-Type: text/html; charset=UTF-8
```

```
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-cache, private
Transfer-Encoding: chunked

<!DOCTYPE HTML>
<html lang="ja">
<head><meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<meta name="Author" content="Houterasu" />
<meta http-equiv="DEFAULT-STYLE" content="IE=edge" />
<meta name="viewport" content="width=device-width,initial-scale=1.0,shrink-to-fit=no" />
<link rel="shortcut icon" href="/app/images/100555157.gif" />
<title>相談窓口検索　法テラス</title>
<link rel="stylesheet" href="/app/css/bootstrap.min.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_layout.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_style.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_pc.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_print.css" type="text/css" media="print" />

</head>
<body id="base" class="container-fluid">
    <!-- scs_jyogai_start -->
<div id="basebg">
    <noscript>
        <p class="jsmessage">法テラス公式ホームページではJavaScriptを使用しています。
          <br/>JavaScriptの使用を有効にしていない場合は、一部の機能が正確に動作しない恐れがあります。
          <br/>お手数ですがJavaScriptの使用を有効にしてください。</p>
    </noscript>
    <div class="blockjump">
        <a id="PTOP"></a>
    </div>

    <div id="blockskip">
        <script src="/app/js/jquery-1.9.1.min.js"></script>
        <script>
          $(function () {
          $("#blockskip a").focus(function () {
          $(this)
          .parent()
          .animate({
          height: '1.5em'
          }, { duration: 'fast' })
          .addClass("show");
          });
          $("#blockskip a").blur(function () {
          $(this)
          .parent()
          .animate({
          height: '1px'
          }, {
          duration: 'fast',
          complete: function () {
          $(this).removeClass("show");
          }
          })
          });
          });
        </script>
        <a href="#">このページの本文へ移動</a>
    </div>
    <div id="baseall" class="no-sub">
        <div class="header_wp">
          <div class="header_wp_in clearfix">
          <div class="header_text_wp">
          <div class="header_text_in sp-none">
          <p>法テラスは、国が設立した法的トラブル解決の総合案内所です。</p>
          <ul class="headlist clearfix col-md-6 col-md-offset-6 col-sm-12 col-xs-12">
          <li>
          <a href="https://www.zoomsight-
sv2.jp/HTRS/controller/index.html#https://www.houterasu.or.jp">音声読み上げ・文字拡大</a>
          </li>
          <li>
          <a href="/en/index.html">English</a>
          </li>
          <li>
          <a href="/k/index.html">携帯サイト</a>
          </li>
          <li>
```

```
            <a href="/sitemap.html">サイトマップ</a>
            </li>
            </ul>
            </div>
            </div>
            <div class="row header_logo_wrap">
            <div class="col-md-3 col-sm-3 col-xs-3 header_logo">
            <a href="/index.html">
            <img class="img-respons
...
...
...
```

問題 3 / 4

TOC

Content-Security-Policy ヘッダーが欠落しています

重大度:	低
CVSS スコア:	5.0
URL:	http://10.228.148.130/app/org/detail/130102044
エンティティー:	130102044 (Page)
リスク:	知識の乏しいユーザーに、ユーザー名、パスワード、クレジット・カード番号、社会保険番号などの秘密情報を提供するように求めることができます ユーザー名、パスワード、マシン名などの Web アプリケーションに関する秘密情報や、秘密のファイルの場所などの情報を取得することができます
原因:	セキュリティーで保護されていない Web アプリケーション・プログラムまたは設定
修正:	Content-Security-Policy ヘッダーを使用するようにサーバーを構成してください

差:

論拠: AppScan は Content-Security-Policy 応答ヘッダーが欠落していることを検出しました。そのため各種クロスサイト注入攻撃にさらされる可能性が高くなります。

テスト要求と応答:

```
GET /app/org/detail/130102044 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.228.148.130/app/org/list?page=2
Cookie: soudanList=1;
laravel_session=eyJpdiI6InhhRU9jRzZWM1FXU1MzYWpIUWlIdmc9PSIsInZhbHVlIjoiSDZDOWorR05weVNnbXB1dWVwO
FpEY1diaG90bUN0UEVKcHFMNE15M29ZWGZ4UnIyUUxVZGpNSW5qaDNZMlErOEJtM3E3MndZSDhQYW45QjdDemEzdEE9PSIsIm
lhYyI6IjA2ODQ5MjgxYmMyZWExZWEzZjY1YTY5YTNiZWY0OTFkZjliMzRmZTRkNjA4YTU3N2E1ZTY1OTlmOWY3MzQ1NTEifQ%
3D%3D; XSRF-
TOKEN=eyJpdiI6ImZDT0h3blNoa0ZkSmp3WDFPYzljZmc9PSIsInZhbHVlIjoiMTE1Z2gxenNvODR2aTVOek0yV1NQU3R2aFV
2eGFBcEVDVlZHU0ZqbHRpMTU1V25DUGZcL3BFRm5JclBPSThoZ1V1NVlxcVdwYzRGRzk2TnBjWVlTT1B3PT0iLCJtYWMiOiI5
MDdhMzIyMzUxNzM4MTM4YTM4ZDZlMTEyMzZkMTA2ODU4OGJmMDQ1MzBiMjgzMzg5YTA5ODNjZDhkOGI1MTY5In0%3D;
PHPSESSID=6ebsdplhncev03jjcb2lklcia0
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


HTTP/1.1 200 OK
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
default-style: IE=edge
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkRDYmFLSUtldDVtUzZwaUl3VEJIWkE9PSIsInZhbHVlIjoiZ1I5cDY1cGJRK1NqcWsybHIxendOK1pQMlF
```

```
nbVp2M20xeWtvSEFhK3BcL1hFOGgrNlBtUE83TG1VdHozbkpsQ29oXC8xYVR4SlRrRzdJRmtGNzRscittdz09IiwibWFjIjoi
NGE3OWM1NjRhZTA3ODA3MGJmMmVhYTM2ZmQ5YzMxNGUyMDRiZDAwNzc0MjkzMWZiMDI4M2Q3NjczYmQ2N2VhZSJ9;
expires=Tue, 12-Jun-2018 10:53:05 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6ImJKYkMrZ2Zsd2RhZlE0bG9qU0N1UkE9PSIsInZhbHVlIjoiOUVSK2IwOVRJZ3pIU3pZazhNV
WQ0eHhmUW93MlwvN1wvb0xwYkl5bnNjeWVvc1Z0U0pwbWxhV3hWcWdwN3kwTGo4MkVBcmJGUVppcmZZdVp0eDJLT0dBZz09Ii
wibWFjIjoiNTAzYzFlZWI3NTk4NGU3NjRjZDNjNTg3ZGJkZjBhODBhOTZkMzNiMmU1MDgyNDkyZTE4YmQ4MmFjMTIwZThkOCJ
9; expires=Tue, 12-Jun-2018 10:53:05 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.30
Connection: Keep-Alive
Date: Tue, 12 Jun 2018 08:53:05 GMT
Keep-Alive: timeout=5, max=99
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-cache, private
Transfer-Encoding: chunked

<!DOCTYPE HTML>
<html lang="ja">
<head><meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<meta name="Author" content="Houterasu" />
<meta http-equiv="DEFAULT-STYLE" content="IE=edge" />
<meta name="viewport" content="width=device-width,initial-scale=1.0,shrink-to-fit=no" />
<link rel="shortcut icon" href="/app/images/100555157.gif" />
<title>相談窓口詳細 法テラス</title>
<link rel="stylesheet" href="/app/css/bootstrap.min.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_layout.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_style.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_pc.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_print.css" type="text/css" media="print" />
    <link rel="stylesheet" href="/app/css/style.tableconverter.css"/>
</head>
<body id="base" class="container-fluid">
    <!-- scs_jyogai_start -->
<div id="basebg">
    <noscript>
        <p class="jsmessage">法テラス公式ホームページではJavaScriptを使用しています。
          <br/>JavaScriptの使用を有効にしていない場合は、一部の機能が正確に動作しない恐れがあります。
          <br/>お手数ですがJavaScriptの使用を有効にしてください。</p>
    </noscript>
    <div class="blockjump">
        <a id="PTOP"></a>
    </div>

    <div id="blockskip">
        <script src="/app/js/jquery-1.9.1.min.js"></script>
        <script>
          $(function () {
          $("#blockskip a").focus(function () {
          $(this)
          .parent()
          .animate({
          height: '1.5em'
          }, { duration: 'fast' })
          .addClass("show");
          });
          $("#blockskip a").blur(function () {
          $(this)
          .parent()
          .animate({
          height: '1px'
          }, {
          duration: 'fast',
          complete: function () {
          $(this).removeClass("show");
          }
          })
          });
          });
        </script>
        <a href="#">このページの本文へ移動</a>
    </div>
    <div id="baseall" class="no-sub">
        <div class="header_wp">
          <div class="header_wp_in clearfix">
          <div class="header_text_wp">
```

```
          <div class="header_text_in sp-none">
          <p>法テラスは、国が設立した法的トラブル解決の総合案内所です。</p>
          <ul class="headlist clearfix col-md-6 col-md-offset-6 col-sm-12 col-xs-12">
          <li>
          <a href="https://www.zoomsight-
sv2.jp/HTRS/controller/index.html#https://www.houterasu.or.jp">音声読み上げ・文字拡大</a>

...
...
...
```

問題 4 / 4

TOC

Content-Security-Policy ヘッダーが欠落しています

重大度:	低
CVSS スコア:	5.0
URL:	http://10.228.148.130/app/org
エンティティー:	org (Page)
リスク:	知識の乏しいユーザーに、ユーザー名、パスワード、クレジット・カード番号、社会保険番号などの秘密情報を提供するように求めることができます ユーザー名、パスワード、マシン名などの Web アプリケーションに関する秘密情報や、秘密のファイルの場所などの情報を取得することができます
原因:	セキュリティーで保護されていない Web アプリケーション・プログラムまたは設定
修正:	Content-Security-Policy ヘッダーを使用するようにサーバーを構成してください

差:

論拠: AppScan は Content-Security-Policy 応答ヘッダーが欠落していることを検出しました。そのため各種クロスサイト注入攻撃にさらされる可能性が高くなります。

テスト要求と応答:

```
GET /app/org HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.228.148.130/app/org/detail/130102044
Cookie: soudanList=1;
laravel_session=eyJpdiI6ImJtWE56S0xGMDBwdkcyVXRaZlRselE9PSIsInZhbHVlIjoiSGxnSlJlNWxzbDR1YUhabkRJR
1VsQ1B0Nk5EVHNjYmxDdmtCbXlDNXFQMUR4M2JwYU53ZkwwS1RYQmtEWllmMmVjTTBSOHQ5cUszVUoyTjg3RHNPdXc9PSIsIm
1hYyI6IjkwNDhkNDZkYTE2NjJmMTM5NWY1MzQ2MjUxYjEzODFhMmRmNjQxNTA5ZTZjZjcwMzVmYzc2ODRiNWZhNDRiMTgifQ%
3D%3D; XSRF-
TOKEN=eyJpdiI6Imc1ZGJiWWQ3SCt3VWFOcG05SFl3OFE9PSIsInZhbHVlIjoiNVd6NllsWmNYTHU0ZzdEa1dXVkd3ckR1eGx
VeGRJZDBuZmlUaGR2ZDFyY1JnNTNiN0FKVjNxend6amNtVzZCMUNvSkNxMkU5YW1LNEVQZFpZVUVHd1E9PSIsIm1hYyI6IjA2
ZDQzMzNhODlkYTJlM2I0NWZkOTBhYWM0YjBhMjJhYjllN2RkYTFiODEzYjNlNjIxNmY3YmYwODBkZjcyZTMifQ%3D%3D;
PHPSESSID=6ebsdplhncev03jjcb2lk1cia0
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


HTTP/1.1 200 OK
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
default-style: IE=edge
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImNSTGdZZU9wNzg1UUFwaWU0bjVpUWc9PSIsInZhbHVlIjoiU1JRNFhoa0NSOVdDNU1lekprSm83NWxSZWp
CSVZyaWw1cm9RejljaXJxRkZONDUwWFFzblV4bUlCdURROThyYTQxXC81M1lmN0FyOGVKVzQ0WjdscGNBPT0iLCJtYWMiOiIy
YTJkNzVlNmIxNDI5NmU0NWIxNTIyNDJkNzhmNmYwMDAzZDZiZTc0NDJmMzRkMDczNWExNTU0ZTBiYWEyN2QzIn0%3D;
```

```
expires=Tue, 12-Jun-2018 10:53:06 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6IlNwVnBOa1g1R1BleEpUUFZTdnUzS3c9PSIsInZhbHVlIjoiUEtoemF3UHNtOE9VRmpoVmxBK
0MzVGJzRmJFQk5VaEYxR29pcGZsV2wrbG9PWmp3MDBXeU83UE11eTkwdWY5SnVGRUxxODRVRmhuYWk1N3hcL0lwV1lRPT0iLC
JtYWMiOiJmNjRmNjc5ZDYxMDJmZjJlY2UzYTU3ZjJkYzM4OTVlYjM2ZDU4ZGUxY2ZjZjllNjY4MjcwZTg5YTNiYzRlMjEyIn0
%3D; expires=Tue, 12-Jun-2018 10:53:06 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.30
Connection: Keep-Alive
Date: Tue, 12 Jun 2018 08:53:06 GMT
Keep-Alive: timeout=5, max=98
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-cache, private
Transfer-Encoding: chunked

<!DOCTYPE HTML>
<html lang="ja">
<head><meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<meta name="Author" content="Houterasu" />
<meta http-equiv="DEFAULT-STYLE" content="IE=edge" />
<meta name="viewport" content="width=device-width,initial-scale=1.0,shrink-to-fit=no" />
<link rel="shortcut icon" href="/app/images/100555157.gif" />
<title>相談窓口検索　法テラス</title>
<link rel="stylesheet" href="/app/css/bootstrap.min.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_layout.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_style.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_pc.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_print.css" type="text/css" media="print" />

</head>
<body id="base" class="container-fluid">
    <!-- scs_jyogai_start -->
<div id="basebg">
    <noscript>
        <p class="jsmessage">法テラス公式ホームページではJavaScriptを使用しています。
          <br/>JavaScriptの使用を有効にしていない場合は、一部の機能が正確に動作しない恐れがあります。
          <br/>お手数ですがJavaScriptの使用を有効にしてください。</p>
    </noscript>
    <div class="blockjump">
        <a id="PTOP"></a>
    </div>

    <div id="blockskip">
        <script src="/app/js/jquery-1.9.1.min.js"></script>
        <script>
          $(function () {
          $("#blockskip a").focus(function () {
          $(this)
          .parent()
          .animate({
          height: '1.5em'
          }, { duration: 'fast' })
          .addClass("show");
          });
          $("#blockskip a").blur(function () {
          $(this)
          .parent()
          .animate({
          height: '1px'
          }, {
          duration: 'fast',
          complete: function () {
          $(this).removeClass("show");
          }
          })
          });
          });
        </script>
        <a href="#">このページの本文へ移動</a>
    </div>
    <div id="baseall" class="no-sub">
        <div class="header_wp">
          <div class="header_wp_in clearfix">
          <div class="header_text_wp">
          <div class="header_text_in sp-none">
          <p>法テラスは、国が設立した法的トラブル解決の総合案内所です。</p>
```

```
          <ul class="headlist clearfix col-md-6 col-md-offset-6 col-sm-12 col-xs-12">
          <li>
          <a href="https://www.zoomsight-
sv2.jp/HTRS/controller/index.html#https://www.houterasu.or.jp">音声読み上げ・文字拡大</a>
          </li>
          <li>

...
...
...
```

低 TRACE および TRACK HTTP メソッドが有効 1

TOC

問題 1 / 1

TOC

TRACE および TRACK HTTP メソッドが有効

重大度:	低
CVSS スコア:	5.0
URL:	http://10.228.148.130/app/org/
エンティティー:	10.228.148.130 (Page)
リスク:	ハッカーが正規のユーザーになりすまし、ユーザーのレコードを表示または改変したり、ユーザーとしてトランザクションを実行するのに使用することができる、カスタマー・セッションおよび Cookie を盗み出したり操作することができる可能性があります
原因:	Web サーバーまたはアプリケーション・サーバーが安全でない方法で設定されています
修正:	Web サーバーの HTTP TRACE サポートを無効にします

差: **パス** 操作元: `/app/org/` 操作先: `/%3Cscript%3Ealert(1234)%3C/script%3E`
方法 操作元: `GET` 操作先: `TRACE`

論拠: レスポンスのコンテンツ・タイプ (message/http) および、レスポンスに含まれるリクエスト・テキストおよびヘッダーのエコーイングが、サーバー上で TRACE/TRACK メソッドが有効になっていることを示しています。

テスト要求と応答:

```
TRACE /%3Cscript%3Ealert(1234)%3C/script%3E HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


HTTP/1.1 200 OK
Transfer-Encoding: chunked
Connection: Keep-Alive
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
Keep-Alive: timeout=5, max=94
Date: Tue, 12 Jun 2018 08:48:03 GMT
```

```
Content-Type: message/http

TRACE /%3Cscript%3Ealert(1234)%3C/script%3E HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP
```

低 X-Content-Type-Options ヘッダーが欠落しています 4

TOC

問題 1 / 4

TOC

X-Content-Type-Options ヘッダーが欠落しています

重大度:	低
CVSS スコア:	5.0
URL:	http://10.228.148.130/app/org/list
エンティティー:	list (Page)
リスク:	知識の乏しいユーザーに、ユーザー名、パスワード、クレジット・カード番号、社会保険番号などの秘密情報を提供するように求めることができます ユーザー名、パスワード、マシン名などの Web アプリケーションに関する秘密情報や、秘密のファイルの場所などの情報を取得することができます
原因:	セキュリティーで保護されていない Web アプリケーション・プログラムまたは設定
修正:	X-Content-Type-Options ヘッダーを使用するようにサーバーを構成してください

差:

論拠: AppScan は X-Content-Type-Options 応答ヘッダーが欠落していることを検出しました。そのためドライブバイ・ダウンロード攻撃にさらされる可能性が高くなります。

テスト要求と応答:

```
GET /app/org/list?page=2 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.228.148.130/app/org/detail/130102044
Cookie: soudanList=1;
laravel_session=eyJpdiI6InlZbzJTVTNzaGRwb2JzQlQxcGtUaFE9PSIsInZhbHVlIjoieHZZUThKRkFaa2lqUkU3UEJWV
zhIMWVDbXI1MEx3aGptcjNHM3I1MzdraE5mdGZ6cFhCbzBma0xHck1BMG5zdEhPNlhNUDd0TjdBcDd5dVdueUVyNFE9PSIsIm
lhYyI6IjJlZjE5ZmFkNDY5YzU0YzcyMzc0Yzc3OTk4OTMwZmIyNTIxZWY4NzI2N2RhZjAxN2ViYTUzNmYxYmM5YzkxMmIifQ%
3D%3D; XSRF-
TOKEN=eyJpdiI6IjB5QnpHN2V6Yk5LcjhpNWlIdFwvZVVRPT0iLCJ2YWx1ZSI6Ims4c1VpTitqM2VwXC9xOFhZczF4cG5kTFp
aaE1uWHRRK29CR25VamhCeG5hRTJtSFNyaW5CdlZ1dEJkbTY3alZ3M04yQzA3V2gxWW9HVjI2VTNKQ1YwUT09IiwibWFjIjoi
M2VlZDIyNjc3YTBhMDZjZGZjNGVkZDM0MWM0MjU1OWI5ZDUxZWU3YjY2N2ZlZWFlOTdkNzNkYmVmODAzMDY0MyJ9;
PHPSESSID=6ebsdplhncev03jjcb2lklcia0
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP
```

```
HTTP/1.1 200 OK
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
default-style: IE=edge
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlQ2dGh4QmswRDRZRHRXYWdkVnByaHc9PSIsInZhbHVlIjoiOVdvTWZQSFhoY1hZd2JNMWpZOGJvcmNKSVh
2dUZUeU10aFNib1ZYbFlwU0NZV3VIZEwwbjNqSnJWbUNjOWh6ZEJjQTVlZUxwYnVYaGVnMm1nUzRiYVE9PSIsIm1hYyI6Ijg4
OGE3ZDM1MTJiN2NmOTZjMzBiM2UzOTg3ZTFmNTBjNDBiN2VjZDE0ZjNhYWM1YmM3ZDE0YTZmZTE3ZDg3ZTQifQ%3D%3D;
expires=Tue, 12-Jun-2018 10:53:04 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6ImtxTWZYM0Fra0podlowRXJUS2JxNXc9PSIsInZhbHVlIjoiUEJVcHh4a1JqOWs4eDVEM0Z3c
zV5dG9lRitmWkc0R3BZYmZVR1hvY2JcL1lsSG9TZ0VDSDczZWZ5djZ4VFVpXC90bzlCQ3ppQUF2QXhFSGdDUVNzT2dWdz09Ii
wibWFjIjoiZDUlY2NiNTU0MjU2NzBlN2E1NzY2YjcxNDhhNmYyMjA2ZmJmYzhlYWNlMTk3YzA0ZTdkNTNmNTVlZmY3ZDdhNSJ
9; expires=Tue, 12-Jun-2018 10:53:04 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.30
Connection: Keep-Alive
Date: Tue, 12 Jun 2018 08:53:04 GMT
Keep-Alive: timeout=5, max=98
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-cache, private
Transfer-Encoding: chunked

<!DOCTYPE HTML>
<html lang="ja">
<head><meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<meta name="Author" content="Houterasu" />
<meta http-equiv="DEFAULT-STYLE" content="IE=edge" />
<meta name="viewport" content="width=device-width,initial-scale=1.0,shrink-to-fit=no" />
<link rel="shortcut icon" href="/app/images/100555157.gif" />
<title>相談窓口一覧 法テラス</title>
<link rel="stylesheet" href="/app/css/bootstrap.min.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_layout.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_style.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_pc.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_print.css" type="text/css" media="print" />
    <link rel="stylesheet" href="/app/css/style.tableconverter.css"/>
</head>
<body id="base" class="container-fluid">
    <!-- scs_jyogai_start -->
<div id="basebg">
    <noscript>
        <p class="jsmessage">法テラス公式ホームページではJavaScriptを使用しています。
          <br/>JavaScriptの使用を有効にしていない場合は、一部の機能が正確に動作しない恐れがあります。
          <br/>お手数ですがJavaScriptの使用を有効にしてください。</p>
    </noscript>
    <div class="blockjump">
        <a id="PTOP"></a>
    </div>

    <div id="blockskip">
        <script src="/app/js/jquery-1.9.1.min.js"></script>
        <script>
          $(function () {
          $("#blockskip a").focus(function () {
          $(this)
          .parent()
          .animate({
          height: '1.5em'
          }, { duration: 'fast' })
          .addClass("show");
          });
          $("#blockskip a").blur(function () {
          $(this)
          .parent()
          .animate({
          height: '1px'
          }, {
          duration: 'fast',
          complete: function () {
          $(this).removeClass("show");
          }
          })
          });
          });
```

```
        </script>
        <a href="#">このページの本文へ移動</a>
    </div>
    <div id="baseall" class="no-sub">
        <div class="header_wp">
          <div class="header_wp_in clearfix">
          <div class="header_text_wp">
          <div class="header_text_in sp-none">
          <p>法テラスは、国が設立した法的トラブル解決の総合案内所です。</p>
          <ul class="headlist clearfix col-md-6 col-md-offset-6 col-sm-12 col-xs-12">
          <li>
          <a href="https://www.zoomsight-
sv2.jp/HTRS/controller/index.html#https://www.houterasu.or.jp">音声読み上げ・文字拡大</a>

...
...
...
```

問題 2 / 4

TOC

X-Content-Type-Options ヘッダーが欠落しています

重大度:	低
CVSS スコア:	5.0
URL:	http://10.228.148.130/app/org/
エンティティー:	(Page)
リスク:	知識の乏しいユーザーに、ユーザー名、パスワード、クレジット・カード番号、社会保険番号などの秘密情報を提供するように求めることができます ユーザー名、パスワード、マシン名などの Web アプリケーションに関する秘密情報や、秘密のファイルの場所などの情報を取得することができます
原因:	セキュリティーで保護されていない Web アプリケーション・プログラムまたは設定
修正:	X-Content-Type-Options ヘッダーを使用するようにサーバーを構成してください

差:

論拠: AppScan は X-Content-Type-Options 応答ヘッダーが欠落していることを検出しました。そのためドライブバイ・ダウンロード攻撃にさらされる可能性が高くなります。

テスト要求と応答:

```
GET /app/org/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


HTTP/1.1 200 OK
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
default-style: IE=edge
Set-Cookie: PHPSESSID=pb2b8dkcag87r9ic36s1d477a2; path=/
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjVRSHVVMEorZWdHUU1oK0EwemFOVlE9PSIsInZhbHVlIjoiVlVhcWVyZHRzRDZ5eFltSWx6S0V2YVpTa25
5Z094ZFVkSDJsZERZTlZyV0puUmxrY1FuVDJjZk5sSzRWZnkrUGNUOFYxalo3RmV4ejkwK3FrSmhyUnc9PSIsImlhYyI6Ijlk
ZmI4OGZmYmNjMDE5NWFkMmZjZmVhMzY4NjU0YzU4OWYyMGU2OTFhMzk0NzEwNzc5ZTRjOWU3NGIwNWQ5MzAifQ%3D%3D;
expires=Tue, 12-Jun-2018 10:53:04 GMT; Max-Age=7200; path=/
Set-Cookie:
```

```
laravel_session=eyJpdiI6IkdMWWxpMFBSNXhxT0V5b0JjeDQzTlE9PSIsInZhbHVlIjoiR25wMWlkcjZtM3p0R24yRzd6Q
3YzdGtwMitGUjU1RlhTNjVsMG0wZlJ4bU1FUXhpYW5hc2Y5NnNwU2E2bnN2UUhuY3BkSXQ2ZTZHWUhadVNNNGRuRVE9PSIsIm
1hYyI6ImY2Y2RhY2NkNTQyZmI3N2UxNDBhN2I5ZGM4MzEzZjJjYWJmZGIyM2I0NTk0ZTc0NGVmNGVlMjA3OWZmZDI5MDAifQ%
3D%3D; expires=Tue, 12-Jun-2018 10:53:04 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.30
Connection: Keep-Alive
Date: Tue, 12 Jun 2018 08:53:04 GMT
Keep-Alive: timeout=5, max=100
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-cache, private
Transfer-Encoding: chunked

<!DOCTYPE HTML>
<html lang="ja">
<head><meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<meta name="Author" content="Houterasu" />
<meta http-equiv="DEFAULT-STYLE" content="IE=edge" />
<meta name="viewport" content="width=device-width,initial-scale=1.0,shrink-to-fit=no" />
<link rel="shortcut icon" href="/app/images/100555157.gif" />
<title>相談窓口検索　法テラス</title>
<link rel="stylesheet" href="/app/css/bootstrap.min.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_layout.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_style.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_pc.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_print.css" type="text/css" media="print" />

</head>
<body id="base" class="container-fluid">
    <!-- scs_jyogai_start -->
<div id="basebg">
    <noscript>
        <p class="jsmessage">法テラス公式ホームページではJavaScriptを使用しています。
          <br/>JavaScriptの使用を有効にしていない場合は、一部の機能が正確に動作しない恐れがあります。
          <br/>お手数ですがJavaScriptの使用を有効にしてください。</p>
    </noscript>
    <div class="blockjump">
        <a id="PTOP"></a>
    </div>

    <div id="blockskip">
        <script src="/app/js/jquery-1.9.1.min.js"></script>
        <script>
          $(function () {
          $("#blockskip a").focus(function () {
          $(this)
          .parent()
          .animate({
          height: '1.5em'
          }, { duration: 'fast' })
          .addClass("show");
          });
          $("#blockskip a").blur(function () {
          $(this)
          .parent()
          .animate({
          height: '1px'
          }, {
          duration: 'fast',
          complete: function () {
          $(this).removeClass("show");
          }
          })
          });
          });
        </script>
        <a href="#">このページの本文へ移動</a>
    </div>
    <div id="baseall" class="no-sub">
        <div class="header_wp">
          <div class="header_wp_in clearfix">
          <div class="header_text_wp">
          <div class="header_text_in sp-none">
          <p>法テラスは、国が設立した法的トラブル解決の総合案内所です。</p>
          <ul class="headlist clearfix col-md-6 col-md-offset-6 col-sm-12 col-xs-12">
          <li>
```

```
          <a href="https://www.zoomsight-
sv2.jp/HTRS/controller/index.html#https://www.houterasu.or.jp">音声読み上げ・文字拡大</a>
          </li>
          <li>
          <a href="/en/index.html">English</a>
          </li>
          <li>
          <a href="/k/index.html">携帯サイト</a>
          </li>
          <li>
          <a href="/sitemap.html">サイトマップ</a>
          </li>
          </ul>
          </div>
          </div>
          <div class="row header_logo_wrap">
          <div class="col-md-3 col-sm-3 col-xs-3 header_logo">
          <a href="/index.html">
          <img class="img-respons
...
...
...
```

問題 3 / 4

TOC

X-Content-Type-Options ヘッダーが欠落しています

重大度:	低
CVSS スコア:	5.0
URL:	http://10.228.148.130/app/org/detail/130102044
エンティティー:	130102044 (Page)
リスク:	知識の乏しいユーザーに、ユーザー名、パスワード、クレジット・カード番号、社会保険番号などの秘密情報を提供するように求めることができます ユーザー名、パスワード、マシン名などの Web アプリケーションに関する秘密情報や、秘密のファイルの場所などの情報を取得することができます
原因:	セキュリティーで保護されていない Web アプリケーション・プログラムまたは設定
修正:	X-Content-Type-Options ヘッダーを使用するようにサーバーを構成してください

差:

論拠: AppScan は X-Content-Type-Options 応答ヘッダーが欠落していることを検出しました。そのためドライブバイ・ダウンロード攻撃にさらされる可能性が高くなります。

テスト要求と応答:

```
GET /app/org/detail/130102044 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.228.148.130/app/org/list?page=2
Cookie: soudanList=1;
laravel_session=eyJpdiI6InhhRU9jRzZWM1FXU1MzYWpIUWlIdmc9PSIsInZhbHVlIjoiSDZDOWorR05weVNnbXB1dWVwO
FpEY1diaG90bUN0UEVKcHFMNE15M29ZWGZ4UnIyUUxVZGpNSW5qaDNZMlErOEJtM3E3MndZSDhQYW45QjdDemEzdEE9PSIsIm
lhYyI6IjA2ODQ5MjgxYmMyZWExZWEzZjY1YTY5YTNiZWY0OTFkZjliMzRmZTRkNjA4YTU3N2E1ZTY1OTlmOWY3MzQ1NTEifQ%
3D%3D; XSRF-
TOKEN=eyJpdiI6ImZDT0h3blNoa0ZkSmp3WDFPYzljZmc9PSIsInZhbHVlIjoiMTE1Z2gxenNvODR2aTVOek0yV1NQU3R2aFV
2eGFBcEVDVlZHU0ZqbHRpMTU1V25DUGZcL3BFRm5JclBPSThoZ1V1NVlxcVdwYzRGRzk2TnBjWVlTT1B3PT0iLCJtYWMiOiI5
MDdhMzIyMzUxNzM4MTM4YTM4ZDZlMTEyMzZkMTA2ODU4OGJmMDQ1MzBiMjgzMzg5YTA5ODNjZDhkOGI1MTY5In0%3D;
PHPSESSID=6ebsdplhncev03jjcb2lk1cia0
Connection: Keep-Alive
Host: 10.228.148.130
```

```
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


HTTP/1.1 200 OK
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
default-style: IE=edge
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkRDYmFLSUtldDVtUzZwaUl3VEJIWkE9PSIsInZhbHVlIjoiZ1I5cDY1cGJRK1NqcWsybHIxendOK1pQMlF
nbVp2M20xeWtvSEFhK3BcL1hFOGgrNlBtUE83TG1VdHozbkpsQ29oXC8xYVR4SlRrRzdJRmtGNzRscittdz09IiwibWFjIjoi
NGE3OWM1NjRhZTA3ODA3MGJmMmVhYTM2ZmQ5YzMxNGUyMDRiZDAwNzc0MjkzMWZiMDI4M2Q3NjczYmQ2N2VhZSJ9;
expires=Tue, 12-Jun-2018 10:53:05 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6ImJKYkMrZ2Zsd2RhZlE0bG9qU0N1UkE9PSIsInZhbHVlIjoiOUVSK2IwOVRJZ3pIU3pZazhNV
WQ0eHhmUW93MlwvN1wvb0xwYkl5bnNjeWVvc1Z0U0pwbWxhV3hWcWdwN3kwTGo4MkVBcmJGUVppcmZZdVp0eDJLT0dBZz09Ii
wibWFjIjoiNTAzYzFlZWI3NTk4NGU3NjRjZDNjNTg3ZGJkZjBhODBhOTZkMzNiMmU1MDgyNDkyZTE4YmQ4MmFjMTIwZThkOCJ
9; expires=Tue, 12-Jun-2018 10:53:05 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.30
Connection: Keep-Alive
Date: Tue, 12 Jun 2018 08:53:05 GMT
Keep-Alive: timeout=5, max=99
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-cache, private
Transfer-Encoding: chunked

<!DOCTYPE HTML>
<html lang="ja">
<head><meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<meta name="Author" content="Houterasu" />
<meta http-equiv="DEFAULT-STYLE" content="IE=edge" />
<meta name="viewport" content="width=device-width,initial-scale=1.0,shrink-to-fit=no" />
<link rel="shortcut icon" href="/app/images/100555157.gif" />
<title>相談窓口詳細　法テラス</title>
<link rel="stylesheet" href="/app/css/bootstrap.min.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_layout.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_style.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_pc.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_print.css" type="text/css" media="print" />
    <link rel="stylesheet" href="/app/css/style.tableconverter.css"/>
</head>
<body id="base" class="container-fluid">
    <!-- scs_jyogai_start -->
<div id="basebg">
    <noscript>
        <p class="jsmessage">法テラス公式ホームページではJavaScriptを使用しています。
          <br/>JavaScriptの使用を有効にしていない場合は、一部の機能が正確に動作しない恐れがあります。
          <br/>お手数ですがJavaScriptの使用を有効にしてください。</p>
    </noscript>
    <div class="blockjump">
        <a id="PTOP"></a>
    </div>

    <div id="blockskip">
        <script src="/app/js/jquery-1.9.1.min.js"></script>
        <script>
          $(function () {
          $("#blockskip a").focus(function () {
          $(this)
          .parent()
          .animate({
          height: '1.5em'
          }, { duration: 'fast' })
          .addClass("show");
          });
          $("#blockskip a").blur(function () {
          $(this)
          .parent()
          .animate({
          height: '1px'
          }, {
          duration: 'fast',
          complete: function () {
          $(this).removeClass("show");
          }
```

```
            })
            });
            });
        </script>
        <a href="#">このページの本文へ移動</a>
    </div>
    <div id="baseall" class="no-sub">
        <div class="header_wp">
          <div class="header_wp_in clearfix">
          <div class="header_text_wp">
          <div class="header_text_in sp-none">
          <p>法テラスは、国が設立した法的トラブル解決の総合案内所です。</p>
          <ul class="headlist clearfix col-md-6 col-md-offset-6 col-sm-12 col-xs-12">
          <li>
          <a href="https://www.zoomsight-
sv2.jp/HTRS/controller/index.html#https://www.houterasu.or.jp">音声読み上げ・文字拡大</a>

...
...
...
```

問題 4 / 4

TOC

X-Content-Type-Options ヘッダーが欠落しています

重大度:	低
CVSS スコア:	5.0
URL:	http://10.228.148.130/app/org
エンティティー:	org (Page)
リスク:	知識の乏しいユーザーに、ユーザー名、パスワード、クレジット・カード番号、社会保険番号などの秘密情報を提供するように求めることができます ユーザー名、パスワード、マシン名などの Web アプリケーションに関する秘密情報や、秘密のファイルの場所などの情報を取得することができます
原因:	セキュリティーで保護されていない Web アプリケーション・プログラムまたは設定
修正:	X-Content-Type-Options ヘッダーを使用するようにサーバーを構成してください

差:

論拠: AppScan は X-Content-Type-Options 応答ヘッダーが欠落していることを検出しました。そのためドライブバイ・ダウンロード攻撃にさらされる可能性が高くなります。

テスト要求と応答:

```
POST /app/org HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.228.148.130/app/org
Cookie: soudanList=;
laravel_session=eyJpdiI6IllvcG5UWkxLZmlkaXRDS0FnWjl1OUE9PSIsInZhbHVlIjoiTG15MlpqczRCUmNGNnA0WFhTR
GM5eGJIUVM3bUpscVwvTVdWRXh4SW1UTzFEemJON1U0aFVyTFVJOVF5QkYzanMzSUxodEN1OFNXQnF2eFdwSU93Mjh3PT0iLC
JtYWMiOiI0ZjVlNjZkNDA3YjcxZGViMjE4NThmMjRmZmZlM2VjZTRlOTYzNjk1NTVhYzhiNTU0NGZiMzRjZmUxNTUxOWMxIn0
%3D; XSRF-
TOKEN=eyJpdiI6IkxGZmpaMXVQQ3RuekpxSTdwQk1jdkE9PSIsInZhbHVlIjoiWFdTXC9SNmRHbEp0dk1kdWhCYlZwYkVyM2N
3ZGhud1VXSjMzN0sweVdJVExUdGZCbVUzWm5MOWdcL2FVUmNtQUlxRXA5SW1JdGhrMzBSbEZMOStzc2xLQT09IiwibWFjIjoi
NTkxNmQxYTM2MWQwZGQzMzhhMzUwM2UyNjk4ZGJkNjZiNDJhNjY4YzczY2Y2MzViMTI2OWEzZGMwNGI0ZTQ2YSJ9;
PHPSESSID=6ebsdplhncev03jjcb2lk1cia0
Connection: Keep-Alive
Host: 10.228.148.130
Pragma: no-cache
Content-Length: 209
```

```
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP
Content-Type: application/x-www-form-urlencoded

_token=yuEor3ontYoqIVemgYB9Md6zAOEcgAoJnyhA89RA&key_pref=4&key_addr=&kankei_kikan=&key_keyword=&k
ey_new=%E6%96%B0%E8%A6%8F&key_update=%E5%A4%89%E6%9B%B4&key_publish=%E5%85%AC%E9%96%8B&submit=%E6
%A4%9C%E7%B4%A2

HTTP/1.1 200 OK
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
default-style: IE=edge
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlpvMEIwYmNud0tIOXRyaVdrbEhJSkE9PSIsInZhbHVlIjoic2NcLzhKVTZUQjVpMmw2SE9IVEQ5dHdPUlB
0V1QwVDBGYnNVbUFKNFo1Z0ZiYWUzb25mb0gybWJNRGZxaUgrVTY5M21tXC9GcEIrc3lBYUhJSHczWnY2dz09IiwibWFjIjoi
YWIzYTk0ZmQzOTA2ZGZiY2ZiYWMxYzlkZDBkMjQ1NjFhMzkwNTU4ZWI2YTM3MmMxMjhjMTViN2E2YjFmNWFlYiJ9;
expires=Tue, 12-Jun-2018 10:53:06 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6ImZ4XC8wdmY5YmJUXC9SMmZDNmt4d3FCZz09IiwidmFsdWUiOiJnamZVc2NtcXREbVZhZlVyN
2hOMTFVcERMNTdmNU1CVDR4QXBTUmJEMHVZcU9xNXdcL25OaVQwT213cFRCdUYwVGRiVlhoXC83WlBxazBrQlVTOFVKejV3PT
0iLCJtYWMiOiJlZGIxZDFjYzY5YmJhMDZkYmYxNjVmN2Q5ODE2M2EzNmM0Yzc5YTQ1NmU4MzZjMmI5MzQ3NTdkOGVkZWQ4YjQ
3In0%3D; expires=Tue, 12-Jun-2018 10:53:06 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.30
Connection: Keep-Alive
Date: Tue, 12 Jun 2018 08:53:06 GMT
Keep-Alive: timeout=5, max=97
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-cache, private
Transfer-Encoding: chunked

<!DOCTYPE HTML>
<html lang="ja">
<head><meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<meta name="Author" content="Houterasu" />
<meta http-equiv="DEFAULT-STYLE" content="IE=edge" />
<meta name="viewport" content="width=device-width,initial-scale=1.0,shrink-to-fit=no" />
<link rel="shortcut icon" href="/app/images/100555157.gif" />
<title>相談窓口検索　法テラス</title>
<link rel="stylesheet" href="/app/css/bootstrap.min.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_layout.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_style.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_pc.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_print.css" type="text/css" media="print" />

</head>
<body id="base" class="container-fluid">
    <!-- scs_jyogai_start -->
<div id="basebg">
    <noscript>
        <p class="jsmessage">法テラス公式ホームページではJavaScriptを使用しています。
          <br/>JavaScriptの使用を有効にしていない場合は、一部の機能が正確に動作しない恐れがあります。
          <br/>お手数ですがJavaScriptの使用を有効にしてください。</p>
    </noscript>
    <div class="blockjump">
        <a id="PTOP"></a>
    </div>

    <div id="blockskip">
        <script src="/app/js/jquery-1.9.1.min.js"></script>
        <script>
          $(function () {
          $("#blockskip a").focus(function () {
          $(this)
          .parent()
          .animate({
          height: '1.5em'
          }, { duration: 'fast' })
          .addClass("show");
          });
          $("#blockskip a").blur(function () {
          $(this)
          .parent()
          .animate({
          height: '1px'
          }, {
```

```
            duration: 'fast',
            complete: function () {
            $(this).removeClass("show");
            }
            })
            });
            });
        </script>
        <a href="#">このページの本文へ移動</a>
    </div>
    <div id="baseall" class="no-sub">
        <div class="header_wp">
          <div class="header_wp_in clearfix">
          <div class="header_text_wp">
          <div class="header_text_in sp-none">
          <p>法テラスは、国が設立した法的トラブル解決の総合案内所です。</p>
          <ul class="headlist clearfix col-md-6 col-md-offset-6 col-sm-12 col-
...
...
...
```

低 X-XSS-Protection ヘッダーが欠落しています 4

TOC

問題 1 / 4

TOC

X-XSS-Protection ヘッダーが欠落しています

重大度:	低
CVSS スコア:	5.0
URL:	http://10.228.148.130/app/org/list
エンティティー:	list (Page)
リスク:	知識の乏しいユーザーに、ユーザー名、パスワード、クレジット・カード番号、社会保険番号などの秘密情報を提供するように求めることができます ユーザー名、パスワード、マシン名などの Web アプリケーションに関する秘密情報や、秘密のファイルの場所などの情報を取得することができます
原因:	セキュリティーで保護されていない Web アプリケーション・プログラムまたは設定
修正:	X-XSS-Protection ヘッダーを使用するようにサーバーを構成してください

差:

論拠: AppScan は X-XSS-Protection 応答ヘッダーが欠落していることを検出しました。そのためクロスサイト・スクリプティング攻撃を許可するおそれがあります。

テスト要求と応答:

```
GET /app/org/list?page=2 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.228.148.130/app/org/detail/130102044
Cookie: soudanList=1;
laravel_session=eyJpdiI6InlZbzJTVTNzaGRwb2JzQlQxcGtUaFE9PSIsInZhbHVlIjoieHZZUThKRkFaa2lqUkU3UEJWV
zhIMWVDbXI1MEx3aGptcjNHM3I1MzdraE5mdGZ6cFhCbzBma0xHck1BMG5zdEhPNlhNUDd0TjdBcDd5dVdueUVyNFE9PSIsIm
1hYyI6IjJlZjE5ZmFkNDY5YzU0YzcyMzc0Yzc3OTk4OTMwZmIyNTIxZWY4NzI2N2RhZjAxN2ViYTUzNmYxYmM5YzkxMmIifQ%
```

```
3D%3D; XSRF-
TOKEN=eyJpdiI6IjB5QnpHN2V6Yk5LcjhpNWlIdFwvZVVRPT0iLCJ2YWx1ZSI6Ims4c1VpTitqM2VwXC9xOFhZczF4cG5kTFp
aaE1uWHRRK29CR25VamhCeG5hRTJtSFNyaW5CdlZ1dEJkbTY3alZ3M04yQzA3V2gxWW9HVjI2VTNKQ1YwUT09IiwibWFjIjoi
M2VlZDIyNjc3YTBhMDZjZGZjNGVkZDM0MWM0MjU1OWI5ZDUxZWU3YjY2N2ZlZWFlOTdkNzNkYmVmODAzMDY0MyJ9;
PHPSESSID=6ebsdplhncev03jjcb2lk1cia0
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


HTTP/1.1 200 OK
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
default-style: IE=edge
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlQ2dGh4QmswRDRZRHRXYWdkVnByaHc9PSIsInZhbHVlIjoiOVdvTWZQSFhoY1hZd2JNMWpZOGJvcmNKSVh
2dUZUeU10aFNib1ZYbFlwU0NZV3VIZEwwbjNqSnJWbUNjOWh6ZEJjQTVlZUxwYnVYaGVnMm1nUzRiYVE9PSIsIm1hYyI6Ijg4
OGE3ZDM1MTJiN2NmOTZjMzBiM2UzOTg3ZTFmNTBjNDBiN2VjZDE0ZjNhYWM1YmM3ZDE0YTZmZTE3ZDg3ZTQifQ%3D%3D;
expires=Tue, 12-Jun-2018 10:53:04 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6ImtxTWZYM0Fra0podlowRXJUS2JxNXc9PSIsInZhbHVlIjoiUEJVcHh4a1JqOWs4eDVEM0Z3c
zV5dG9lRitmWkc0R3BZYmZVR1hvY2JcL1lsSG9TZ0VDSDczZWZ5djZ4VFVpXC90bzlCQ3ppQUF2QXhFSGdDUVNzT2dWdz09Ii
wibWFjIjoiZDU1Y2NiNTU0MjU2NzBlN2E1NzY2YjcxNDhhNmYyMjA2ZmJmYzhlYWNlMTk3YzA0ZTdkNTNmNTVlZmY3ZDdhNSJ
9; expires=Tue, 12-Jun-2018 10:53:04 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.30
Connection: Keep-Alive
Date: Tue, 12 Jun 2018 08:53:04 GMT
Keep-Alive: timeout=5, max=98
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-cache, private
Transfer-Encoding: chunked

<!DOCTYPE HTML>
<html lang="ja">
<head><meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<meta name="Author" content="Houterasu" />
<meta http-equiv="DEFAULT-STYLE" content="IE=edge" />
<meta name="viewport" content="width=device-width,initial-scale=1.0,shrink-to-fit=no" />
<link rel="shortcut icon" href="/app/images/100555157.gif" />
<title>相談窓口一覧　法テラス</title>
<link rel="stylesheet" href="/app/css/bootstrap.min.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_layout.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_style.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_pc.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_print.css" type="text/css" media="print" />
    <link rel="stylesheet" href="/app/css/style.tableconverter.css"/>
</head>
<body id="base" class="container-fluid">
    <!-- scs_jyogai_start -->
<div id="basebg">
    <noscript>
        <p class="jsmessage">法テラス公式ホームページではJavaScriptを使用しています。
          <br/>JavaScriptの使用を有効にしていない場合は、一部の機能が正確に動作しない恐れがあります。
          <br/>お手数ですがJavaScriptの使用を有効にしてください。</p>
    </noscript>
    <div class="blockjump">
        <a id="PTOP"></a>
    </div>

    <div id="blockskip">
        <script src="/app/js/jquery-1.9.1.min.js"></script>
        <script>
          $(function () {
          $("#blockskip a").focus(function () {
          $(this)
          .parent()
          .animate({
          height: '1.5em'
          }, { duration: 'fast' })
          .addClass("show");
          });
          $("#blockskip a").blur(function () {
          $(this)
          .parent()
```

```
            .animate({
            height: '1px'
            }, {
            duration: 'fast',
            complete: function () {
            $(this).removeClass("show");
            }
            })
            });
            });
        </script>
        <a href="#">このページの本文へ移動</a>
    </div>
    <div id="baseall" class="no-sub">
        <div class="header_wp">
          <div class="header_wp_in clearfix">
          <div class="header_text_wp">
          <div class="header_text_in sp-none">
          <p>法テラスは、国が設立した法的トラブル解決の総合案内所です。</p>
          <ul class="headlist clearfix col-md-6 col-md-offset-6 col-sm-12 col-xs-12">
          <li>
          <a href="https://www.zoomsight-
sv2.jp/HTRS/controller/index.html#https://www.houterasu.or.jp">音声読み上げ・文字拡大</a>

...
...
...
```

問題 2 / 4

TOC

X-XSS-Protection ヘッダーが欠落しています

重大度:	低
CVSS スコア:	5.0
URL:	http://10.228.148.130/app/org/
エンティティー:	(Page)
リスク:	知識の乏しいユーザーに、ユーザー名、パスワード、クレジット・カード番号、社会保険番号などの秘密情報を提供するように求めることができます ユーザー名、パスワード、マシン名などの Web アプリケーションに関する秘密情報や、秘密のファイルの場所などの情報を取得することができます
原因:	セキュリティーで保護されていない Web アプリケーション・プログラムまたは設定
修正:	X-XSS-Protection ヘッダーを使用するようにサーバーを構成してください

差:

論拠: AppScan は X-XSS-Protection 応答ヘッダーが欠落していることを検出しました。そのためクロスサイト・スクリプティング攻撃を許可するおそれがあります。

テスト要求と応答:

```
GET /app/org/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP
```

```
HTTP/1.1 200 OK
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
default-style: IE=edge
Set-Cookie: PHPSESSID=pb2b8dkcag87r9ic36s1d477a2; path=/
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjVRSHVVMEorZWdHUU1oK0EwemFOVlE9PSIsInZhbHVlIjoiVlVhcWVyZHRzRDZ5eFltSWx6S0V2YVpTa25
5Z094ZFVkSDJsZERZTlZyV0puUmxrY1FuVDJjZk5sSzRWZnkrUGNUOFYxalo3RmV4ejkwK3FrSmhyUnc9PSIsIm1hYyI6Ijlk
ZmI4OGZmYmNjMDE5NWFkMmZjZmVhMzY4NjU0YzU4OWYyMGU2OTFhMzk0NzEwNzc5ZTRjOWU3NGIwNWQ5MzAifQ%3D%3D;
expires=Tue, 12-Jun-2018 10:53:04 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6IkdMWWxpMFBSNXhxT0V5b0JjeDQzTlE9PSIsInZhbHVlIjoiR25wMWlkcjZtM3p0R24yRzd6Q
3YzdGtwMitGUjU1RlhTNjVsMG0wZlJ4bU1FUXhpYW5hc2Y5NnNwU2E2bnN2UUhuY3BkSXQ2ZTZHWUhadVNNNGRuRVE9PSIsIm
1hYyI6ImY2Y2RhY2NkNTQyZmI3N2UxNDBhN2I5ZGM4MzEzZjJjYWJmZGIyM2I0NTk0ZTc0NGVmNGVlMjA3OWZmZDI5MDAifQ%
3D%3D; expires=Tue, 12-Jun-2018 10:53:04 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.30
Connection: Keep-Alive
Date: Tue, 12 Jun 2018 08:53:04 GMT
Keep-Alive: timeout=5, max=100
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-cache, private
Transfer-Encoding: chunked

<!DOCTYPE HTML>
<html lang="ja">
<head><meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<meta name="Author" content="Houterasu" />
<meta http-equiv="DEFAULT-STYLE" content="IE=edge" />
<meta name="viewport" content="width=device-width,initial-scale=1.0,shrink-to-fit=no" />
<link rel="shortcut icon" href="/app/images/100555157.gif" />
<title>相談窓口検索　法テラス</title>
<link rel="stylesheet" href="/app/css/bootstrap.min.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_layout.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_style.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_pc.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_print.css" type="text/css" media="print" />

</head>
<body id="base" class="container-fluid">
    <!-- scs_jyogai_start -->
<div id="basebg">
    <noscript>
        <p class="jsmessage">法テラス公式ホームページではJavaScriptを使用しています。
          <br/>JavaScriptの使用を有効にしていない場合は、一部の機能が正確に動作しない恐れがあります。
          <br/>お手数ですがJavaScriptの使用を有効にしてください。</p>
    </noscript>
    <div class="blockjump">
        <a id="PTOP"></a>
    </div>

    <div id="blockskip">
        <script src="/app/js/jquery-1.9.1.min.js"></script>
        <script>
          $(function () {
          $("#blockskip a").focus(function () {
          $(this)
          .parent()
          .animate({
          height: '1.5em'
          }, { duration: 'fast' })
          .addClass("show");
          });
          $("#blockskip a").blur(function () {
          $(this)
          .parent()
          .animate({
          height: '1px'
          }, {
          duration: 'fast',
          complete: function () {
          $(this).removeClass("show");
          }
          })
          });
          });
        </script>
```

```
        <a href="#">このページの本文へ移動</a>
    </div>
    <div id="baseall" class="no-sub">
        <div class="header_wp">
          <div class="header_wp_in clearfix">
          <div class="header_text_wp">
          <div class="header_text_in sp-none">
          <p>法テラスは、国が設立した法的トラブル解決の総合案内所です。</p>
          <ul class="headlist clearfix col-md-6 col-md-offset-6 col-sm-12 col-xs-12">
          <li>
          <a href="https://www.zoomsight-
sv2.jp/HTRS/controller/index.html#https://www.houterasu.or.jp">音声読み上げ・文字拡大</a>
          </li>
          <li>
          <a href="/en/index.html">English</a>
          </li>
          <li>
          <a href="/k/index.html">携帯サイト</a>
          </li>
          <li>
          <a href="/sitemap.html">サイトマップ</a>
          </li>
          </ul>
          </div>
          </div>
          <div class="row header_logo_wrap">
          <div class="col-md-3 col-sm-3 col-xs-3 header_logo">
          <a href="/index.html">
          <img class="img-respons
...
...
...
```

問題 3 / 4

TOC

X-XSS-Protection ヘッダーが欠落しています

重大度:	低
CVSS スコア:	5.0
URL:	http://10.228.148.130/app/org/detail/130102044
エンティティー:	130102044 (Page)
リスク:	知識の乏しいユーザーに、ユーザー名、パスワード、クレジット・カード番号、社会保険番号などの秘密情報を提供するように求めることができます ユーザー名、パスワード、マシン名などの Web アプリケーションに関する秘密情報や、秘密のファイルの場所などの情報を取得することができます
原因:	セキュリティーで保護されていない Web アプリケーション・プログラムまたは設定
修正:	X-XSS-Protection ヘッダーを使用するようにサーバーを構成してください

差:

論拠: AppScan は X-XSS-Protection 応答ヘッダーが欠落していることを検出しました。そのためクロスサイト・スクリプティング攻撃を許可するおそれがあります。

テスト要求と応答:

```
GET /app/org/detail/130102044 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.228.148.130/app/org/list?page=2
Cookie: soudanList=1;
```

```
laravel_session=eyJpdiI6InhhRU9jRzZWM1FXU1MzYWpIUWlIdmc9PSIsInZhbHVlIjoiSDZDOWorR05weVNnbXB1dWVwO
FpEY1diaG90bUN0UEVKcHFMNE15M29ZWGZ4UnIyUUxVZGpNSW5qaDNZMlErOEJtM3E3MndZSDhQYW45QjdDemEzdEE9PSIsIm
1hYyI6IjA2ODQ5MjgxYmMyZWExZWEzZjY1YTY5YTNiZWY0OTFkZjliMzRmZTRkNjA4YTU3N2E1ZTY1OTlmOWY3MzQ1NTEifQ%
3D%3D; XSRF-
TOKEN=eyJpdiI6ImZDT0h3blNoa0ZkSmp3WDFPYzljZmc9PSIsInZhbHVlIjoiMTE1Z2gxenNvODR2aTVOek0yV1NQU3R2aFV
2eGFBcEVDVlZHU0ZqbHRpMTU1V25DUGZcL3BFRm5JclBPSThoZ1V1NVlxcVdwYzRGRzk2TnBjWVlTT1B3PT0iLCJtYWMiOiI5
MDdhMzIyMzUxNzM4MTM4YTM4ZDZlMTEyMzZkMTA2ODU4OGJmMDQ1MzBiMjgzMzg5YTA5ODNjZDhkOGI1MTY5In0%3D;
PHPSESSID=6ebsdplhncev03jjcb2lk1cia0
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


HTTP/1.1 200 OK
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
default-style: IE=edge
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkRDYmFLSUtldDVtUzZwaUl3VEJIWkE9PSIsInZhbHVlIjoiZ1I5cDY1cGJRK1NqcWsybHIxendOK1pQMlF
nbVp2M20xeWtvSEFhK3BcL1hFOGgrNlBtUE83TG1VdHozbkpsQ29oXC8xYVR4SlRrRzdJRmtGNzRscittdz09IiwibWFjIjoi
NGE3OWM1NjRhZTA3ODA3MGJmMmVhYTM2ZmQ5YzMxNGUyMDRiZDAwNzc0MjkzMWZiMDI4M2Q3NjczYmQ2N2VhZSJ9;
expires=Tue, 12-Jun-2018 10:53:05 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6ImJKYkMrZ2Zsd2RhZlE0bG9qU0N1UkE9PSIsInZhbHVlIjoiOUVSK2IwOVRJZ3pIU3pZazhNV
WQ0eHhmUW93MlwvN1wvb0xwYkl5bnNjeWVvc1Z0U0pwbWxhV3hWcWdwN3kwTGo4MkVBcmJGUVppcmZZdVp0eDJLT0dBZz09Ii
wibWFjIjoiNTAzYzFlZWI3NTk4NGU3NjRjZDNjNTg3ZGJkZjBhODBhOTZkMzNiMmU1MDgyNDkyZTE4YmQ4MmFjMTIwZThkOCJ
9; expires=Tue, 12-Jun-2018 10:53:05 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.30
Connection: Keep-Alive
Date: Tue, 12 Jun 2018 08:53:05 GMT
Keep-Alive: timeout=5, max=99
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-cache, private
Transfer-Encoding: chunked

<!DOCTYPE HTML>
<html lang="ja">
<head><meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<meta name="Author" content="Houterasu" />
<meta http-equiv="DEFAULT-STYLE" content="IE=edge" />
<meta name="viewport" content="width=device-width,initial-scale=1.0,shrink-to-fit=no" />
<link rel="shortcut icon" href="/app/images/100555157.gif" />
<title>相談窓口詳細　法テラス</title>
<link rel="stylesheet" href="/app/css/bootstrap.min.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_layout.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_style.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_pc.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_print.css" type="text/css" media="print" />
    <link rel="stylesheet" href="/app/css/style.tableconverter.css"/>
</head>
<body id="base" class="container-fluid">
    <!-- scs_jyogai_start -->
<div id="basebg">
    <noscript>
        <p class="jsmessage">法テラス公式ホームページではJavaScriptを使用しています。
          <br/>JavaScriptの使用を有効にしていない場合は、一部の機能が正確に動作しない恐れがあります。
          <br/>お手数ですがJavaScriptの使用を有効にしてください。</p>
    </noscript>
    <div class="blockjump">
        <a id="PTOP"></a>
    </div>

    <div id="blockskip">
        <script src="/app/js/jquery-1.9.1.min.js"></script>
        <script>
          $(function () {
          $("#blockskip a").focus(function () {
          $(this)
          .parent()
          .animate({
          height: '1.5em'
          }, { duration: 'fast' })
          .addClass("show");
          });
```

```
            $("#blockskip a").blur(function () {
            $(this)
            .parent()
            .animate({
            height: '1px'
            }, {
            duration: 'fast',
            complete: function () {
            $(this).removeClass("show");
            }
            })
            });
            });
        </script>
        <a href="#">このページの本文へ移動</a>
    </div>
    <div id="baseall" class="no-sub">
        <div class="header_wp">
          <div class="header_wp_in clearfix">
          <div class="header_text_wp">
          <div class="header_text_in sp-none">
          <p>法テラスは、国が設立した法的トラブル解決の総合案内所です。</p>
          <ul class="headlist clearfix col-md-6 col-md-offset-6 col-sm-12 col-xs-12">
          <li>
          <a href="https://www.zoomsight-
sv2.jp/HTRS/controller/index.html#https://www.houterasu.or.jp">音声読み上げ・文字拡大</a>

...
...
...
```

問題 4 / 4

TOC

X-XSS-Protection ヘッダーが欠落しています

重大度:	低
CVSS スコア:	5.0
URL:	http://10.228.148.130/app/org
エンティティー:	org (Page)
リスク:	知識の乏しいユーザーに、ユーザー名、パスワード、クレジット・カード番号、社会保険番号などの秘密情報を提供するように求めることができます ユーザー名、パスワード、マシン名などの Web アプリケーションに関する秘密情報や、秘密のファイルの場所などの情報を取得することができます
原因:	セキュリティーで保護されていない Web アプリケーション・プログラムまたは設定
修正:	X-XSS-Protection ヘッダーを使用するようにサーバーを構成してください

差:

論拠: AppScan は X-XSS-Protection 応答ヘッダーが欠落していることを検出しました。そのためクロスサイト・スクリプティング攻撃を許可するおそれがあります。

テスト要求と応答:

```
GET /app/org HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.228.148.130/app/org/detail/130102044
Cookie: soudanList=1;
laravel_session=eyJpdiI6ImJtWE56S0xGMDBwdkcyVXRaZlRselE9PSIsInZhbHVlIjoiSGxnSlJlNWxzbDR1YUhabkRJR
1VsQ1B0Nk5EVHNjYmxDdmtCbXlDNXFQMUR4M2JwYU53ZkwwS1RYQmtEWllmMmVjTTBSOHQ5cUszVUoyTjg3RHNPdXc9PSIsIm
```

```
1hYyI6IjkwNDhkNDZkYTE2NjJmMTM5NWY1MzQ2MjUxYjEzODFhMmRmNjQxNTA5ZTZjZjcwMzVmYzc2ODRiNWZhNDRiMTgifQ%
3D%3D; XSRF-
TOKEN=eyJpdiI6Imc1ZGJiWWQ3SCt3VWFOcG05SFl3OFE9PSIsInZhbHVlIjoiNVd6NllsWmNYTHU0ZzdEa1dXVkd3ckR1eGx
VeGRJZDBuZmlUaGR2ZDFyY1JnNTNiN0FKVjNxend6amNtVzZCMUNvSkNxMkU5YW1LNEVQZFpZVUVHd1E9PSIsIm1hYyI6IjA2
ZDQzMzNhODlkYTJlM2I0NWZkOTBhYWM0YjBhMjJhYjllN2RkYTFiODEzYjNlNjIxNmY3YmYwODBkZjcyZTMifQ%3D%3D;
PHPSESSID=6ebsdplhncev03jjcb2lk1cia0
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


HTTP/1.1 200 OK
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
default-style: IE=edge
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImNSTGdZZU9wNzg1UUFwaWU0bjVpUWc9PSIsInZhbHVlIjoiU1JRNFhoa0NSOVdDNU1lekprSm83NWxSZWp
CSVZyaWw1cm9RejljaXJxRkZONDUwWFFzblV4bUlCdURROThyYTQxXC81M1lmN0FyOGVKVzQ0WjdscGNBPT0iLCJtYWMiOiIy
YTJkNzVlNmIxNDI5NmU0NWIxNTIyNDJkNzhmNmYwMDAzZDZiZTc0NDJmMzRkMDczNWExNTU0ZTBiYWEyN2QzIn0%3D;
expires=Tue, 12-Jun-2018 10:53:06 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6IlNwVnBOa1g1R1BleEpUUFZTdnUzS3c9PSIsInZhbHVlIjoiUEtoemF3UHNtOE9VRmpoVmxBK
0MzVGJzRmJFQk5VaEYxR29pcGZsV2wrbG9PWmp3MDBXeU83UE11eTkwdWY5SnVGRUxxODRVRmhuYWk1N3hcL0lwV1lRPT0iLC
JtYWMiOiJmNjRmNjc5ZDYxMDJmZjJlY2UzYTU3ZjJkYzM4OTVlYjM2ZDU4ZGUxY2ZjZjllNjY4MjcwZTg5YTNiYzRlMjEyIn0
%3D; expires=Tue, 12-Jun-2018 10:53:06 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.30
Connection: Keep-Alive
Date: Tue, 12 Jun 2018 08:53:06 GMT
Keep-Alive: timeout=5, max=98
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-cache, private
Transfer-Encoding: chunked

<!DOCTYPE HTML>
<html lang="ja">
<head><meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<meta name="Author" content="Houterasu" />
<meta http-equiv="DEFAULT-STYLE" content="IE=edge" />
<meta name="viewport" content="width=device-width,initial-scale=1.0,shrink-to-fit=no" />
<link rel="shortcut icon" href="/app/images/100555157.gif" />
<title>相談窓口検索　法テラス</title>
<link rel="stylesheet" href="/app/css/bootstrap.min.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_layout.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_style.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_pc.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_print.css" type="text/css" media="print" />

</head>
<body id="base" class="container-fluid">
    <!-- scs_jyogai_start -->
<div id="basebg">
    <noscript>
        <p class="jsmessage">法テラス公式ホームページではJavaScriptを使用しています。
          <br/>JavaScriptの使用を有効にしていない場合は、一部の機能が正確に動作しない恐れがあります。
          <br/>お手数ですがJavaScriptの使用を有効にしてください。</p>
    </noscript>
    <div class="blockjump">
        <a id="PTOP"></a>
    </div>

    <div id="blockskip">
        <script src="/app/js/jquery-1.9.1.min.js"></script>
        <script>
          $(function () {
          $("#blockskip a").focus(function () {
          $(this)
          .parent()
          .animate({
          height: '1.5em'
          }, { duration: 'fast' })
          .addClass("show");
          });
          $("#blockskip a").blur(function () {
          $(this)
```

```
            .parent()
            .animate({
            height: '1px'
            }, {
            duration: 'fast',
            complete: function () {
            $(this).removeClass("show");
            }
            })
            });
            });
        </script>
        <a href="#">このページの本文へ移動</a>
    </div>
    <div id="baseall" class="no-sub">
        <div class="header_wp">
          <div class="header_wp_in clearfix">
          <div class="header_text_wp">
          <div class="header_text_in sp-none">
          <p>法テラスは、国が設立した法的トラブル解決の総合案内所です。</p>
          <ul class="headlist clearfix col-md-6 col-md-offset-6 col-sm-12 col-xs-12">
          <li>
          <a href="https://www.zoomsight-
sv2.jp/HTRS/controller/index.html#https://www.houterasu.or.jp">音声読み上げ・文字拡大</a>
          </li>
          <li>

...
...
...
```

低 セッション Cookie に HttpOnly 属性がありません 2

TOC

問題 1 / 2

TOC

セッション Cookie に HttpOnly 属性がありません

重大度:	低
CVSS スコア:	5.0
URL:	http://10.228.148.130/app/org/
エンティティー:	XSRF-TOKEN (Cookie)
リスク:	ハッカーが正規のユーザーになりすまし、ユーザーのレコードを表示または改変したり、ユーザーとしてトランザクションを実行するのに使用することができる、カスタマー・セッションおよび Cookie を盗み出したり操作することができる可能性があります
原因:	Web アプリケーションが HttpOnly 属性のないセッション Cookie を設定しています
修正:	すべてのセッション Cookie に HttpOnly 属性を追加してください。

差:

論拠: AppScan は、HttpOnly 属性のないセッション Cookie が使用されていることを検出しました。

テスト要求と応答:

```
GET /app/org/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


HTTP/1.1 200 OK
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
default-style: IE=edge
Set-Cookie: PHPSESSID=ejf4ddf6hjnlkf43hdt0oostj0; path=/
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImttMjBmTm8zZENHV0xJaEVTaHNWbXc9PSIsInZhbHVlIjoiZU1xY0k4YjMwcXRIb0w1Skg0WU0rck5tMkN
UYmJyWTBpUWtZXC9JNG9pM2tScU5EZnRhVHdybGhoRDI2b1krbEhVZnFNVndRWjdwYm5saXY0cjNcL21hUT09IiwibWFjIjoi
MjliZWRiNTI2YmMwMDUzMGEwZTdiZWMwNjY0ZmM3NmI2OTNlMTkxZmJjN2Q1YTU4YzdkOGU4Y2Y4MzQzMjE3NyJ9;
expires=Tue, 12-Jun-2018 10:54:39 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6ImxBOHY2MmxNVjZXYjc2d0w2S21xVGc9PSIsInZhbHVlIjoieVJvQnNvdTEwUWZ2MExGZWs1a
3RUSE43bTdkbnNQV29GOFNTQmdtNEtDbzRjcElObE1EZ2ZNSHlRZFVZSmRmOFU4NXg3WWtVYXNZYVY3K0I4Wmo5SWc9PSIsIm
1hYyI6IjI5OTJhZTJmZTE2YTM5ZmJhYzk3NTNkMmYxODY0ODU2ZmViOGRhYTRkYjAxYjViN2IwZTljZWM4YTRkMDZhZjQifQ%
3D%3D; expires=Tue, 12-Jun-2018 10:54:39 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.30
Connection: Keep-Alive
Date: Tue, 12 Jun 2018 08:54:39 GMT
Keep-Alive: timeout=5, max=92
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-cache, private
Transfer-Encoding: chunked

<!DOCTYPE HTML>
<html lang="ja">
<head><meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<meta name="Author" content="Houterasu" />
<meta http-equiv="DEFAULT-STYLE" content="IE=edge" />
<meta name="viewport" content="width=device-width,initial-scale=1.0,shrink-to-fit=no" />
<link rel="shortcut icon" href="/app/images/100555157.gif" />
<title>相談窓口検索　法テラス</title>
<link rel="stylesheet" href="/app/css/bootstrap.min.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_layout.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_style.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_pc.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_print.css" type="text/css" media="print" />

</head>
<body id="base" class="container-fluid">
    <!-- scs_jyogai_start -->
<div id="basebg">
    <noscript>
        <p class="jsmessage">法テラス公式ホームページではJavaScriptを使用しています。
          <br/>JavaScriptの使用を有効にしていない場合は、一部の機能が正確に動作しない恐れがあります。
          <br/>お手数ですがJavaScriptの使用を有効にしてください。</p>
    </noscript>
    <div class="blockjump">
        <a id="PTOP"></a>
    </div>

    <div id="blockskip">
        <script src="/app/js/jquery-1.9.1.min.js"></script>
        <script>
          $(function () {
          $("#blockskip a").focus(function () {
          $(this)
          .parent()
          .animate({
          height: '1.5em'
          }, { duration: 'fast' })
          .addClass("show");
          });
          $("#blockskip a").blur(function () {
          $(this)
          .parent()
          .animate({
          height: '1px'
```

```
            }, {
            duration: 'fast',
            complete: function () {
            $(this).removeClass("show");
            }
            })
            });
            });
        </script>
        <a href="#">このページの本文へ移動</a>
    </div>
    <div id="baseall" class="no-sub">
        <div class="header_wp">
          <div class="header_wp_in clearfix">
          <div class="header_text_wp">
          <div class="header_text_in sp-none">
          <p>法テラスは、国が設立した法的トラブル解決の総合案内所です。</p>
          <ul class="headlist clearfix col-md-6 col-md-offset-6 col-sm-12 col-xs-12">
          <li>
          <a href="https://www.zoomsight-
sv2.jp/HTRS/controller/index.html#https://www.houterasu.or.jp">音声読み上げ・文字拡大</a>
          </li>
          <li>
          <a href="/en/index.html">English</a>
          </li>
          <li>
          <a href="/k/index.html">携帯サイト</a>
          </li>
          <li>
          <a href="/sitemap.html">サイトマップ</a>
          </li>
          </ul>
          </div>
          </div>
          <div class="row header_logo_wrap">
          <div class="col-md-3 col-sm-3 col-xs-3 header_logo">
          <a href="/index.html">
          <img class="img-responsive"
...
...
...
```

問題 2 / 2

TOC

セッション Cookie に HttpOnly 属性がありません

重大度:	低
CVSS スコア:	5.0
URL:	http://10.228.148.130/app/org/
エンティティー:	PHPSESSID (Cookie)
リスク:	ハッカーが正規のユーザーになりすまし、ユーザーのレコードを表示または改変したり、ユーザーとしてトランザクションを実行するのに使用することができる、カスタマー・セッションおよび Cookie を盗み出したり操作することができる可能性があります
原因:	Web アプリケーションが HttpOnly 属性のないセッション Cookie を設定しています
修正:	すべてのセッション Cookie に HttpOnly 属性を追加してください。

差:

論拠: AppScan は、HttpOnly 属性のないセッション Cookie が使用されていることを検出しました。

テスト要求と応答:

```
GET /app/org/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


HTTP/1.1 200 OK
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
default-style: IE=edge
Set-Cookie: PHPSESSID=tik7c3t755he053bdmreve15e1; path=/
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InNwR3p5MnFZWlBycTU4RWtLQTNwZ1E9PSIsInZhbHVlIjoiVVNwSFNPNzJrMFloS1hLXC83M0N4Q0I5UjB
1NXFqZXBZczRRREZGR3pGbnVlK2NFV2hmbmlCVHIzME9ZQnNQK1ZxVlFtZEtLaTVtbFZYVUxMazg0THJBPT0iLCJtYWMiOiI0
NWYwMWYxNDI5ZmYyMTM2NmI3Njg1YjQyYjliNTVhOTEzZDI1MTAwNjBjOTUyMDE2YmExZjQ1NDMyYjVhMTE3In0%3D;
expires=Tue, 12-Jun-2018 10:54:41 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6InF5UklGeU1Mclh3bEM5OGF1QWxST0E9PSIsInZhbHVlIjoiOWthWFdiY3Y0RVYwYXBZcWI4M
jJBSndTZVFObGlibUNhclZ2aXlvSGhYUTVsUFBiVWJ5Z0NFV2w5QWZpMVF1TjZGNkxncFwvaFZZQnNqSlRjaURVNzhBPT0iLC
JtYWMiOiI1MzA4NGNlM2QzMjk5ZDBlZjM1MTdkMDFhNDE5NjA1NzZjZTA3NGJjOTAzMGEwNjEwZTYwMmQxMjdjODg4ZTQ4In0
%3D; expires=Tue, 12-Jun-2018 10:54:41 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.30
Connection: Keep-Alive
Date: Tue, 12 Jun 2018 08:54:41 GMT
Keep-Alive: timeout=5, max=94
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-cache, private
Transfer-Encoding: chunked

<!DOCTYPE HTML>
<html lang="ja">
<head><meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<meta name="Author" content="Houterasu" />
<meta http-equiv="DEFAULT-STYLE" content="IE=edge" />
<meta name="viewport" content="width=device-width,initial-scale=1.0,shrink-to-fit=no" />
<link rel="shortcut icon" href="/app/images/100555157.gif" />
<title>相談窓口検索　法テラス</title>
<link rel="stylesheet" href="/app/css/bootstrap.min.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_layout.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_style.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_pc.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_print.css" type="text/css" media="print" />

</head>
<body id="base" class="container-fluid">
    <!-- scs_jyogai_start -->
<div id="basebg">
    <noscript>
        <p class="jsmessage">法テラス公式ホームページではJavaScriptを使用しています。
          <br/>JavaScriptの使用を有効にしていない場合は、一部の機能が正確に動作しない恐れがあります。
          <br/>お手数ですがJavaScriptの使用を有効にしてください。</p>
    </noscript>
    <div class="blockjump">
        <a id="PTOP"></a>
    </div>

    <div id="blockskip">
        <script src="/app/js/jquery-1.9.1.min.js"></script>
        <script>
          $(function () {
          $("#blockskip a").focus(function () {
          $(this)
          .parent()
          .animate({
          height: '1.5em'
          }, { duration: 'fast' })
          .addClass("show");
          });
          $("#blockskip a").blur(function () {
          $(this)
```

```
            .parent()
            .animate({
            height: '1px'
            }, {
            duration: 'fast',
            complete: function () {
            $(this).removeClass("show");
            }
            })
            });
            });
        </script>
        <a href="#">このページの本文へ移動</a>
    </div>
    <div id="baseall" class="no-sub">
        <div class="header_wp">
          <div class="header_wp_in clearfix">
          <div class="header_text_wp">
          <div class="header_text_in sp-none">
          <p>法テラスは、国が設立した法的トラブル解決の総合案内所です。</p>
          <ul class="headlist clearfix col-md-6 col-md-offset-6 col-sm-12 col-xs-12">
          <li>
          <a href="https://www.zoomsight-
sv2.jp/HTRS/controller/index.html#https://www.houterasu.or.jp">音声読み上げ・文字拡大</a>
          </li>
          <li>
          <a href="/en/index.html">English</a>
          </li>
          <li>
          <a href="/k/index.html">携帯サイト</a>
          </li>
          <li>
          <a href="/sitemap.html">サイトマップ</a>
          </li>
          </ul>
          </div>
          </div>
          <div class="row header_logo_wrap">
          <div class="col-md-3 col-sm-3 col-xs-3 header_logo">
          <a href="/index.html">
          <img class="img-responsive"
...
...
...
```

低 ボディ・パラメーターをクエリーで送信 1 TOC

問題 1 / 1 TOC

ボディ・パラメーターをクエリーで送信

重大度:	低
CVSS スコア:	5.0
URL:	http://10.228.148.130/app/org
エンティティー:	org (Page)
リスク:	知識の乏しいユーザーに、ユーザー名、パスワード、クレジット・カード番号、社会保険番号などの秘密情報を提供するように求めることができます ユーザー名、パスワード、マシン名などの Web アプリケーションに関する秘密情報や、秘密のファイルの場所などの情報を取得することができます
原因:	セキュリティーで保護されていない Web アプリケーション・プログラムまたは設定
修正:	クエリー・ストリングで送信されるボディー・パラメーターを受け入れる受け入れません

差: **ボディー・パラメーター** 要求から削除されました: `yuEor3ontYoqIVemgYB9Md6zAOEcgAoJnyhA89RA`
クエリー・パラメーター 要求に追加されました: `yuEor3ontYoqIVemgYB9Md6zAOEcgAoJnyhA89RA`
ボディー・パラメーター 要求から削除されました: `4`
クエリー・パラメーター 要求に追加されました: `4`
ボディー・パラメーター 要求から削除されました: `—`
クエリー・パラメーター 要求に追加されました: `—`
ボディー・パラメーター 要求から削除されました: `—`
クエリー・パラメーター 要求に追加されました: `—`
ボディー・パラメーター 要求から削除されました: `—`
クエリー・パラメーター 要求に追加されました: `—`
ボディー・パラメーター 要求から削除されました: `新規`
クエリー・パラメーター 要求に追加されました: `新規`
ボディー・パラメーター 要求から削除されました: `変更`
クエリー・パラメーター 要求に追加されました: `変更`
ボディー・パラメーター 要求から削除されました: `公開`
クエリー・パラメーター 要求に追加されました: `公開`
ボディー・パラメーター 要求から削除されました: `検索`
クエリー・パラメーター 要求に追加されました: `検索`
方法 操作元: `POST` 操作先: `GET`

論拠: 「テスト応答」と「オリジナルの応答」が同じである (つまり、アプリケーションが、クエリーで送信されたボディ・パラメーターを処理した) ため、テスト結果では脆弱性が示されていると考えられます。

テスト要求と応答:

```
GET
/app/org?_token=yuEor3ontYoqIVemgYB9Md6zAOEcgAoJnyhA89RA&key_pref=4&key_addr=&kankei_kikan=&key_k
eyword=&key_new=%E6%96%B0%E8%A6%8F&key_update=%E5%A4%89%E6%9B%B4&key_publish=%E5%85%AC%E9%96%8B&s
ubmit=%E6%A4%9C%E7%B4%A2 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.228.148.130/app/org
Cookie: soudanList=;
laravel_session=eyJpdiI6IllvcG5UWkxLZmlkaXRDS0FnWjl1OUE9PSIsInZhbHVlIjoiTG15MlpqczRCUmNGNnA0WFhTR
GM5eGJIUVM3bUpscVwvTVdWRXh4SW1UTzFEemJON1U0aFVyTFVJOVF5QkYzanMzSUxodEN1OFNXQnF2eFdwSU93Mjh3PT0iLC
JtYWMiOiI0ZjVlNjZkNDA3YjcxZGViMjE4NThmMjRmZmZlM2VjZTRlOTYzNjk1NTVhYzhiNTU0NGZiMzRjZmUxNTUxOWMxIn0
%3D; XSRF-
TOKEN=eyJpdiI6IkxGZmpaMXVQQ3RuekpxSTdwQk1jdkE9PSIsInZhbHVlIjoiWFdTXC9SNmRHbEp0dk1kdWhCYlZwYkVyM2N
3ZGhud1VXSjMzN0sweVdJVExUdGZCbVUzWm5MOWdcL2FVUmNtQUlxRXA5SW1JdGhrMzBSbEZMOStzc2xLQT09IiwibWFjIjoi
NTkxNmQxYTM2MWQwZGQzMzhhMzUwM2UyNjk4ZGJkNjZiNDJhNjY4YzczY2Y2MzViMTI2OWEzZGMwNGI0ZTQ2YSJ9;
PHPSESSID=6ebsdplhncev03jjcb2lk1cia0
Connection: Keep-Alive
Host: 10.228.148.130
Pragma: no-cache
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
```

```
Accept-Language: ja-JP
Content-Type: application/x-www-form-urlencoded


HTTP/1.1 200 OK
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
default-style: IE=edge
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkhQc1JqazRBYW5lMitaZWVVckxDMFE9PSIsInZhbHVlIjoiekwzWHRcL2VCS29xa3RJU2JHMnBnMVZaZDl
pU2VBelYrSGFMZndQK2NHNWZRNHNvc2E1Q1V2cnByclRFaFFraTNWSOdqYTJ1eTh5VmF2NWJqUUhPV1NnPT0iLCJtYWMiOiI3
NTVmMGMyNWNlYjZmYjRmNTljM2MxNDU0ZmE2MTgyNGZiMjE4ZmZlOWM1MDFlMGYwNGY4OWJiYzgxMjAyMzlkIn0%3D;
expires=Tue, 12-Jun-2018 10:53:29 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6InhGMkgwd1c2cXA5QjhISDVzUXRsZ3c9PSIsInZhbHVlIjoiRjZJb0pDeGNmVEVkWWc3azM4b
TVLSlhuaHAxUmMzZ0dKUFFPaUE2QTBSSzk0cWJtU0p2XC9OWWdzMWZncWxsWmdwaldQNlFhTWlacjhJZ3VsRG92ZFVnPT0iLC
JtYWMiOiJkNzc3NzZiYWFlZTJhZGRkOTY1NGRiNzNlOTRkZDM5Yzg1MmQzZTU5MzhmYTBjNjQwMTFlMzc0MmU5MGZiYTE2In0
%3D; expires=Tue, 12-Jun-2018 10:53:29 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.30
Connection: Keep-Alive
Date: Tue, 12 Jun 2018 08:53:29 GMT
Keep-Alive: timeout=5, max=100
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-cache, private
Transfer-Encoding: chunked

<!DOCTYPE HTML>
<html lang="ja">
<head><meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<meta name="Author" content="Houterasu" />
<meta http-equiv="DEFAULT-STYLE" content="IE=edge" />
<meta name="viewport" content="width=device-width,initial-scale=1.0,shrink-to-fit=no" />
<link rel="shortcut icon" href="/app/images/100555157.gif" />
<title>相談窓口検索　法テラス</title>
<link rel="stylesheet" href="/app/css/bootstrap.min.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_layout.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_style.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_pc.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_print.css" type="text/css" media="print" />

</head>
<body id="base" class="container-fluid">
    <!-- scs_jyogai_start -->
<div id="basebg">
    <noscript>
        <p class="jsmessage">法テラス公式ホームページではJavaScriptを使用しています。
          <br/>JavaScriptの使用を有効にしていない場合は、一部の機能が正確に動作しない恐れがあります。
          <br/>お手数ですがJavaScriptの使用を有効にしてください。</p>
    </noscript>
    <div class="blockjump">
        <a id="PTOP"></a>
    </div>

    <div id="blockskip">
        <script src="/app/js/jquery-1.9.1.min.js"></script>
        <script>
          $(function () {
          $("#blockskip a").focus(function () {
          $(this)
          .parent()
          .animate({
          height: '1.5em'
          }, { duration: 'fast' })
          .addCla
...
...
...

          </ul>
          </div>
          </div>
        </div>
          <input type="hidden" name="key_new" id="key_new" value="新規" />
          <input type="hidden" name="key_update" id="key_update" value="変更" />
          <input type="hidden" name="key_publish" id="key_publish" value="公開" />
          <div class="commandbox">
```

```
            <input type="button" class="command-btn" value="検索" />
            <input type="submit" name="submit" class="command-submit" id="command-submit" hidden
value="検索" />
            <input type="button" name="btn-clear" class="clear-btn" value="クリア" />
            </div>
          </fieldset>
          </form>
...
...
...
```

オリジナルの応答

≈

テスト応答

低 一時ファイルのダウンロード 1

TOC

問題 1 / 1

TOC

一時ファイルのダウンロード

重大度:	低
CVSS スコア:	5.0
URL:	http://10.228.148.130/app/org/detail/130102044
エンティティー:	130102044 (Page)
リスク:	アプリケーション・ロジック、およびユーザー名やパスワードなどのその他の秘密情報を公開する可能性のある一時スクリプト・ファイルをダウンロードできます
原因:	テンポラリー・ファイルが製作環境に残されています
修正:	仮想ディレクトリーから古いバージョンのファイルを削除します

差: **パス** 操作元: `/app/org/detail/130102044` 操作先: `/app/org/detail/1301020441`

論拠: テストでソース・コード・ファイルの取得を試みました。レスポンスがエラーを発生させず、非 HTML コンテ

ンツを含んでいたことから、ソース・コードの取得に成功したことが示されています。

テスト要求と応答:

```
GET /app/org/detail/1301020441 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.228.148.130/app/org/list?page=2
Cookie: soudanList=1;
laravel_session=eyJpdiI6InhhRU9jRzZWM1FXU1MzYWpIUWlIdmc9PSIsInZhbHVlIjoiSDZDOWorR05weVNnbXB1dWVwO
FpEY1diaG90bUN0UEVKcHFMNE15M29ZWGZ4UnIyUUxVZGpNSW5qaDNZMlErOEJtM3E3MndZSDhQYW45QjdDemEzdEE9PSIsIm
1hYyI6IjA2ODQ5MjgxYmMyZWExZWEzZjY1YTY5YTNiZWY0OTFkZjliMzRmZTRkNjA4YTU3N2E1ZTY1OTlmOWY3MzQ1NTEifQ%
3D%3D; XSRF-
TOKEN=eyJpdiI6ImZDT0h3blNoa0ZkSmp3WDFPYzljZmc9PSIsInZhbHVlIjoiMTE1Z2gxenNvODR2aTVOek0yV1NQU3R2aFV
2eGFBcEVDVlZHU0ZqbHRpMTU1V25DUGZcL3BFRm5JclBPSThoZ1V1NVlxcVdwYzRGRzk2TnBjWVlTT1B3PT0iLCJtYWMiOiI5
MDdhMzIyMzUxNzM4MTM4YTM4ZDZlMTEyMzZkMTA2ODU4OGJmMDQ1MzBiMjgzMzg5YTA5ODNjZDhkOGI1MTY5In0%3D;
PHPSESSID=6ebsdplhncev03jjcb2lk1cia0
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


HTTP/1.1 200 OK
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
default-style: IE=edge
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IlcyNmlONmhtTU1ubFhxVFBQdk9vTHc9PSIsInZhbHVlIjoibDN5SjM2MHJEXC9LalhLUWE5bzViRFZEbVJ
GcGN3UndFVThJR1N3N2VwZFwvZzZOdk1QalB3elN1eDJkakdxelwvc3NQQmtqY0tcL3lORFRHajVGVjZZYmV3PT0iLCJtYWMi
OiIwZDYwZTVhNzA3ZmUxM2YyN2FhY2YyNzViMWQxMWU1NTcyZTVhOTJlNzRhOTc4MjFiY2IwMjI2NDFlM2M1ZGQ4In0%3D;
expires=Tue, 12-Jun-2018 11:10:05 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6InhvS0s3c2tFK0R3TGlIOXVaajdGUEE9PSIsInZhbHVlIjoiTWwwMElCZlZFZXhqQWRYYlwva
DJldW9ubUlIMUlJdjYxRTlGU0szbjlJNm1VOVUrTm12Z3o1UUhoeEo5bUNaQk1pblFOOVN2Y285Z0dCV00wNWlyZ2J3PT0iLC
JtYWMiOiIyMTY2Y2EwODE5ODExN2M4NzIyMDc3OWVhMTg2YzhkNWFhZTA4MGU2YjZiNTRhNDQ0MDI2MTVmY2EyOTY5MDk5In0
%3D; expires=Tue, 12-Jun-2018 11:10:05 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.30
Connection: Keep-Alive
Date: Tue, 12 Jun 2018 09:10:04 GMT
Keep-Alive: timeout=5, max=100
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-cache, private
Transfer-Encoding: chunked

<!DOCTYPE HTML>
<html lang="ja">
<head><meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<meta name="Author" content="Houterasu" />
<meta http-equiv="DEFAULT-STYLE" content="IE=edge" />
<meta name="viewport" content="width=device-width,initial-scale=1.0,shrink-to-fit=no" />
<link rel="shortcut icon" href="/app/images/100555157.gif" />
<title>相談窓口詳細　法テラス</title>
<link rel="stylesheet" href="/app/css/bootstrap.min.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_layout.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_style.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_pc.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_print.css" type="text/css" media="print" />
    <link rel="stylesheet" href="/app/css/style.tableconverter.css"/>
</head>
<body id="base" class="container-fluid">
    <!-- scs_jyogai_start -->
<div id="basebg">
    <noscript>
        <p class="jsmessage">法テラス公式ホームページではJavaScriptを使用しています。
          <br/>JavaScriptの使用を有効にしていない場合は、一部の機能が正確に動作しない恐れがあります。
          <br/>お手数ですがJavaScriptの使用を有効にしてください。</p>
    </noscript>
    <div class="blockjump">
        <a id="PTOP"></a>
    </div>

    <div id="blockskip">
        <script src="/app/js/jquery-1.9.1.min.js"></script>
        <script>
```

```
            $(function () {
            $("#blockskip a").focus(function () {
            $(this)
            .parent()
            .animate({
            height: '1.5em'
            }, { duration: 'fast' })
            .addClass("show");
            });
            $("#blockskip a").blur(function () {
            $(this)
            .parent()
            .animate({
            height: '1px'
            }, {
            duration: 'fast',
            complete: function () {
            $(this).removeClass("show");
            }
            })
            });
            });
        </script>
        <a href="#">このページの本文へ移動</a>
    </div>
    <div id="baseall" class="no-sub">
        <div class="header_wp">
          <div class="header_wp_in clearfix">
          <div class="header_text_wp">
          <div class="header_text_in sp-none">
          <p>法テラスは、国が設立した法的トラブル解決の総合案内所です。</p>
          <ul class="headlist clearfix col-md-6 col-md-offset-6 col-sm-12 col-xs-12">
          <li>
          <a href="https://www.zoomsight-
sv2.jp/HTRS/controller/index.html#https://www.houterasu.or.
...
...
...
```

低 秘密セッション情報を含むパーマネント Cookie 2 TOC

問題 1 / 2 TOC

秘密セッション情報を含むパーマネント Cookie

重大度:	低
CVSS スコア:	5.0
URL:	http://10.228.148.130/app/org/
エンティティー:	laravel_session (Cookie)
リスク:	パーマネント Cookie としてディスク上に保存されたセッション情報 (Cookie) を盗み出せる可能性があります
原因:	Web アプリケーションがパーマネント Cookie に秘密のセッション情報を (ディスク上) を格納しています
修正:	秘密のセッション情報をパーマネント Cookie に保存しないようにします

差:

論拠: AppScan が、セッション ID Cookie がクライアント・マシンに保存されていることを検出しました。

テスト要求と応答:

```
GET /app/org/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


HTTP/1.1 200 OK
Content-Length: 39101
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
default-style: IE=edge
Set-Cookie: PHPSESSID=6ebsdplhncev03jjcb2lk1cia0; path=/
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjB0UE1NelFobDVTbTNmeUlPOERVamc9PSIsInZhbHVlIjoiejczaG1cL2ZQaFA5bnd6cDRsaGxmQXgzM01
EOFwvMzgxY3lNZ2JUT3NoR0VKUkpJMVE3ZUNCZ3djMUhvbkxDS3U5eHRMRzk1eGRWeVwva1BuQm9WcU1Bb2c9PSIsIm1hYyI6
IjNhM2UwODQxOWYzYmIyMTljMjk4OGUyNDc0NGMyYWMwYjExZGZmOTEwYzlkNTQyMDAwYTUxZTgzMjRmODgwYmEifQ%3D%3D;
expires=Tue, 12-Jun-2018 10:44:01 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6IjRoSVA5cFgyUFwvcVwveTZST3l3OEVmUT09IiwidmFsdWUiOiJtSFwvS0prOFwvdmpaNEljQ
lVIMU5IVEhFQWRIeW12ZGxkYThHWTZnXC84bnVoV1JtakpubnJWVzVuekQ2alpEenRDQ0xxSzA3TGFTN0NQc1g4cnJTWVRaUT
09IiwibWFjIjoiNzFjMzc2Y2ZhZTMyYmU1ZDVhNzc5NmViZDZiODEzYWNlZWJiYjYyZjljYTA2NzBkNTE4MTdkOGNkZjY4ZTN
hNSJ9; expires=Tue, 12-Jun-2018 10:44:01 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.30
Connection: Keep-Alive
Date: Tue, 12 Jun 2018 08:44:01 GMT
Keep-Alive: timeout=5, max=100
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-cache, private

<!DOCTYPE HTML>
<html lang="ja">
<head><meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<meta name="Author" content="Houterasu" />
<meta http-equiv="DEFAULT-STYLE" content="IE=edge" />
<meta name="viewport" content="width=device-width,initial-scale=1.0,shrink-to-fit=no" />
<link rel="shortcut icon" href="/app/images/100555157.gif" />
<title>相談窓口検索　法テラス</title>
<link rel="stylesheet" href="/app/css/bootstrap.min.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_layout.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_style.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_pc.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_print.css" type="text/css" media="print" />

</head>
<body id="base" class="container-fluid">
    <!-- scs_jyogai_start -->
<div id="basebg">
    <noscript>
        <p class="jsmessage">法テラス公式ホームページではJavaScriptを使用しています。
          <br/>JavaScriptの使用を有効にしていない場合は、一部の機能が正確に動作しない恐れがあります。
          <br/>お手数ですがJavaScriptの使用を有効にしてください。</p>
    </noscript>
    <div class="blockjump">
        <a id="PTOP"></a>
    </div>

    <div id="blockskip">
        <script src="/app/js/jquery-1.9.1.min.js"></script>
        <script>
          $(function () {
          $("#blockskip a").focus(function () {
          $(this)
          .parent()
          .animate({
          height: '1.5em'
          }, { duration: 'fast' })
```

```
            .addClass("show");
            });
            $("#blockskip a").blur(function () {
            $(this)
            .parent()
            .animate({
            height: '1px'
            }, {
            duration: 'fast',
            complete: function () {
            $(this).removeClass("show");
            }
            })
            });
            });
        </script>
        <a href="#">このページの本文へ移動</a>
    </div>
    <div id="baseall" class="no-sub">
        <div class="header_wp">
          <div class="header_wp_in clearfix">
          <div class="header_text_wp">
          <div class="header_text_in sp-none">
          <p>法テラスは、国が設立した法的トラブル解決の総合案内所です。</p>
          <ul class="headlist clearfix col-md-6 col-md-offset-6 col-sm-12 col-xs-12">
          <li>
          <a href="https://www.zoomsight-
sv2.jp/HTRS/controller/index.html#https://www.houterasu.or.jp">音声読み上げ・文字拡大</a>
          </li>
          <li>
          <a href="/en/index.html">English</a>
          </li>
          <li>
          <a href="/k/index.html">携帯サイト</a>
          </li>
          <li>
          <a href="/sitemap.html">サイトマップ</a>
          </li>
          </ul>
          </div>
          </div>
          <div class="row header_logo_wrap">
          <div class="col-md-3 col-sm-3 col-xs-3 header_logo">
          <a href="/index.html">
          <img class="img-responsi
...
...
...
```

問題 2 / 2

TOC

秘密セッション情報を含むパーマネント Cookie

重大度:	低
CVSS スコア:	5.0
URL:	http://10.228.148.130/app/org/
エンティティー:	XSRF-TOKEN (Cookie)
リスク:	パーマネント Cookie としてディスク上に保存されたセッション情報 (Cookie) を盗み出せる可能性があります
原因:	Web アプリケーションがパーマネント Cookie に秘密のセッション情報を (ディスク上) を格納しています
修正:	秘密のセッション情報をパーマネント Cookie に保存しないようにします

差:

論拠: AppScan が、セッション ID Cookie がクライアント・マシンに保存されていることを検出しました。

テスト要求と応答:

```
GET /app/org/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


HTTP/1.1 200 OK
Content-Length: 39101
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
default-style: IE=edge
Set-Cookie: PHPSESSID=6ebsdplhncev03jjcb2lk1cia0; path=/
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjB0UE1NelFobDVTbTNmeUlPOERVamc9PSIsInZhbHVlIjoiejczaG1cL2ZQaFA5bnd6cDRsaGxmQXgzM01
EOFwvMzgxY3lNZ2JUT3NoR0VKUkpJMVE3ZUNCZ3djMUhvbkxDS3U5eHRMRzk1eGRWeVwva1BuQm9WcU1Bb2c9PSIsIm1hYyI6
IjNhM2UwODQxOWYzYmIyMTljMjk4OGUyNDc0NGMyYWMwYjExZGZmOTEwYzlkNTQyMDAwYTUxZTgzMjRmODgwYmEifQ%3D%3D;
expires=Tue, 12-Jun-2018 10:44:01 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6IjRoSVA5cFgyUFwvcVwveTZST3l3OEVmUT09IiwidmFsdWUiOiJtSFwvS0prOFwvdmpaNEljQ
1VIMU5IVEhFQWRIeW12ZGxkYThHWTZnXC84bnVoV1JtakpubnJWVzVuekQ2alpEenRDQ0xxSzA3TGFTN0NQc1g4cnJTWVRaUT
09IiwibWFjIjoiNzFjMzc2Y2ZhZTMyYmU1ZDVhNzc5NmViZDZiODEzYWNlZWJiYjYyZjljYTA2NzBkNTE4MTdkOGNkZjY4ZTN
hNSJ9; expires=Tue, 12-Jun-2018 10:44:01 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.30
Connection: Keep-Alive
Date: Tue, 12 Jun 2018 08:44:01 GMT
Keep-Alive: timeout=5, max=100
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-cache, private

<!DOCTYPE HTML>
<html lang="ja">
<head><meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<meta name="Author" content="Houterasu" />
<meta http-equiv="DEFAULT-STYLE" content="IE=edge" />
<meta name="viewport" content="width=device-width,initial-scale=1.0,shrink-to-fit=no" />
<link rel="shortcut icon" href="/app/images/100555157.gif" />
<title>相談窓口検索　法テラス</title>
<link rel="stylesheet" href="/app/css/bootstrap.min.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_layout.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/hweb_style.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_pc.css" type="text/css"/>
<link rel="stylesheet" href="/app/css/style_print.css" type="text/css" media="print" />

</head>
<body id="base" class="container-fluid">
    <!-- scs_jyogai_start -->
<div id="basebg">
    <noscript>
        <p class="jsmessage">法テラス公式ホームページではJavaScriptを使用しています。
          <br/>JavaScriptの使用を有効にしていない場合は、一部の機能が正確に動作しない恐れがあります。
          <br/>お手数ですがJavaScriptの使用を有効にしてください。</p>
    </noscript>
    <div class="blockjump">
        <a id="PTOP"></a>
    </div>

    <div id="blockskip">
        <script src="/app/js/jquery-1.9.1.min.js"></script>
        <script>
          $(function () {
          $("#blockskip a").focus(function () {
          $(this)
          .parent()
          .animate({
          height: '1.5em'
```

```
          }, { duration: 'fast' })
          .addClass("show");
          });
          $("#blockskip a").blur(function () {
          $(this)
          .parent()
          .animate({
          height: '1px'
          }, {
          duration: 'fast',
          complete: function () {
          $(this).removeClass("show");
          }
          })
          });
          });
        </script>
        <a href="#">このページの本文へ移動</a>
    </div>
    <div id="baseall" class="no-sub">
        <div class="header_wp">
          <div class="header_wp_in clearfix">
          <div class="header_text_wp">
          <div class="header_text_in sp-none">
          <p>法テラスは、国が設立した法的トラブル解決の総合案内所です。</p>
          <ul class="headlist clearfix col-md-6 col-md-offset-6 col-sm-12 col-xs-12">
          <li>
          <a href="https://www.zoomsight-
sv2.jp/HTRS/controller/index.html#https://www.houterasu.or.jp">音声読み上げ・文字拡大</a>
          </li>
          <li>
          <a href="/en/index.html">English</a>
          </li>
          <li>
          <a href="/k/index.html">携帯サイト</a>
          </li>
          <li>
          <a href="/sitemap.html">サイトマップ</a>
          </li>
          </ul>
          </div>
          </div>
          <div class="row header_logo_wrap">
          <div class="col-md-3 col-sm-3 col-xs-3 header_logo">
          <a href="/index.html">
          <img class="img-responsi
...
...
...
```

低 非表示のディレクトリーを検出 6 TOC

問題 1 / 6 TOC

非表示のディレクトリーを検出

重大度:	低
CVSS スコア:	5.0
URL:	http://10.228.148.130/cgi-bin/
エンティティー:	cgi-bin/ (Page)
リスク:	攻撃者が Web サイトをマップするのに利用できるサイトのファイル・システム構造についての情報を取得することができます
原因:	Web サーバーまたはアプリケーション・サーバーが安全でない方法で設定されています
修正:	禁止されているリソースについて「404 - Not Found」レスポンス・ステータス・コードを送出するか、完全に削除します

差: **パス** 操作元: `/app/org/` 操作先: `/cgi-bin/`

論拠: テストでサーバー上の隠しディレクトリーの検出を試みました。403 Forbidden レスポンスが返されました。これは、アクセスは許可されなかったものの、ディレクトリーの存在が漏洩したことを示しています。

テスト要求と応答:

```
GET /cgi-bin/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


HTTP/1.1 403 Forbidden
Connection: Keep-Alive
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
Content-Length: 210
Keep-Alive: timeout=5, max=100
Date: Tue, 12 Jun 2018 09:31:13 GMT
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access /cgi-bin/
on this server.</p>
</body></html>
```

問題 2 / 6

TOC

非表示のディレクトリーを検出

重大度:	低
CVSS スコア:	5.0
URL:	http://10.228.148.130/app/images/
エンティティー:	images/ (Page)
リスク:	攻撃者が Web サイトをマップするのに利用できるサイトのファイル・システム構造についての情報を取得することができます
原因:	Web サーバーまたはアプリケーション・サーバーが安全でない方法で設定されています
修正:	禁止されているリソースについて「404 - Not Found」レスポンス・ステータス・コードを送出するか、完全に削除します

差: **パス** 操作元: `/app/org/` 操作先: `/app/images/`

論拠: テストでサーバー上の隠しディレクトリーの検出を試みました。403 Forbidden レスポンスが返されました。これは、アクセスは許可されなかったものの、ディレクトリーの存在が漏洩したことを示しています。

テスト要求と応答:

```
GET /app/images/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


HTTP/1.1 403 Forbidden
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
Content-Length: 213
Date: Tue, 12 Jun 2018 09:32:55 GMT
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access /app/images/
on this server.</p>
</body></html>
```

非表示のディレクトリーを検出

重大度:	低
CVSS スコア:	5.0
URL:	http://10.228.148.130/app/js/
エンティティー:	js/ (Page)
リスク:	攻撃者が Web サイトをマップするのに利用できるサイトのファイル・システム構造についての情報を取得することができます
原因:	Web サーバーまたはアプリケーション・サーバーが安全でない方法で設定されています
修正:	禁止されているリソースについて「404 - Not Found」レスポンス・ステータス・コードを送出するか、完全に削除します

差: **パス** 操作元: `/app/org/` 操作先: `/app/js/`

論拠: テストでサーバー上の隠しディレクトリーの検出を試みました。403 Forbidden レスポンスが返されました。これは、アクセスは許可されなかったものの、ディレクトリーの存在が漏洩したことを示しています。

テスト要求と応答:

```
GET /app/js/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


HTTP/1.1 403 Forbidden
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
Content-Length: 209
Date: Tue, 12 Jun 2018 09:30:23 GMT
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access /app/js/
on this server.</p>
</body></html>
```

非表示のディレクトリーを検出

重大度:	低
CVSS スコア:	5.0
URL:	http://10.228.148.130/app/uploads/
エンティティー:	uploads/ (Page)
リスク:	攻撃者が Web サイトをマップするのに利用できるサイトのファイル・システム構造についての情報を取得することができます
原因:	Web サーバーまたはアプリケーション・サーバーが安全でない方法で設定されています
修正:	禁止されているリソースについて「404 - Not Found」レスポンス・ステータス・コードを送出するか、完全に削除します

差: **パス** 操作元: `/app/org/` 操作先: `/app/uploads/`

論拠: テストでサーバー上の隠しディレクトリーの検出を試みました。403 Forbidden レスポンスが返されました。これは、アクセスは許可されなかったものの、ディレクトリーの存在が漏洩したことを示しています。

テスト要求と応答:

```
GET /app/uploads/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


HTTP/1.1 403 Forbidden
Connection: Keep-Alive
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
Content-Length: 214
Keep-Alive: timeout=5, max=100
Date: Tue, 12 Jun 2018 09:44:45 GMT
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access /app/uploads/
on this server.</p>
</body></html>
```

問題 5 / 6

TOC

非表示のディレクトリーを検出

重大度:	低
CVSS スコア:	5.0
URL:	http://10.228.148.130/mrtg/
エンティティー:	mrtg/ (Page)
リスク:	攻撃者が Web サイトをマップするのに利用できるサイトのファイル・システム構造についての情報を取得することができます
原因:	Web サーバーまたはアプリケーション・サーバーが安全でない方法で設定されています
修正:	禁止されているリソースについて「404 - Not Found」レスポンス・ステータス・コードを送出するか、完全に削除します

差: **パス** 操作元: `/app/org/` 操作先: `/mrtg/`

論拠: テストでサーバー上の隠しディレクトリーの検出を試みました。403 Forbidden レスポンスが返されました。これは、アクセスは許可されなかったものの、ディレクトリーの存在が漏洩したことを示しています。

テスト要求と応答:

```
GET /mrtg/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


HTTP/1.1 403 Forbidden
Connection: Keep-Alive
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
Content-Length: 207
Keep-Alive: timeout=5, max=100
Date: Tue, 12 Jun 2018 09:52:40 GMT
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access /mrtg/
on this server.</p>
</body></html>
```

問題 6 / 6

TOC

非表示のディレクトリーを検出

重大度:	低
CVSS スコア:	5.0
URL:	http://10.228.148.130/app/css/
エンティティー:	css/ (Page)
リスク:	攻撃者が Web サイトをマップするのに利用できるサイトのファイル・システム構造についての情報を取得することができます
原因:	Web サーバーまたはアプリケーション・サーバーが安全でない方法で設定されています
修正:	禁止されているリソースについて「404 - Not Found」レスポンス・ステータス・コードを送出するか、完全に削除します

差: **パス** 操作元: `/app/org/` 操作先: `/app/css/`

論拠: テストでサーバー上の隠しディレクトリーの検出を試みました。403 Forbidden レスポンスが返されました。これは、アクセスは許可されなかったものの、ディレクトリーの存在が漏洩したことを示しています。

テスト要求と応答:

```
GET /app/css/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


HTTP/1.1 403 Forbidden
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
Content-Length: 210
Date: Tue, 12 Jun 2018 09:33:04 GMT
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access /app/css/
on this server.</p>
</body></html>
```

情 アプリケーション・エラー 9 TOC

問題 1 / 9 TOC

アプリケーション・エラー

重大度:	情報
CVSS スコア:	0.0
URL:	http://10.228.148.130/app/org/list
エンティティー:	page (Parameter)
リスク:	秘密のデバッグ情報を収集することができます
原因:	受信したパラメーター値について、適切な境界チェックが行われませんでした ユーザーの入力が必要なデータ型式に一致することを確認するための検証が行われませんでした
修正:	パラメーター値が期待される範囲とタイプであることを確認します。デバッグ・エラー・メッセージおよび例外を出力しないようにします。

差: **パラメーター** 操作元: 1 操作先: %00

論拠: アプリケーションが、秘密情報を公開する可能性のある未定義の状態を示すエラー・メッセージを返しました。

テスト要求と応答:

```
GET /app/org/list?page=%00 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.228.148.130/app/org/list?page=2
Cookie: soudanList=1;
laravel_session=eyJpdiI6ImhoMWVQRGt1SDdCTVVwdHR2eVppQVE9PSIsInZhbHVlIjoibXczK0VqREQ1T0VKaWJiYXpra
kw3RkVUOG5uK1Rvd1VNTVZ1Y1NFRmRhVWoxWjFQRU41Zm9TRnFHSEdCMFozTGhHTjJhbzJ4TzhMeTJtZ1wvQks4a1Z3PT0iLC
JtYWMiOiJjMTk0MDliYjQ3NGRmMzUzMzc3ODYwNTUzM2M3MTY1YTE0YjUxNWJjZTBjMGY4NGViNTY2ZDM4ODhiZmJiY2U5In0
%3D; XSRF-
TOKEN=eyJpdiI6Im9HSUkxSzk2aldaU09YQzRISE5yckE9PSIsInZhbHVlIjoiMm5UXC9aa3o0V0JNZUZtMCt5bU1oN0FtRkR
ibjkrRUFrMDBcLzJ2UFlGS0xDM1h1bWM1TjRDMGh2d29uVTlGaGtwRGlBWk14ais3MUxMZ2E2b2N3bWRnQT09IiwibWFjIjoi
YTQ5NmY1NmE0MTJlZDA0OTlhMDFlMjFkMzk4ZTI0ZDQ3MWQwZGIxMDBmMzNlNjU3YjZlYTlkOTQyZTNjZWFkNiJ9;
PHPSESSID=6ebsdplhncev03jjcb2lk1cia0
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


HTTP/1.1 500 Internal Server Error
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjVMWFZpSitoNTBNa2R6anMwd1hsYWc9PSIsInZhbHVlIjoiZEZkSWtxUmpoeEx5YWxIOUtCQ0dsTE4rdGQ
lV1dWS1JNcm5WYzJnSTBqeUE4eUpYbEFsWm1LUlJlUXd3ZjhMVTgzUWNFazRCYkRWSEM0WElWWlplb0E9PSIsIm1hYyI6IjI5
MTYzYzIyNGIyYzU1ZDYzMjBjOTc5OTdhODY5ZDRmZjUzYmE5YmI5YWQwMGFhNzRhZTRiNzQ2MjEyZGQzZmMifQ%3D%3D;
expires=Tue, 12-Jun-2018 10:56:48 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6Ik5iaDY3dit2NVwvWDBmRGh1elU4MXJnPT0iLCJ2YWx1ZSI6IjFyd2dtcFREY1wvcW5GMGh1N
```

```
k1nTUdVdFpvT1FOZmpjbG1Zb3FaRUZCdGtiZ3ZtUlQyRFwvYkxXSFlEWUxYQUZDYThVUUJqT2NuMWxYR21tejM1UlJpOFE9PS
IsIm1hYyI6IjFhYjRkZjIwYjMzZmQwNzczYzI5MGM0MWE3OTI2YThhMDFmZDAwMDc1ZWUyZTlkZjYwMzFlYThkOGE4NzE4MzI
ifQ%3D%3D; expires=Tue, 12-Jun-2018 10:56:48 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.30
Connection: close
Date: Tue, 12 Jun 2018 08:56:48 GMT
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-cache, private
Transfer-Encoding: chunked

<!DOCTYPE html>
<html>
    <head>
        <meta charset="UTF-8" />
        <meta name="robots" content="noindex,nofollow" />
        <style>          body { background-color: #F9F9F9; color: #222; font: 14px/1.4 Helvetica,
Arial, sans-serif; margin: 0; padding-bottom: 45px; }

          a { cursor: pointer; text-decoration: none; }
          a:hover { text-decoration: underline; }
          abbr[title] { border-bottom: none; cursor: help; text-decoration: none; }

          code, pre { font: 13px/1.5 Consolas, Monaco, Menlo, "Ubuntu Mono", "Liberation Mono",
monospace; }

          table, tr, th, td { background: #FFF; border-collapse: collapse; vertical-align: top; }
          table { background: #FFF; border: 1px solid #E0E0E0; box-shadow: 0px 0px 1px rgba(128,
128, 128, .2); margin: 1em 0; width: 100%; }
          table th, table td { border: solid #E0E0E0; border-width: 1px 0; padding: 8px 10px; }
          table th { background-color: #E0E0E0; font-weight: bold; text-align: left; }

          .hidden-xs-down { display: none; }
          .block { display: block; }
          .break-long-words { -ms-word-break: break-all; word-break: break-all; word-break:
break-word; -webkit-hyphens: auto; -moz-hyphens: auto; hyphens: auto; }
          .text-muted { color: #999; }

          .container { max-width: 1024px; margin: 0 auto; padding: 0 15px; }
          .container::after { content: ""; display: table; clear: both; }

          .exception-summary { background: #B0413E; border-bottom: 2px solid rgba(0, 0, 0, 0.1);
border-top: 1px solid rgba(0, 0, 0, .3); flex: 0 0 auto; margin-bottom: 30px; }

          .exception-message-wrapper { display: flex; align-items: center; min-height: 70px; }
          .exception-message { flex-grow: 1; padding: 30px 0; }
          .exception-message, .exception-message a { color: #FFF; font-size: 21px; font-weight:
400; margin: 0; }
          .exception-message.long { font-size: 18px; }
          .exception-message a { border-bottom: 1px solid rgba(255, 255, 255, 0.5); font-size:
inherit; text-decoration: none; }
          .exception-message a:hover { border-bottom-color: #ffffff; }

          .exception-illustration { flex-basis: 111px; flex-shrink: 0; height: 66px; margin-left:
15px; opacity: .7; }

          .trace + .trace { margin-top: 30px; }
          .trace-head .trace-class { color: #222; font-size: 18px; font-weight: bold; line-
height: 1.3; margin: 0; position: relative; }

          .trace-message { font-size: 14px; font-weight: normal; margin: .5em 0 0; }

          .trace-file-path, .trace-file-path a { color: #222; margin-top: 3px; font-size: 13px; }
          .trace-class { color: #B0413E; }
          .trace-type { padding: 0 2px; }

...
...
...
```

問題 2 / 9

TOC

アプリケーション・エラー

重大度:	情報
CVSS スコア:	0.0
URL:	http://10.228.148.130/app/org
エンティティー:	key_addr (Parameter)
リスク:	秘密のデバッグ情報を収集することができます
原因:	受信したパラメーター値について、適切な境界チェックが行われませんでした ユーザーの入力が必要なデータ型式に一致することを確認するための検証が行われませんでした
修正:	パラメーター値が期待される範囲とタイプであることを確認します。デバッグ・エラー・メッセージおよび例外を出力しないようにします。

差: **パラメーター** 操作元: `key_addr` 操作先: `__ORIG_VAL__.`

論拠: アプリケーションが、秘密情報を公開する可能性のある未定義の状態を示すエラー・メッセージを返しました。

テスト要求と応答:

```
POST /app/org HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.228.148.130/app/org
Cookie: soudanList=;
laravel_session=eyJpdiI6IlNyRlkyallKc2dKNGpGdWFFVDVLOXc9PSIsInZhbHVlIjoiWlFpUTkzUVphcHVBYnFIZzM5T
015bjgxVFBOUEllbXROY1Y0N1g0YmNydnI4RUZia0dZeGE3dlwvdXZCbGg5NnowQWdlVmhEQ0x4Y1c0YVJnUjJwS0RBPT0iLC
JtYWMiOiJjNGNiMzM5MTFmN2JhMGI5YmJmNmEwMTczMDhlNDE0MmNlMWI0NjYwNjJjNDM0YzdkZWYyNTYzZGEzNmU3MmM5In0
%3D; XSRF-
TOKEN=eyJpdiI6IjdlUWlKaHZ3NFZiS1F4ZDZrUld3dmc9PSIsInZhbHVlIjoiWVRaOE9wbVpOMDNpNzJPaW9Mak50cUxxVld
0OUdXZTVKbk5Sd1ZKVU5zd2RnWTFqcTNSbG1ucERIN1dJOFM4QVpsZnBCbHc3ZEx0NENORzQyUHI0Z3c9PSIsIm1hYyI6IjFl
YWQ5NDRkZThiOTFiZTM5OGNhMGJmMTVmZDAwNzdlNjdlNGE4OGE4ZWNmY2U1MDY5ODg1MzQ5NThiMGZmNjIifQ%3D%3D;
PHPSESSID=6ebsdplhncev03jjcb2lk1cia0
Connection: Keep-Alive
Host: 10.228.148.130
Pragma: no-cache
Content-Length: 211
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP
Content-Type: application/x-www-form-urlencoded

_token=yuEor3ontYoqIVemgYB9Md6zAOEcgAoJnyhA89RA&key_pref=13&key_addr.=&kankei_kikan=&key_keyword=
&key_new=%E6%96%B0%E8%A6%8F&key_update=%E5%A4%89%E6%9B%B4&key_publish=%E5%85%AC%E9%96%8B&submit=%
E6%A4%9C%E7%B4%A2

HTTP/1.1 500 Internal Server Error
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
Set-Cookie: XSRF-
TOKEN=eyJpdiI6InlaWjA2WXBhR1lJQjVxdHFlZEU0dmc9PSIsInZhbHVlIjoiaVcyeXJQYnJlSWJycTZLckduajBzY2tWdk9
lNlJWTTByY3dBUkw2RmxuTzFxYjl0aW96cTdodnlzRTFFRW1oMDQycVIrZjhvWEdnck0rakpHSkVXcEE9PSIsIm1hYyI6ImVj
ZGIxMTg2ZDNiZmI1MmI0NDg4MmIwMzI4N2E5ZjYwZDE2Yzk1YThmNWIwMmU2NmJiOTk2OTM4NmQ4ZjA1MDMifQ%3D%3D;
expires=Tue, 12-Jun-2018 11:01:01 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6Ik9mcEdOMjFVbkYwSHptQ2Z2Z3ZWQXc9PSIsInZhbHVlIjoianRuN1lJSXY3MzVrenk1enhER
m8rUTdBS20yNEl5SDFYdDNKNjBGdTFTVXE3S1wvQ3FMQ0hma3o1YlRzdU52U3E3d0RkNDRrVHYyMXNcL1Irb1RRNDAwZz09Ii
wibWFjIjoiMjE4OWQ3N2JjODVkM2YyZWY1YTFkNjZiZDIyYmIyNzhlYzRlZGQ3MzZkNGE2NGQyYjI0MjAzMjkwNWQwNmRiMCJ
9; expires=Tue, 12-Jun-2018 11:01:01 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.30
Connection: close
Date: Tue, 12 Jun 2018 09:01:01 GMT
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
```

```
Cache-Control: no-cache, private
Transfer-Encoding: chunked

<!DOCTYPE html>
<html>
    <head>
        <meta charset="UTF-8" />
        <meta name="robots" content="noindex,nofollow" />
        <style>         body { background-color: #F9F9F9; color: #222; font: 14px/1.4 Helvetica,
Arial, sans-serif; margin: 0; padding-bottom: 45px; }

          a { cursor: pointer; text-decoration: none; }
          a:hover { text-decoration: underline; }
          abbr[title] { border-bottom: none; cursor: help; text-decoration: none; }

          code, pre { font: 13px/1.5 Consolas, Monaco, Menlo, "Ubuntu Mono", "Liberation Mono",
monospace; }

          table, tr, th, td { background: #FFF; border-collapse: collapse; vertical-align: top; }
          table { background: #FFF; border: 1px solid #E0E0E0; box-shadow: 0px 0px 1px rgba(128,
128, 128, .2); margin: 1em 0; width: 100%; }
          table th, table td { border: solid #E0E0E0; border-width: 1px 0; padding: 8px 10px; }
          table th { background-color: #E0E0E0; font-weight: bold; text-align: left; }

          .hidden-xs-down { display: none; }
          .block { display: block; }
          .break-long-words { -ms-word-break: break-all; word-break: break-all; word-break:
break-word; -webkit-hyphens: auto; -moz-hyphens: auto; hyphens: auto; }
          .text-muted { color: #999; }

          .container { max-width: 1024px; margin: 0 auto; padding: 0 15px; }
          .container::after { content: ""; display: table; clear: both; }

          .exception-summary { background: #B0413E; border-bottom: 2px solid rgba(0, 0, 0, 0.1);
border-top: 1px solid rgba(0, 0, 0, .3); flex: 0 0 auto; margin-bottom: 30px; }

          .exception-message-wrapper { display: flex; align-items: center; min-height: 70px; }
          .exception-message { flex-grow: 1; padding: 30px 0; }
          .exception-message, .exception-message a { color: #FFF; font-size: 21px; font-weight:
400; margin: 0; }
          .exception-message.long { font-size: 18px; }
          .exception-message a { border-bottom: 1px solid rgba(255, 255, 255, 0.5); font-size:
inherit; text-decoration: none; }
          .exception-message a:hover { border-bottom-color: #ffffff; }

          .exception-illustration { flex-basis: 111px; flex-shrink: 0; height: 66px; margin-left:
15px; opacity: .7; }

          .trace + .trace { margin-top: 30px; }
          .trace-head .trace-class { color: #222; font-size: 18px; font-weight: bold; line-
height: 1.3; margin: 0; position: relative; }

          .trace-message { font-size: 14p
...
...
...
```

問題 3 / 9

TOC

アプリケーション・エラー

重大度:	情報
CVSS スコア:	0.0
URL:	http://10.228.148.130/app/home/trackLog
エンティティー:	key_track_log (Parameter)
リスク:	秘密のデバッグ情報を収集することができます
原因:	受信したパラメーター値について、適切な境界チェックが行われませんでした ユーザーの入力が必要なデータ型式に一致することを確認するための検証が行われませんでした
修正:	パラメーター値が期待される範囲とタイプであることを確認します。デバッグ・エラー・メッセージおよび例外を出力しないようにします。

差: **パラメーター** 操作元: `key_track_log` 操作先: `__ORIG_VAL__[]`

論拠: アプリケーションが、秘密情報を公開する可能性のある未定義の状態を示すエラー・メッセージを返しました。

テスト要求と応答:

```
POST /app/home/trackLog HTTP/1.1
Content-Length: 168
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 10.228.148.130
Cookie: soudanList=;
laravel_session=eyJpdiI6IjRoSVA5cFgyUFwvcVwveTZST3l3OEVmUT09IiwidmFsdWUiOiJtSFwvS0prOFwvdmpaNEljQ
1VIMU5IVEhFQWRIeW12ZGxkYThHWTZnXC84bnVoV1JtakpubnJWVzVuekQ2alpEenRDQ0xxSzA3TGFTN0NQc1g4cnJTWVRaUT
09IiwibWFjIjoiNzFjMzc2Y2ZhZTMyYmU1ZDVhNzc5NmViZDZiODEzYWNlZWJiYjYyZjljYTA2NzBkNTE4MTdkOGNkZjY4ZTN
hNSJ9; XSRF-
TOKEN=eyJpdiI6IjB0UE1NelFobDVTbTNmeUlPOERVamc9PSIsInZhbHVlIjoiejczaG1cL2ZQaFA5bnd6cDRsaGxmQXgzM01
EOFwvMzgxY3lNZ2JUT3NoR0VKUkpJMVE3ZUNCZ3djMUhvbkxDS3U5eHRMRzk1eGRWeVwva1BuQm9WcU1Bb2c9PSIsIm1hYyI6
IjNhM2UwODQxOWYzYmIyMTljMjk4OGUyNDc0NGMyYWMwYjExZGZmOTEwYzlkNTQyMDAwYTUxZTgzMjRmODgwYmEifQ%3D%3D;
PHPSESSID=6ebsdplhncev03jjcb2lk1cia0
X-Requested-With: XMLHttpRequest
Connection: Keep-Alive
Referer: http://10.228.148.130/app/org/
Accept: text/plain, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: ja-JP
Pragma: no-cache

_token=yuEor3ontYoqIVemgYB9Md6zAOEcgAoJnyhA89RA&key_screen=GC0010.%E7%9B%B8%E8%AB%87%E7%AA%93%E5%
8F%A3%E6%A4%9C%E7%B4%A2&key_track_log%5B%5D=%E3%82%AF%E3%83%AA%E3%82%A2

HTTP/1.1 500 Internal Server Error
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImdCd2I4MlVTREdUZGZsODF6dXErZlE9PSIsInZhbHVlIjoiQVduVlBkZkxEYWN4V3ptcEhvcjFJZkxidTF
JeTZTUnZKdVNudjBOdjlWV1RpWmNmdHBhdERkTFVDNGRLTUsycjF0eG41M21sbTJQc3ljbTJ0dzlZY1E9PSIsIm1hYyI6Ijkx
YWQzYTYwOTk2MjU3NDYwMjE2ZGQyMTJlYjI4ZThmNDIwYzhhMDMxMWJmYzlkZjYzMmQ2YjcyNjZiMDMxZWQifQ%3D%3D;
expires=Tue, 12-Jun-2018 10:58:21 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6Ik4wRU5KSlNLT3dKMnhEcnQzWXVmQUE9PSIsInZhbHVlIjoicmxLRmkzQWVmeEFDVWFkNm1xV
2l3dWpacjg2S2RuSU9NSkg5MnFBRWdNUUdqY3UyOWg1TUxkMnlTbWViZmwxbysxY2ZuU0NSYUorVFNBQ0p0ek9DK0E9PSIsIm
1hYyI6IjQ4YmViYjRlMjEyNDFjYTg5NjA3N2E0Y2NmYjMzMjI1Njc2ZmQ1NzQ2ZjBkNmYxNmEzODNmMDI5YzA1OTIxZjQifQ%
3D%3D; expires=Tue, 12-Jun-2018 10:58:21 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.30
Connection: close
Date: Tue, 12 Jun 2018 08:58:21 GMT
Content-Type: application/json
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-cache, private
Transfer-Encoding: chunked

{
```

```
"message": "Array to string conversion",
"exception": "ErrorException",
"file": "/var/www/app/app/Helpers/CommonHelper.php",
"line": 52,
"trace": [
{
"function": "handleError",
"class": "Illuminate\\Foundation\\Bootstrap\\HandleExceptions",
"type": "->"
        }       ,
{
"file": "/var/www/app/app/Helpers/CommonHelper.php",
"line": 52,
"function": "str_replace"
        }       ,
{
"file": "/var/www/app/app/Http/Controllers/HomeController.php",
"line": 39,
"function": "pushAction",
"class": "App\\Helpers\\CommonHelper",
"type": "->"
        }       ,
{
"function": "trackLog",
"class": "App\\Http\\Controllers\\HomeController",
"type": "->"
        }       ,
{
"file": "/var/www/app/vendor/laravel/framework/src/Illuminate/Routing/Controller.php",
"line": 54,
"function": "call_user_func_array"
        }       ,
{
"file": "/var/www/app/vendor/laravel/framework/src/Illuminate/Routing/ControllerDispatcher.php",
"line": 45,
"function": "callAction",
"class": "Illuminate\\Routing\\Controller",
"type": "->"
        }       ,
```

```
{
"file": "/var/www/app/vendor/laravel/framework/src/Illuminate/Routing/Route.php",
"line": 212,
"function": "dispatch",
"class": "Illuminate\\Routing\\ControllerDispatcher",
"type": "->"
         }       ,
{
"file": "/var/www/app/vendor/laravel/framework/src/Illuminate/Routing/Route.php",
"line": 169,
"function": "runController",
"class": "Illuminate\\Routing\\Route",
"type": "->"
         }       ,
{
"file": "/var/www/app/vendor/laravel/framework/src/Illuminate/Routing/Router.php",
"line": 658,
"function": "run",
"class": "Illuminate\\Routing\\Route",
"type": "->"
         }       ,
{
"file": "/var/www/app/vendor/laravel/framework/src/Illuminate/Routing/Pipeline.php",
"line": 30,
"function": "Illuminate\\Routing\\{closure}",
"class": "Illuminate\\Routing\\Router",
"type": "->"
         }       ,
{
"file": "/var/www/app/app/Http/Middleware/RedirectIfAuthenticated.php",
"line": 24,
"function": "Illuminate\\Routing\\{closure}",
"class": "Illuminate\\Routing\\Pipeline",
"type": "->"
         }       ,
{
"file": "/var/www/app/vendor/laravel/framework/src/Illuminate/Pipeline/Pipeline.php",
"line": 149,
"function": "handle",
```

```
"class": "App\\Http\\Middleware\\RedirectIfAuthenticated",

"type": "->"

         }       ,

{

"file": "/var/www/app/vendor/laravel/framework/src/Illuminate/Routing/Pipeline.php",

"line": 53,

"function": "Illuminate\\Pipeline\\{closure}",

"c
...
...
...
```

問題 4 / 9

TOC

アプリケーション・エラー

重大度:	情報
CVSS スコア:	0.0
URL:	http://10.228.148.130/app/home/trackLog
エンティティー:	key_screen (Parameter)
リスク:	秘密のデバッグ情報を収集することができます
原因:	受信したパラメーター値について、適切な境界チェックが行われませんでした ユーザーの入力が必要なデータ型式に一致することを確認するための検証が行われませんでした
修正:	パラメーター値が期待される範囲とタイプであることを確認します。デバッグ・エラー・メッセージおよび例外を出力しないようにします。

差: **パラメーター** 操作元: `key_screen` 操作先: `__ORIG_VAL__[]`

論拠: アプリケーションが、秘密情報を公開する可能性のある未定義の状態を示すエラー・メッセージを返しました。

テスト要求と応答:

```
POST /app/home/trackLog HTTP/1.1
Content-Length: 168
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 10.228.148.130
Cookie: soudanList=;
laravel_session=eyJpdiI6IjRoSVA5cFgyUFwvcVwveTZST3l3OEVmUT09IiwidmFsdWUiOiJtSFwvS0prOFwvdmpaNEljQ
1VIMU5IVEhFQWRIeW12ZGxkYThHWTZnXC84bnVoV1JtakpubnJWVzVuekQ2alpEenRDQ0xxSzA3TGFTN0NQc1g4cnJTWVRaUT
09IiwibWFjIjoiNzFjMzc2Y2ZhZTMyYmU1ZDVhNzc5NmViZDZiODEzYWNlZWJiYjYyZjljYTA2NzBkNTE4MTdkOGNkZjY4ZTN
hNSJ9; XSRF-
TOKEN=eyJpdiI6IjB0UE1NelFobDVTbTNmeUlPOERVamc9PSIsInZhbHVlIjoiejczaG1cL2ZQaFA5bnd6cDRsaGxmQXgzM01
EOFwvMzgxY3lNZ2JUT3NoR0VKUkpJMVE3ZUNCZ3djMUhvbkxDS3U5eHRMRzk1eGRWeVwva1BuQm9WcU1Bb2c9PSIsIm1hYyI6
IjNhM2UwODQxOWYzYmIyMTljMjk4OGUyNDc0NGMyYWMwYjExZGZmOTEwYzlkNTQyMDAwYTUxZTgzMjRmODgwYmEifQ%3D%3D;
PHPSESSID=6ebsdplhncev03jjcb2lklcia0
X-Requested-With: XMLHttpRequest
Connection: Keep-Alive
Referer: http://10.228.148.130/app/org/
Accept: text/plain, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
```

```
Accept-Language: ja-JP
Pragma: no-cache

_token=yuEor3ontYoqIVemgYB9Md6zAOEcgAoJnyhA89RA&key_screen%5B%5D=GC0010.%E7%9B%B8%E8%AB%87%E7%AA%
93%E5%8F%A3%E6%A4%9C%E7%B4%A2&key_track_log=%E3%82%AF%E3%83%AA%E3%82%A2

HTTP/1.1 500 Internal Server Error
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImxlR3RWVU43M1BGVEpDZ2hRSzVBaHc9PSIsInZhbHVlIjoialpSd1V4bTdYREZGTFVCYUtMTWpWeDZQV0R
wdFJjblNYS1M4T0VLTHBDV0RwTGpIZzBkVGFjV3grYWZCMTlvajBtNFRkMXFuZ3lTSktFcFY3Q0hWOEE9PSIsImlhYyI6IjQx
MDkzM2I2NWUzZGYwYTUyNTA5MTNmNWRhOTRhNTAzOWNlNjQ3YWM2M2IyYzBlODA1MWQ3MWJjN2U4YzRlNWQifQ%3D%3D;
expires=Tue, 12-Jun-2018 10:58:27 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6IkhyYXdVeXpZSHJJcDBkV0d5Q3kwWWc9PSIsInZhbHVlIjoiYnlMTHRMRDJrNytQN1lnTnVJS
HVJakR3TnlLT3FRaE5nVGxUK0MzWkhIcGYyTjY3ak5zd3E3MDRmOEdRV0d5bUhBR0RXM1RDTFdXemlUV2J6OFJRakE9PSIsIm
1hYyI6IjhhMGU1MWEwMzdjY2QxOWM5ZTViYzljZjg5NTRiNDE4YzgyZDk2ZWMyM2NjYTE1NzBmM2M2NDRlN2U4ZmI3NjEifQ%
3D%3D; expires=Tue, 12-Jun-2018 10:58:27 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.30
Connection: close
Date: Tue, 12 Jun 2018 08:58:27 GMT
Content-Type: application/json
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-cache, private
Transfer-Encoding: chunked

{

"message": "Array to string conversion",

"exception": "ErrorException",

"file": "/var/www/app/app/Helpers/CommonHelper.php",

"line": 53,

"trace": [

{

"file": "/var/www/app/app/Helpers/CommonHelper.php",

"line": 53,

"function": "handleError",

"class": "Illuminate\\Foundation\\Bootstrap\\HandleExceptions",

"type": "->"

        }       ,

{

"file": "/var/www/app/app/Http/Controllers/HomeController.php",

"line": 39,

"function": "pushAction",

"class": "App\\Helpers\\CommonHelper",

"type": "->"

        }       ,

{

"function": "trackLog",

"class": "App\\Http\\Controllers\\HomeController",

"type": "->"

        }       ,
```

```
{
"file": "/var/www/app/vendor/laravel/framework/src/Illuminate/Routing/Controller.php",
"line": 54,
"function": "call_user_func_array"
        }       ,
{
"file": "/var/www/app/vendor/laravel/framework/src/Illuminate/Routing/ControllerDispatcher.php",
"line": 45,
"function": "callAction",
"class": "Illuminate\\Routing\\Controller",
"type": "->"
        }       ,
{
"file": "/var/www/app/vendor/laravel/framework/src/Illuminate/Routing/Route.php",
"line": 212,
"function": "dispatch",
"class": "Illuminate\\Routing\\ControllerDispatcher",
"type": "->"
        }       ,
{
"file": "/var/www/app/vendor/laravel/framework/src/Illuminate/Routing/Route.php",
"line": 169,
"function": "runController",
"class": "Illuminate\\Routing\\Route",
"type": "->"
        }       ,
{
"file": "/var/www/app/vendor/laravel/framework/src/Illuminate/Routing/Router.php",
"line": 658,
"function": "run",
"class": "Illuminate\\Routing\\Route",
"type": "->"
        }       ,
{
"file": "/var/www/app/vendor/laravel/framework/src/Illuminate/Routing/Pipeline.php",
"line": 30,
"function": "Illuminate\\Routing\\{closure}",
"class": "Illuminate\\Routing\\Router",
"type": "->"
```

```
          }       ,
{
"file": "/var/www/app/app/Http/Middleware/RedirectIfAuthenticated.php",
"line": 24,
"function": "Illuminate\\Routing\\{closure}",
"class": "Illuminate\\Routing\\Pipeline",
"type": "->"
          }       ,
{
"file": "/var/www/app/vendor/laravel/framework/src/Illuminate/Pipeline/Pipeline.php",
"line": 149,
"function": "handle",
"class": "App\\Http\\Middleware\\RedirectIfAuthenticated",
"type": "->"
          }       ,
{
"file": "/var/www/app/vendor/laravel/framework/src/Illuminate/Routing/Pipeline.php",
"line": 53,
"function": "Illuminate\\Pipeline\\{closure}",
"class": "Illuminate\\Pipeline\\Pipeline",
...
...
...
```


問題 5 / 9

TOC

アプリケーション・エラー

重大度:	情報
CVSS スコア:	0.0
URL:	http://10.228.148.130/app/org
エンティティー:	key_update (Parameter)
リスク:	秘密のデバッグ情報を収集することができます
原因:	受信したパラメーター値について、適切な境界チェックが行われませんでした ユーザーの入力が必要なデータ型式に一致することを確認するための検証が行われませんでした
修正:	パラメーター値が期待される範囲とタイプであることを確認します。デバッグ・エラー・メッセージおよび例外を出力しないようにします。

差: **パラメーター** 操作元: `key_update` 操作先: `__ORIG_VAL__.`

論拠: アプリケーションが、秘密情報を公開する可能性のある未定義の状態を示すエラー・メッセージを返しました。

テスト要求と応答:

```
POST /app/org HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.228.148.130/app/org
Cookie: soudanList=;
laravel_session=eyJpdiI6IlNyRlkyallKc2dKNGpGdWFFVDVLOXc9PSIsInZhbHVlIjoiWlFpUTkzUVphcHVBYnFIZzM5T
015bjgxVFBOUEllbXROY1Y0N1g0YmNydnI4RUZia0dZeGE3dlwvdXZCbGg5NnowQWdlVmhEQ0x4Y1c0YVJnUjJwS0RBPT0iLC
JtYWMiOiJjNGNiMzM5MTFmN2JhMGI5YmJmNmEwMTczMDhlNDE0MmNlMWI0NjYwNjJjNDM0YzdkZWYyNTYzZGEzNmU3MmM5In0
%3D; XSRF-
TOKEN=eyJpdiI6IjdlUWlKaHZ3NFZiS1F4ZDZrUld3dmc9PSIsInZhbHVlIjoiWVRaOE9wbVpOMDNpNzJPaW9Mak50cUxxVld
0OUdXZTVKbk5Sd1ZKVU5zd2RnWTFqcTNSbG1ucERIN1dJOFM4QVpsZnBCbHc3ZEx0NENORzQyUHI0Z3c9PSIsIm1hYyI6IjFl
YWQ5NDRkZThiOTFiZTM5OGNhMGJmMTVmZDAwNzdlNjdlNGE4OGE4ZWNmY2U1MDY5ODg1MzQ5NThiMGZmNjIifQ%3D%3D;
PHPSESSID=6ebsdplhncev03jjcb2lk1cia0
Connection: Keep-Alive
Host: 10.228.148.130
Pragma: no-cache
Content-Length: 211
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP
Content-Type: application/x-www-form-urlencoded

_token=yuEor3ontYoqIVemgYB9Md6zAOEcgAoJnyhA89RA&key_pref=13&key_addr=&kankei_kikan=&key_keyword=&
key_new=%E6%96%B0%E8%A6%8F&key_update.=%E5%A4%89%E6%9B%B4&key_publish=%E5%85%AC%E9%96%8B&submit=%
E6%A4%9C%E7%B4%A2

HTTP/1.1 500 Internal Server Error
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IktCVUc1eDFlMWZSNnljRFJtbFloTnc9PSIsInZhbHVlIjoiQklEQUlXUjQyYU41N3B5RFNMcVJHdkdkVFE
3anpsZGdcL3V4NmF2S2RyeUpmZnpSbVFXVWxCZDNReE9XUEVxZjgyMHFENzJFSjg3SldJZ1ZjVWlCRWJ3PT0iLCJtYWMiOiI3
NmFhYTE0NmY0MjIyMmIzMjNjZTk3OTdiNDAwMmYwYWY1ZDZhZTUxZTRiYzI4MTU2MDJlNDFmMzgzNDEyMWFmIn0%3D;
expires=Tue, 12-Jun-2018 11:06:29 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6IllKRVBDTm0zaWExUFVIR254XC9QNG5nPT0iLCJ2YWx1ZSI6IkRpK2xpdnRpVnVSZXlrOUNuV
21ONFo4MWVneW94U0RacHRDeklVOGo4MnN3ZXM0SUlqOEpzVjVVOWpFenN6aFJCeW83b2NBdFRJV0Fudks0OTdCSWZnPT0iLC
JtYWMiOiJiZjg4NTgyOTdiN2E4YjlhY2M2NGJmNTEyMWQ2Mzg4OTMzYjAzYzhlOWFkY2QzYWFiNzRmMTEwODA5ZWFmZDk0In0
%3D; expires=Tue, 12-Jun-2018 11:06:29 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.30
Connection: close
Date: Tue, 12 Jun 2018 09:06:29 GMT
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-cache, private
Transfer-Encoding: chunked

<!DOCTYPE html>
<html>
    <head>
        <meta charset="UTF-8" />
        <meta name="robots" content="noindex,nofollow" />
        <style>          body { background-color: #F9F9F9; color: #222; font: 14px/1.4 Helvetica,
Arial, sans-serif; margin: 0; padding-bottom: 45px; }

          a { cursor: pointer; text-decoration: none; }
          a:hover { text-decoration: underline; }
          abbr[title] { border-bottom: none; cursor: help; text-decoration: none; }

          code, pre { font: 13px/1.5 Consolas, Monaco, Menlo, "Ubuntu Mono", "Liberation Mono",
monospace; }

          table, tr, th, td { background: #FFF; border-collapse: collapse; vertical-align: top; }
          table { background: #FFF; border: 1px solid #E0E0E0; box-shadow: 0px 0px 1px rgba(128,
128, 128, .2); margin: 1em 0; width: 100%; }
          table th, table td { border: solid #E0E0E0; border-width: 1px 0; padding: 8px 10px; }
          table th { background-color: #E0E0E0; font-weight: bold; text-align: left; }

          .hidden-xs-down { display: none; }
          .block { display: block; }
          .break-long-words { -ms-word-break: break-all; word-break: break-all; word-break:
break-word; -webkit-hyphens: auto; -moz-hyphens: auto; hyphens: auto; }
```

```
            .text-muted { color: #999; }

            .container { max-width: 1024px; margin: 0 auto; padding: 0 15px; }
            .container::after { content: ""; display: table; clear: both; }

            .exception-summary { background: #B0413E; border-bottom: 2px solid rgba(0, 0, 0, 0.1);
border-top: 1px solid rgba(0, 0, 0, .3); flex: 0 0 auto; margin-bottom: 30px; }

            .exception-message-wrapper { display: flex; align-items: center; min-height: 70px; }
            .exception-message { flex-grow: 1; padding: 30px 0; }
            .exception-message, .exception-message a { color: #FFF; font-size: 21px; font-weight:
400; margin: 0; }
            .exception-message.long { font-size: 18px; }
            .exception-message a { border-bottom: 1px solid rgba(255, 255, 255, 0.5); font-size:
inherit; text-decoration: none; }
            .exception-message a:hover { border-bottom-color: #ffffff; }

            .exception-illustration { flex-basis: 111px; flex-shrink: 0; height: 66px; margin-left:
15px; opacity: .7; }

            .trace + .trace { margin-top: 30px; }
            .trace-head .trace-class { color: #222; font-size: 18px; font-weight: bold; line-
height: 1.3; margin: 0; position: relative; }

            .trace-message { font-size: 14p
...
...
...
```

問題 6 / 9

TOC

アプリケーション・エラー

重大度:	情報
CVSS スコア:	0.0
URL:	http://10.228.148.130/app/org
エンティティー:	kankei_kikan (Parameter)
リスク:	秘密のデバッグ情報を収集することができます
原因:	受信したパラメーター値について、適切な境界チェックが行われませんでした ユーザーの入力が必要なデータ型式に一致することを確認するための検証が行われませんでした
修正:	パラメーター値が期待される範囲とタイプであることを確認します。デバッグ・エラー・メッセージおよび例外を出力しないようにします。

差: **パラメーター** 操作元: `kankei_kikan` 操作先: `__ORIG_VAL__[]`

論拠: アプリケーションが、秘密情報を公開する可能性のある未定義の状態を示すエラー・メッセージを返しました。

テスト要求と応答:

```
POST /app/org HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.228.148.130/app/org
Cookie: soudanList=;
laravel_session=eyJpdiI6IlNyRlkyallKc2dKNGpGdWFFVDVLOXc9PSIsInZhbHVlIjoiWlFpUTkzUVphcHVBYnFIZzM5T
015bjgxVFBOUEllbXROY1Y0N1g0YmNydnI4RUZia0dZeGE3dlwvdXZCbGg5NnowQWdlVmhEQ0x4Y1c0YVJnUjJwS0RBPT0iLC
JtYWMiOiJjNGNiMzM5MTFmN2JhMGI5YmJmNmEwMTczMDhlNDE0MmNlMWI0NjYwNjJjNDM0YzdkZWYyNTYzZGEzNmU3MmM5In0
%3D; XSRF-
TOKEN=eyJpdiI6IjdlUWlKaHZ3NFZiS1F4ZDZrUld3dmc9PSIsInZhbHVlIjoiWVRaOE9wbVpOMDNpNzJPaW9Mak50cUxxVld
```

```
0OUdXZTVKbk5Sd1ZKVU5zd2RnWTFqcTNSbG1ucERIN1dJOFM4QVpsZnBCbHc3ZEx0NENORzQyUHI0Z3c9PSIsIm1hYyI6IjFl
YWQ5NDRkZThiOTFiZTM5OGNhMGJmMTVmZDAwNzdlNjdlNGE4OGE4ZWNmY2U1MDY5ODg1MzQ5NThiMGZmNjIifQ%3D%3D;
PHPSESSID=6ebsdplhncev03jjcb2lk1cia0
Connection: Keep-Alive
Host: 10.228.148.130
Pragma: no-cache
Content-Length: 216
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP
Content-Type: application/x-www-form-urlencoded

_token=yuEor3ontYoqIVemgYB9Md6zAOEcgAoJnyhA89RA&key_pref=13&key_addr=&kankei_kikan%5B%5D=&key_key
word=&key_new=%E6%96%B0%E8%A6%8F&key_update=%E5%A4%89%E6%9B%B4&key_publish=%E5%85%AC%E9%96%8B&sub
mit=%E6%A4%9C%E7%B4%A2

HTTP/1.1 500 Internal Server Error
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjVseWMwdHVINUtvVVgrUXJiUkVXa3c9PSIsInZhbHVlIjoiTEJqSitoM3plbjRxTUVicXZySjhFKzE5aE9
wRENab3haMG91WnVLRUJUXC93VDlcL0Z6Tk5leEpjSHo2d2ZxNGlIdXdMVzZXcjlvamU1S21DcDhmd2tPUT09IiwibWFjIjoi
NDRjYmNiYzg3ZjY5ZDMyZjU2YTc4YjAxYTM2Yzc5OGIxYjA0N2FiMDcwYTlhNTM5ZDg4M2MxZmYzYjgwYTIzYyJ9;
expires=Tue, 12-Jun-2018 11:01:37 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6InYyYW13VmR2TFJmUG1tZ21kUGh4WHc9PSIsInZhbHVlIjoibVkrREdDRjJURUFObFlrRTJya
Uxsell1SlRURlJCRUdiRVpPQnhHT28wSFNid3J4a0lsT3p2MnRwRWIxdm1mSU5TS3drZVwvZUtlTDVBTzRqMVpyZEVBPT0iLC
JtYWMiOiI2M2JlNDJjMzBhZmVhODAzNDRmMWEzZjBmMmZhM2VlZjE0YTU1Njk5ZTcyZDlkZGY4OTI2YzI4Y2QzYWQ5ZWIyIn0
%3D; expires=Tue, 12-Jun-2018 11:01:37 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.30
Connection: close
Date: Tue, 12 Jun 2018 09:01:37 GMT
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-cache, private
Transfer-Encoding: chunked

<!DOCTYPE html>
<html>
    <head>
        <meta charset="UTF-8" />
        <meta name="robots" content="noindex,nofollow" />
        <style>         body { background-color: #F9F9F9; color: #222; font: 14px/1.4 Helvetica,
Arial, sans-serif; margin: 0; padding-bottom: 45px; }

          a { cursor: pointer; text-decoration: none; }
          a:hover { text-decoration: underline; }
          abbr[title] { border-bottom: none; cursor: help; text-decoration: none; }

          code, pre { font: 13px/1.5 Consolas, Monaco, Menlo, "Ubuntu Mono", "Liberation Mono",
monospace; }

          table, tr, th, td { background: #FFF; border-collapse: collapse; vertical-align: top; }
          table { background: #FFF; border: 1px solid #E0E0E0; box-shadow: 0px 0px 1px rgba(128,
128, 128, .2); margin: 1em 0; width: 100%; }
          table th, table td { border: solid #E0E0E0; border-width: 1px 0; padding: 8px 10px; }
          table th { background-color: #E0E0E0; font-weight: bold; text-align: left; }

          .hidden-xs-down { display: none; }
          .block { display: block; }
          .break-long-words { -ms-word-break: break-all; word-break: break-all; word-break:
break-word; -webkit-hyphens: auto; -moz-hyphens: auto; hyphens: auto; }
          .text-muted { color: #999; }

          .container { max-width: 1024px; margin: 0 auto; padding: 0 15px; }
          .container::after { content: ""; display: table; clear: both; }

          .exception-summary { background: #B0413E; border-bottom: 2px solid rgba(0, 0, 0, 0.1);
border-top: 1px solid rgba(0, 0, 0, .3); flex: 0 0 auto; margin-bottom: 30px; }

          .exception-message-wrapper { display: flex; align-items: center; min-height: 70px; }
          .exception-message { flex-grow: 1; padding: 30px 0; }
          .exception-message, .exception-message a { color: #FFF; font-size: 21px; font-weight:
400; margin: 0; }
          .exception-message.long { font-size: 18px; }
          .exception-message a { border-bottom: 1px solid rgba(255, 255, 255, 0.5); font-size:
inherit; text-decoration: none; }
```

```
            .exception-message a:hover { border-bottom-color: #ffffff; }

            .exception-illustration { flex-basis: 111px; flex-shrink: 0; height: 66px; margin-left:
15px; opacity: .7; }

            .trace + .trace { margin-top: 30px; }
            .trace-head .trace-class { color: #222; font-size: 18px; font-weight: bold; line-
height: 1.3; margin: 0; position: relative; }

            .trace-message { font-size:
...
...
...
```

問題 7 / 9

TOC

アプリケーション・エラー

重大度:	情報
CVSS スコア:	0.0
URL:	http://10.228.148.130/app/org
エンティティー:	key_keyword (Parameter)
リスク:	秘密のデバッグ情報を収集することができます
原因:	受信したパラメーター値について、適切な境界チェックが行われませんでした ユーザーの入力が必要なデータ型式に一致することを確認するための検証が行われませんでした
修正:	パラメーター値が期待される範囲とタイプであることを確認します。デバッグ・エラー・メッセージおよび例外を出力しないようにします。

差: **パラメーター** 操作元: `key_keyword` 操作先: `__ORIG_VAL__.`

論拠: アプリケーションが、秘密情報を公開する可能性のある未定義の状態を示すエラー・メッセージを返しました。

テスト要求と応答:

```
POST /app/org HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.228.148.130/app/org
Cookie: soudanList=;
laravel_session=eyJpdiI6IlNyRlkyallKc2dKNGpGdWFFVDVLOXc9PSIsInZhbHVlIjoiWlFpUTkzUVphcHVBYnFIZzM5T
015bjgxVFBOUEllbXROY1Y0N1g0YmNydnI4RUZia0dZeGE3dlwvdXZCbGg5NnowQWdlVmhEQ0x4Y1c0YVJnUjJwS0RBPT0iLC
JtYWMiOiJjNGNiMzM5MTFmN2JhMGI5YmJmNmEwMTczMDhlNDE0MmNlMWI0NjYwNjJjNDM0YzdkZWYyNTYzZGEzNmU3MmM5In0
%3D; XSRF-
TOKEN=eyJpdiI6IjdlUWlKaHZ3NFZiS1F4ZDZrUld3dmc9PSIsInZhbHVlIjoiWVRaOE9wbVpOMDNpNzJPaW9Mak50cUxxVld
0OUdXZTVKbk5Sd1ZKVU5zd2RnWTFqcTNSbG1ucERIN1dJOFM4QVpsZnBCbHc3ZEx0NENORzQyUHI0Z3c9PSIsIm1hYyI6IjFl
YWQ5NDRkZThiOTFiZTM5OGNhMGJmMTVmZDAwNzdlNjdlNGE4OGE4ZWNmY2U1MDY5ODg1MzQ5NThiMGZmNjIifQ%3D%3D;
PHPSESSID=6ebsdplhncev03jjcb2lklcia0
Connection: Keep-Alive
Host: 10.228.148.130
Pragma: no-cache
Content-Length: 211
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP
Content-Type: application/x-www-form-urlencoded

_token=yuEor3ontYoqIVemgYB9Md6zAOEcgAoJnyhA89RA&key_pref=13&key_addr=&kankei_kikan=&key_keyword.=
&key_new=%E6%96%B0%E8%A6%8F&key_update=%E5%A4%89%E6%9B%B4&key_publish=%E5%85%AC%E9%96%8B&submit=%
E6%A4%9C%E7%B4%A2
```

```
HTTP/1.1 500 Internal Server Error
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IitGOFVtUmVLSGNheEdNdXd6eU5WWEE9PSIsInZhbHVlIjoiZW5MeENKNzZaQTBNNUV0SktISHdiS1wvUG0
0ek5TNU1tMG1wNDRqQndkaEtGbUNNQnphN2dEclA5SjhzU0pBQkgyN2J5Q1UwK2FNSmJIWGl3UzF6Q1FnPT0iLCJtYWMiOiIz
NzQ1NGNlMWNlMzQyNzJkZTExMTBjNzMyYmEwODY3YWExZjY1NDg3M2E1OWRjYTkxZjBkM2VmYTZlYjY5MDRhIn0%3D;
expires=Tue, 12-Jun-2018 11:01:40 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6Im83WHBWMytiWjQ1dnpCVWFRa1Y2MUE9PSIsInZhbHVlIjoiWW51VzVtOWxLNit3aVpaSkNGa
WdGRmNjWnNLWDI3ZTNUTnErTWtRZFl1XC94UktrMHZ3R2ZmOHhRNGVHbVJkMVhJZ1VVZ2t5V09WOEpxMEh6dCtWOXhnPT0iLC
JtYWMiOiJhOGQ3ZThhNTllNjY5N2NhMjI3Yzk5MmY4ZmFmNTVhZDQ5ZTAwNjUxMjNiOWQ3Y2I4NzlkMzYwNzMzMWE1N2M2In0
%3D; expires=Tue, 12-Jun-2018 11:01:40 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.30
Connection: close
Date: Tue, 12 Jun 2018 09:01:40 GMT
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-cache, private
Transfer-Encoding: chunked

<!DOCTYPE html>
<html>
    <head>
        <meta charset="UTF-8" />
        <meta name="robots" content="noindex,nofollow" />
        <style>          body { background-color: #F9F9F9; color: #222; font: 14px/1.4 Helvetica,
Arial, sans-serif; margin: 0; padding-bottom: 45px; }

          a { cursor: pointer; text-decoration: none; }
          a:hover { text-decoration: underline; }
          abbr[title] { border-bottom: none; cursor: help; text-decoration: none; }

          code, pre { font: 13px/1.5 Consolas, Monaco, Menlo, "Ubuntu Mono", "Liberation Mono",
monospace; }

          table, tr, th, td { background: #FFF; border-collapse: collapse; vertical-align: top; }
          table { background: #FFF; border: 1px solid #E0E0E0; box-shadow: 0px 0px 1px rgba(128,
128, 128, .2); margin: 1em 0; width: 100%; }
          table th, table td { border: solid #E0E0E0; border-width: 1px 0; padding: 8px 10px; }
          table th { background-color: #E0E0E0; font-weight: bold; text-align: left; }

          .hidden-xs-down { display: none; }
          .block { display: block; }
          .break-long-words { -ms-word-break: break-all; word-break: break-all; word-break:
break-word; -webkit-hyphens: auto; -moz-hyphens: auto; hyphens: auto; }
          .text-muted { color: #999; }

          .container { max-width: 1024px; margin: 0 auto; padding: 0 15px; }
          .container::after { content: ""; display: table; clear: both; }

          .exception-summary { background: #B0413E; border-bottom: 2px solid rgba(0, 0, 0, 0.1);
border-top: 1px solid rgba(0, 0, 0, .3); flex: 0 0 auto; margin-bottom: 30px; }

          .exception-message-wrapper { display: flex; align-items: center; min-height: 70px; }
          .exception-message { flex-grow: 1; padding: 30px 0; }
          .exception-message, .exception-message a { color: #FFF; font-size: 21px; font-weight:
400; margin: 0; }
          .exception-message.long { font-size: 18px; }
          .exception-message a { border-bottom: 1px solid rgba(255, 255, 255, 0.5); font-size:
inherit; text-decoration: none; }
          .exception-message a:hover { border-bottom-color: #ffffff; }

          .exception-illustration { flex-basis: 111px; flex-shrink: 0; height: 66px; margin-left:
15px; opacity: .7; }

          .trace + .trace { margin-top: 30px; }
          .trace-head .trace-class { color: #222; font-size: 18px; font-weight: bold; line-
height: 1.3; margin: 0; position: relative; }

          .trace-message { font-size: 14p
...
...
...
```

アプリケーション・エラー

重大度:	情報
CVSS スコア:	0.0
URL:	http://10.228.148.130/app/org
エンティティー:	key_pref (Parameter)
リスク:	秘密のデバッグ情報を収集することができます
原因:	受信したパラメーター値について、適切な境界チェックが行われませんでした ユーザーの入力が必要なデータ型式に一致することを確認するための検証が行われませんでした
修正:	パラメーター値が期待される範囲とタイプであることを確認します。デバッグ・エラー・メッセージおよび例外を出力しないようにします。

差: **パラメーター** 操作元: `key_pref` 操作先: `__ORIG_VAL__[]`

論拠: アプリケーションが、秘密情報を公開する可能性のある未定義の状態を示すエラー・メッセージを返しました。

テスト要求と応答:

```
POST /app/org HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.228.148.130/app/org
Cookie: soudanList=;
laravel_session=eyJpdiI6IlNyRlkyallKc2dKNGpGdWFFVDVLOXc9PSIsInZhbHVlIjoiWlFpUTkzUVphcHVBYnFIZzM5T
015bjgxVFBOUEllbXROY1Y0N1g0YmNydnI4RUZia0dZeGE3dlwvdXZCbGg5NnowQWdlVmhEQ0x4Y1c0YVJnUjJwS0RBPT0iLC
JtYWMiOiJjNGNiMzM5MTFmN2JhMGI5YmJmNmEwMTczMDhlNDE0MmNlMWI0NjYwNjJjNDM0YzdkZWYyNTYzZGEzNmU3MmM5In0
%3D; XSRF-
TOKEN=eyJpdiI6IjdlUWlKaHZ3NFZiS1F4ZDZrUld3dmc9PSIsInZhbHVlIjoiWVRaOE9wbVpOMDNpNzJPaW9Mak50cUxxVld
0OUdXZTVKbk5Sd1ZKVU5zd2RnWTFqcTNSbG1ucERIN1dJOFM4QVpsZnBCbHc3ZEx0NENORzQyUHI0Z3c9PSIsIm1hYyI6IjFl
YWQ5NDRkZThiOTFiZTM5OGNhMGJmMTVmZDAwNzdlNjdlNGE4OGE4ZWNmY2U1MDY5ODg1MzQ5NThiMGZmNjIifQ%3D%3D;
PHPSESSID=6ebsdplhncev03jjcb2lk1cia0
Connection: Keep-Alive
Host: 10.228.148.130
Pragma: no-cache
Content-Length: 216
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP
Content-Type: application/x-www-form-urlencoded

_token=yuEor3ontYoqIVemgYB9Md6zAOEcgAoJnyhA89RA&key_pref%5B%5D=13&key_addr=&kankei_kikan=&key_key
word=&key_new=%E6%96%B0%E8%A6%8F&key_update=%E5%A4%89%E6%9B%B4&key_publish=%E5%85%AC%E9%96%8B&sub
mit=%E6%A4%9C%E7%B4%A2

HTTP/1.1 500 Internal Server Error
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
Set-Cookie: XSRF-
TOKEN=eyJpdiI6Ikg5b3FKT1l3bHlRbFZ4RHlwSHFrclE9PSIsInZhbHVlIjoib09VN0s4Z25lZDN2eVptc01DTWIrb04wbW1
6Q3ZBbkdcLzJzNUtMVFRlWnF4Ukd1azNnMm5jY0xwUnNpd2RhN1VKdVFZU2E2cDQ1OTFDWHVnMlJBUXRBPT0iLCJtYWMiOiI3
MjUxNjQ5MDE4ZmEzYmZmMWZlZTFiOGU5N2RlM2MwODhjNDJmNjc2MjkyOWJhNTgzN2UyZGIzN2M0OTUxODVjIn0%3D;
expires=Tue, 12-Jun-2018 11:00:47 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6IkRQcTVaUnRLaEdtU2RydFwvd3ozNEZ3PT0iLCJ2YWx1ZSI6IjdTNnhZUktPVVdxM2ZwaUNiK
zhqZTFKS1hSNzdSeTdaYVFkN1JVMGh3bjVxeTc1UnZ4OFlyVjl1UUhaNUtVaWVTckEyc0NFZDN5T3VETmJGZDE1WnRBPT0iLC
JtYWMiOiIwNGJkNGRlMDFlOTk5YzdmZDkzYTgzZjU0NWIwOTM2YTY4ZTcwZjhiYWZiZWMzNDkyZjQ3OGU1NjM2ZTYyNTk2In0
%3D; expires=Tue, 12-Jun-2018 11:00:47 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.30
```

```
Connection: close
Date: Tue, 12 Jun 2018 09:00:47 GMT
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-cache, private
Transfer-Encoding: chunked

<!DOCTYPE html>
<html>
    <head>
        <meta charset="UTF-8" />
        <meta name="robots" content="noindex,nofollow" />
        <style>          body { background-color: #F9F9F9; color: #222; font: 14px/1.4 Helvetica,
Arial, sans-serif; margin: 0; padding-bottom: 45px; }

          a { cursor: pointer; text-decoration: none; }
          a:hover { text-decoration: underline; }
          abbr[title] { border-bottom: none; cursor: help; text-decoration: none; }

          code, pre { font: 13px/1.5 Consolas, Monaco, Menlo, "Ubuntu Mono", "Liberation Mono",
monospace; }

          table, tr, th, td { background: #FFF; border-collapse: collapse; vertical-align: top; }
          table { background: #FFF; border: 1px solid #E0E0E0; box-shadow: 0px 0px 1px rgba(128,
128, 128, .2); margin: 1em 0; width: 100%; }
          table th, table td { border: solid #E0E0E0; border-width: 1px 0; padding: 8px 10px; }
          table th { background-color: #E0E0E0; font-weight: bold; text-align: left; }

          .hidden-xs-down { display: none; }
          .block { display: block; }
          .break-long-words { -ms-word-break: break-all; word-break: break-all; word-break:
break-word; -webkit-hyphens: auto; -moz-hyphens: auto; hyphens: auto; }
          .text-muted { color: #999; }

          .container { max-width: 1024px; margin: 0 auto; padding: 0 15px; }
          .container::after { content: ""; display: table; clear: both; }

          .exception-summary { background: #B0413E; border-bottom: 2px solid rgba(0, 0, 0, 0.1);
border-top: 1px solid rgba(0, 0, 0, .3); flex: 0 0 auto; margin-bottom: 30px; }

          .exception-message-wrapper { display: flex; align-items: center; min-height: 70px; }
          .exception-message { flex-grow: 1; padding: 30px 0; }
          .exception-message, .exception-message a { color: #FFF; font-size: 21px; font-weight:
400; margin: 0; }
          .exception-message.long { font-size: 18px; }
          .exception-message a { border-bottom: 1px solid rgba(255, 255, 255, 0.5); font-size:
inherit; text-decoration: none; }
          .exception-message a:hover { border-bottom-color: #ffffff; }

          .exception-illustration { flex-basis: 111px; flex-shrink: 0; height: 66px; margin-left:
15px; opacity: .7; }

          .trace + .trace { margin-top: 30px; }
          .trace-head .trace-class { color: #222; font-size: 18px; font-weight: bold; line-
height: 1.3; margin: 0; position: relative; }

          .trace-message { font-size
...
...
...
```

問題 9 / 9

TOC

アプリケーション・エラー

重大度:	情報
CVSS スコア:	0.0
URL:	http://10.228.148.130/app/org
エンティティー:	key_new (Parameter)
リスク:	秘密のデバッグ情報を収集することができます
原因:	受信したパラメーター値について、適切な境界チェックが行われませんでした ユーザーの入力が必要なデータ型式に一致することを確認するための検証が行われませんでした
修正:	パラメーター値が期待される範囲とタイプであることを確認します。デバッグ・エラー・メッセージおよび例外を出力しないようにします。

差: **パラメーター** 操作元: `key_new` 操作先: `__ORIG_VAL__.`

論拠: アプリケーションが、秘密情報を公開する可能性のある未定義の状態を示すエラー・メッセージを返しました。

テスト要求と応答:

```
POST /app/org HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.228.148.130/app/org
Cookie: soudanList=;
laravel_session=eyJpdiI6IlNyRlkyallKc2dKNGpGdWFFVDVLOXc9PSIsInZhbHVlIjoiWlFpUTkzUVphcHVBYnFIZzM5T
015bjgxVFBOUEllbXROY1Y0N1g0YmNydnI4RUZia0dZeGE3dlwvdXZCbGg5NnowQWdlVmhEQ0x4Y1c0YVJnUjJwS0RBPT0iLC
JtYWMiOiJjNGNiMzM5MTFmN2JhMGI5YmJmNmEwMTczMDhlNDE0MmNlMWI0NjYwNjJjNDM0YzdkZWYyNTYzZGEzNmU3MmM5In0
%3D; XSRF-
TOKEN=eyJpdiI6IjdlUWlKaHZ3NFZiS1F4ZDZrUld3dmc9PSIsInZhbHVlIjoiWVRaOE9wbVpOMDNpNzJPaW9Mak50cUxxVld
0OUdXZTVKbk5Sd1ZKVU5zd2RnWTFqcTNSbG1ucERIN1dJOFM4QVpsZnBCbHc3ZEx0NENORzQyUHI0Z3c9PSIsIm1hYyI6IjFl
YWQ5NDRkZThiOTFiZTM5OGNhMGJmMTVmZDAwNzdlNjdlNGE4OGE4ZWNmY2U1MDY5ODg1MzQ5NThiMGZmNjIifQ%3D%3D;
PHPSESSID=6ebsdplhncev03jjcb2lk1cia0
Connection: Keep-Alive
Host: 10.228.148.130
Pragma: no-cache
Content-Length: 211
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP
Content-Type: application/x-www-form-urlencoded

_token=yuEor3ontYoqIVemgYB9Md6zAOEcgAoJnyhA89RA&key_pref=13&key_addr=&kankei_kikan=&key_keyword=&
key_new.=%E6%96%B0%E8%A6%8F&key_update=%E5%A4%89%E6%9B%B4&key_publish=%E5%85%AC%E9%96%8B&submit=%
E6%A4%9C%E7%B4%A2

HTTP/1.1 500 Internal Server Error
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IkJUNTVKSG8zV3B1d1wvaGZqUXo3akt3PT0iLCJ2YWx1ZSI6ImdnMjMxeFFRVzRWbEZRbDJmUEM3TGNhZzl
CV3ZjekFmUXUxYmltMDhhSW41emUwb2kyRlwvM25qblwvb3MybUFUMTdhUk1NUHNpNjQ4aGhUYlR4aEU1eEE9PSIsIm1hYyI6
IjY4Zjg3YTJmOGQwOWZiMzQ5OTQ1ODI2NzE0NTQ0Njg3MmQxZmFiNDViOGRjZDhkY2VlOWY4NGFjZDNlN2M1ZGYifQ%3D%3D;
expires=Tue, 12-Jun-2018 11:06:17 GMT; Max-Age=7200; path=/
Set-Cookie:
laravel_session=eyJpdiI6Inc0N2F2S1VTWU5Ia3JtMEppYUNoRHc9PSIsInZhbHVlIjoickpMNjh6MXJ0UTJ3WFAwYjdLd
GlXaXRNR09FRkg2MFpkUnRhRDJvUWNrUXdMUUNqbUtYc1A1Z1NOalREWWZEeDlIdkVESm5QUVwvMTJFTDUrTEhVXC9QUT09Ii
wibWFjIjoiZDgyYWMxODRhYmJmMTY1YjgxNmUzZmEwZmI5MjQzYzkxZjc5MTY5YTA2YmI3MWVlN2E1MjdlZmYzODc3OThiMiJ
9; expires=Tue, 12-Jun-2018 11:06:17 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
X-Powered-By: PHP/7.0.30
Connection: close
Date: Tue, 12 Jun 2018 09:06:17 GMT
Content-Type: text/html; charset=UTF-8
Pragma: no-cache
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-cache, private
Transfer-Encoding: chunked
```

```
<!DOCTYPE html>
<html>
    <head>
        <meta charset="UTF-8" />
        <meta name="robots" content="noindex,nofollow" />
        <style>          body { background-color: #F9F9F9; color: #222; font: 14px/1.4 Helvetica,
Arial, sans-serif; margin: 0; padding-bottom: 45px; }

          a { cursor: pointer; text-decoration: none; }
          a:hover { text-decoration: underline; }
          abbr[title] { border-bottom: none; cursor: help; text-decoration: none; }

          code, pre { font: 13px/1.5 Consolas, Monaco, Menlo, "Ubuntu Mono", "Liberation Mono",
monospace; }

          table, tr, th, td { background: #FFF; border-collapse: collapse; vertical-align: top; }
          table { background: #FFF; border: 1px solid #E0E0E0; box-shadow: 0px 0px 1px rgba(128,
128, 128, .2); margin: 1em 0; width: 100%; }
          table th, table td { border: solid #E0E0E0; border-width: 1px 0; padding: 8px 10px; }
          table th { background-color: #E0E0E0; font-weight: bold; text-align: left; }

          .hidden-xs-down { display: none; }
          .block { display: block; }
          .break-long-words { -ms-word-break: break-all; word-break: break-all; word-break:
break-word; -webkit-hyphens: auto; -moz-hyphens: auto; hyphens: auto; }
          .text-muted { color: #999; }

          .container { max-width: 1024px; margin: 0 auto; padding: 0 15px; }
          .container::after { content: ""; display: table; clear: both; }

          .exception-summary { background: #B0413E; border-bottom: 2px solid rgba(0, 0, 0, 0.1);
border-top: 1px solid rgba(0, 0, 0, .3); flex: 0 0 auto; margin-bottom: 30px; }

          .exception-message-wrapper { display: flex; align-items: center; min-height: 70px; }
          .exception-message { flex-grow: 1; padding: 30px 0; }
          .exception-message, .exception-message a { color: #FFF; font-size: 21px; font-weight:
400; margin: 0; }
          .exception-message.long { font-size: 18px; }
          .exception-message a { border-bottom: 1px solid rgba(255, 255, 255, 0.5); font-size:
inherit; text-decoration: none; }
          .exception-message a:hover { border-bottom-color: #ffffff; }

          .exception-illustration { flex-basis: 111px; flex-shrink: 0; height: 66px; margin-left:
15px; opacity: .7; }

          .trace + .trace { margin-top: 30px; }
          .trace-head .trace-class { color: #222; font-size: 18px; font-weight: bold; line-
height: 1.3; margin: 0; position: relative; }

          .trace-message { font-size:
...
...
...
```

情 クライアント側 (JavaScript) Cookie 参照 2 TOC

問題 1 / 2 TOC

クライアント側 (JavaScript) Cookie 参照

重大度:	情報
CVSS スコア:	0.0
URL:	http://10.228.148.130/app/js/functionCommon.js
エンティティー:	// Back browser when button clicked (Page)
リスク:	この攻撃による最悪のケースのシナリオは、コンテキストとクライアント側で作成された Cookie の役割によって異なります
原因:	クライアント側に Cookie を作成します
修正:	ビジネスおよびセキュリティー・ロジックをクライアント側から削除します

差:

論拠: AppScan が JavaScript に含まれる Cookie への参照を検出しました。

テスト要求と応答:

```
GET /app/js/functionCommon.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.228.148.130/app/org/
Cookie:
laravel_session=eyJpdiI6InJ1QXF2czE3RG5qVzZHckJXXC9UMFVBPT0iLCJ2YWx1ZSI6IjM0eHpiVTFPVTh2OVpnXC9ZV
nplOFZRelwvWkxxdU1SODFRalBNU1hkaTRzeGVqeWlXOWh6eGhpXC82bThadEszdFIxMm1nMUpGajlIYjk2RGtEQ09ta1JRPT
0iLCJtYWMiOiJjNmE1NjllMmU2MGVmNTc0ZjM0NDVmNDhiMGIzY2NkMWU0MjA2MTQ5ZDBkNzU4ZmRlMDM2NjA5MWRkN2I2M2Y
2In0%3D; XSRF-
TOKEN=eyJpdiI6IjQzVkRzYWV2UFlmcVNTYlwvV0Q3UzJnPT0iLCJ2YWx1ZSI6InBOalZCOEJFcGhaWUpoMkRuVkdtelFaeUM
3R09QQzhlVnJLdGFYN2RVeEVLVjRpNHBzcWlzZXE1XC9CYWFHTkI0eDZmZkZ2ZG5XTWY0NWZPVGpNdTRQZz09IiwibWFjIjoi
ODc1MDMzNDUwOWY2NTcxNzljNmU5NGMyNTA1MzkxZTA0NjdiMDIyYjFlMmNkNjU2N2Q1ZDliNDViNzZmNTAzYyJ9;
PHPSESSID=6ebsdplhncev03jjcb2lk1cia0
Host: 10.228.148.130
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Last-Modified: Tue, 12 Jun 2018 00:55:34 GMT
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
Accept-Ranges: bytes
Content-Length: 3454
ETag: "d7e-56e6752d8fb87"
Date: Tue, 12 Jun 2018 08:45:57 GMT
Content-Type: application/javascript

// Back browser when button clicked
init();
function init(){
 $('.openNav').on('click', function () {
         openNav();
 })
 $('.closebtn').on('click', function () {
         closeNav();
 })
}
function goBack() {
    window.history.back();
}

function checkValidateFile(idForm, idFile) {
    $('.clsMess').remove();

    // Check require
    var fileName = $(idFile).val();
    if (fileName == null || fileName == '') {
        $('.clsMessageErr').removeClass('noDisplay');
        $('.clsMessageErr').html(messRequire);
        return;
    }
```

```
    // Check extention file
    var extension = fileName.substr( (fileName.lastIndexOf('.') +1));
    if (extension.toLowerCase() != extensionFile) {
        $('.clsMessageErr').removeClass('noDisplay');
        $('.clsMessageErr').html(messExtent);
        return;
    }

    // Check file exists
    var size = $(idFile)[0].files[0].size;
    if (size === 0) {
        $('.clsMessageErr').removeClass('noDisplay');
        $('.clsMessageErr').html(messExists);
        return ;
    }

    // Check size File
    var maxSizeCheck = Number(maxSizeFile);
    if (Number($(idFile)[0].files[0].size) > maxSizeCheck) {
        $('.clsMessageErr').removeClass('noDisplay');
        $('.clsMessageErr').html(messMaxSize);
        return;
    }

    $(idForm).submit();
}

function checkSpecialCharacter(value) {
    var priceRegex = /^[^\\'"&©®%$<>{}]+$/;
    return priceRegex.test(value);
}

function clearMess() {
    $('.clsMess').remove();
    if (!$('.clsMessageErr').hasClass('noDisplay')) {
        $('.clsMessageErr').html('');
        $('.clsMessageErr').addClass('noDisplay');
    }

}

function trackLog(screen, trackName) {
    $.ajax({
        url: urlTrackLog,
        type: 'POST',
        data:{ '_token' : __token, 'key_screen' : screen, 'key_track_log' : trackName},
        dataType: 'text',
        async: false,
        success: function (res) {
        }
    });
}

function openNav() {
    document.getElementById("mySidenav").style.width = "100%";
    // document.getElementById("base").style.marginLeft = "110";
}

/* Set the width of the side navigation to 0 and the left margin of the page content to 0 */
function closeNav() {
    document.getElementById("mySidenav").style.width = "0";
    // document.getElementById("base").style.marginLeft = "0";
}

function clearMessgeWhenBackBrowser(key) {
    if (typeof readCookie(key) != 'undefined' && readCookie(key) != ''){
        $('.error-msg').remove();
        $('.error-msg-client').addClass('error-msg-no-display');
        eraseCookie(key);
    }
}

function createCookie(name,value,days) {
    if (days) {
        var date = new Date();
        date.setTime(date.getTime()+(days*24*60*60*1000));
        var expires = "; expires="+date.toGMTString();
```

```
    }
    else var expires = "";
    document.cookie = name+"="+value+expires+"; path=/";
}

function readCookie(name) {
    var nameEQ = name + "=";
    var ca = document.cookie.split(';');
    for(var i=0;i < ca.length;i++) {
        var c = ca[i];
        while (c.charAt(0)==' ') c = c.substring(1,c.length);
        if (c.indexOf(nameEQ) == 0) return c.substring(nameEQ.length,c.length);
    }
    return null;
}

function eraseCookie(name) {
    createCookie(name, '', false);
}
function monthDiff(d1, d2) {
 var months;
     months = (d2.getFullYear() - d1.getFullYear()) * 12;
     months -= d1.getMonth() + 1;
     months += d2.getMonth();
 return months <= 0 ? 0 : months;
}
```

問題 2 / 2

TOC

クライアント側 (JavaScript) Cookie 参照

重大度:	情報
CVSS スコア:	0.0
URL:	http://10.228.148.130/app/js/jquery.cookie.js
エンティティー:	/*! (Page)
リスク:	この攻撃による最悪のケースのシナリオは、コンテキストとクライアント側で作成された Cookie の役割によって異なります
原因:	クライアント側に Cookie を作成します
修正:	ビジネスおよびセキュリティー・ロジックをクライアント側から削除します

差:

論拠: AppScan が JavaScript に含まれる Cookie への参照を検出しました。

テスト要求と応答:

```
GET /app/js/jquery.cookie.js HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.228.148.130/app/org/
Cookie:
laravel_session=eyJpdiI6InJ1QXF2czE3RG5qVzZHckJXXC9UMFVBPT0iLCJ2YWx1ZSI6IjM0eHpiVTFPVTh2OVpnXC9ZV
nplOFZRelwvWkxxdU1SODFRalBNU1hkaTRzeGVqeWlXOWh6eGhpXC82bThadEszdFIxMm1nMUpGajlIYjk2RGtEQ09ta1JRPT
0iLCJtYWMiOiJjNmE1NjllMmU2MGVmNTc0ZjM0NDVmNDhiMGIzY2NkMWU0MjA2MTQ5ZDBkNzU4ZmRlMDM2NjA5MWRkN2I2M2Y
2In0%3D; XSRF-
TOKEN=eyJpdiI6IjQzVkRzYWV2UFlmcVNTYlwvV0Q3UzJnPT0iLCJ2YWx1ZSI6InBOalZCOEJFcGhaWUpoMkRuVkdtelFaeUM
3R09QQzhlVnJLdGFYN2RVeEVLVjRpNHBzcWlzZXE1XC9CYWFHTkI0eDZmZkZ2ZG5XTWY0NWZPVGpNdTRQZz09IiwibWFjIjoi
ODc1MDMzNDUwOWY2NTcxNzljNmU5NGMyNTA1MzkxZTA0NjdiMDIyYjFlMmNkNjU2N2Q1ZDliNDViNzZmNTAzYyJ9;
PHPSESSID=6ebsdplhncev03jjcb2lklcia0
Host: 10.228.148.130
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Last-Modified: Tue, 12 Jun 2018 00:55:34 GMT
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
Accept-Ranges: bytes
Content-Length: 2320
ETag: "910-56e6752e3ec4f"
Date: Tue, 12 Jun 2018 08:45:57 GMT
Content-Type: application/javascript

/*!
 * jQuery Cookie Plugin v1.3.1
 * https://github.com/carhartl/jquery-cookie
 *
 * Copyright 2013 Klaus Hartl
 * Released under the MIT license
 */
(function (factory) {
 if (typeof define === 'function' && define.amd) {
         // AMD. Register as anonymous module.
         define(['jquery'], factory);
 } else {
         // Browser globals.
         factory(jQuery);
        }
}(function ($) {

 var pluses = /\+/g;

 function raw(s) {
         return s;
        }

 function decoded(s) {
         return decodeURIComponent(s.replace(pluses, ' '));
        }

 function converted(s) {
         if (s.indexOf('"') === 0) {
                 // This is a quoted cookie as according to RFC2068, unescape
                 s = s.slice(1, -1).replace(/\\"/g, '"').replace(/\\\\/g, '\\');
                }
         try {
                 return config.json ? JSON.parse(s) : s;
         } catch(er) {}
        }

 var config = $       .cookie = function (key, value, options) {

         // write
         if (value !== undefined) {
                 options = $.extend({}, config.defaults, options);

                 if (typeof options.expires === 'number') {
                         var days = options.expires, t = options.expires = new Date();
                         t.setDate(t.getDate() + days);
                        }

                 value = config.json ? JSON.stringify(value) : String(value);

                 return (document       .cookie = [
                         config.raw ? key : encodeURIComponent(key),
                         '='       ,
                         config.raw ? value : encodeURIComponent(value),
                         options.expires ? '; expires=' + options.expires.toUTCString() :
'', // use expires attribute, max-age is not supported by IE
                         options.path    ? '; path=' + options.path : '',
                         options.domain  ? '; domain=' + options.domain : '',
                         options.secure  ? '; secure' : ''
                 ].join(''));
                }

         // read
         var decode = config.raw ? raw : decoded;
         var cookies = document.cookie.split('; ');
```

```
        var result = key ? undefined : {};
        for (var i = 0, l = cookies.length; i < l; i++) {
                var parts = cookies[i].split('=');
                var name = decode(parts.shift());
                var cookie = decode(parts.join('='));

                if (key && key === name) {
                        result = converted(cookie);
                        break;
                       }

                if (!key) {
                        result[name] = converted(cookie);
                       }
               }

        return result;
};

config.defaults = {};

$.removeCookie = function (key, options) {
        if ($.cookie(key) !== undefined) {
                // Must not alter options, thus extending a fresh object...
                $.cookie(key, '', $.extend({}, options, { expires: -1 }));
                return true;
               }
        return false;
};

}));
```

情 内部 IP の開示パターンを発見 5 TOC

問題 1 / 5 TOC

内部 IP の開示パターンを発見	
重大度:	情報
CVSS スコア:	0.0
URL:	http://10.228.148.130/app/org/list
エンティティー:	list (Page)
リスク:	ユーザー名、パスワード、マシン名などの Web アプリケーションに関する秘密情報や、秘密のファイルの場所などの情報を取得することができます
原因:	セキュリティーで保護されていない Web アプリケーション・プログラムまたは設定
修正:	Web サイトから内部 IP アドレスを削除します

差:

論拠: AppScan が、内部 IP アドレスと思われるものを含むレスポンスを検出しました。

テスト要求と応答:

```
GET /app/org/list?page=2 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.228.148.130/app/org/detail/130102044
Cookie: soudanList=1;
laravel_session=eyJpdiI6InlZbzJTVTNzaGRwb2JzQlQxcGtUaFE9PSIsInZhbHVlIjoieHZZUThKRkFaa2lqUkU3UEJWV
zhIMWVDbXI1MEx3aGptcjNHM3I1MzdraE5mdGZ6cFhCbzBma0xHck1BMG5zdEhPNlhNUDd0TjdBcDd5dVdueUVyNFE9PSIsIm
1hYyI6IjJlZjE5ZmFkNDY5YzU0YzcyMzc0Yzc3OTk4OTMwZmIyNTIxZWY4NzI2N2RhZjAxN2ViYTUzNmYxYmM5YzkxMmIifQ%
3D%3D; XSRF-
TOKEN=eyJpdiI6IjB5QnpHN2V6Yk5LcjhpNWlIdFwvZVVRPT0iLCJ2YWx1ZSI6Ims4c1VpTitqM2VwXC9xOFhZczF4cG5kTFp
aaE1uWHRRK29CR25VamhCeG5hRTJtSFNyaW5CdlZ1dEJkbTY3alZ3M04yQzA3V2gxWW9HVjI2VTNKQ1YwUT09IiwibWFjIjoi
M2VlZDIyNjc3YTBhMDZjZGZjNGVkZDM0MWM0MjU1OWI5ZDUxZWU3YjY2N2ZlZWFlOTdkNzNkYmVmODAzMDY0MyJ9;
PHPSESSID=6ebsdplhncev03jjcb2lk1cia0
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


...
...
...
          </div>
          <div class="row header_logo_wrap">
          <div class="col-md-3 col-sm-3 col-xs-3 header_logo">
          <a href="/index.html">
          <img class="img-responsive" src="http://10.228.148.130/app/images/logo_pc.gif" alt="日
本司法支援センター　法テラス:トップページへ"
          />
          </a>
          </div>
          <div class="col-md-6 col-sm-6 col-xs-6 header_L">
          <a>
          <img class="img-responsive" src="http://10.228.148.130/app/images/head_text01.gif"
alt="法的トラブルでお困りの方　法テラス・サポートダイヤル　電話番号:0570-078374　平日9時から21時　土曜9時から17時"
          />
          </a>
          </div>
          <div class="col-md-3 col-sm-3 col-xs-3 header_R">
          <a href="https://www.houterasu.or.jp/cgi-bin/formmail/formmail.cgi?d=toiawase">
          <img class="img-responsive" src="http://10.228.148.130/app/images/head_text02.gif"
alt="メールでのお問い合わせ　24時間受付中"
          />
          </a>
          </div>
          </div>
...
...
...

          </div>
          <div class="pankuzu clearfix sp-none">
          <ul class="clearfix">
          <li class="pk-img">
          <img src="http://10.228.148.130/app/images/c_icon_pankuzu.png" width="15" height="13"
alt="現在のページ" />
          </li>
          <li>
          <a href="/index.html">トップページ</a>
          </li>
...
...
...

          <!-- ▼テンプレート▼ -->
<div class="main-inner">

    <div class="commandbox backbox">
        <a href="http://10.228.148.130/app/org" class="back noCommon"><span class="text">戻る
</span></a>
    </div>

    <p class="countbox">ヒット件数<span class="count">40</span>件</p>
...
...
...
    <ul class="pager">
```

```
          <li class="prev"><a href="http://10.228.148.130/app/org/list?page=1" rel="prev">前へ
</a></li>
...
...
...
          <li class="waves-effect"><a href="http://10.228.148.130/app/org/list?page=1">1</a></li>
          <li class="active current"><a href>2</a></li>



...
...
...

        </tr>

          <tr>
          <td><span class="number">21</span></td>
          <td><a class="question" href="http://10.228.148.130/app/org/detail/130102044">日本司法支
援センター東京地方事務所　上野出張所</a></td>
          <td><span class="madoguti">民事法律扶助相談（労働相談）</span></td>
          <td><span class="jusyo">台東区上野2-7-13 JTB・損保ジャパン日本興亜上野共同ビル6階</span></td>
          <td>
          <span class="mendan">
...
...
...

          </td>
          </tr>
          <tr>
          <td><span class="number">22</span></td>
          <td><a class="question" href="http://10.228.148.130/app/org/detail/130102086">日本司法支
援センター東京地方事務所</a></td>
          <td><span class="madoguti">民事法律扶助（高齢者・障がい者相談）</span></td>
          <td><span class="jusyo">新宿区西新宿1-24-1 エステック情報ビル13F</span></td>
          <td>
          <span class="mendan">
...
...
...

          </td>
          </tr>
          <tr>
          <td><span class="number">23</span></td>
          <td><a class="question" href="http://10.228.148.130/app/org/detail/130102105">日本司法支
援センター東京地方事務所　上野出張所</a></td>
          <td><span class="madoguti">民事法律扶助（高齢者・障がい者相談）</span></td>
          <td><span class="jusyo">台東区上野2-7-13 JTB・損保ジャパン日本興亜上野共同ビル6階</span></td>
          <td>
          <span class="mendan">
...
...
...

          </td>
          </tr>
          <tr>
          <td><span class="number">24</span></td>
          <td><a class="question" href="http://10.228.148.130/app/org/detail/130102111">日本司法支
援センター東京地方事務所</a></td>
          <td><span class="madoguti">民事法律扶助（インターネットに関する相談）</span></td>
          <td><span class="jusyo">新宿区西新宿1-24-1 エステック情報ビル13F</span></td>
          <td>
          <span class="mendan">
...
...
...

          </td>
          </tr>
          <tr>
          <td><span class="number">25</span></td>
          <td><a class="question" href="http://10.228.148.130/app/org/detail/130100001">日本司法支
援センター東京地方事務所</a></td>
          <td><span class="madoguti">情報提供窓口</span></td>
          <td><span class="jusyo">新宿区西新宿1-24-1 エステック情報ビル13F</span></td>
```

```
          <td>
          <span class="mendan">
...
...
...

          </td>
          </tr>
          <tr>
          <td><span class="number">26</span></td>
          <td><a class="question" href="http://10.228.148.130/app/org/detail/130100002">日本司法支
援センター東京地方事務所</a></td>
          <td><span class="madoguti">民事法律扶助(一般相談・クレサラ)</span></td>
          <td><span class="jusyo">新宿区西新宿1-24-1 エステック情報ビル13F</span></td>
          <td>
          <span class="mendan">
...
...
...

          </td>
          </tr>
          <tr>
          <td><span class="number">27</span></td>
          <td><a class="question" href="http://10.228.148.130/app/org/detail/130100003">日本司法支
援センター東京地方事務所</a></td>
          <td><span class="madoguti">犯罪被害者支援窓口</span></td>
          <td><span class="jusyo">新宿区西新宿1-24-1 エステック情報ビル13F</span></td>
          <td>
          <span class="mendan">
...
...
...

          </td>
          </tr>
          <tr>
          <td><span class="number">28</span></td>
          <td><a class="question" href="http://10.228.148.130/app/org/detail/130100010">日本司法支
援センター東京地方事務所 池袋出張所</a></td>
          <td><span class="madoguti">民事法律扶助(一般相談・クレサラ)</span></td>
          <td><span class="jusyo">豊島区東池袋1-35-3 池袋センタービル6階</span></td>
          <td>
          <span class="mendan">
...
...
...

          </td>
          </tr>
          <tr>
          <td><span class="number">29</span></td>
          <td><a class="question" href="http://10.228.148.130/app/org/detail/130100013">日本司法支
援センター東京地方事務所 八王子出張所</a></td>
          <td><span class="madoguti">情報提供窓口</span></td>
          <td><span class="jusyo">八王子市明神町4-7-14　八王子ONビル4階</span></td>
          <td>
          <span class="mendan">
...
...
...

          </td>
          </tr>
          <tr>
          <td><span class="number">30</span></td>
          <td><a class="question" href="http://10.228.148.130/app/org/detail/130100014">日本司法支
援センター東京地方事務所 八王子出張所</a></td>
          <td><span class="madoguti">民事法律扶助相談(一般相談・クレサラ)</span></td>
          <td><span class="jusyo">八王子市明神町4-7-14 八王子ONビル4階</span></td>
          <td>
          <span class="mendan">
...
...
...

          </td>
          </tr>
```

```
          <tr>
          <td><span class="number">31</span></td>
          <td><a class="question" href="http://10.228.148.130/app/org/detail/130102044">日本司法支
援センター東京地方事務所　上野出張所</a></td>
          <td><span class="madoguti">民事法律扶助相談（労働相談）</span></td>
          <td><span class="jusyo">台東区上野2-7-13 JTB・損保ジャパン日本興亜上野共同ビル6階</span></td>
          <td>
          <span class="mendan">
...
...
...

          </td>
          </tr>
          <tr>
          <td><span class="number">32</span></td>
          <td><a class="question" href="http://10.228.148.130/app/org/detail/130102086">日本司法支
援センター東京地方事務所</a></td>
          <td><span class="madoguti">民事法律扶助（高齢者・障がい者相談）</span></td>
          <td><span class="jusyo">新宿区西新宿1-24-1 エステック情報ビル13F</span></td>
          <td>
          <span class="mendan">
...
...
...

          </td>
          </tr>
          <tr>
          <td><span class="number">33</span></td>
          <td><a class="question" href="http://10.228.148.130/app/org/detail/130102105">日本司法支
援センター東京地方事務所　上野出張所</a></td>
          <td><span class="madoguti">民事法律扶助（高齢者・障がい者相談）</span></td>
          <td><span class="jusyo">台東区上野2-7-13 JTB・損保ジャパン日本興亜上野共同ビル6階</span></td>
          <td>
          <span class="mendan">
...
...
...

          </td>
          </tr>
          <tr>
          <td><span class="number">34</span></td>
          <td><a class="question" href="http://10.228.148.130/app/org/detail/130102111">日本司法支
援センター東京地方事務所</a></td>
          <td><span class="madoguti">民事法律扶助（インターネットに関する相談）</span></td>
          <td><span class="jusyo">新宿区西新宿1-24-1 エステック情報ビル13F</span></td>
          <td>
          <span class="mendan">
...
...
...

          </td>
          </tr>
          <tr>
          <td><span class="number">35</span></td>
          <td><a class="question" href="http://10.228.148.130/app/org/detail/130100001">日本司法支
援センター東京地方事務所</a></td>
          <td><span class="madoguti">情報提供窓口</span></td>
          <td><span class="jusyo">新宿区西新宿1-24-1 エステック情報ビル13F</span></td>
          <td>
          <span class="mendan">
...
...
...

          </td>
          </tr>
          <tr>
          <td><span class="number">36</span></td>
          <td><a class="question" href="http://10.228.148.130/app/org/detail/130100002">日本司法支
援センター東京地方事務所</a></td>
          <td><span class="madoguti">民事法律扶助（一般相談・クレサラ）</span></td>
          <td><span class="jusyo">新宿区西新宿1-24-1 エステック情報ビル13F</span></td>
          <td>
          <span class="mendan">
```

```
...
...
...

          </td>
          </tr>
          <tr>
          <td><span class="number">37</span></td>
          <td><a class="question" href="http://10.228.148.130/app/org/detail/130100003">日本司法支
援センター東京地方事務所</a></td>
          <td><span class="madoguti">犯罪被害者支援窓口</span></td>
          <td><span class="jusyo">新宿区西新宿1-24-1 エステック情報ビル13F</span></td>
          <td>
          <span class="mendan">
...
...
...

          </td>
          </tr>
          <tr>
          <td><span class="number">38</span></td>
          <td><a class="question" href="http://10.228.148.130/app/org/detail/130100010">日本司法支
援センター東京地方事務所 池袋出張所</a></td>
          <td><span class="madoguti">民事法律扶助(一般相談・クレサラ)</span></td>
          <td><span class="jusyo">豊島区東池袋1-35-3 池袋センタービル6階</span></td>
          <td>
          <span class="mendan">
...
...
...

          </td>
          </tr>
          <tr>
          <td><span class="number">39</span></td>
          <td><a class="question" href="http://10.228.148.130/app/org/detail/130100013">日本司法支
援センター東京地方事務所 八王子出張所</a></td>
          <td><span class="madoguti">情報提供窓口</span></td>
          <td><span class="jusyo">八王子市明神町4-7-14　八王子ONビル4階</span></td>
          <td>
          <span class="mendan">
...
...
...

          </td>
          </tr>
          <tr>
          <td><span class="number">40</span></td>
          <td><a class="question" href="http://10.228.148.130/app/org/detail/130100014">日本司法支
援センター東京地方事務所 八王子出張所</a></td>
          <td><span class="madoguti">民事法律扶助相談(一般相談・クレサラ)</span></td>
          <td><span class="jusyo">八王子市明神町4-7-14 八王子ONビル4階</span></td>
          <td>
          <span class="mendan">
...
...
...

    <ul class="pager">

          <li class="prev"><a href="http://10.228.148.130/app/org/list?page=1" rel="prev">前へ
</a></li>
...
...
...
          <li class="waves-effect"><a href="http://10.228.148.130/app/org/list?page=1">1</a></li>
          <li class="active current"><a href>2</a></li>



    </ul>

    <div class="commandbox backbox">
        <a href="http://10.228.148.130/app/org" class="back noCommon"><span class="text">戻る
</span></a>
```

```
    </div>
<!-- ▲テンプレート▲ -->
...
...
...
          <!-- /div main-inner -->
          <!-- ▼フッタ▼ -->
<!-- scs_jyogai_start -->
<hr />
<div class="guidance"><img src="http://10.228.148.130/app/images/spacer.gif" alt="本文ここまで"
width="1" height="1" /></div>
</div><!-- /div main-inner -->
</div><!-- /div main -->
</div><!-- /div wrap -->
<hr />
...
...
...

 </ul>
 </div>
</div>
</div>
<div class="foot_logo"><img src="http://10.228.148.130/app/images/foot_logo.gif" alt="日本司法支援
センター 法テラス" /></div>
<div class="page-top"><a href="#PTOP"><img
src="http://10.228.148.130/app/images/foot_pagetop.png" alt="ページの先頭へ" width="84" height="87"
/></a></div>
</div><!-- /div baseall -->
</div><!-- /div basebg -->
<!-- scs_jyogai_end -->          </div>
          </div>
          </div>
          </div>
        </div>
    </div>
    <div class="foot_copy" id="copy">Copyright &copy; Houterasu All rights reserved.<div
class="guidance"><img src="http://10.228.148.130/app/images/spacer.gif" alt="フッターここまで"
width="1" height="1" /><a href="#PTOP"><img src="http://10.228.148.130/app/images/spacer.gif"
alt="このページのトップに戻る" width="1" height="1" /></a></div></div>
    <script>
...
...
...
  var __lang_MR0002 = "パスワードが誤っています。パスワードを確認し、再度入力して下さい。";
  var __lang_GM0050_err_msg = "From～Toの期間を正しく指定してください";
  var __lang_GM0050_err_msg_month = "From～Toの期間が25ヶ月を超えています。正しく指定してください";
  var __lang_GM0060_err_msg = "From～Toの期間を正しく指定してください";
  var urlTrackLog = 'http://10.228.148.130/app/home/trackLog';
  var __token = 'yuEor3ontYoqIVemgYB9Md6zAOEcgAoJnyhA89RA';
  var btnBack = '戻る';
  var btnChoose = 'ファイルを選択';
  var btnClear = 'クリア';
...
...
...
```

問題 2 / 5

TOC

内部 IP の開示パターンを発見

重大度:	情報
CVSS スコア:	0.0
URL:	http://10.228.148.130/app/org/detail/130100001
エンティティー:	130100001 (Page)
リスク:	ユーザー名、パスワード、マシン名などの Web アプリケーションに関する秘密情報や、秘密のファイルの場所などの情報を取得することができます
原因:	セキュリティーで保護されていない Web アプリケーション・プログラムまたは設定
修正:	Web サイトから内部 IP アドレスを削除します

差:

論拠: AppScan が、内部 IP アドレスと思われるものを含むレスポンスを検出しました。

テスト要求と応答:

```
GET /app/org/detail/130100001 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.228.148.130/app/org/list
Cookie: soudanList=1;
laravel_session=eyJpdiI6Illma1B5MWNuZnlKSUp5Q2NmVnJiREE9PSIsInZhbHVlIjoiTloycnhLa3FWQnd3dkRFb3FRR
CtcL1dGVkVrNmxKblRVZUwreWRsSHVtVGF0b254MmRaMDFnNDNuVTZcL3p0TU54ajZDeWRBK292K2dQM1pSWDVscXFBZz09Ii
wibWFjIjoiMmNlOTBmM2U2OGRlN2ZiYjA4Mzg0YTE5ZWI0MmYzNGYwOTIzZWQ1MGE5ZWNkYjM3OWIyNzU0YjI2ODYwNTJjYSJ
9; XSRF-
TOKEN=eyJpdiI6ImZOWXR2U3ZrQXZCTUFDdXVJb3VjTEE9PSIsInZhbHVlIjoicXp2bEJGNWZXSFwva0RYNEQwY09cL1ByaEh
3R2c2RDJmeUpMVjYxbUhKRXlUQnZYYnlYcnpJUzRPSG0zdHh4Y0JVc1dPZ3hkRUh3c1I2M1pncldzS0VcL1E9PSIsIm1hYyI6
IjY3ZTEwYTMyMjk1OThkNzdiNjY1ZDU1ZjkzZTNlZDAwYzQ0NDE4NGE4OTM2NmM2NDM4NTlhYWZhZWU0ZWIwZjcifQ%3D%3D;
PHPSESSID=6ebsdplhncev03jjcb2lk1cia0
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


...
...
...
          </div>
          <div class="row header_logo_wrap">
          <div class="col-md-3 col-sm-3 col-xs-3 header_logo">
          <a href="/index.html">
          <img class="img-responsive" src="http://10.228.148.130/app/images/logo_pc.gif" alt="日
本司法支援センター 法テラス:トップページへ"
          />
          </a>
          </div>
          <div class="col-md-6 col-sm-6 col-xs-6 header_L">
          <a>
          <img class="img-responsive" src="http://10.228.148.130/app/images/head_text01.gif"
alt="法的トラブルでお困りの方 法テラス・サポートダイヤル 電話番号:0570-078374 平日9時から21時 土曜9時から17時"
          />
          </a>
          </div>
          <div class="col-md-3 col-sm-3 col-xs-3 header_R">
          <a href="https://www.houterasu.or.jp/cgi-bin/formmail/formmail.cgi?d=toiawase">
          <img class="img-responsive" src="http://10.228.148.130/app/images/head_text02.gif"
alt="メールでのお問い合わせ 24時間受付中"
          />
          </a>
          </div>
          </div>
...
...
...
```

```
          </div>
          <div class="pankuzu clearfix sp-none">
          <ul class="clearfix">
          <li class="pk-img">
          <img src="http://10.228.148.130/app/images/c_icon_pankuzu.png" width="15" height="13"
alt="現在のページ" />
          </li>
          <li>
          <a href="/index.html">トップページ</a>
          </li>
...
...
...

          <!-- ▲ヘッダ▲ -->
          <!-- ▼テンプレート▼ -->
<div class="main-inner">
        <div class="commandbox backbox">
        <a href="http://10.228.148.130/app/org/list"  class="back noCommon"><span class="text">戻
る</span></a>
    </div>
...
...
...
          <td></td>
        </tr>
    </table>
        <ul class="banner-wrap">
          <li><a  href="http://10.228.148.130/app/faq"><img class="img-responsive push-faq"
src="http://10.228.148.130/app/images/con_img12.jpg" alt="バナー1" /></a></li>
          <li><a href="http://10.228.148.130/app/org"><img class="img-responsive push-soudan"
src="http://10.228.148.130/app/images/con_img13.jpg" alt="バナー2" /></a></li>
          <li><a href="https://www.houterasu.or.jp/cgi-bin/formmail_enquete/formamil.cgi?
d=enquete"><img class="img-responsive push-anketo"
src="http://10.228.148.130/app/images/con_img14.jpg" alt="バナー3" /></a></li>
        </ul>
    <!-- scs_jyogai_end -->
...
...
...
    <div class="commandbox backbox">
        <a href="http://10.228.148.130/app/org/list"  class="back noCommon"><span class="text">戻
る</span></a>
    </div>
    <!-- ▲テンプレート▲ -->
...
...
...
          <!-- /div main-inner -->
          <!-- ▼フッタ▼ -->
<!-- scs_jyogai_start -->
<hr />
<div class="guidance"><img src="http://10.228.148.130/app/images/spacer.gif" alt="本文ここまで"
width="1" height="1" /></div>
</div><!-- /div main-inner -->
</div><!-- /div main -->
</div><!-- /div wrap -->
<hr />
...
...
...

 </ul>
 </div>
</div>
</div>
<div class="foot_logo"><img src="http://10.228.148.130/app/images/foot_logo.gif" alt="日本司法支援
センター 法テラス" /></div>
<div class="page-top"><a href="#PTOP"><img
src="http://10.228.148.130/app/images/foot_pagetop.png" alt="ページの先頭へ" width="84" height="87"
/></a></div>
</div><!-- /div baseall -->
</div><!-- /div basebg -->
<!-- scs_jyogai_end -->          </div>
          </div>
          </div>
          </div>
        </div>
```

```
    </div>
    <div class="foot_copy" id="copy">Copyright &copy; Houterasu All rights reserved.<div
class="guidance"><img src="http://10.228.148.130/app/images/spacer.gif" alt="フッターここまで"
width="1" height="1" /><a href="#PTOP"><img src="http://10.228.148.130/app/images/spacer.gif"
alt="このページのトップに戻る" width="1" height="1" /></a></div></div>
    <script>
...
...
...
  var __lang_MR0002 = "パスワードが誤っています。パスワードを確認し、再度入力して下さい。";
  var __lang_GM0050_err_msg = "From～Toの期間を正しく指定してください";
  var __lang_GM0050_err_msg_month = "From～Toの期間が25ヶ月を超えています。正しく指定してください";
  var __lang_GM0060_err_msg = "From～Toの期間を正しく指定してください";
  var urlTrackLog = 'http://10.228.148.130/app/home/trackLog';
  var __token = 'yuEor3ontYoqIVemgYB9Md6zAOEcgAoJnyhA89RA';
  var btnBack = '戻る';
  var btnChoose = 'ファイルを選択';
  var btnClear = 'クリア';
...
...
...
```

問題 3 / 5

TOC

内部 IP の開示パターンを発見

重大度:	情報
CVSS スコア:	0.0
URL:	http://10.228.148.130/app/org/
エンティティー:	(Page)
リスク:	ユーザー名、パスワード、マシン名などの Web アプリケーションに関する秘密情報や、秘密のファイルの場所などの情報を取得することができます
原因:	セキュリティーで保護されていない Web アプリケーション・プログラムまたは設定
修正:	Web サイトから内部 IP アドレスを削除します

差:

論拠: AppScan が、内部 IP アドレスと思われるものを含むレスポンスを検出しました。

テスト要求と応答:

```
GET /app/org/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


HTTP/1.1 200 OK
Server: Apache/2.4.6 (CentOS) PHP/7.0.30
defau
...
...
...

          </div>
          <div class="row header_logo_wrap">
```

```
          <div class="col-md-3 col-sm-3 col-xs-3 header_logo">
          <a href="/index.html">
          <img class="img-responsive" src="http://10.228.148.130/app/images/logo_pc.gif" alt="日
本司法支援センター 法テラス:トップページへ"
          />
          </a>
          </div>
          <div class="col-md-6 col-sm-6 col-xs-6 header_L">
          <a>
          <img class="img-responsive" src="http://10.228.148.130/app/images/head_text01.gif"
alt="法的トラブルでお困りの方 法テラス・サポートダイヤル 電話番号:0570-078374 平日9時から21時 土曜9時から17時"
          />
          </a>
          </div>
          <div class="col-md-3 col-sm-3 col-xs-3 header_R">
          <a href="https://www.houterasu.or.jp/cgi-bin/formmail/formmail.cgi?d=toiawase">
          <img class="img-responsive" src="http://10.228.148.130/app/images/head_text02.gif"
alt="メールでのお問い合わせ 24時間受付中"
          />
          </a>
          </div>
          </div>
...
...
...

          </div>
          <div class="pankuzu clearfix sp-none">
          <ul class="clearfix">
          <li class="pk-img">
          <img src="http://10.228.148.130/app/images/c_icon_pankuzu.png" width="15" height="13"
alt="現在のページ" />
          </li>
          <li>
          <a href="/index.html">トップページ</a>
          </li>
...
...
...

    <p>相談窓口を以下の項目から検索することができます。<br />
お知りになりたい内容を入力または選択してください(※複数の選択も可能です)。</p>
        <div class="error-msg-client error-msg-no-display"></div>
    <div class="search-box">
        <form method="POST" action="http://10.228.148.130/app/org" accept-charset="UTF-8"
id="request" class="form-inline"><input name="_token" type="hidden"
value="7qDHk5YaDJfMl9rqbJ501gvZg1XbHVZTQcmBe64p">
          <fieldset>
        <legend class="hidden">相談窓口検索</legend>
        <div class="panel-body">
...
...
...

          <!-- /div main-inner -->
          <!-- ▼フッタ▼ -->
<!-- scs_jyogai_start -->
<hr />
<div class="guidance"><img src="http://10.228.148.130/app/images/spacer.gif" alt="本文ここまで"
width="1" height="1" /></div>
</div><!-- /div main-inner -->
</div><!-- /div main -->
</div><!-- /div wrap -->
<hr />
...
...
...

 </ul>
 </div>
</div>
</div>
<div class="foot_logo"><img src="http://10.228.148.130/app/images/foot_logo.gif" alt="日本司法支援
センター 法テラス" /></div>
<div class="page-top"><a href="#PTOP"><img
src="http://10.228.148.130/app/images/foot_pagetop.png" alt="ページの先頭へ" width="84" height="87"
/></a></div>
</div><!-- /div baseall -->
```

```
</div><!-- /div basebg -->
<!-- scs_jyogai_end -->          </div>
          </div>
          </div>
          </div>
        </div>
    </div>
    <div class="foot_copy" id="copy">Copyright &copy; Houterasu All rights reserved.<div
class="guidance"><img src="http://10.228.148.130/app/images/spacer.gif" alt="フッターここまで"
width="1" height="1" /><a href="#PTOP"><img src="http://10.228.148.130/app/images/spacer.gif"
alt="このページのトップに戻る" width="1" height="1" /></a></div></div>
    <script>
...
...
...
  var __lang_MR0002 = "パスワードが誤っています。パスワードを確認し、再度入力して下さい。";
  var __lang_GM0050_err_msg = "From～Toの期間を正しく指定してください";
  var __lang_GM0050_err_msg_month = "From～Toの期間が25ヶ月を超えています。正しく指定してください";
  var __lang_GM0060_err_msg = "From～Toの期間を正しく指定してください";
  var urlTrackLog = 'http://10.228.148.130/app/home/trackLog';
  var __token = '7qDHk5YaDJfMl9rqbJ501gvZg1XbHVZTQcmBe64p';
  var btnBack = '戻る';
  var btnChoose = 'ファイルを選択';
  var btnClear = 'クリア';
...
...
...

        function getStringBytes() {
          var url = "http://10.228.148.130/app/get-string-bytes";
          var keyword = $("#input-assist").val();
          var key_address = $("#key_addr").val();
          var max_length = $("#input-assist").attr('maxLength');
          if ((keyword.length > parseInt(max_length)/2) ||  (key_address.length >
parseInt(max_length)/2)) {
...
...
...
```

問題 4 / 5

TOC

内部 IP の開示パターンを発見

重大度:	情報
CVSS スコア:	0.0
URL:	http://10.228.148.130/app/org
エンティティー:	org (Page)
リスク:	ユーザー名、パスワード、マシン名などの Web アプリケーションに関する秘密情報や、秘密のファイルの場所などの情報を取得することができます
原因:	セキュリティーで保護されていない Web アプリケーション・プログラムまたは設定
修正:	Web サイトから内部 IP アドレスを削除します

差:

論拠: AppScan が、内部 IP アドレスと思われるものを含むレスポンスを検出しました。

テスト要求と応答:

```
POST /app/org HTTP/1.1
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.228.148.130/app/org
Cookie: soudanList=;
laravel_session=eyJpdiI6IllvcG5UWkxLZmlkaXRDS0FnWjl1OUE9PSIsInZhbHVlIjoiTG15MlpqczRCUmNGNnA0WFhTR
GM5eGJIUVM3bUpscVwvTVdWRXh4SW1UTzFEemJON1U0aFVyTFVJOVF5QkYzanMzSUxodEN1OFNXQnF2eFdwSU93Mjh3PT0iLC
JtYWMiOiI0ZjVlNjZkNDA3YjcxZGViMjE4NThmMjRmZmZlM2VjZTRlOTYzNjklNTVhYzhiNTU0NGZiMzRjZmUxNTUxOWMxIn0
%3D; XSRF-
TOKEN=eyJpdiI6IkxGZmpaMXVQQ3RuekpxSTdwQk1jdkE9PSIsInZhbHVlIjoiWFdTXC9SNmRHbEp0dk1kdWhCYlZwYkVyM2N
3ZGhud1VXSjMzN0sweVdJVExUdGZCbVUzWm5MOWdcL2FVUmNtQUlxRXA5SW1JdGhrMzBSbEZMOStzc2xLQT09IiwibWFjIjoi
NTkxNmQxYTM2MWQwZGQzMzhhMzUwM2UyNjk4ZGJkNjZiNDJhNjY4YzczY2Y2MzViMTI2OWEzZGMwNGI0ZTQ2YSJ9;
PHPSESSID=6ebsdplhncev03jjcb2lk1cia0
Connection: Keep-Alive
Host: 10.228.148.130
Pragma: no-cache
Content-Length: 209
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP
Content-Type: application/x-www-form-urlencoded


...
...
...

          </div>
          <div class="row header_logo_wrap">
          <div class="col-md-3 col-sm-3 col-xs-3 header_logo">
          <a href="/index.html">
          <img class="img-responsive" src="http://10.228.148.130/app/images/logo_pc.gif" alt="日
本司法支援センター　法テラス:トップページへ"
          />
          </a>
          </div>
          <div class="col-md-6 col-sm-6 col-xs-6 header_L">
          <a>
          <img class="img-responsive" src="http://10.228.148.130/app/images/head_text01.gif"
alt="法的トラブルでお困りの方　法テラス・サポートダイヤル　電話番号:0570-078374　平日9時から21時　土曜9時から17時"
          />
          </a>
          </div>
          <div class="col-md-3 col-sm-3 col-xs-3 header_R">
          <a href="https://www.houterasu.or.jp/cgi-bin/formmail/formmail.cgi?d=toiawase">
          <img class="img-responsive" src="http://10.228.148.130/app/images/head_text02.gif"
alt="メールでのお問い合わせ　24時間受付中"
          />
          </a>
          </div>
          </div>
...
...
...

          </div>
          <div class="pankuzu clearfix sp-none">
          <ul class="clearfix">
          <li class="pk-img">
          <img src="http://10.228.148.130/app/images/c_icon_pankuzu.png" width="15" height="13"
alt="現在のページ" />
          </li>
          <li>
          <a href="/index.html">トップページ</a>
          </li>
...
...
...

お知りになりたい内容を入力または選択してください（※複数の選択も可能です）。</p>
          <div class="error-msg">検索結果が見つかりませんでした。</div>
        <div class="error-msg-client error-msg-no-display"></div>
    <div class="search-box">
        <form method="POST" action="http://10.228.148.130/app/org" accept-charset="UTF-8"
id="request" class="form-inline"><input name="_token" type="hidden"
value="yuEor3ontYoqIVemgYB9Md6zAOEcgAoJnyhA89RA">
          <fieldset>
        <legend class="hidden">相談窓口検索</legend>
        <div class="panel-body">
...
```

```
...
...

          <!-- /div main-inner -->
          <!-- ▼フッタ▼ -->
<!-- scs_jyogai_start -->
<hr />
<div class="guidance"><img src="http://10.228.148.130/app/images/spacer.gif" alt="本文ここまで"
width="1" height="1" /></div>
</div><!-- /div main-inner -->
</div><!-- /div main -->
</div><!-- /div wrap -->
<hr />
...
...
...

 </ul>
 </div>
</div>
</div>
<div class="foot_logo"><img src="http://10.228.148.130/app/images/foot_logo.gif" alt="日本司法支援
センター 法テラス" /></div>
<div class="page-top"><a href="#PTOP"><img
src="http://10.228.148.130/app/images/foot_pagetop.png" alt="ページの先頭へ" width="84" height="87"
/></a></div>
</div><!-- /div baseall -->
</div><!-- /div basebg -->
<!-- scs_jyogai_end -->          </div>
          </div>
          </div>
          </div>
        </div>
    </div>
    <div class="foot_copy" id="copy">Copyright &copy; Houterasu All rights reserved.<div
class="guidance"><img src="http://10.228.148.130/app/images/spacer.gif" alt="フッターここまで"
width="1" height="1" /><a href="#PTOP"><img src="http://10.228.148.130/app/images/spacer.gif"
alt="このページのトップに戻る" width="1" height="1" /></a></div></div>
    <script>
...
...
...
  var __lang_MR0002 = "パスワードが誤っています。パスワードを確認し、再度入力して下さい。";
  var __lang_GM0050_err_msg = "From～Toの期間を正しく指定してください";
  var __lang_GM0050_err_msg_month = "From～Toの期間が25ヶ月を超えています。正しく指定してください";
  var __lang_GM0060_err_msg = "From～Toの期間を正しく指定してください";
  var urlTrackLog = 'http://10.228.148.130/app/home/trackLog';
  var __token = 'yuEor3ontYoqIVemgYB9Md6zAOEcgAoJnyhA89RA';
  var btnBack = '戻る';
  var btnChoose = 'ファイルを選択';
  var btnClear = 'クリア';
...
...
...

        function getStringBytes() {
          var url = "http://10.228.148.130/app/get-string-bytes";
          var keyword = $("#input-assist").val();
          var key_address = $("#key_addr").val();
          var max_length = $("#input-assist").attr('maxLength');
          if ((keyword.length > parseInt(max_length)/2) ||  (key_address.length >
parseInt(max_length)/2)) {
...
...
...
```

問題 5 / 5

TOC

内部 IP の開示パターンを発見

重大度:	情報
CVSS スコア:	0.0
URL:	http://10.228.148.130/app/org/detail/130102044
エンティティー:	130102044 (Page)
リスク:	ユーザー名、パスワード、マシン名などの Web アプリケーションに関する秘密情報や、秘密のファイルの場所などの情報を取得することができます
原因:	セキュリティーで保護されていない Web アプリケーション・プログラムまたは設定
修正:	Web サイトから内部 IP アドレスを削除します

差:

論拠: AppScan が、内部 IP アドレスと思われるものを含むレスポンスを検出しました。

テスト要求と応答:

```
GET /app/org/detail/130102044 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://10.228.148.130/app/org/list?page=2
Cookie: soudanList=1;
laravel_session=eyJpdiI6InhhRU9jRzZWM1FXU1MzYWpIUWlIdmc9PSIsInZhbHVlIjoiSDZDOWorR05weVNnbXB1dWVwO
FpEY1diaG90bUN0UEVKcHFMNE15M29ZWGZ4UnIyUUxVZGpNSW5qaDNZMlErOEJtM3E3MndZSDhQYW45QjdDemEzdEE9PSIsIm
1hYyI6IjA2ODQ5MjgxYmMyZWExZWEzZjY1YTY5YTNiZWY0OTFkZjliMzRmZTRkNjA4YTU3N2E1ZTY1OTlmOWY3MzQ1NTEifQ%
3D%3D; XSRF-
TOKEN=eyJpdiI6ImZDT0h3blNoa0ZkSmp3WDFPYzljZmc9PSIsInZhbHVlIjoiMTE1Z2gxenNvODR2aTVOek0yV1NQU3R2aFV
2eGFBcEVDVlZHU0ZqbHRpMTU1V25DUGZcL3BFRm5JclBPSThoZ1V1NVlxcVdwYzRGRzk2TnBjWVlTT1B3PT0iLCJtYWMiOiI5
MDdhMzIyMzUxNzM4MTM4YTM4ZDZlMTEyMzZkMTA2ODU4OGJmMDQ1MzBiMjgzMzg5YTA5ODNjZDhkOGI1MTY5In0%3D;
PHPSESSID=6ebsdplhncev03jjcb2lklcia0
Connection: Keep-Alive
Host: 10.228.148.130
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg,
application/x-ms-xbap, */*
Accept-Language: ja-JP


...
...
...
          </div>
          <div class="row header_logo_wrap">
          <div class="col-md-3 col-sm-3 col-xs-3 header_logo">
          <a href="/index.html">
          <img class="img-responsive" src="http://10.228.148.130/app/images/logo_pc.gif" alt="日
本司法支援センター 法テラス:トップページへ"
          />
          </a>
          </div>
          <div class="col-md-6 col-sm-6 col-xs-6 header_L">
          <a>
          <img class="img-responsive" src="http://10.228.148.130/app/images/head_text01.gif"
alt="法的トラブルでお困りの方 法テラス・サポートダイヤル 電話番号:0570-078374 平日9時から21時 土曜9時から17時"
          />
          </a>
          </div>
          <div class="col-md-3 col-sm-3 col-xs-3 header_R">
          <a href="https://www.houterasu.or.jp/cgi-bin/formmail/formmail.cgi?d=toiawase">
          <img class="img-responsive" src="http://10.228.148.130/app/images/head_text02.gif"
alt="メールでのお問い合わせ 24時間受付中"
          />
          </a>
          </div>
          </div>
...
...
...
```

```
          </div>
          <div class="pankuzu clearfix sp-none">
          <ul class="clearfix">
          <li class="pk-img">
          <img src="http://10.228.148.130/app/images/c_icon_pankuzu.png" width="15" height="13"
alt="現在のページ" />
          </li>
          <li>
          <a href="/index.html">トップページ</a>
          </li>
...
...
...

          <!-- ▲ヘッダ▲ -->
          <!-- ▼テンプレート▼ -->
<div class="main-inner">
        <div class="commandbox backbox">
        <a href="http://10.228.148.130/app/org/list?page=2"  class="back noCommon"><span
class="text">戻る</span></a>
    </div>
...
...
...
          <td></td>
        </tr>
    </table>
        <ul class="banner-wrap">
          <li><a  href="http://10.228.148.130/app/faq"><img class="img-responsive push-faq"
src="http://10.228.148.130/app/images/con_img12.jpg" alt="バナー1" /></a></li>
          <li><a href="http://10.228.148.130/app/org"><img class="img-responsive push-soudan"
src="http://10.228.148.130/app/images/con_img13.jpg" alt="バナー2" /></a></li>
          <li><a href="https://www.houterasu.or.jp/cgi-bin/formmail_enquete/formamil.cgi?
d=enquete"><img class="img-responsive push-anketo"
src="http://10.228.148.130/app/images/con_img14.jpg" alt="バナー3" /></a></li>
        </ul>
    <!-- scs_jyogai_end -->
...
...
...
    <div class="commandbox backbox">
        <a href="http://10.228.148.130/app/org/list?page=2"  class="back noCommon"><span
class="text">戻る</span></a>
    </div>
    <!-- ▲テンプレート▲ -->
...
...
...
          <!-- /div main-inner -->
          <!-- ▼フッタ▼ -->
<!-- scs_jyogai_start -->
<hr />
<div class="guidance"><img src="http://10.228.148.130/app/images/spacer.gif" alt="本文ここまで"
width="1" height="1" /></div>
</div><!-- /div main-inner -->
</div><!-- /div main -->
</div><!-- /div wrap -->
<hr />
...
...
...

 </ul>
 </div>
</div>
</div>
<div class="foot_logo"><img src="http://10.228.148.130/app/images/foot_logo.gif" alt="日本司法支援
センター 法テラス" /></div>
<div class="page-top"><a href="#PTOP"><img
src="http://10.228.148.130/app/images/foot_pagetop.png" alt="ページの先頭へ" width="84" height="87"
/></a></div>
</div><!-- /div baseall -->
</div><!-- /div basebg -->
<!-- scs_jyogai_end -->          </div>
          </div>
          </div>
          </div>
        </div>
```

```
    </div>
    <div class="foot_copy" id="copy">Copyright &copy; Houterasu All rights reserved.<div
class="guidance"><img src="http://10.228.148.130/app/images/spacer.gif" alt="フッターここまで"
width="1" height="1" /><a href="#PTOP"><img src="http://10.228.148.130/app/images/spacer.gif"
alt="このページのトップに戻る" width="1" height="1" /></a></div></div>
    <script>
...
...
...
  var __lang_MR0002 = "パスワードが誤っています。パスワードを確認し、再度入力して下さい。";
  var __lang_GM0050_err_msg = "From～Toの期間を正しく指定してください";
  var __lang_GM0050_err_msg_month = "From～Toの期間が25ヶ月を超えています。正しく指定してください";
  var __lang_GM0060_err_msg = "From～Toの期間を正しく指定してください";
  var urlTrackLog = 'http://10.228.148.130/app/home/trackLog';
  var __token = 'yuEor3ontYoqIVemgYB9Md6zAOEcgAoJnyhA89RA';
  var btnBack = '戻る';
  var btnChoose = 'ファイルを選択';
  var btnClear = 'クリア';
...
...
...
```

推奨される修正

高 有害な文字のインジェクションに対して考えられる解決策を確認します TOC

このタスクで修正される問題のタイプ

- クロスサイト・スクリプティング
- フレームからのフィッシング

全般

クロスサイト・スクリプティング

いくつかの防止方法があります。
[1] 戦略: ライブラリーまたはフレームワーク
- ライブラリーやフレームワークを十分に検査し、このような弱点を発生させないようにするか、または発生しても簡単に回避できるような構成にしてください。

正しくエンコードされた出力を生成しやすくするライブラリーやフレームワークとしては、例えば、Microsoft の Anti-XSS Library、OWASP ESAPI Encoding モジュール、Apache Wicket などがあります。

[2] データが使用されるコンテキスト、および必要なエンコードを理解してください。- これは、異なるコンポーネント間でデータを送信する場合、または Web ページやマルチパート・メール・メッセージなど、複数のエンコードを同時に組み込むことができる出力を生成する場合に、特に重要です。必要となるエンコード方法を判別するには、必要なすべての通信プロトコルおよびデータ表現を調べます。
別の Web ページに出力されるデータ (特に、外部入力から受信されたデータ) に関しては、すべての非英数字で適切なエンコードを使用してください。
同一出力文書の各所で別々のエンコードが必要になることがあります。これは、出力が以下のいずれの箇所に組み込まれているのかによって異なります。
[-] HTML 本文
[-] 要素属性 (src="XYZ" など)
[-] URI
[-] JavaScript セクション
[-] カスケーディング・スタイル・シートおよびスタイル・プロパティー
HTML エンティティー・エンコードは HTML 本文にのみ適していることに注意してください。
必要なエンコードおよびエスケープのタイプについて詳しくは、XSS Prevention Cheat Sheet (http://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet)
を参照してください。

[3] 戦略: 攻撃対象領域の特定および縮小
- 信頼されない入力がソフトウェアに入り込む可能性のある潜在的な領域をすべて把握してください。

このような領域としては、パラメーター/引数、Cookie、ネットワークから読み取られる任意の項目、環境変数、DNS の逆引き、クエリー結果、

要求ヘッダー、URL コンポーネント、電子メール、ファイル、ファイル名、データベース、
アプリケーションにデータを渡す任意の外部システムがあります。
このような入力は、API コールによって間接的に取り込まれる可能性がありますのでご注意ください。

[4] 戦略: 出力エンコード
- 生成される Web ページごとに、ISO-8859-1 や UTF-8 などの文字エンコードを使用および指定してください。
エンコードが指定されていない場合、Web ブラウザーは、Web ページで実際に使用されているエンコードを推測して、異なるエンコードを選択することがあります。
これにより、Web ブラウザーで特定のシーケンスが特殊なシーケンスとして扱われ、クライアントが巧妙な XSS 攻撃にさらされるおそれがあります。
エンコード/エスケープに関する他の防止方法については、CWE-116 を参照してください。

[5] 戦略: 攻撃対象領域の特定および縮小
- ユーザーのセッション Cookie に対する XSS 攻撃を防止できるように、セッション Cookie を HttpOnly に設定してください。
HttpOnly 属性をサポートするブラウザー (最新バージョンの Internet Explorer や Firefox など) では、HttpOnly 属性によって、document.cookie を
使用する悪質なクライアント・サイド・スクリプトがユーザーのセッション Cookie にアクセスできなくなります。
ただし HttpOnly はすべてのブラウザーでサポートされているわけではないため、これは完全なソリューションではありません。
さらに HTTP ヘッダー (Set-Cookie ヘッダーを含む) に HttpOnly フラグが設定されていても、XMLHTTPRequest やその他の強力なブラウザー・テクノロジーではそのようなヘッダーに対しても読み取りアクセスを実行することができます。

[6] 戦略: 入力検証
- すべての入力に悪意があると見なしてください。「既知の有効なデータを受け入れる」入力検証方法 (仕様に正確に適合する受け入れ可能な入力のホワイトリスト) を使用してください。仕様に正確に適合しない入力はすべて拒否してください。あるいは、そのような入力を、仕様に正確に適合する入力に変換してください。悪質な入力や誤った形式の入力が登録されたブラックリストを過信しないようにしてください。ただし潜在的な攻撃の検出や、全面的に拒否すべき誤った形式の入力の判別には、ブラックリストは役立つことがあります。
入力検証を実行する際は、関連すると思われるすべてのプロパティー (入力の長さ、入力のタイプ、許容される値の完全な範囲、入力の欠落または余分な入力、構文、すべての関連フィールドにおける整合性、ビジネス・ルールへの適合など) を考慮してください。ビジネス・ルール・ロジックの一例を挙げると、「boat」は、英数字のみが含まれているため構文的には有効ですが、「赤」や「青」などの色が必要な場合には有効ではありません。Web ページを動的に構成するときは、要求内で必要なパラメーター値に基づいて文字セットを制限する厳格なホワイトリストを使用してください。すべての入力を検証およびクレンジングする必要があります。ユーザーが指定することになるパラメーターだけでなく、要求に含まれるデータ (隠しフィールド、Cookie、ヘッダー、URL 自体を含む) もすべて対象となります。サイトで再表示されることが予期されるフィールドのみを検証するケースが多いようですが、これでは XSS の脆弱性が解決されません。要求から得られる他のデータがアプリケーション・サーバーやアプリケーションで反映されて、それを開発チームが予期していないということは、珍しくありません。また、現在は反映されていないフィールドを、今後、開発者が使用することがあります。そのため、HTTP 要求のすべての部分を検証することをお勧めします。
入力を検証することで多少の多層防御が行われる可能性がありますが、XSS 対策として最も有効なソリューションは、適切に出力をエンコードし、エスケープし、引用することです。入力を検証することで、出力に表示されるものが効果的に制限されます。入力を検証したからといって必ずしも XSS が防止されるわけではありません (特に、任意の文字を含めることができるフリー・フォーム・テキスト・フィールドをサポートする必要がある場合)。例えば、チャット・アプリケーションでは、ハートのエモーティコン (「<3」) は、一般的に使用されるため、検証ステップをパスすると考えられます。しかし、「<」文字が含まれているため、このエモーティコンを Web ページに直接挿入することはできません。エスケープするなどの処理が必要となります。この場合、「<」を除去すれば、XSS のリスクは減りますが、エモーティコンが記録されないため、動作は正しいものではなくなります。これは取るに足りない問題のようにも考えられますが、不等式を表す必要がある数学的なフォーラムでは重要な問題となります。
検証で間違いを犯しても (例えば、100 個の入力フィールドのうち 1 つを忘れるなどしても)、エンコードが適切であれば、インジェクション・ベースの攻撃からは依然として保護されます。単独のプロパティーのみを対象にしなければ、入力検証は依然として有効な方法です。入力を検証することで攻撃対象領域が大幅に減り、一部の攻撃を検出できるようになり、正しいエンコードでは扱われない他のセキュリティー上の利点がもたらされる可能性があります。
入力検証は、アプリケーション内で、十分に定義されたインターフェースにおいて行ってください。こうすることで、コンポーネントを再利用したり別の場所に移動したりしてもアプリケーションを保護できます。

フレームからのフィッシング

いくつかの防止方法があります。
[1] 戦略: ライブラリーまたはフレームワーク

- ライブラリーやフレームワークを十分に検査し、このような弱点を発生させないようにするか、または発生しても簡単に回避できるような構成にしてください。

正しくエンコードされた出力を生成しやすくするライブラリーやフレームワークとしては、例えば、Microsoft の Anti-XSS Library、OWASP ESAPI Encoding モジュール、Apache Wicket などがあります。

[2] データが使用されるコンテキスト、および必要なエンコードを理解してください。
- これは、異なるコンポーネント間でデータを送信する場合、または Web ページやマルチパート・メール・メッセージなど、複数のエンコードを同時に組み込むことができる出力を生成する場合に、特に重要です。必要となるエンコード方法を判別するには、必要なすべての通信プロトコルおよびデータ表現を調べます。

別の Web ページに出力されるデータ (特に、外部入力から受信されたデータ) に関しては、すべての非英数字で適切なエンコードを使用してください。
同一出力文書の各所で別々のエンコードが必要になることがあります。これは、出力が以下のいずれの箇所に組み込まれているのかによって異なります。
[-] HTML 本文
[-] 要素属性 (src="XYZ" など)
[-] URI
[-] JavaScript セクション
[-] カスケーディング・スタイル・シートおよびスタイル・プロパティー
HTML エンティティー・エンコードは HTML 本文にのみ適していることに注意してください。
必要なエンコードおよびエスケープのタイプについて詳しくは、XSS Prevention Cheat Sheet (http://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet)
を参照してください。

[3] 戦略: 攻撃対象領域の特定および縮小
- 信頼されない入力がソフトウェアに入り込む可能性のある潜在的な領域をすべて把握してください。

このような領域としては、パラメーター/引数、Cookie、ネットワークから読み取られる任意の項目、環境変数、DNS の逆引き、クエリー結果、
要求ヘッダー、URL コンポーネント、電子メール、ファイル、ファイル名、データベース、
アプリケーションにデータを渡す任意の外部システムがあります。
このような入力は、API コールによって間接的に取り込まれる可能性がありますのでご注意ください。

[4] 戦略: 出力エンコード
- 生成される Web ページごとに、ISO-8859-1 や UTF-8 などの文字エンコードを使用および指定してください。

エンコードが指定されていない場合、Web ブラウザーは、Web ページで実際に使用されているエンコードを推測して、異なるエンコードを選択することがあります。
これにより、Web ブラウザーで特定のシーケンスが特殊なシーケンスとして扱われ、クライアントが巧妙な XSS 攻撃にさらされるおそれがあります。
エンコード/エスケープに関する他の防止方法については、CWE-116 を参照してください。

[5] 戦略: 攻撃対象領域の特定および縮小
- ユーザーのセッション Cookie に対する XSS 攻撃を防止できるように、セッション Cookie を HttpOnly に設定してください。

HttpOnly 属性をサポートするブラウザー (最新バージョンの Internet Explorer や Firefox など) では、HttpOnly 属性によって、document.cookie を
使用する悪質なクライアント・サイド・スクリプトがユーザーのセッション Cookie にアクセスできなくなります。
ただし HttpOnly はすべてのブラウザーでサポートされているわけではないため、これは完全なソリューションではありません。
さらに HTTP ヘッダー (Set-Cookie ヘッダーを含む) に HttpOnly フラグが設定されていても、XMLHTTPRequest やその他の強力なブラウザー・テクノロジーではそのようなヘッダーに対しても読み取りアクセスを実行することができます。

[6] 戦略: 入力検証
- すべての入力に悪意があると見なしてください。「既知の有効なデータを受け入れる」入力検証方法 (仕様に正確に適合する受け入れ可能な入力のホワイトリスト) を使用してください。仕様に正確に適合しない入力はすべて拒否してください。あるいは、そのような入力を、仕様に正確に適合する入力に変換してください。悪質な入力や誤った形式の入力が登録されたブラックリストに過度に依存しないでください。ただし潜在的な攻撃の検出や、全面的に拒否すべき誤った形式の入力の判別には、ブラックリストは役立つことがあります。

入力検証を実行する際は、関連すると思われるすべてのプロパティー (入力の長さ、入力のタイプ、許容される値の完全な範囲、入力の欠落または余分な入力、構文、すべての関連フィールドにおける整合性、ビジネス・ルールへの適合など) を考慮してください。ビジネス・ルール・ロジックの一例を挙げると、「boat」は、英数字のみが含まれているため構文的には有効ですが、「赤」や「青」などの色が必要な場合には有効ではありません。Web ページを動的に構成するときは、要求内で必要なパラメーター値に基づいて文字セットを制限する厳格なホワイトリストを使用してください。すべての入力を検証およびクレンジン

グする必要があります。ユーザーが指定することになるパラメーターだけでなく、要求に含まれるデータ (隠しフィールド、Cookie、ヘッダー、URL 自体を含む) もすべて対象となります。
サイトで再表示されることが予期されるフィールドのみを検証するケースが
多いようですが、これでは XSS の脆弱性が解決されません。開発チームが予期しなかったデータが要求から得られ、そのデータがアプリケーション・サーバーやアプリケーションで反映されることは、珍しくありません。また、現在は反映されていないフィールドを、今後、開発者が使用することがあります。そのため、HTTP 要求のすべての部分を検証することをお勧めします。
入力を検証することで多少の多層防御が行われる可能性がありますが、XSS 対策として最も有効なソリューションは、適切に出力をエンコードし、エスケープし、引用することです。その理由は、出力に表示されるものを効果的に制限できるからです。入力を検証したからといって必ずしも XSS が防止されるわけではありません (特に、任意の文字を含めることができるフリー・フォーム・テキスト・フィールドをサポートする必要がある場合)。例えば、チャット・アプリケーションでは、ハートのエモーティコン (「<3」) は、一般的に使用されるため、検証ステップをパスすると考えられます。しかし、「<」文字が含まれているため、このエモーティコンを Web ページに直接挿入することはできません。エスケープするなどの処理が必要となります。この場合、「<」を除去すれば、XSS のリスクは減りますが、エモーティコンが記録されないため、動作は正しいものではなくなります。これは取るに足りない問題のようにも考えられますが、不等式を表す必要がある数学的なフォーラムでは重要な問題となります。
検証で間違いを犯しても (例えば、100 個の入力フィールドのうち 1 つを忘れるなどしても)、エンコードが適切であれば、インジェクション・ベースの攻撃からは依然として保護されます。単独のプロパティーのみを対象にしなければ、入力検証は依然として有効な方法です。入力を検証することで攻撃対象領域が大幅に減り、一部の攻撃を検出できるようになり、正しいエンコードでは扱われない他のセキュリティー上の利点がもたらされる可能性があります。
入力検証は、アプリケーション内で、十分に定義されたインターフェースにおいて行ってください。こうすることで、コンポーネントを再利用したり別の場所に移動したりしてもアプリケーションを保護できます。

.Net

クロスサイト・スクリプティング

[1] ご使用のサーバーを .NET Framework 2.0 (またはそれ以降) にアップグレードすることをお勧めします。このアップグレード版には、クロスサイト・スクリプティング攻撃に対する保護を行う、固有のセキュリティー・チェックが含まれています。
[2] 検証コントロールを使用すると、Web Forms ページに入力検証機能を追加できます。検証コントロールは、すべての一般的なタイプの標準的検証 (たとえば、範囲内の有効なデータまた値のテスト) を行うための使いやすいメカニズムを提供しています。検証コントロールは、カスタム記述した検証もサポートしており、ユーザーに対してエラー情報を表示する方法を完全にカスタマイズすることができます。検証コントロールは、HTML と Web サーバー・コントロールの両方を含む Web のフォーム・ページのクラス・ファイルで処理される任意のコントロールとともに使用することができます。

ユーザーの入力が正しい値だけであることを確かめるために、次の検証コントロールの 1 つを使うことができます。

[1]「RangeValidator」: ユーザーのエントリー (値) が指定された下限と上限の間であることをチェックします。数字、英字、および日付のペアで示した範囲をチェックすることができます。

[2]「RegularExpressionValidator」: 正規表現により定義されたパターンとエントリーが一致していることをチェックします。この検証タイプにより、社会保障番号、電子メール・アドレス、電話番号、郵便番号等といった予想可能な文字のシーケンスをチェックできます。

クロスサイト・スクリプティングのブロックに役立つ可能性のある正規表現の例:

- 基本的なクロスサイト・スクリプティングのバリアントを拒否する正規表現として以下のものが考えられます。^([^<]|\<[^a-zA-Z])*[<]?$
- 上記のすべての文字を拒否する汎用正規表現として以下のものが考えられます。^([^\<\>\"\'\%\;\)\(\&\+]*)$

重要な注意事項: 検証コントロールは、ユーザーの入力をブロックしたりページ処理のフローを変更することはありません。エラー・ステータスを設定し、エラー・メッセージを送出するだけです。アプリケーション固有のアクションをさらに実行する前に、プログラマーは必ずコード内のコントロールの状態をテストしてください。

ユーザーの入力を検証する方法には 2 つの方法があります:

1. 一般的なエラー状態のテスト:
コードで、ページの IsValid プロパティーをテストしてください。このプロパティーは、ページの全検証コントロールの IsValid プロパティーの値の論理和を結果として返します。検証コントロールの 1 つが無効に設定されている場合、ページのプロパ

ティーは false を返します。

2. 各コントロールのエラー状態のテスト:
ページの Validators コレクション (すべての検証コントロールへの参照を含みます) に含まれるものをチェックしてください。そうすることで、各検証コントロールの IsValid プロパティーを調べることが可能となります。最後に、Microsoft Anti-Cross Site Scripting Library (v1.5 以上) を使用して、信頼できないユーザー入力をエンコードすることをお勧めします。

Anti-Cross Site Scripting Library は、以下のメソッドを公開しています。

[1] HtmlEncode - HTML で使用される入力文字列をエンコードします。
[2] HtmlAttributeEncode - HTML 属性で使用される入力文字列をエンコードします。
[3] JavaScriptEncode - JavaScript で使用される入力文字列をエンコードします。
[4] UrlEncode - Universal Resource Locator (URL) で使用される入力文字列をエンコードします。
[5] VisualBasicScriptEncode - Visual Basic Script で使用される入力文字列をエンコードします。
[6] XmlEncode - XML で使用される入力文字列をエンコードします。
[7] XmlAttributeEncode - XML 属性で使用される入力文字列をエンコードします。

Microsoft Anti-Cross Site Scripting Library を適切に使用して ASP.NET Web アプリケーションを保護するためには、以下を実行する必要があります。

ステップ 1: 出力を生成する ASP.NET コードを見直す
ステップ 2: 信頼できない入力パラメーターが出力に含まれているか判別する
ステップ 3: 信頼できない入力が出力として使用されるコンテキストを判別し、使用するエンコード・メソッドを決定する
ステップ 4: 出力をエンコードする

ステップ 3 の例:

注: 信頼できない入力が HTML 属性の設定に使用される場合は、Microsoft.Security.Application.HtmlAttributeEncode メソッドを使用して信頼できない入力をエンコードする必要があります。
また、信頼できない入力が JavaScript のコンテキストで使用される場合は、
Microsoft.Security.Application.JavaScriptEncode を使用してエンコードする必要があります。

```
   // Vulnerable code
   // Note that untrusted input is being treated as an HTML attribute
   Literal1.Text = "<hr noshade size=[untrusted input here]>";


   // Modified code
   Literal1.Text = "<hr noshade size="+Microsoft.Security.Application.AntiXss.HtmlAttributeEncode([untrusted
 input here])+">";
```

ステップ 4 の例:
出力のエンコードについて留意すべき重要事項を以下にいくつか挙げます。

[1] 出力は 1 回、エンコードする必要があります。
[2] 出力のエンコードは、できるだけ、出力の実際の書き込みの近くで行う必要があります。例えば、アプリケーションがユーザー入力を読み込み、その入力を処理してから何らかの形式でそれを再度書き込む場合は、エンコードは出力が書き込まれる直前に行われる必要があります。

```
   // Incorrect sequence
   protected void Button1_Click(object sender, EventArgs e)
   {
       // Read input
       String Input = TextBox1.Text;
       // Encode untrusted input
       Input = Microsoft.Security.Application.AntiXss.HtmlEncode(Input);
       // Process input
```

```
        ...
        // Write Output
        Response.Write("The input you gave was"+Input);
    }


    // Correct Sequence
    protected void Button1_Click(object sender, EventArgs e)
    {
        // Read input
        String Input = TextBox1.Text;
        // Process input
        ...
        // Encode untrusted input and write output
        Response.Write("The input you gave was"+
            Microsoft.Security.Application.AntiXss.HtmlEncode(Input));
    }
```

フレームからのフィッシング

J2EE

クロスサイト・スクリプティング

** 入力データの検証

ユーザーの利便性のためにユーザー検証をクライアント層で行うこともできます。しかし、Servlet を使用するデータ検証はサーバー層で行う必要があります。クライアント側のデータ検証は、例えば Javascript を無効にすることによって簡単にバイパスできるため、本質的に安全ではありません。

一般的には、次の項目を検証するサーバー側ユーティリティー・ルーチンを提供する Web アプリケーション・フレームワークが理想とされます。
[1] 必須フィールド
[2] フィールドのデータ型 (デフォルトでは、HTTP 要求パラメーターはすべて String)
[3] フィールドの長さ
[4] フィールドの範囲
[5] フィールドのオプション
[6] フィールドのパターン
[7] Cookie の値
[8] HTTP 応答

効果的な方法は、上記ルーチンを Validator ユーティリティー・クラスの静的メソッドとして実装することです。次のセクションでは、validator クラスの例について説明します。

[1] 必須フィールド
常に、フィールドが Null でなく、前後の空白スペースを除いて、その長さがゼロより大きいことをチェックします。
次に、要求されたフィールドを検証する例を示します。

```
    // Java example to validate required fields
    public Class Validator {
        ...
        public static boolean validateRequired(String value) {
            boolean isFieldValid = false;
            if (value != null && value.trim().length() > 0) {
            isFieldValid = true;
            }
            return isFieldValid;
        }
        ...
    }
    ...
    String fieldValue = request.getParameter("fieldName");
```

```
if (Validator.validateRequired(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

[2] フィールドのデータ型: Web アプリケーションでは、入力パラメーターの型は多くありません。例えば、HTTP 要求パラメーターや Cookie の値はすべて String 型です。開発者は入力のデータ型が正しいかどうかを確認する必要があります。フィールドの値を希望するプリミティブなデータ型に安全に変換できるかどうかをチェックするには、Java プリミティブ・ラッパー・クラスを使用します。

次に、数値フィールド (int 型) を検証する例を示します。

```
// Java example to validate that a field is an int number
public Class Validator {
    ...
    public static boolean validateInt(String value) {
        boolean isFieldValid = false;
        try {
        Integer.parseInt(value);
        isFieldValid = true;
        } catch (Exception e) {
        isFieldValid = false;
        }
        return isFieldValid;
    }
    ...
}
...
// check if the HTTP request parameter is of type int
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

効果的な方法は、HTTP 要求パラメーターをすべて対応するデータ型に変換することです。例えば、次の例に示すように、開発者は、要求パラメーターの「integerValue」を要求属性に格納して使用します。

```
// Example to convert the HTTP request parameter to a primitive wrapper data type
// and store this value in a request attribute for further processing
String fieldValue = request.getParameter("fieldName");
if (Validator.validateInt(fieldValue)) {
    // convert fieldValue to an Integer
    Integer integerValue = Integer.getInteger(fieldValue);
    // store integerValue in a request attribute
    request.setAttribute("fieldName", integerValue);
}
...
// Use the request attribute for further processing
Integer integerValue = (Integer)request.getAttribute("fieldName");
...
```

アプリケーションが処理する必要がある Java の主なデータ型は次のとおりです。
- Byte
- Short
- Integer

- Long
- Float
- Double
- Date

[3] フィールドの長さ: 常に、入力パラメーター (HTTP 要求パラメーターまたは Cookie 値のどちらか) の長さが最小値から最大値までの間であることを確認します。

次に、userName フィールドの長さが 8 文字から 20 文字までの間であることを検証する例を示します。

```
// Example to validate the field length
public Class Validator {
    ...
    public static boolean validateLength(String value, int minLength, int maxLength) {
        String validatedValue = value;
        if (!validateRequired(value)) {
        validatedValue = "";
        }
        return (validatedValue.length() >= minLength &&
        validatedValue.length() <= maxLength);
    }
    ...
}
...
String userName = request.getParameter("userName");
if (Validator.validateRequired(userName)) {
    if (Validator.validateLength(userName, 8, 20)) {
        // userName is valid, continue further processing
        ...
    }
}
```

[4] フィールドの範囲: 常に、入力パラメーターが関数の要件で定義された範囲内であることを確認します。

入力データ numberOfChoices の値が 10 から 20 の間であることを検証する例を示します。

```
// Example to validate the field range
public Class Validator {
    ...
    public static boolean validateRange(int value, int min, int max) {
        return (value >= min && value <= max);
    }
    ...
}
...
String fieldValue = request.getParameter("numberOfChoices");
if (Validator.validateRequired(fieldValue)) {
    if (Validator.validateInt(fieldValue)) {
        int numberOfChoices = Integer.parseInt(fieldValue);
        if (Validator.validateRange(numberOfChoices, 10, 20)) {
        // numberOfChoices is valid, continue processing request
        ...
        }
    }
}
```

[5] フィールドのオプション: 多くの場合 Web アプリケーションはユーザーに対して一連のオプションを提示して、ユーザーにそのいずれかを選択するよう促しますが (例えば SELECT HTML タグを使用するなどして)、選択された値が使用可能なオプションのいずれかであるかどうかをサーバー側で検証を実行して確認することはできません。悪意のあるユーザーが任意の

オプションの値を簡単に変更できることに注意してください。選択されたユーザーの値が、関数の仕様で定義されている許可されたオプションであることを必ず検証してください。

許可されたオプションのリストに対してユーザーの選択を検証する例を示します。

```
// Example to validate user selection against a list of options
public Class Validator {
    ...
    public static boolean validateOption(Object[] options, Object value) {
        boolean isValidValue = false;
        try {
        List list = Arrays.asList(options);
        if (list != null) {
        isValidValue = list.contains(value);
        }
        } catch (Exception e) {
        }
        return isValidValue;
    }
    ...
}
...
// Allowed options
String[] options = {"option1", "option2", "option3");
// Verify that the user selection is one of the allowed options
String userSelection = request.getParameter("userSelection");
if (Validator.validateOption(options, userSelection)) {
    // valid user selection, continue processing request
    ...
}
```

[6] フィールドのパターン
関数の仕様で定義されるように、ユーザーの入力がパターンに一致していることを常にチェックしてください。例えば、userName フィールドが大文字小文字を区別せずに英数字のみ許可している場合、次の正規表現を使用します:
^[a-zA-Z0-9]*$

Java 1.3 またはそれ以前のバージョンには、正規表現パッケージが含まれていません。Java 1.3 ではサポートされないため、Apache Regular Expression Package (下記のリソースを参照) を使用することを推奨します。正規表現で検証を実行する例を示します。

```
// Example to validate that a given value matches a specified pattern
// using the Apache regular expression package
import org.apache.regexp.RE;
import org.apache.regexp.RESyntaxException;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
        RE r = new RE(expression);
        match = r.match(value);
        }
        return match;
    }
    ...
}
...
// Verify that the userName request parameter is alphanumeric
String userName = request.getParameter("userName");
if (Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    // userName is valid, continue processing request
    ...
}
```

Java 1.4 には、新しく正規表現パッケージ (java.util.regex) が導入されています。新しい Java 1.4 の正規表現パッケージを使用した Validator.matchPattern の変更バージョンは以下のようになります。

```
// Example to validate that a given value matches a specified pattern
// using the Java 1.4 regular expression package
import java.util.regex.Pattern;
import java.util.regexe.Matcher;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
        match = Pattern.matches(expression, value);
        }
        return match;
    }
    ...
}
```

[7] Cookie の値
Cookie の値を検証するために javax.servlet.http.Cookie オブジェクトを使用してください。アプリケーションの仕様に応じて、(上記と) 同じ検証規則 (要求された値の検証や長さの検証など) が Cookie の値にも適用されます。

要求された Cookie の値を検証する例は次のとおりです。

```
// Example to validate a required cookie value
// First retrieve all available cookies submitted in the HTTP request
Cookie[] cookies = request.getCookies();
if (cookies != null) {
    // find the "user" cookie
    for (int i=0; i<cookies.length; ++i) {
        if (cookies[i].getName().equals("user")) {
        // validate the cookie value
        if (Validator.validateRequired(cookies[i].getValue()) {
        // valid cookie value, continue processing request
        ...
        }
        }
    }
}
```

[8] HTTP 応答
[8-1] ユーザー入力のフィルタリング
クロスサイト・スクリプティングからアプリケーションを保護するには、危険な文字を対応する文字エンティティーに変換して、HTML をサニタイズします。HTML で危険な文字は次のとおりです。
< > " ' % ;) (& +

危険な文字を対応する文字エンティティーに変換して、指定された文字列をフィルタリングする例は次のとおりです。

```
// Example to filter sensitive data to prevent cross-site scripting
public Class Validator {
    ...
    public static String filter(String value) {
        if (value == null) {
```

```
            return null;
            }
            StringBuffer result = new StringBuffer(value.length());
            for (int i=0; i<value.length(); ++i) {
            switch (value.charAt(i)) {
            case '<':
            result.append("&lt;");
            break;
            case '>':
            result.append("&gt;");
            break;
            case '"':
            result.append("&quot;");
            break;
            case '\'':
            result.append("&#39;");
            break;
            case '%':
            result.append("&#37;");
            break;
            case ';':
            result.append("&#59;");
            break;
            case '(':
            result.append("&#40;");
            break;
            case ')':
            result.append("&#41;");
            break;
            case '&':
            result.append("&amp;");
            break;
            case '+':
            result.append("&#43;");
            break;
            default:
            result.append(value.charAt(i));
            break;
            }
            return result;
        }
        ...
    }
    ...
    // Filter the HTTP response using Validator.filter
    PrintWriter out = response.getWriter();
    // set output response
    out.write(Validator.filter(response));
    out.close();
```

Java Servlet API 2.3 にはフィルターが導入されており、HTTP リクエストまたはレスポンスをインターセプトして変換する機能をサポートしています。

Validator.filter を使用して応答をサニタイズする Servlet フィルターの使用例は次のとおりです。

```
    // Example to filter all sensitive characters in the HTTP response using a Java Filter.
    // This example is for illustration purposes since it will filter all content in the response, including
HTML tags!
    public class SensitiveCharsFilter implements Filter {
        ...
        public void doFilter(ServletRequest request,
            ServletResponse response,
            FilterChain chain)
            throws IOException, ServletException {

            PrintWriter out = response.getWriter();
            ResponseWrapper wrapper = new ResponseWrapper((HttpServletResponse)response);
            chain.doFilter(request, wrapper);

            CharArrayWriter caw = new CharArrayWriter();
```

```
            caw.write(Validator.filter(wrapper.toString()));

            response.setContentType("text/html");
            response.setContentLength(caw.toString().length());
            out.write(caw.toString());
            out.close();
        }
        ...
        public class CharResponseWrapper extends HttpServletResponseWrapper {
            private CharArrayWriter output;

            public String toString() {
            return output.toString();
            }

            public CharResponseWrapper(HttpServletResponse response){
            super(response);
            output = new CharArrayWriter();
            }

            public PrintWriter getWriter(){
            return new PrintWriter(output);
            }
        }
    }

    }
```

[8-2] Cookie のセキュリティー保護
Cookie に機密データを保存する場合、HTTPS や SSL などの安全なプロトコルを利用して Cookie が送信されるようにブラウザーに指示するために、Cookie.setSecure(boolean flag) を使用して HTTP 応答の Cookie のセキュリティー・フラグが設定されるようにしてください。

「user」の Cookie をセキュリティー保護する例は次のとおりです。

```
// Example to secure a cookie, i.e. instruct the browser to
// send the cookie using a secure protocol
Cookie cookie = new Cookie("user", "sensitive");
cookie.setSecure(true);
response.addCookie(cookie);
```

推奨される Java ツール・サーバー側で検証を行う Java フレームワークは主に次の 2 つです。
[1] Jakarta Commons Validator (Struts 1.1 と統合)Jakarta Commons Validator は、上記のデータ検証仕様をすべて実装する強力なフレームワークです。これらの規則は、フォーム・フィールドの入力認証規則を定義する XML ファイルで構成されています。Struts の [bean:write] タグを使用することで、記述された全データに対する [8] HTTP 応答の危険な文字の出力フィルタリングを Struts がデフォルトでサポートしています。このフィルタリングは、「filter=false」フラグを設定することにより無効にできます。

Struts は次の基本的な入力検証を定義しますが、カスタム検証が定義される場合もあります。
required: フィールドに空白以外の文字が含まれている場合に成功します。
mask: 値がマスク属性によって与えられた正規表現に一致する場合に成功します。
range: 値が min 属性および max 属性により与えられた値 ((value >= min) および (value <= max)) の範囲内である場合に成功します。
maxLength: フィールドの長さが max 属性以下である場合に成功します。
minLength: フィールドの長さが min 属性以上である場合に成功します。
byte、short、integer、long、float、double: 値を対応するプリミティブ型に変換できる場合に成功します。
date: 値が有効な日付を示す場合に成功します。日付のパターンを指定することも可能です。
creditCard: 値が有効なクレジット・カードの番号である場合に成功します。
e-mail: 値が有効な電子メール・アドレスである場合に成功します。

次に、Struts Validator を使用して、loginForm の userName フィールドを検証する例を示します。

```
<form-validation>
    <global>
        ...
        <validator name="required"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateRequired"
        msg="errors.required">
        </validator>
        <validator name="mask"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateMask"
        msg="errors.invalid">
        </validator>
        ...
    </global>
    <formset>
        <form name="loginForm">
        <!-- userName is required and is alpha-numeric case insensitive -->
        <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayname"/>
        <var>
        <var-name>mask</var-name>
        <var-value>^[a-zA-Z0-9]*$</var-value>
        </var>
        </field>
        ...
        </form>
        ...
    </formset>
</form-validation>
```

[2] JavaServer Faces Technology: JavaServer Faces Technology は、UI コンポーネントの表現、各コンポーネントの状態の管理、イベントの処理、および入力の検証を行う、一連の Java API (JSR 127) です。

JavaServer Faces API は次の基本的な検証を実装しますが、カスタム検証も定義される場合があります。
validate_doublerange: コンポーネントの DoubleRangeValidator を登録します。
validate_length: コンポーネントの LengthValidator を登録します。
validate_longrange: コンポーネントの LongRangeValidator を登録します。
validate_required: コンポーネントの RequiredValidator を登録します。
validate_stringrange: コンポーネントの StringRangeValidator を登録します。
validator: コンポーネントのカスタムの Validator を登録します。

JavaServer Faces API は、次の UIInput および UIOutput Renderers (Tags) を定義します。
input_date: java.text.Date インスタンスでフォーマットされた java.util.Date を受け取ります。
output_date: java.text.Date インスタンスでフォーマットされた java.util.Date を表示します。
input_datetime: java.text.DateTime インスタンスでフォーマットされた java.util.Date を受け取ります。
output_datetime: java.text.DateTime インスタンスでフォーマットされた java.util.Date を表示します。
input_number: java.text.NumberFormat でフォーマットされた数値データ型 (java.lang.Number またはプリミティブ型) を表示します。
output_number: java.text.NumberFormat でフォーマットされた数値データ型 (java.lang.Number またはプリミティブ型) を表示します。
input_text: 1 行の文字列を受け取ります。
output_text: 1 行の文字列を表示します。
input_time: java.text.DateFormat タイム・インスタンスでフォーマットされた java.util.Date を受け取ります。
output_time: java.text.DateFormat タイム・インスタンスでフォーマットされた java.util.Date を表示します。
input_hidden: ページの作成者がページで hidden 変数を使用することを許可します。
input_secret: 空白なしの 1 行のテキストを受け取り、入力の度にアスタリスクのセットとして表示します。
input_textarea: 複数行のテキストを受け取ります。
output_errors: ページ全体のエラー・メッセージまたは指定のクライアント識別子に関連するエラー・メッセージを表示します。
output_label: ネストされたコンポーネントを指定インプット・フィールドのラベルとして表示します。

output_message: 配置されたメッセージを表示します。

次に、JavaServer Faces を使用して、loginForm の userName フィールドを検証する例を示します。

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
  <h:form formName="loginForm" >
    <h:input_text id="userName" size="20" modelReference="UserBean.userName">
        <f:validate_required/>
        <f:validate_length minimum="8" maximum="20"/>
    </h:input_text>
    <!-- display errors if present -->
    <h:output_errors id="loginErrors" clientId="userName"/>
    <h:command_button id="submit" label="Submit" commandName="submit" /><p>
  </h:form>
</f:use_faces>
```

参照リンク:
Java API 1.3 -
http://java.sun.com/j2se/1.3/docs/api/
Java API 1.4 -
http://java.sun.com/j2se/1.4/docs/api/
Java Servlet API 2.3 -
http://java.sun.com/products/servlet/2.3/javadoc/
Java Regular Expression Package -
http://jakarta.apache.org/regexp/
Jakarta Validator -
http://jakarta.apache.org/commons/validator/
JavaServer Faces Technology -
http://java.sun.com/j2ee/javaserverfaces/

** エラーの処理:

多くの J2EE Web アプリケーション・アーキテクチャーは Model View Controller (MVC) パターンに準拠しています。このパターンでは、Servlet は Controller として動作します。Servlet はアプリケーションの処理を EJB Session Bean (Model) のような JavaBean に委託します。次に、Servlet は要求を JSP (View) に転送して、処理の結果をレンダリングします。必要な処理が実際に行われたことを確認するために、Servlet はすべての入力、出力、リターン・コード、エラー・コード、および既知の例外をチェックする必要があります。

データの検証は悪意のあるデータの改ざんからアプリケーションを保護することはできますが、アプリケーションが内部的なエラー・メッセージ (例外スタック・トレースなど) を不注意で公開するような状況を防ぐには、適切なエラー処理を実行するための方策が必要です。適切なエラー処理の方策を立てる際には、次の点に注意します。

[1] エラーの定義
[2] エラーの報告
[3] エラーのレンダリング
[4] エラーのマッピング

[1] エラーの定義
アプリケーション・レイヤー (Servlet など) でのハード・コーディングされたエラー・メッセージは避けてください。アプリケーションには既知のアプリケーション障害にマップするエラー・キーを使用するようにしてください。効果的な方法は、HTML フォーム・フィールドや他の Bean プロパティーの検証規則にマップするエラー・キーを定義することです。例えば「user_name」フィールドが必須フィールドであり、このフィールドには英数字を入力する必要があり、さらにデータベース内で他に同じ名前が存在してはならない場合は、次のようなエラー・キーを定義します。

(a) ERROR_USERNAME_REQUIRED: このエラー・キーを使用すると、「user_name」フィールドが必須フィールドであることをユーザーに通知するメッセージが表示されます。
(b) ERROR_USERNAME_ALPHANUMERIC: このエラー・キーを使用すると、「user_name」フィールドの値が英数字でなければならないことをユーザーに通知するメッセージが表示されます。
(c) ERROR_USERNAME_DUPLICATE: このエラー・キーを使用すると、「user_name」の値がデータベース内で重複していることをユーザーに通知するメッセージが表示されます。
(d) ERROR_USERNAME_INVALID: このエラー・キーを使用すると、「user_name」の値が無効であることをユーザーに通知する一般的なメッセージが表示されます。
効果的な方法は、アプリケーション・エラーを格納および報告するために使用する、次のようなフレームワーク Java クラスを定義することです。
- ErrorKeys: すべてのエラー・キーを定義します。

```
// Example: ErrorKeys defining the following error keys:
//    - ERROR_USERNAME_REQUIRED
//    - ERROR_USERNAME_ALPHANUMERIC
//    - ERROR_USERNAME_DUPLICATE
//    - ERROR_USERNAME_INVALID
//    ...
public Class ErrorKeys {
    public static final String ERROR_USERNAME_REQUIRED = "error.username.required";
    public static final String ERROR_USERNAME_ALPHANUMERIC = "error.username.alphanumeric";
    public static final String ERROR_USERNAME_DUPLICATE = "error.username.duplicate";
    public static final String ERROR_USERNAME_INVALID = "error.username.invalid";
    ...
}
```

- Error: 個々のエラーをカプセル化します。

```
// Example: Error encapsulates an error key.
// Error is serializable to support code executing in multiple JVMs.
public Class Error implements Serializable {

    // Constructor given a specified error key
    public Error(String key) {
    this(key, null);
    }

    // Constructor given a specified error key and array of placeholder objects
    public Error(String key, Object[] values) {
    this.key = key;
    this.values = values;
    }

    // Returns the error key
    public String getKey() {
    return this.key;
    }

    // Returns the placeholder values
    public Object[] getValues() {
    return this.values;
    }

    private String key = null;
    private Object[] values = null;
}
```

- Errors: エラーの集合をカプセル化します。

```
    // Example: Errors encapsulates the Error objects being reported to the presentation layer.
    // Errors are stored in a HashMap where the key is the bean property name and value is an
    // ArrayList of Error objects.
    public Class Errors implements Serializable {

        // Adds an Error object to the Collection of errors for the specified bean property.
        public void addError(String property, Error error) {
        ArrayList propertyErrors = (ArrayList)errors.get(property);
        if (propertyErrors == null) {
        propertyErrors = new ArrayList();
        errors.put(property, propertyErrors);
        }
        propertyErrors.put(error);
        }

        // Returns true if there are any errors
        public boolean hasErrors() {
        return (errors.size > 0);
        }

        // Returns the Errors for the specified property
        public ArrayList getErrors(String property) {
        return (ArrayList)errors.get(property);
        }

        private HashMap errors = new HashMap();
    }
```

次に、上記フレームワーク・クラスを使用して、「user_name」フィールドの検証エラーを処理する例を示します。

```
// Example to process validation errors of the "user_name" field.
Errors errors = new Errors();
String userName = request.getParameter("user_name");
// (a) Required validation rule
if (!Validator.validateRequired(userName)) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_REQUIRED));
} // (b) Alpha-numeric validation rule
else if (!Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_ALPHANUMERIC));
}
else
{
    // (c) Duplicate check validation rule
    // We assume that there is an existing UserValidationEJB session bean that implements
    // a checkIfDuplicate() method to verify if the user already exists in the database.
    try {
        ...
        if (UserValidationEJB.checkIfDuplicate(userName)) {
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE));
        }
    } catch (RemoteException e) {
        // log the error
        logger.error("Could not validate user for specified userName: " + userName);
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE);
    }
}
// set the errors object in a request attribute called "errors"
request.setAttribute("errors", errors);
...
```

[2] エラーの報告
Web 層のアプリケーション・エラーを報告する方法は 2 つあります。
(a) Servlet エラー・メカニズム
(b) JSP エラー・メカニズム

[2-a] Servlet エラー・メカニズム
　Servlet は次の方法のいずれかでエラーを報告します。
- 入力 JSP へ転送する (すでにエラーを要求属性に格納している)
- HTTP エラー・コードを引数として response.sendError を呼び出す
- 例外をスローする

効果的な方法は、既知のアプリケーション・エラー (セクション [1] を参照) をすべて処理し、要求属性にそれらを格納し、入力 JSP に転送することです。入力 JSP はエラー・メッセージを表示して、ユーザーにデータを入力し直すように促す必要があります。次に、入力 JSP (userInput.jsp) に転送する例を示します。

```
// Example to forward to the userInput.jsp following user validation errors
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd != null) {
    rd.forward(request, response);
}
```

Servletが既知のJSPページに転送できない場合、2番目の選択肢は、HttpServletResponse.SC_INTERNAL_SERVER_ERROR(状態コード500)を引数としてresponse.sendErrorメソッドを呼び出す方法です。さまざまな HTTP 状態コードの詳細については、javax.servlet.http.HttpServletResponse の javadoc を参照してください。次に、HTTP エラーを返す例を示します。

```
// Example to return a HTTP error code
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd == null) {
    // messages is a resource bundle with all message keys and values
    response.sendError(HttpServletResponse.SC_INTERNAL_SERVER_ERROR,
        messages.getMessage(ErrorKeys.ERROR_USERNAME_INVALID));
}
```

最後の手段として、Servlet は例外をスローすることができます。この例外は、次のクラスのうちの 1 つのサブクラスである必要があります。
- RuntimeException
- ServletException
- IOException

[2-b] JSP エラー・メカニズム
JSP ページには、次の例のように errorPage ディレクティブを定義して、実行時例外を処理する機能があります。

```
<%@ page errorPage="/errors/userValidation.jsp" %>
```

エラー・トラップできない JSP の例外は指定された errorPage に転送され、オリジナルの例外は javax.servlet.jsp.jspException と呼ばれる要求パラメーターとして設定されます。エラー・ページは、isErrorPage 命令を含んでいる必要があります:

```
<%@ page isErrorPage="true" %>
```

isErrorPage ディレクティブが指定されると、「exception」変数はスローされる例外オブジェクトに初期化されます。

[3] エラーのレンダリング
J2SE Internationalization API は、アプリケーション・リソースを外部化し、メッセージをフォーマットする次のようなユーティリティー・クラスを提供します。

(a) リソース・バンドル
(b) メッセージ・フォーマット

[3-a] リソース・バンドル
リソース・バンドルは、ローカライズされたデータとそれを使用するソース・コードを分離することによって国際化対応をサポートします。各リソース・バンドルは、特定のロケールに対するキーと値のペアのマッピングを格納しています。

通常は java.util.PropertyResourceBundle を使用または拡張して、外部プロパティー・ファイルにコンテンツを格納します。次に例を示します。

```
##############################################
# ErrorMessages.properties
##############################################
# required user name error message
error.username.required=User name field is required

# invalid user name format
error.username.alphanumeric=User name must be alphanumeric

# duplicate user name error message
error.username.duplicate=User name {0} already exists, please choose another one

...
```

異なるロケールをサポートするために、複数のリソースを定義できます (これが「リソース・バンドル」という名前の由来)。例えば、バンドル・ファミリーのフランス語をサポートするために ErrorMessages_fr.properties を定義できます。要求されたロケールのリソースが存在しない場合は、デフォルトのメンバーが使用されます。上記例では、デフォルトのリソースは ErrorMessages.properties です。アプリケーション (JSP または Servlet) はユーザーのロケールに従って適切なリソースからコンテンツを取得します。

[3-b] メッセージ・フォーマット
J2SE 標準クラス java.util.MessageFormat は、置換プレースホルダー付きのメッセージを作成する一般的な方法です。MessageFormat オブジェクトは、次のような書式指示子が埋め込まれたパターン文字列を持っています。

```
// Example to show how to format a message using placeholder parameters
String pattern = "User name {0} already exists, please choose another one";
String userName = request.getParameter("user_name");
Object[] args = new Object[1];
args[0] = userName;
String message = MessageFormat.format(pattern, args);
```

次に、より理解しやすい例として、ResourceBundle と MessageFormat を使用してエラー・メッセージを表示する例を示します。

```
// Example to render an error message from a localized ErrorMessages resource (properties file)
// Utility class to retrieve locale-specific error messages
```

```
public Class ErrorMessageResource {

    // Returns the error message for the specified error key in the environment locale
    public String getErrorMessage(String errorKey) {
        return getErrorMessage(errorKey, defaultLocale);
    }

    // Returns the error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Locale locale) {
        return getErrorMessage(errorKey, null, locale);
    }

    // Returns a formatted error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Object[] args, Locale locale) {
        // Get localized ErrorMessageResource
        ResourceBundle errorMessageResource = ResourceBundle.getBundle("ErrorMessages", locale);
        // Get localized error message
        String errorMessage = errorMessageResource.getString(errorKey);
        if (args != null) {
        // Format the message using the specified placeholders args
        return MessageFormat.format(errorMessage, args);
        } else {
        return errorMessage;
        }
    }

    // default environment locale
    private Locale defaultLocale = Locale.getDefaultLocale();
}
...
// Get the user's locale
Locale userLocale = request.getLocale();
// Check if there were any validation errors
Errors errors = (Errors)request.getAttribute("errors");
if (errors != null && errors.hasErrors()) {
    // iterate through errors and output error messages corresponding to the "user_name" property
    ArrayList userNameErrors = errors.getErrors("user_name");
    ListIterator iterator = userNameErrors.iterator();
    while (iterator.hasNext()) {
        // Get the next error object
        Error error = (Error)iterator.next();
        String errorMessage = ErrorMessageResource.getErrorMessage(error.getKey(), userLocale);
        output.write(errorMessage + "\r\n");
    }
}
```

上記例のようにエラー・メッセージを何度も表示する場合は、独自のJSPタグ (displayErrors等) を定義することが推奨されます。

[4] エラーのマッピング
通常 Servlet Containerは、応答状態コードまたは例外のどちらかに対応するデフォルトのエラー・ページを返します。状態コードまたは例外と Web リソースとのマッピングは、カスタム・エラー・ページを使用して指定できます。効果的な方法は、内部のエラーの状態を公開しない静的なエラー・ページを開発することです (デフォルトでは、ほとんどの Servlet コンテナーは内部エラー・メッセージを報告します)。このマッピングは、次の例のように、Web Deployment Descriptor (web.xml) で設定されます。

```
<!-- Mapping of HTTP error codes and application exceptions to error pages -->
<error-page>
  <exception-type>UserValidationException</exception-type>
  <location>/errors/validationError.html</error-page>
</error-page>
<error-page>
  <error-code>500</exception-type>
  <location>/errors/internalError.html</error-page>
</error-page>
<error-page>
...
</error-page>
```

```
...
```

推奨される Java ツール・サーバー側で検証を行う Java フレームワークは主に次の 2 つです。
[1] Jakarta Commons Validator (Struts 1.1 と統合)[1] Jakarta Commons Validator (Struts 1.1 と統合):
Jakarta Commons Validator は、上記のようなエラー処理メカニズムを定義する Java フレームワークです。検証規則は、フォーム・フィールドの入力検証規則とそれに対応する検証エラー・キーを定義する XML ファイルとして設定されます。Struts は、リソース・バンドルとメッセージ・フォーマットを使用してローカライズ・アプリケーションを構築するための国際化対応をサポートします。

次に、Struts Validator を使用して、loginForm の userName フィールドを検証する例を示します。

```
<form-validation>
    <global>
        ...
        <validator name="required"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateRequired"
        msg="errors.required">
        </validator>
        <validator name="mask"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateMask"
        msg="errors.invalid">
        </validator>
        ...
    </global>
    <formset>
        <form name="loginForm">
        <!-- userName is required and is alpha-numeric case insensitive -->
        <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayname"/>
        <var>
        <var-name>mask</var-name>
        <var-value>^[a-zA-Z0-9]*$</var-value>
        </var>
        </field>
        ...
        </form>
        ...
    </formset>
</form-validation>
```

次の例に示すように、Struts JSP タグ・ライブラリーは、格納されたエラー・メッセージを条件付きで表示する「errors」タグを定義します。

```
<%@ page language="java" %>
<%@ taglib uri="/WEB-INF/struts-html.tld" prefix="html" %>
<%@ taglib uri="/WEB-INF/struts-bean.tld" prefix="bean" %>
<html:html>
<head>
<body>
    <html:form action="/logon.do">
    <table border="0" width="100%">
    <tr>
        <th align="right">
        <html:errors property="username"/>
        <bean:message key="prompt.username"/>
        </th>
        <td align="left">
```

```
            <html:text property="username" size="16"/>
            </td>
        </tr>
        <tr>
        <td align="right">
            <html:submit><bean:message key="button.submit"/></html:submit>
        </td>
        <td align="right">
            <html:reset><bean:message key="button.reset"/></html:reset>
        </td>
        </tr>
        </table>
        </html:form>
    </body>
    </html:html>
```

[2] JavaServer Faces Technology
JavaServer Faces Technology は、UI コンポーネントの表現、各コンポーネントの状態の管理、イベントの処理、入力の検証、および国際化対応のサポートを行う、一連の Java API (JSR 127) です。

JavaServer Faces API は「output_errors」という UIOutput Renderer を定義します。それはページ全体のエラー・メッセージまたは指定されたクライアント識別子に関連するエラー・メッセージを表示します。

次に、JavaServer Faces を使用して、loginForm の userName フィールドを検証する例を示します。

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
  <h:form formName="loginForm" >
    <h:input_text id="userName" size="20" modelReference="UserBean.userName">
        <f:validate_required/>
        <f:validate_length minimum="8" maximum="20"/>
    </h:input_text>
    <!-- display errors if present -->
    <h:output_errors id="loginErrors" clientId="userName"/>
    <h:command_button id="submit" label="Submit" commandName="submit" /><p>
  </h:form>
</f:use_faces>
```

参照リンク:
Java API 1.3 -
http://java.sun.com/j2se/1.3/docs/api/
Java API 1.4 -
http://java.sun.com/j2se/1.4/docs/api/
Java Servlet API 2.3 -
http://java.sun.com/products/servlet/2.3/javadoc/
Java Regular Expression Package -
http://jakarta.apache.org/regexp/
Jakarta Validator -
http://jakarta.apache.org/commons/validator/
JavaServer Faces Technology -
http://java.sun.com/j2ee/javaserverfaces/

フレームからのフィッシング

PHP

** 入力データの検証

データ検証は、ユーザーの利便性のためにクライアント層で行うこともできますが、必ずサーバー層で行う必要があります。クライアント側のデータ検証は、例えば Javascript を無効にすることによって簡単にバイパスできるため、本質的に安全ではありません。

一般的には、次の項目を検証するサーバー側ユーティリティー・ルーチンを提供する Web アプリケーション・フレームワークが理想とされます。
[1] 必須フィールド
[2] フィールドのデータ型 (デフォルトでは、HTTP 要求パラメーターはすべて String)
[3] フィールドの長さ
[4] フィールドの範囲
[5] フィールドのオプション
[6] フィールドのパターン
[7] Cookie の値
[8] HTTP 応答

効果的な方法は、各アプリケーション・パラメーターを検証する関数を実装することです。以下のセクションでは、チェックの例について示しています。

[1] 必須フィールド
常に、フィールドが Null でなく、前後の空白スペースを除いて、その長さがゼロより大きいことをチェックします。
次に、要求されたフィールドを検証する例を示します。

```
// PHP example to validate required fields
function validateRequired($input) {
    ...
    $pass = false;
    if (strlen(trim($input))>0){
        $pass = true;
    }
    return $pass;
    ...
}
...
if (validateRequired($fieldName)) {
    // fieldName is valid, continue processing request
    ...
}
```

[2] フィールドのデータ型: Web アプリケーションでは、入力パラメーターの型は多くありません。例えば、HTTP 要求パラメーターや Cookie の値はすべて String 型です。開発者は入力のデータ型が正しいかどうかを確認する必要があります。

[3] フィールドの長さ: 常に、入力パラメーター (HTTP 要求パラメーターまたは Cookie 値のどちらか) の長さが最小値から最大値までの間であることを確認します。

[4] フィールドの範囲: 常に、入力パラメーターが関数の要件で定義された範囲内であることを確認します。

[5] フィールドのオプション: 多くの場合 Web アプリケーションはユーザーに対して一連のオプションを提示して、ユーザーにそのいずれかを選択するよう促しますが (例えば SELECT HTML タグを使用するなどして)、選択された値が使用可能なオプションのいずれかであるかどうかをサーバー側で検証を実行して確認することはできません。悪意のあるユーザーが任意のオプションの値を簡単に変更できることに注意してください。選択されたユーザーの値が、関数の仕様で定義されている許可されたオプションであることを必ず検証してください。

[6] フィールドのパターン: 関数の仕様で定義されるように、ユーザーの入力がパターンに一致していることを常にチェックして

ください。例えば、userName フィールドが大文字小文字を区別せずに英数字のみ許可している場合、次の正規表現を使用します:
^[a-zA-Z0-9]+$

[7] Cookie の値: アプリケーションの仕様に応じて、(上記と) 同じ検証規則 (要求された値の検証や長さの検証など) が Cookie の値にも適用されます。

[8] HTTP 応答

[8-1] ユーザー入力のフィルタリング: クロスサイト・スクリプティングからアプリケーションを保護するには、開発者が、危険な文字を対応する文字エンティティーに変換して HTML をサニタイズする必要があります。HTML で危険な文字は次のとおりです。
< > " ' % ;) (& +

PHP には、htmlentities() などの自動サニタイズ・ユーティリティー関数がいくつかあります。

```
$input = htmlentities($input, ENT_QUOTES, 'UTF-8');
```

さらに、クロスサイト・スクリプティングの UTF-7 バリアントを防止するために、明示的に応答の Content-Type ヘッダーを定義します。以下の例を参照してください。

```
<?php

header('Content-Type: text/html; charset=UTF-8');

?>
```

[8-2] Cookie のセキュリティー保護

秘密データを Cookie に格納して SSL を介して転送するときには、まず HTTP 応答に Cookie のセキュリティー・フラグを設定します。これによって、SSL 接続ではこの Cookie のみを使用するようにブラウザーに指示します。

Cookie のセキュリティーを保つ方法については、以下のコード例を使用することができます。

```
<$php

    $value = "some_value";
    $time = time()+3600;
    $path = "/application/";
    $domain = ".example.com";
    $secure = 1;

    setcookie("CookieName", $value, $time, $path, $domain, $secure, TRUE);
?>
```

さらに、HttpOnly フラグを使用することをお勧めします。HttpOnly フラグが TRUE に設定されているとき、Cookie は HTTP プロトコルでのみアクセスできるようになっています。つまり、この Cookie は JavaScript のようなスクリプト言語ではアクセスできなくなります。この設定によって、XSS 攻撃による ID の盗用を効果的に減殺することができます (ただしすべてのブラウ

ザーがサポートしている訳ではありません)。

HttpOnly フラグは PHP 5.2.0 で追加されました。

参照リンク:

[1] HTTP-only Cookies によるクロスサイト・スクリプティングの防止:
http://msdn2.microsoft.com/en-us/library/ms533046.aspx
[2] PHP セキュリティー・コンソーシアム:
http://phpsec.org/
[3] PHP & Web アプリケーション・セキュリティー・ブログ (Chris Shiflett):
http://shiflett.org/

フレームからのフィッシング

中 ディレクトリーの一覧表示を拒否するようにサーバーの設定を変更し、使用できる最新のセキュリティー・パッチをインストールします TOC

このタスクで修正される問題のタイプ

- ディレクトリーの一覧作成

全般

[1] Web サーバーを、ディレクトリーの一覧作成を拒否するように設定します。

[2] お使いの Web サーバーまたは Web アプリケーションに存在する問題に対応した個別のセキュリティー・パッチをダウンロードします。ディレクトリーの一覧作成に関する既知の問題の中には、このアドバイザリーの「リファレンス」フィールドに記載されているものもあります。
[3] 短いファイル名 (8.3 DOS 形式) の問題を修正するには、このアドバイザリーの「リファレンス」フィールドにある CERT アドバイザリーによる次善の対策を活用します。
a. Web サーバーのみによって保護するファイルには、8.3 形式の短いファイル名のみを使用します。FAT ファイル・システム (16 ビット) では、「Win31FileSystem」レジストリー・キー (レジストリー・パス: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem\) を有効にする (1 に設定する) ことで、この形式の使用を強制することができます。
b. NTFS (32 ビット) では、「NtfsDisable8dot3NameCreation」レジストリー・キー (レジストリー・パス: HKEY_LOCAL_MACHINE\System\ CurrentControlSet\Control\FileSystem\) を有効にする (1 に設定する) ことで、長いファイル名を持つファイルに対する 8.3 対応の短いファイル名の作成を無効にすることができます。ただし、この方法は 16 ビット・アプリケーションとの互換性に問題を生じる場合があります。
c. NTFS ベースの ACL (ディレクトリーまたはファイル・レベルのアクセス・コントロール・リスト) を使用して、Web サーバーによるセキュリティーを拡大または置換します。

低 Content-Security-Policy ヘッダーを使用するようにサーバーを構成してください TOC

このタスクで修正される問題のタイプ

- Content-Security-Policy ヘッダーが欠落しています

全般

「Content-Security-Policy」ヘッダーを送信するように、サーバーを構成してください。

それぞれ下記のリンクを参照してください。
Apache の場合
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
IIS の場合
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
nginx の場合
http://nginx.org/en/docs/http/ngx_http_headers_module.html

低 Web サーバーの HTTP TRACE サポートを無効にします TOC

このタスクで修正される問題のタイプ

- TRACE および TRACK HTTP メソッドが有効

全般

Web サーバーの HTTP TRACE サポートを無効にします。

Apache Web サーバーおよび Microsoft IIS 用の可能な回避策は次のとおりです。

- Apache HTTP サーバー: Apache mod_rewrite モジュールを使用して、HTTP TRACE 要求を拒否するか、サイトの要件およびポリシーを満たすために必要なメソッドのみを許可します。

- Microsoft Internet Information Services (IIS): URLScan ツールを使用して、HTTP TRACE 要求を拒否するか、サイトの要件およびポリシーを満たすために必要なメソッドのみを許可します。

低 Web サイトから内部 IP アドレスを削除します TOC

このタスクで修正される問題のタイプ

- 内部 IP の開示パターンを発見

全般

内部 IP は、通常は Web アプリケーション/サーバーが生成するエラー・メッセージや、HTML/JavaScript のコメントで公開されます。[1] Web アプリケーション/サーバーで、問題となる可能性のある詳細なエラー・メッセージをオフにします。[2] 該当するパッチをすべてインストールします。[3] 内部 IP 情報を HTML/JavaScript コメントに残さないようにします。

低 X-Content-Type-Options ヘッダーを使用するようにサーバーを構成してください TOC

このタスクで修正される問題のタイプ

- X-Content-Type-Options ヘッダーが欠落しています

全般

すべての発信要求において「X-Content-Type-Options」ヘッダーに値「nosniff」を付与して送信するように、サーバーを構成してください。

それぞれ下記のリンクを参照してください。
Apache の場合
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
IIS の場合
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
nginx の場合
http://nginx.org/en/docs/http/ngx_http_headers_module.html

低 X-XSS-Protection ヘッダーを使用するようにサーバーを構成してください TOC

このタスクで修正される問題のタイプ

- X-XSS-Protection ヘッダーが欠落しています

全般

すべての発信要求において「X-XSS-Protection」ヘッダーに値「1」(つまり「有効」) を付与して送信するように、サーバーを構成してください。

それぞれ下記のリンクを参照してください。
Apache の場合

http://httpd.apache.org/docs/2.2/mod/mod_headers.html
IIS の場合
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
nginx の場合
http://nginx.org/en/docs/http/ngx_http_headers_module.html

低 クエリー・ストリングで送信されるボディー・パラメーターを受け入れる受け入れません TOC

このタスクで修正される問題のタイプ

- ボディ・パラメーターをクエリーで送信

全般

照会にリストされた POST パラメーターの処理を許可しないようにアプリケーションを再プログラミングします

低 すべてのセッション Cookie に HttpOnly 属性を追加してください。 TOC

このタスクで修正される問題のタイプ

- セッション Cookie に HttpOnly 属性がありません

全般

基本的に、Cookie に必要な属性は name フィールドのみです。一般的なオプションの属性には、comment、domain、path などがあります。
セッション Cookie がスクリプトによってアクセスされないようにするには、HttpOnly 属性を適切に設定する必要があります。

低 パラメーター値が期待される範囲とタイプであることを確認します。デバッグ・エラー・メッセージおよび例外を出力しないようにします。 TOC

このタスクで修正される問題のタイプ

- アプリケーション・エラー

全般

[1] 着信した要求に対しすべてが想定されるパラメーターと値であることを確認してください。パラメーターがなくなっている場合には、適切なエラー・メッセージを表示するか、デフォルト値を使用してください。
[2] アプリケーションは、入力が (デコーディング後に) 有効な文字で構成されていることを検証する必要があります。例えば、Null バイト (%00 とエンコードされる)、アポストロフィー、引用符などを含む入力値は拒否します。
[3] 必要な範囲と型の値を確実に指定します。アプリケーションの特定のパラメーターにはそれに対応した特定のセットに含まれている値が必要である場合、受信した値が実際にそのセットに含まれているようにアプリケーション側で指定する必要があります。例えば、アプリケーションが 10..99 の範囲の値を必要としている場合には、値が数値で 10..99 の範囲になるようにする必要があります。
[4] データがクライアントから提供されたセットに含まれていることを検証します。
[5] デバッグのエラー・メッセージおよび稼働環境での例外メッセージを出力しないでください。

.Net

ASP.NET でのデバッグを無効にするには、web.config ファイルを編集し、次の記述を追加します。

```
<compilation
    debug="false"
/>
```

詳しくは、
http://support.microsoft.com/default.aspx?scid=kb;en-us;815157
の「HOW TO: Disable Debugging for ASP.NET Applications」を参照してください。
検証コントロールを使用して Web フォーム・ページに入力検証を追加できます。検証コントロールにより、(例えば範囲内の有効な日付または値のテスト等) 全ての共通型に簡単に使用できる標準的な検証、カスタム化した検証を提供する方法が追加されます。さらに、検証コントロールにより、ユーザーに表示するエラー情報を完全にカスタマイズできるようになります。検証コントロールは、HTML および Web サーバー・コントロールを含む、Web フォーム・ページのクラス・ファイルで処理される任意のコントロールと一緒に使用できます。

すべての必要なパラメーターが要求に存在するように、RequiredFieldValidator 検証コントロールを使用します。このコントロールによって、ユーザーが Web フォームのエントリーをスキップしないようにします。

ユーザーの入力が正しい値だけであることを確かめるために、次の検証コントロールの 1 つを使うことができます。

[1] 「RangeValidator」: ユーザーのエントリー (値) が指定された下限と上限の間であることをチェックします。数字、英字、および日付のペアで示した範囲をチェックすることができます。

[2] 「RegularExpressionValidator」: 正規表現により定義されたパターンとエントリーが一致していることをチェックします。この検証タイプにより、社会保障番号、電子メール・アドレス、電話番号、郵便番号等といった予想可能な文字のシーケンスをチェックできます。

重要な注意事項: 検証コントロールは、ユーザーの入力をブロックしたりページ処理のフローを変更することはありません。エラー・ステータスを設定し、エラー・メッセージを送出するだけです。アプリケーション固有のアクションをさらに実行する前に、プログラマーは必ずコード内のコントロールの状態をテストしてください。

ユーザーの入力を検証する方法には 2 つの方法があります:

1. 一般的なエラー状態のテスト:

コードで、ページの IsValid プロパティーをチェックしてください。このプロパティーは、ページの全検証コントロールの IsValid プロパティーの値の論理和を結果として返します。検証コントロールの 1 つが無効に設定されている場合、ページのプロパティーは false を返します。

2. 各コントロールのエラー状態のテスト:

ページの Validators コレクション (すべての検証コントロールへの参照を含みます) に含まれるものをチェックしてください。そ

うすることで、各検証コントロールの IsValid プロパティーを調べることが可能となります。

J2EE

** 入力データの検証

データ検証は、ユーザーの利便性のためにクライアント層で行うこともできますが、必ず Servlet を使用するサーバー層で行う必要があります。クライアント側のデータ検証は、例えば Javascript を無効にすることによって簡単にバイパスできるため、本質的に安全ではありません。

一般的には、次の項目を検証するサーバー側ユーティリティー・ルーチンを提供する Web アプリケーション・フレームワークが理想とされます。
[1] 必須フィールド
[2] フィールドのデータ型 (デフォルトでは、HTTP 要求パラメーターはすべて String)
[3] フィールドの長さ
[4] フィールドの範囲
[5] フィールドのオプション
[6] フィールドのパターン
[7] Cookie の値
[8] HTTP 応答

効果的な方法は、上記ルーチンを Validator ユーティリティー・クラスの静的メソッドとして実装することです。次のセクションでは、validator クラスの例について説明します。

[1] 必須フィールド
常に、フィールドが Null でなく、前後の空白スペースを除いて、その長さがゼロより大きいことをチェックします。
次に、要求されたフィールドを検証する例を示します。

```
// Java example to validate required fields
public Class Validator {
    ...
    public static boolean validateRequired(String value) {
        boolean isFieldValid = false;
        if (value != null && value.trim().length() > 0) {
        isFieldValid = true;
        }
        return isFieldValid;
    }
    ...
}
...
String fieldValue = request.getParameter("fieldName");
if (Validator.validateRequired(fieldValue)) {
    // fieldValue is valid, continue processing request
    ...
}
```

[2] フィールドのデータ型: Web アプリケーションでは、入力パラメーターの型は多くありません。例えば、HTTP 要求パラメーターや Cookie の値はすべて String 型です。開発者は入力のデータ型が正しいかどうかを確認する必要があります。フィールドの値を希望するプリミティブなデータ型に安全に変換できるかどうかをチェックするには、Java プリミティブ・ラッパー・クラスを使用します。

次に、数値フィールド (int 型) を検証する例を示します。

```
// Java example to validate that a field is an int number
public Class Validator {
    ...
    public static boolean validateInt(String value) {
        boolean isFieldValid = false;
```

```
            try {
            Integer.parseInt(value);
            isFieldValid = true;
            } catch (Exception e) {
            isFieldValid = false;
            }
            return isFieldValid;
        }
        ...
    }
    ...
    // check if the HTTP request parameter is of type int
    String fieldValue = request.getParameter("fieldName");
    if (Validator.validateInt(fieldValue)) {
        // fieldValue is valid, continue processing request
        ...
    }
```

効果的な方法は、HTTP 要求パラメーターをすべて対応するデータ型に変換することです。次の例に示すように、開発者は、要求パラメーターの integerValue を要求属性に格納して使用します。

```
    // Example to convert the HTTP request parameter to a primitive wrapper data type
    // and store this value in a request attribute for further processing
    String fieldValue = request.getParameter("fieldName");
    if (Validator.validateInt(fieldValue)) {
        // convert fieldValue to an Integer
        Integer integerValue = Integer.getInteger(fieldValue);
        // store integerValue in a request attribute
        request.setAttribute("fieldName", integerValue);
    }
    ...
    // Use the request attribute for further processing
    Integer integerValue = (Integer)request.getAttribute("fieldName");
    ...
```

アプリケーションが処理する必要がある Java の主なデータ型は次のとおりです。
- Byte
- Short
- Integer
- Long
- Float
- Double
- Date

[3] フィールドの長さ: 常に、入力パラメーター (HTTP 要求パラメーターまたは Cookie 値のどちらか) の長さが最小値から最大値までの間であることを確認します。

次に、userName フィールドの長さが 8 文字から 20 文字までの間であることを検証する例を示します。

```
    // Example to validate the field length
    public Class Validator {
        ...
        public static boolean validateLength(String value, int minLength, int maxLength) {
            String validatedValue = value;
            if (!validateRequired(value)) {
            validatedValue = "";
            }
            return (validatedValue.length() >= minLength &&
            validatedValue.length() <= maxLength);
```

```
    }
    ...
}
...
String userName = request.getParameter("userName");
if (Validator.validateRequired(userName)) {
    if (Validator.validateLength(userName, 8, 20)) {
        // userName is valid, continue further processing
        ...
    }
}
```

[4] フィールドの範囲: 常に、入力パラメーターが関数の要件で定義された範囲内であることを確認します。

入力データ numberOfChoices の値が 10 から 20 の間であることを検証する例を示します。

```
// Example to validate the field range
public Class Validator {
    ...
    public static boolean validateRange(int value, int min, int max) {
        return (value >= min && value <= max);
    }
    ...
}
...
String fieldValue = request.getParameter("numberOfChoices");
if (Validator.validateRequired(fieldValue)) {
    if (Validator.validateInt(fieldValue)) {
        int numberOfChoices = Integer.parseInt(fieldValue);
        if (Validator.validateRange(numberOfChoices, 10, 20)) {
        // numberOfChoices is valid, continue processing request
        ...
        }
    }
}
```

[5] フィールドのオプション: 多くの場合 Web アプリケーションはユーザーに対して一連のオプションを提示して、ユーザーにそのいずれかを選択するよう促しますが (例えば SELECT HTML タグを使用するなどして)、選択された値が使用可能なオプションのいずれかであるかどうかをサーバー側で検証を実行して確認することはできません。悪意のあるユーザーが任意のオプションの値を簡単に変更できることに注意してください。選択されたユーザーの値が、関数の仕様で定義されている許可されたオプションであることを必ず検証してください。

許可されたオプションのリストに対してユーザーの選択を検証する例を示します。

```
// Example to validate user selection against a list of options
public Class Validator {
    ...
    public static boolean validateOption(Object[] options, Object value) {
        boolean isValidValue = false;
        try {
        List list = Arrays.asList(options);
        if (list != null) {
        isValidValue = list.contains(value);
        }
        } catch (Exception e) {
        }
        return isValidValue;
    }
    ...
}
...
```

```
// Allowed options
String[] options = {"option1", "option2", "option3");
// Verify that the user selection is one of the allowed options
String userSelection = request.getParameter("userSelection");
if (Validator.validateOption(options, userSelection)) {
    // valid user selection, continue processing request
    ...
}
```

[6] フィールドのパターン
関数の仕様で定義されるように、ユーザーの入力がパターンに一致していることを常にチェックしてください。例えば、userName フィールドが大文字小文字を区別せずに英数字のみ許可している場合、次の正規表現を使用します:
^[a-zA-Z0-9]*$

Java 1.3 またはそれ以前のバージョンには、正規表現パッケージが含まれていません。Java 1.3 ではサポートされないため、Apache Regular Expression Package (下記のリソースを参照) を使用することを推奨します。
正規表現で検証を実行する例を示します。

```
// Example to validate that a given value matches a specified pattern
// using the Apache regular expression package
import org.apache.regexp.RE;
import org.apache.regexp.RESyntaxException;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
        RE r = new RE(expression);
        match = r.match(value);
        }
        return match;
    }
    ...
}
...
// Verify that the userName request parameter is alpha-numeric
String userName = request.getParameter("userName");
if (Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    // userName is valid, continue processing request
    ...
}
```

Java 1.4 には、新しく正規表現パッケージ (java.util.regex) が導入されています。新しい Java 1.4 の正規表現パッケージを使用した Validator.matchPattern の変更バージョンは以下のようになります。

```
// Example to validate that a given value matches a specified pattern
// using the Java 1.4 regular expression package
import java.util.regex.Pattern;
import java.util.regexe.Matcher;
public Class Validator {
    ...
    public static boolean matchPattern(String value, String expression) {
        boolean match = false;
        if (validateRequired(expression)) {
        match = Pattern.matches(expression, value);
        }
        return match;
    }
    ...
}
```

[7] Cookie の値
Cookie の値を検証するために javax.servlet.http.Cookie オブジェクトを使用してください。アプリケーションの仕様に応じて、(上記と) 同じ検証規則 (要求された値の検証や長さの検証など) が Cookie の値にも適用されます。
要求された Cookie の値を検証する例です。

```
// Example to validate a required cookie value
// First retrieve all available cookies submitted in the HTTP request
Cookie[] cookies = request.getCookies();
if (cookies != null) {
    // find the "user" cookie
    for (int i=0; i<cookies.length; ++i) {
        if (cookies[i].getName().equals("user")) {
        // validate the cookie value
        if (Validator.validateRequired(cookies[i].getValue()) {
        // valid cookie value, continue processing request
        ...
        }
        }
    }
}
```

[8] HTTP 応答
[8-1] ユーザー入力のフィルタリング
クロスサイト・スクリプティングからアプリケーションを保護するには、危険な文字を対応する文字エンティティーに変換して、HTML をサニタイズします。HTML で危険な文字は次のとおりです。
< > " ' % ;) (& +

危険な文字を対応する文字エンティティーに変換して、指定された文字列をフィルタリングする例は次のとおりです。

```
// Example to filter sensitive data to prevent cross-site scripting
public Class Validator {
    ...
    public static String filter(String value) {
        if (value == null) {
        return null;
        }
        StringBuffer result = new StringBuffer(value.length());
        for (int i=0; i<value.length(); ++i) {
        switch (value.charAt(i)) {
        case '<':
        result.append("&lt;");
        break;
        case '>':
        result.append("&gt;");
        break;
        case '"':
        result.append("&quot;");
        break;
        case '\'':
        result.append("&#39;");
        break;
        case '%':
        result.append("&#37;");
        break;
        case ';':
        result.append("&#59;");
        break;
        case '(':
        result.append("&#40;");
        break;
        case ')':
```

```
            result.append("&#41;");
            break;
            case '&':
            result.append("&amp;");
            break;
            case '+':
            result.append("&#43;");
            break;
            default:
            result.append(value.charAt(i));
            break;
            }
            return result;
        }
        ...
    }
    ...
    // Filter the HTTP response using Validator.filter
    PrintWriter out = response.getWriter();
    // set output response
    out.write(Validator.filter(response));
    out.close();
```

Java Servlet API 2.3 にはフィルターが導入されており、HTTP 要求または応答をインターセプトして変換する機能をサポートしています。

Validator.filter を使用して応答をサニタイズする Servlet フィルターの使用例は次のとおりです。

```
    // Example to filter all sensitive characters in the HTTP response using a Java Filter.
    // This example is for illustration purposes since it will filter all content in the response, including
HTML tags!
    public class SensitiveCharsFilter implements Filter {
        ...
        public void doFilter(ServletRequest request,
            ServletResponse response,
            FilterChain chain)
            throws IOException, ServletException {

            PrintWriter out = response.getWriter();
            ResponseWrapper wrapper = new ResponseWrapper((HttpServletResponse)response);
            chain.doFilter(request, wrapper);

            CharArrayWriter caw = new CharArrayWriter();
            caw.write(Validator.filter(wrapper.toString()));

            response.setContentType("text/html");
            response.setContentLength(caw.toString().length());
            out.write(caw.toString());
            out.close();
        }
        ...
        public class CharResponseWrapper extends HttpServletResponseWrapper {
            private CharArrayWriter output;

            public String toString() {
            return output.toString();
            }

            public CharResponseWrapper(HttpServletResponse response){
            super(response);
            output = new CharArrayWriter();
            }

            public PrintWriter getWriter(){
            return new PrintWriter(output);
            }
        }
    }

    }
```

[8-2] Cookie のセキュリティー保護
Cookie に機密データを保存する場合、HTTPS や SSL などの安全なプロトコルを利用して Cookie が送信されるようにブラウザーに指示するために、Cookie.setSecure(boolean flag) を使用して HTTP 応答の Cookie のセキュリティー・フラグが設定されるようにしてください。

「user」の Cookie をセキュリティー保護する例は次のとおりです。

```
// Example to secure a cookie, i.e. instruct the browser to
// send the cookie using a secure protocol
Cookie cookie = new Cookie("user", "sensitive");
cookie.setSecure(true);
response.addCookie(cookie);
```

推奨される JAVA ツール: サーバー側で検証を行う Java フレームワークは主に次の 2 つです。
[1] Jakarta Commons Validator (Struts 1.1 と統合)Jakarta Commons Validator は、上記のデータ検証仕様をすべて実装する強力なフレームワークです。これらの規則は、フォーム・フィールドの入力認証規則を定義する XML ファイルで構成されています。Struts の [bean:write] タグを使用することで、記述された全データに対する [8] HTTP 応答の危険な文字の出力フィルタリングを Struts がデフォルトでサポートしています。このフィルタリングは、「filter=false」フラグを設定することにより無効にできます。

Struts は次の基本的な入力検証を定義しますが、カスタム検証が定義される場合もあります。
required: フィールドに空白以外の文字が含まれている場合に成功します。
mask: 値がマスク属性によって与えられた正規表現に一致する場合に成功します。
range: 値が min 属性および max 属性により与えられた値 ((value >= min) および (value <= max)) の範囲内である場合に成功します。
maxLength: フィールドの長さが max 属性以下である場合に成功します。
minLength: フィールドの長さが min 属性以上である場合に成功します。
byte、short、integer、long、float、double: 値を対応するプリミティブ型に変換できる場合に成功します。
date: 値が有効な日付を示す場合に成功します。日付のパターンを指定することも可能です。
creditCard: 値が有効なクレジット・カードの番号である場合に成功します。
e-mail: 値が有効な電子メール・アドレスである場合に成功します。

次に、Struts Validator を使用して、loginForm の userName フィールドを検証する例を示します。

```
<form-validation>
    <global>
        ...
        <validator name="required"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateRequired"
        msg="errors.required">
        </validator>
        <validator name="mask"
        classname="org.apache.struts.validator.FieldChecks"
        method="validateMask"
        msg="errors.invalid">
        </validator>
        ...
    </global>
    <formset>
        <form name="loginForm">
        <!-- userName is required and is alpha-numeric case insensitive -->
        <field property="userName" depends="required,mask">
        <!-- message resource key to display if validation fails -->
        <msg name="mask" key="login.userName.maskmsg"/>
        <arg0 key="login.userName.displayname"/>
        <var>
```

```
            <var-name>mask</var-name>
            <var-value>^[a-zA-Z0-9]*$</var-value>
            </var>
            </field>
            ...
            </form>
            ...
        </formset>
    </form-validation>
```

[2] JavaServer Faces Technology: JavaServer Faces Technology は、UI コンポーネントの表現、各コンポーネントの状態の管理、イベントの処理および入力の検証を行う、一連の Java API (JSR 127) です。

JavaServer Faces API は次の基本的な検証を実装しますが、カスタム検証も定義される場合があります。
validate_doublerange: コンポーネントの DoubleRangeValidator を登録します。
validate_length: コンポーネントの LengthValidator を登録します。
validate_longrange: コンポーネントの LongRangeValidator を登録します。
validate_required: コンポーネントの RequiredValidator を登録します。
validate_stringrange: コンポーネントの StringRangeValidator を登録します。
validator: コンポーネントのカスタムの Validator を登録します。

JavaServer Faces API は、次の UIInput および UIOutput Renderer (Tag) を定義します。
input_date: java.text.Date インスタンスでフォーマットされた java.util.Date を受け取ります。
output_date: java.text.Date インスタンスでフォーマットされた java.util.Date を表示します。
input_datetime: java.text.DateTime インスタンスでフォーマットされた java.util.Date を受け取ります。
output_datetime: java.text.DateTime インスタンスでフォーマットされた java.util.Date を表示します。
input_number: java.text.NumberFormat でフォーマットされた数値データ型 (java.lang.Number またはプリミティブ型) を表示します。
output_number: java.text.NumberFormat でフォーマットされた数値データ型 (java.lang.Number またはプリミティブ型) を表示します。
input_text: 1 行の文字列を受け取ります。
output_text: 1 行の文字列を表示します。
input_time: java.text.DateFormat タイム・インスタンスでフォーマットされた java.util.Date を受け取ります。
output_time: java.text.DateFormat タイム・インスタンスでフォーマットされた java.util.Date を表示します。
input_hidden: ページの作成者がページで hidden 変数を使用することを許可します。
input_secret: 空白なしの 1 行のテキストを受け取り、入力の度にアスタリスクのセットとして表示します。
input_textarea: 複数行のテキストを受け取ります。
output_errors: ページ全体のエラー・メッセージまたは指定のクライアント識別子に関連するエラー・メッセージを表示します。
output_label: ネストされたコンポーネントを指定インプット・フィールドのラベルとして表示します。
output_message: 配置されたメッセージを表示します。

次に、JavaServer Faces を使用して、loginForm の userName フィールドを検証する例を示します。

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
  <h:form formName="loginForm" >
    <h:input_text id="userName" size="20" modelReference="UserBean.userName">
        <f:validate_required/>
        <f:validate_length minimum="8" maximum="20"/>
    </h:input_text>
    <!-- display errors if present -->
    <h:output_errors id="loginErrors" clientId="userName"/>
    <h:command_button id="submit" label="Submit" commandName="submit" /><p>
  </h:form>
</f:use_faces>
```

参照リンク:
Java API 1.3 -
http://java.sun.com/j2se/1.3/docs/api/
Java API 1.4 -
http://java.sun.com/j2se/1.4/docs/api/
Java Servlet API 2.3 -
http://java.sun.com/products/servlet/2.3/javadoc/
Java Regular Expression Package -
http://jakarta.apache.org/regexp/
Jakarta Validator -
http://jakarta.apache.org/commons/validator/
JavaServer Faces Technology -
http://java.sun.com/j2ee/javaserverfaces/

** エラーの処理:

多くの J2EE Web アプリケーション・アーキテクチャーは Model View Controller (MVC) パターンに準拠しています。このパターンでは、Servlet は Controller として動作します。Servlet はアプリケーションの処理を EJB Session Bean (Model) のような JavaBean に委託します。次に、Servlet は要求を JSP (View) に転送して、処理の結果をレンダリングします。必要な処理が実際に行われたことを確認するために、Servlet はすべての入力、出力、リターン・コード、エラー・コード、および既知の例外をチェックする必要があります。

データの検証は悪意のあるデータの改ざんからアプリケーションを保護することはできますが、アプリケーションが内部的なエラー・メッセージ (例外スタック・トレースなど) を不注意で公開するような状況を防ぐには、適切なエラー処理を実行するための方策が必要です。適切なエラー処理の方策を立てる際には、次の点に注意します。

[1] エラーの定義
[2] エラーの報告
[3] エラーのレンダリング
[4] エラーのマッピング

[1] エラーの定義
アプリケーション・レイヤー (Servlet など) でのハード・コーディングされたエラー・メッセージは避けてください。アプリケーションには既知のアプリケーション障害にマップするエラー・キーを使用するようにしてください。効果的な方法は、HTML フォーム・フィールドや他の Bean プロパティーの検証規則にマップするエラー・キーを定義することです。例えば「user_name」フィールドが必須フィールドであり、このフィールドには英数字を入力する必要があり、さらにデータベース内で他に同じ名前が存在してはならない場合は、次のようなエラー・キーを定義します。

(a) ERROR_USERNAME_REQUIRED: このエラー・キーを使用すると、「user_name」フィールドが必須フィールドであることをユーザーに通知するメッセージが表示されます。
(b) ERROR_USERNAME_ALPHANUMERIC: このエラー・キーを使用すると、「user_name」フィールドの値が英数字でなければならないことをユーザーに通知するメッセージが表示されます。
(c) ERROR_USERNAME_DUPLICATE: このエラー・キーを使用すると、「user_name」の値がデータベース内で重複していることをユーザーに通知するメッセージが表示されます。
(d) ERROR_USERNAME_INVALID: このエラー・キーを使用すると、「user_name」の値が無効であることをユーザーに通知する一般的なメッセージが表示されます。
効果的な方法は、アプリケーション・エラーを格納および報告するために使用する、次のようなフレームワーク Java クラスを定義することです。
- ErrorKeys: すべてのエラー・キーを定義します。

```
// Example: ErrorKeys defining the following error keys:
//    - ERROR_USERNAME_REQUIRED
//    - ERROR_USERNAME_ALPHANUMERIC
//    - ERROR_USERNAME_DUPLICATE
//    - ERROR_USERNAME_INVALID
//    ...
public Class ErrorKeys {
    public static final String ERROR_USERNAME_REQUIRED = "error.username.required";
    public static final String ERROR_USERNAME_ALPHANUMERIC = "error.username.alphanumeric";
    public static final String ERROR_USERNAME_DUPLICATE = "error.username.duplicate";
```

```
    public static final String ERROR_USERNAME_INVALID = "error.username.invalid";
    ...
}
```

- Error: 個々のエラーをカプセル化します。

```
// Example: Error encapsulates an error key.
// Error is serializable to support code executing in multiple JVMs.
public Class Error implements Serializable {

    // Constructor given a specified error key
    public Error(String key) {
    this(key, null);
    }

    // Constructor given a specified error key and array of placeholder objects
    public Error(String key, Object[] values) {
    this.key = key;
    this.values = values;
    }

    // Returns the error key
    public String getKey() {
    return this.key;
    }

    // Returns the placeholder values
    public Object[] getValues() {
    return this.values;
    }

    private String key = null;
    private Object[] values = null;
}
```

- Errors: エラーの集合をカプセル化します。

```
// Example: Errors encapsulates the Error objects being reported to the presentation layer.
// Errors are stored in a HashMap where the key is the bean property name and value is an
// ArrayList of Error objects.
public Class Errors implements Serializable {

    // Adds an Error object to the Collection of errors for the specified bean property.
    public void addError(String property, Error error) {
    ArrayList propertyErrors = (ArrayList)errors.get(property);
    if (propertyErrors == null) {
    propertyErrors = new ArrayList();
    errors.put(property, propertyErrors);
    }
    propertyErrors.put(error);
    }

    // Returns true if there are any errors
    public boolean hasErrors() {
    return (errors.size > 0);
    }

    // Returns the Errors for the specified property
    public ArrayList getErrors(String property) {
    return (ArrayList)errors.get(property);
    }

    private HashMap errors = new HashMap();
}
```

次に、上記フレームワーク・クラスを使用して、「user_name」フィールドの検証エラーを処理する例を示します。

```
// Example to process validation errors of the "user_name" field.
Errors errors = new Errors();
String userName = request.getParameter("user_name");
// (a) Required validation rule
if (!Validator.validateRequired(userName)) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_REQUIRED));
} // (b) Alpha-numeric validation rule
else if (!Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) {
    errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_ALPHANUMERIC));
}
else
{
    // (c) Duplicate check validation rule
    // We assume that there is an existing UserValidationEJB session bean that implements
    // a checkIfDuplicate() method to verify if the user already exists in the database.
    try {
        ...
        if (UserValidationEJB.checkIfDuplicate(userName)) {
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE));
        }
    } catch (RemoteException e) {
        // log the error
        logger.error("Could not validate user for specified userName: " + userName);
        errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE);
    }
}
// set the errors object in a request attribute called "errors"
request.setAttribute("errors", errors);
...
```

[2] エラーの報告
Web 層のアプリケーション・エラーを報告する方法は 2 つあります。
(a) Servlet エラー・メカニズム
(b) JSP エラー・メカニズム

[2-a] Servlet エラー・メカニズム
　Servlet は次の方法のいずれかでエラーを報告します。
- 入力 JSP へ転送する (すでにエラーを要求属性に格納している)
- HTTP エラー・コードを引数として response.sendError を呼び出す
- 例外をスローする

効果的な方法は、既知のアプリケーション・エラー (セクション [1] を参照) をすべて処理し、要求属性にそれらを格納し、入力 JSP に転送することです。入力 JSP はエラー・メッセージを表示して、ユーザーにデータを入力し直すように促す必要があります。次に、入力 JSP (userInput.jsp) に転送する例を示します。

```
// Example to forward to the userInput.jsp following user validation errors
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd != null) {
    rd.forward(request, response);
}
```

Servlet が既知の JSP ページに転送できない場合、2 番目の選択肢は、

HttpServletResponse.SC_INTERNAL_SERVER_ERROR (状態コード 500) を引数として response.sendError メソッドを呼び出す方法です。さまざまな HTTP 状態コードの詳細については、javax.servlet.http.HttpServletResponse の javadoc を参照してください。次に、HTTP エラーを返す例を示します。

```
// Example to return a HTTP error code
RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp");
if (rd == null) {
    // messages is a resource bundle with all message keys and values
    response.sendError(HttpServletResponse.SC_INTERNAL_SERVER_ERROR,
        messages.getMessage(ErrorKeys.ERROR_USERNAME_INVALID));
}
```

最後の手段として、Servlet は例外をスローすることができます。この例外は、次のクラスのうちの 1 つのサブクラスである必要があります。
- RuntimeException
- ServletException
- IOException

[2-b] JSP エラー・メカニズム: JSP ページには、次の例のように errorPage ディレクティブを定義して、実行時例外を処理する機能があります。

```
<%@ page errorPage="/errors/userValidation.jsp" %>
```

エラー・トラップできない JSP の例外は指定された errorPage に転送され、オリジナルの例外は javax.servlet.jsp.jspException と呼ばれる要求パラメーターとして設定されます。エラー・ページは、次のように isErrorPage ディレクティブを含む必要があります。

```
<%@ page isErrorPage="true" %>
```

isErrorPage ディレクティブが指定されると、「exception」変数はスローされる例外オブジェクトに初期化されます。

[3] エラーのレンダリング
J2SE Internationalization API は、アプリケーション・リソースを外部化し、メッセージをフォーマットする次のようなユーティリティー・クラスを提供します。

(a) リソース・バンドル
(b) メッセージ・フォーマット

[3-a] リソース・バンドル
リソース・バンドルは、ローカライズされたデータとそれを使用するソース・コードを分離することによって国際化対応をサポートします。各リソース・バンドルは、特定のロケールに対するキーと値のペアのマッピングを格納しています。

通常は java.util.PropertyResourceBundle を使用または拡張して、外部プロパティー・ファイルにコンテンツを格納します。次に例を示します。

```
################################################
```

```
# ErrorMessages.properties
##############################################
# required user name error message
error.username.required=User name field is required

# invalid user name format
error.username.alphanumeric=User name must be alphanumeric

# duplicate user name error message
error.username.duplicate=User name {0} already exists, please choose another one

...
```

異なるロケールをサポートするために、複数のリソースを定義できます (これが「リソース・バンドル」という名前の由来)。例えば、バンドル・ファミリーのフランス語をサポートするために ErrorMessages_fr.properties を定義できます。要求されたロケールのリソースが存在しない場合は、デフォルトのメンバーが使用されます。上記例では、デフォルトのリソースは ErrorMessages.properties です。アプリケーション (JSP または Servlet) はユーザーのロケールに従って適切なリソースからコンテンツを取得します。

[3-b] メッセージ・フォーマット
J2SE 標準クラス java.util.MessageFormat は、置換プレースホルダー付きのメッセージを作成する一般的な方法です。MessageFormat オブジェクトは、次のような書式指示子が埋め込まれたパターン文字列を持っています。

```
// Example to show how to format a message using placeholder parameters
String pattern = "User name {0} already exists, please choose another one";
String userName = request.getParameter("user_name");
Object[] args = new Object[1];
args[0] = userName;
String message = MessageFormat.format(pattern, args);
```

次に、より理解しやすい例として、ResourceBundle と MessageFormat を使用してエラー・メッセージを表示する例を示します。

```
// Example to render an error message from a localized ErrorMessages resource (properties file)
// Utility class to retrieve locale-specific error messages
public Class ErrorMessageResource {

    // Returns the error message for the specified error key in the environment locale
    public String getErrorMessage(String errorKey) {
        return getErrorMessage(errorKey, defaultLocale);
    }

    // Returns the error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Locale locale) {
        return getErrorMessage(errorKey, null, locale);
    }

    // Returns a formatted error message for the specified error key in the specified locale
    public String getErrorMessage(String errorKey, Object[] args, Locale locale) {
        // Get localized ErrorMessageResource
        ResourceBundle errorMessageResource = ResourceBundle.getBundle("ErrorMessages", locale);
        // Get localized error message
        String errorMessage = errorMessageResource.getString(errorKey);
        if (args != null) {
        // Format the message using the specified placeholders args
        return MessageFormat.format(errorMessage, args);
        } else {
        return errorMessage;
        }
    }
```

```
        // default environment locale
        private Locale defaultLocale = Locale.getDefaultLocale();
    }
    ...
    // Get the user's locale
    Locale userLocale = request.getLocale();
    // Check if there were any validation errors
    Errors errors = (Errors)request.getAttribute("errors");
    if (errors != null && errors.hasErrors()) {
        // iterate through errors and output error messages corresponding to the "user_name" property
        ArrayList userNameErrors = errors.getErrors("user_name");
        ListIterator iterator = userNameErrors.iterator();
        while (iterator.hasNext()) {
            // Get the next error object
            Error error = (Error)iterator.next();
            String errorMessage = ErrorMessageResource.getErrorMessage(error.getKey(), userLocale);
            output.write(errorMessage + "\r\n");
        }
    }
```

上記例のようにエラー・メッセージを何度も表示する場合は、独自の JSP タグ (displayErrors 等) を定義することが推奨されます。

[4] エラーのマッピング
通常 Servlet Containerは、応答状態コードまたは例外のどちらかに対応するデフォルトのエラー・ページを返します。状態コードまたは例外と Web リソースとのマッピングは、カスタム・エラー・ページを使用して指定できます。効果的な方法は、内部のエラーの状態を公開しない静的なエラー・ページを開発することです (デフォルトでは、ほとんどの Servlet コンテナーは内部エラー・メッセージを報告します)。このマッピングは、次の例のように、Web Deployment Descriptor (web.xml) で設定されます。

```
    <!-- Mapping of HTTP error codes and application exceptions to error pages -->
    <error-page>
      <exception-type>UserValidationException</exception-type>
      <location>/errors/validationError.html</error-page>
    </error-page>
    <error-page>
      <error-code>500</exception-type>
      <location>/errors/internalError.html</error-page>
    </error-page>
    <error-page>
    ...
    </error-page>
    ...
```

推奨される JAVA ツール: サーバー側で検証を行う Java フレームワークは主に次の 2 つです。
[1] Jakarta Commons Validator (Struts 1.1 と統合)[1] Jakarta Commons Validator (Struts 1.1 と統合):
Jakarta Commons Validator は、上記のようなエラー処理メカニズムを定義する Java フレームワークです。検証規則は、フォーム・フィールドの入力検証規則とそれに対応する検証エラー・キーを定義する XML ファイルとして設定されます。Struts は、リソース・バンドルとメッセージ・フォーマットを使用してローカライズ・アプリケーションを構築するための国際化対応をサポートします。

次に、Struts Validator を使用して、loginForm の userName フィールドを検証する例を示します。

```
    <form-validation>
        <global>
            ...
            <validator name="required"
            classname="org.apache.struts.validator.FieldChecks"
            method="validateRequired"
```

```
            msg="errors.required">
            </validator>
            <validator name="mask"
            classname="org.apache.struts.validator.FieldChecks"
            method="validateMask"
            msg="errors.invalid">
            </validator>
            ...
        </global>
        <formset>
            <form name="loginForm">
            <!-- userName is required and is alpha-numeric case insensitive -->
            <field property="userName" depends="required,mask">
            <!-- message resource key to display if validation fails -->
            <msg name="mask" key="login.userName.maskmsg"/>
            <arg0 key="login.userName.displayname"/>
            <var>
            <var-name>mask</var-name>
            <var-value>^[a-zA-Z0-9]*$</var-value>
            </var>
            </field>
            ...
            </form>
            ...
        </formset>
    </form-validation>
```

次の例に示すように、Struts JSP タグ・ライブラリーは、格納されたエラー・メッセージを条件付きで表示する「errors」タグを定義します。

```
    <%@ page language="java" %>
    <%@ taglib uri="/WEB-INF/struts-html.tld" prefix="html" %>
    <%@ taglib uri="/WEB-INF/struts-bean.tld" prefix="bean" %>
    <html:html>
    <head>
    <body>
        <html:form action="/logon.do">
        <table border="0" width="100%">
        <tr>
            <th align="right">
            <html:errors property="username"/>
            <bean:message key="prompt.username"/>
            </th>
            <td align="left">
            <html:text property="username" size="16"/>
            </td>
        </tr>
        <tr>
        <td align="right">
            <html:submit><bean:message key="button.submit"/></html:submit>
        </td>
        <td align="right">
            <html:reset><bean:message key="button.reset"/></html:reset>
        </td>
        </tr>
        </table>
        </html:form>
    </body>
    </html:html>
```

[2] JavaServer Faces Technology
JavaServer Faces Technology は、UI コンポーネントの表現、各コンポーネントの状態の管理、イベントの処理、入力の検証、および国際化対応のサポートを行う、一連の Java API (JSR 127) です。

JavaServer Faces API は「output_errors」という UIOutput Renderer を定義します。それはページ全体のエラー・メッセージまたは指定されたクライアント識別子に関連するエラー・メッセージを表示します。

次に、JavaServer Faces を使用して、loginForm の userName フィールドを検証する例を示します。

```
<%@ taglib uri="http://java.sun.com/jsf/html" prefix="h" %>
<%@ taglib uri="http://java.sun.com/jsf/core" prefix="f" %>
...
<jsp:useBean id="UserBean"
    class="myApplication.UserBean" scope="session" />
<f:use_faces>
  <h:form formName="loginForm" >
    <h:input_text id="userName" size="20" modelReference="UserBean.userName">
        <f:validate_required/>
        <f:validate_length minimum="8" maximum="20"/>
    </h:input_text>
    <!-- display errors if present -->
    <h:output_errors id="loginErrors" clientId="userName"/>
    <h:command_button id="submit" label="Submit" commandName="submit" /><p>
  </h:form>
</f:use_faces>
```

参照リンク:
Java API 1.3 -
http://java.sun.com/j2se/1.3/docs/api/
Java API 1.4 -
http://java.sun.com/j2se/1.4/docs/api/
Java Servlet API 2.3 -
http://java.sun.com/products/servlet/2.3/javadoc/
Java Regular Expression Package -
http://jakarta.apache.org/regexp/
Jakarta Validator -
http://jakarta.apache.org/commons/validator/
JavaServer Faces Technology -
http://java.sun.com/j2ee/javaserverfaces/

PHP

** 入力データの検証

データ検証は、ユーザーの利便性のためにクライアント層で行うこともできますが、必ずサーバー層で行う必要があります。クライアント側のデータ検証は、例えば Javascript を無効にすることによって簡単にバイパスできるため、本質的に安全ではありません。

一般的には、次の項目を検証するサーバー側ユーティリティー・ルーチンを提供する Web アプリケーション・フレームワークが理想とされます。
[1] 必須フィールド
[2] フィールドのデータ型 (デフォルトでは、HTTP 要求パラメーターはすべて String)
[3] フィールドの長さ
[4] フィールドの範囲
[5] フィールドのオプション
[6] フィールドのパターン
[7] Cookie の値
[8] HTTP 応答

効果的な方法は、各アプリケーション・パラメーターを検証する関数を実装することです。以下のセクションでは、チェックの例について示しています。

[1] 必須フィールド
常に、フィールドが Null でなく、前後の空白スペースを除いて、その長さがゼロより大きいことをチェックします。

次に、要求されたフィールドを検証する例を示します。

```
// PHP example to validate required fields
function validateRequired($input) {
    ...
    $pass = false;
    if (strlen(trim($input))>0){
        $pass = true;
    }
    return $pass;
    ...
}
...
if (validateRequired($fieldName)) {
    // fieldName is valid, continue processing request
    ...
}
```

[2] フィールドのデータ型: Web アプリケーションでは、入力パラメーターの型は多くありません。例えば、HTTP 要求パラメーターや Cookie の値はすべて String 型です。開発者は入力のデータ型が正しいかどうかを確認する必要があります。

[3] フィールドの長さ: 常に、入力パラメーター (HTTP 要求パラメーターまたは Cookie 値のどちらか) の長さが最小値から最大値までの間であることを確認します。

[4] フィールドの範囲: 常に、入力パラメーターが関数の要件で定義された範囲内であることを確認します。

[5] フィールドのオプション: 多くの場合 Web アプリケーションはユーザーに対して一連のオプションを提示して、ユーザーにそのいずれかを選択するよう促しますが (例えば SELECT HTML タグを使用するなどして)、選択された値が使用可能なオプションのいずれかであるかどうかをサーバー側で検証を実行して確認することはできません。悪意のあるユーザーが任意のオプションの値を簡単に変更できることに注意してください。選択されたユーザーの値が、関数の仕様で定義されている許可されたオプションであることを必ず検証してください。

[6] フィールドのパターン: 関数の仕様で定義されるように、ユーザーの入力がパターンに一致していることを常にチェックしてください。例えば、userName フィールドが大文字小文字を区別せずに英数字のみ許可している場合、次の正規表現を使用します:
^[a-zA-Z0-9]+$

[7] Cookie の値: アプリケーションの仕様に応じて、(上記と) 同じ検証規則 (要求された値の検証や長さの検証など) が Cookie の値にも適用されます。

[8] HTTP 応答

[8-1] ユーザー入力のフィルタリング: クロスサイト・スクリプティングからアプリケーションを保護するには、開発者が、危険な文字を対応する文字エンティティーに変換して HTML をサニタイズする必要があります。HTML で危険な文字は次のとおりです。
< > " ' % ;) (& +

PHP には、htmlentities() などの自動サニタイズ・ユーティリティー関数がいくつかあります。

```
$input = htmlentities($input, ENT_QUOTES, 'UTF-8');
```

さらに、クロスサイト・スクリプティングの UTF-7 バリアントを防止するために、明示的に応答の Content-Type ヘッダーを定義します。以下の例を参照してください。

```
<?php

header('Content-Type: text/html; charset=UTF-8');

?>
```

[8-2] Cookie のセキュリティー保護

秘密データを Cookie に格納して SSL を介して転送するときには、まず HTTP 応答に Cookie のセキュリティー・フラグを設定します。これによって、SSL 接続ではこの Cookie のみを使用するようにブラウザーに指示します。

Cookie のセキュリティーを保つ方法については、以下のコード例を使用することができます。

```
<$php

    $value = "some_value";
    $time = time()+3600;
    $path = "/application/";
    $domain = ".example.com";
    $secure = 1;

    setcookie("CookieName", $value, $time, $path, $domain, $secure, TRUE);
?>
```

さらに、HttpOnly フラグを使用することをお勧めします。HttpOnly フラグが TRUE に設定されているとき、Cookie は HTTP プロトコルでのみアクセスできるようになっています。つまり、この Cookie は JavaScript のようなスクリプト言語ではアクセスできなくなります。この設定によって、XSS 攻撃による ID の盗用を効果的に減殺することができます (ただしすべてのブラウザーがサポートしている訳ではありません)。

HttpOnly フラグは PHP 5.2.0 で追加されました。

参照リンク:

[1] HTTP-only Cookies によるクロスサイト・スクリプティングの防止:
http://msdn2.microsoft.com/en-us/library/ms533046.aspx
[2] PHP セキュリティー・コンソーシアム:
http://phpsec.org/
[3] PHP & Web アプリケーション・セキュリティー・ブログ (Chris Shiflett):
http://shiflett.org/

低 ビジネスおよびセキュリティー・ロジックをクライアント側から削除します TOC

このタスクで修正される問題のタイプ

- クライアント側 (JavaScript) Cookie 参照

全般

[1] ビジネス/セキュリティーのロジックをクライアント側に配置しないようにします。[2] サイトにセキュリティー上の脅威を与える可能性のある、セキュリティーで保護されていないクライアント側の Java スクリプトを見つけて削除します。

低 仮想ディレクトリーから古いバージョンのファイルを削除します TOC

このタスクで修正される問題のタイプ

- 一時ファイルのダウンロード

全般

仮想 Web サーバーのルートにバックアップ・バージョンまたは一時バージョンのファイルを保管しないでください。エディターを使用して「その場」でこれらのファイルを編集すると、このような状況が発生しがちです。サイトを更新するときには、これらのファイルを仮想ルート以外のディレクトリーに移すかコピーし、そこで編集してから仮想ルートに戻してください。仮想ルートの下には、実際に使用されるファイルのみが存在するようにします。

低 禁止されているリソースについて「404 - Not Found」レスポンス・ステータス・コードを送出するか、完全に削除します TOC

このタスクで修正される問題のタイプ

- 非表示のディレクトリーを検出

全般

禁止されているリソースが必要でない場合には、サイトから削除します。可能であれば、「403 - Forbidden」の代わりに「404 - Not Found」レスポンス・ステータス・コードを返すようにします。この変更によって、サイト内のディレクトリーの存在をわかりにくくし、サイトの構造が公開されるのを防止します。

低 秘密のセッション情報をパーマネント Cookie に保存しないようにします TOC

このタスクで修正される問題のタイプ

- 秘密セッション情報を含むパーマネント Cookie

全般

ユーザー資格情報またはセッション・トークンなどの機密性の高いセッション情報が、非パーマネント Cookie (RAM Cookie) にのみ保存されることを確認してください。パーマネント Cookie に保存されないようにするには、Cookie の「Expires」フィールドを設定しないでおきます。

アドバイザリー

クロスサイト・スクリプティング

TOC

テスト・タイプ:
アプリケーション・レベル・テスト

脅威の分類:
クロスサイト・スクリプティング

原因:
ユーザーの入力内容に対する有害文字の除去が適切に行われませんでした

セキュリティー・リスク:
ハッカーが正規のユーザーになりすまし、ユーザーのレコードを表示または改変したり、ユーザーとしてトランザクションを実行するのに使用することができる、カスタマー・セッションおよび Cookie を盗み出したり操作することができる可能性があります

影響を受ける製品:

CWE:
79

X-Force:
6784

参考資料:
CERT アドバイザリー CA-2000-02
Microsoft How To: Prevent Cross-Site Scripting Security Issues (Q252985)
Microsoft How To: Prevent Cross-Site Scripting in ASP.NET
Microsoft How To: Protect From Injection Attacks in ASP.NET
Microsoft How To: Use Regular Expressions to Constrain Input in ASP.NET
Microsoft .NET Anti-Cross Site Scripting Library
クロスサイト・スクリプティング研修モジュール

技術的な説明:
ユーザー制御可能な入力が、Web ページとして使用される出力に組み込まれる前にアプリケーションによって正しく無効化されていないことが AppScan で検出されました。

これは、クロスサイト・スクリプティング攻撃に利用されるおそれがあります。
クロスサイト・スクリプティング (XSS) の脆弱性は、以下の状況で発生します。
[1] 信頼されないデータが Web アプリケーションに取り込まれる (通常は Web 要求から)。
[2] 信頼されないデータが含まれた Web ページが Web アプリケーションから動的に生成される。
[3] ページ生成時に、Web ブラウザーで実行できるコンテンツ (JavaScript、HTML タグ、HTML 属性、マウス・イベント、Flash、ActiveX など) がデータに組み込まれることがアプリケーション側で阻止されない。
[4] 被攻撃者が、生成された Web ページ (信頼されないデータを使用してインジェクションされた悪質なスクリプトを含む) に Web ブラウザーからアクセスする。
[5] スクリプトが、Web サーバーから送られてきた Web ページに由来するスクリプトであるため、被攻撃者の Web ブラウザーによって、Web サーバーのドメインのコンテキストで悪質なスクリプトが実行される。
[6] 事実上、Web ブラウザーの同一生成元ポリシー (あるドメイン内のスクリプトが別のドメインにおいてリソースにアクセスしたりコードを実行したりできてはならないことが述べられている) の趣旨に対する違反がある。
悪質なスクリプトがインジェクションされると、攻撃者は多くの悪質なアクティビティーを実行できるようになります。
攻撃者は、セッション情報が含まれていると考えられる Cookie など、私的情報を被攻撃者のマシンから自分の手元に転送できます。
攻撃者は、被攻撃者になりすまして悪質な要求を Web サイトに送信できます (このような状況は、そのサイトを管理する管理者特権が被攻撃者にある場合に、そのサイトにとって特に危険となる可能性があります)。
攻撃者はフィッシング攻撃を使用して、信頼されている Web サイトを模倣し、被攻撃者を騙してパスワードを入力させることができます。
そうすることで、攻撃者は本物の Web サイト上で被攻撃者のアカウントを悪用できるようになります。
さらに、スクリプトによって Web ブラウザー自体の脆弱性が悪用される場合もあります。
場合によっては、被攻撃者のマシンが乗っ取られることもあります (これは「ドライブ・バイ・ハッキング」と呼ばれることがあります)。
XSS には大きく分けて 3 つのタイプがあります。

タイプ 1: 折り返し型 XSS (「非持続型」とも呼ばれる)
サーバーは HTTP 要求から直接、データを読み取り、HTTP 応答にそのデータを反映します。
折り返し型 XSS 攻撃の場合、攻撃者は被攻撃者が脆弱な Web アプリケーションへ危険なコンテンツを送るように仕向けます。
その後、そのコンテンツが被攻撃者に折り返されて、Web ブラウザーで実行されます。
悪質なコンテンツを送信するメカニズムとして最も一般的なものは、公式に掲示された URL に悪質なコンテンツをパラメーターとして組み込んだり、
被攻撃者に直接、電子メールを送信したりする方法です。
この方法で構成された URL は、多くのフィッシング・スキームの根幹を成すものです。
これによって、攻撃者は、脆弱なサイトを指す URL にアクセスするように被攻撃者を誘導します。
攻撃者のコンテンツがサイトから被攻撃者に折り返されると、そのコンテンツが被攻撃者のブラウザーで実行されます。

タイプ 2: 蓄積型 XSS (「持続型」とも呼ばれる)
アプリケーションが、データベース、メッセージ・フォーラム、訪問者のログ、または信頼される他のデータ・ストアに、危険なデータを格納します。
次に、危険なデータがアプリケーションに読み込まれ、動的なコンテンツに組み込まれます。
攻撃者の観点から言えば、悪質なコンテンツをインジェクションする最適な場所は、多くのユーザー、または特に攻撃者の興味を引くユーザーに表示される場所の中です。
通常、攻撃者の興味を引くユーザーとは、アプリケーションにおいて高い特権を持つユーザー、すなわち攻撃者にとって価値のある機密データを扱うユーザーのことです。
このようなユーザーの 1 人が悪質なコンテンツを実行した場合、攻撃者は、このユーザーになりすまして特権操作を実行したり、
このユーザーが扱う機密データに対するアクセス権限を入手したりできるようになる可能性があります。
例えば、攻撃者がログ・メッセージに XSS をインジェクションしたとします。
その場合、管理者がログを表示したときに、ログ・メッセージが正しく処理されない可能性があります。

タイプ 0: DOM ベース XSS
DOM ベース XSS の場合、XSS をページにインジェクションする処理はクライアント側で行われます。
一方、他のタイプの場合、インジェクションはサーバー側で行われます。
通常、DOM ベース XSS では、サーバーで制御され、クライアントに送信される、信頼されるスクリプト (Javascript など) が使用されます。
このスクリプトは、ユーザーがフォームを送信する前にフォームに対してサニティー・チェックを実行するスクリプトです。
サーバーにあるスクリプトにより、ユーザー指定のデータが
処理されて Web ページに (動的 HTML を使用するなどして) インジェクションされると、DOM ベース XSS が使用可能になります。

以下の例は、応答でパラメーター値を返すスクリプトを示したものです。
このパラメーター値は GET 要求を使用してスクリプトに送信され、HTML に埋め込まれた応答で返されます。

```
[REQUEST]
GET /index.aspx?name=JSmith HTTP/1.1
```

```
[RESPONSE]
HTTP/1.1 200 OK
Server: SomeServer
Date: Sun, 01 Jan 2002 00:31:19 GMT
Content-Type: text/html
Accept-Ranges: bytes
Content-Length: 27

<HTML>
Hello JSmith
</HTML>
```

攻撃者がさらに攻撃を強める可能性があります。

```
[ATTACK REQUEST]
GET /index.aspx?name=>"'><script>alert('PWND')</script> HTTP/1.1
```

```
[ATTACK RESPONSE]
HTTP/1.1 200 OK
Server: SomeServer
Date: Sun, 01 Jan 2002 00:31:19 GMT
Content-Type: text/html
Accept-Ranges: bytes
Content-Length: 83

<HTML>
Hello >"'><script>alert('PWND')</script>
</HTML>
```

この場合、JavaScript コードがブラウザーで実行されます (>"'> の部分は、ここでは無関係です)。

ディレクトリーの一覧作成

TOC

テスト・タイプ:

インフラストラクチャー・テスト

脅威の分類:

ディレクトリー索引付け

原因:

ディレクトリー・ブラウジングが有効になっています

セキュリティー・リスク:

制限のかけられたファイルを含む可能性のある Web アプリケーションの仮想ディレクトリーの内容を、表示およびダウンロードすることができます

影響を受ける製品:

CWE:

548

X-Force:

52580

参考資料:

Apache directory listing (CAN-2001-0729)
Microsoft IIS 5.0+WebDav support - directory listing
Jrun directory listing
CERT アドバイザリー CA-98.04

技術的な説明:

***
別のディレクトリー一覧作成テストが同じリソース上で成功している場合、この問題は「脆弱ではない」として表示される場合があります。
***

Web サーバーは通常、スクリプトおよびテキストのコンテンツを格納しているディレクトリーの一覧作成を許可しないように設定されています。しかし、Web サーバーが正しく設定されていない場合には、ファイルではなく特定のディレクトリーに対してリクエストを送信することで、ディレクトリーの一覧を取得することができます。「some_dir」という名前のディレクトリーの一覧作成のリクエスト例:
http://TARGET/some_dir/

ディレクトリーの一覧を取得するもうひとつの方法として、Web サーバーにディレクトリーの内容一覧を強制的に返させる不正な HTTP リクエストである URL Trickery 攻撃のように、Web サーバーおよび Web アプリケーションの特定の問題を悪用する方法があります。これらのセキュリティーの欠陥は、お使いのアプリケーションまたはサービスのベンダーからパッチをダウンロードして、解決する必要があります。

Win32 オペレーティング・システム上で動作している一部の Web サーバーでは、短いファイル名 (8.3 DOS 形式) を使用することでアクセス・コントロールがバイパスされる場合があります。 たとえば、ディレクトリー /longdirname/ は Web サーバーによる閲覧が拒否されますが、その DOS 8.3 形式の記述である /LONGDI~1/ は閲覧することができます。

注: ディレクトリーの一覧は、通常は Web サイト上のリンクからは公開されない Web ディレクトリー内のファイルの場所を特定するために、攻撃者が使用します。秘密の情報を格納している可能性のある Web アプリケーションの設定ファイルおよびその他のコンポーネントを、この方法で閲覧することができます。

フレームからのフィッシング

TOC

テスト・タイプ:
アプリケーション・レベル・テスト

脅威の分類:
コンテンツ・スプーフィング

原因:
ユーザーの入力内容に対する有害文字の除去が適切に行われませんでした

セキュリティー・リスク:
知識の乏しいユーザーに、ユーザー名、パスワード、クレジット・カード番号、社会保険番号などの秘密情報を提供するように求めることができます

影響を受ける製品:

CWE:
79

X-Force:
52829

参考資料:
FTC Consumer Alert - 「How Not to Get Hooked by a 'Phishing' Scam」

技術的な説明:
フィッシングとは、攻撃者が正当な事業体になりすますソーシャル・エンジニアリング技法のことです。攻撃者はこの事業体と契約等の関係にある被攻撃者に対して機密情報 (多くの場合、ID やパスワード認証などの資格情報) を入力させて、被攻撃者の機密情報を獲得します。獲得された情報は、攻撃者によって利用されます。基本的に、フィッシングは一種の情報収集です。

攻撃者は、悪質なコンテンツを含むフレームまたは I フレーム・タグをインジェクションできます。サイトを閲覧しているユーザーは、よほど注意深くないと元のサイトから悪意のあるサイトに移動していることに気付きません。攻撃者は、ユーザーに再度ログインを行わせ、ログインに必要な資格情報を取得するのです。
元のサイトに偽のサイトを組む込むことで、攻撃者はフィッシング行為をよりもっともらしく見せることができます。

Content-Security-Policy ヘッダーが欠落しています

TOC

テスト・タイプ:
アプリケーション・レベル・テスト

脅威の分類:
情報漏えい

原因:
セキュリティーで保護されていない Web アプリケーション・プログラムまたは設定

セキュリティー・リスク:
- ユーザー名、パスワード、マシン名などの Web アプリケーションに関する秘密情報や、秘密のファイルの場所などの情報を取得することができます
- 知識の乏しいユーザーに、ユーザー名、パスワード、クレジット・カード番号、社会保険番号などの秘密情報を提供するように求めることができます

影響を受ける製品:

CWE:
200

参考資料:
便利な HTTP ヘッダーのリスト
Content Security Policy の概要

技術的な説明:
「Content-Security-Policy」ヘッダーは、ブラウザーのページのレンダリング方法を変更し、さまざまなクロスサイト注入 (クロスサイト・スクリプティングなど) から保護するために設計されています。Web サイトの正しい操作を妨げない方法で、ヘッダー値を正しく設定することが大切です。例えば、インライン JavaScript の実行を妨げるようにヘッダーが設定されている場合、Web サイトではインライン JavaScript をそのページで使用できません。

TRACE および TRACK HTTP メソッドが有効

TOC

テスト・タイプ:
インフラストラクチャー・テスト

脅威の分類:
機能の悪用

原因:
Web サーバーまたはアプリケーション・サーバーが安全でない方法で設定されています

セキュリティー・リスク:
ハッカーが正規のユーザーになりすまし、ユーザーのレコードを表示または改変したり、ユーザーとしてトランザクションを実行するのに使用することができる、カスタマー・セッションおよび Cookie を盗み出したり操作することができる可能性があります

影響を受ける製品:

CWE:
16

X-Force:
31774

参考資料:
CERT 発行の脆弱性情報
XST Article by WhiteHat Security
Bugtraq メッセージ
RFC2616

技術的な説明:
RFC2616 (セクション 9.8 - HTTP の「TRACE」メソッド):
「TRACE メソッドは、要求メッセージのアプリケーション層ループバックをリモートで呼び出すために使用されます。要求の最終的な受信者は、受信したメッセージを 200 (OK) の entity-body の応答としてクライアントに反映する必要があります...。TRACE を使用すると、クライアントは要求チェーンのもう一方の端で何が受信されるかを確認し、そのデータをテストまたは診断情報として使用できます....」RFC2616 で指定されているように、HTTP ヘッダーを含む完全な HTTP 要求が TRACE 応答の本文の中に送り返されます。HTTP ヘッダーには、セッション・トークン、Cookie、認証の資格情報などの重要情報が含まれている場合があります。TRACE 応答の本文は DOM (Document Object Model) インターフェースを介してスクリプト・コードにアクセスできるので、攻撃者が Web ブラウザーの問題 (クロスドメイン問題) を悪用して、重要なヘッダー情報を読み取り、Microsoft Internet Explorer 6.0 SP1 で導入された「HttpOnly」という Cookie 属性をバイパスすることが可能です。

X-Content-Type-Options ヘッダーが欠落しています

TOC

テスト・タイプ:
アプリケーション・レベル・テスト

脅威の分類:
情報漏えい

原因:
セキュリティーで保護されていない Web アプリケーション・プログラムまたは設定

セキュリティー・リスク:
- ユーザー名、パスワード、マシン名などの Web アプリケーションに関する秘密情報や、秘密のファイルの場所などの情報を取得することができます
- 知識の乏しいユーザーに、ユーザー名、パスワード、クレジット・カード番号、社会保険番号などの秘密情報を提供するように求めることができます

影響を受ける製品:

CWE:

200

参考資料:

便利な HTTP ヘッダーのリスト
MIME タイプのセキュリティー・リスクの低減

技術的な説明:

「X-Content-Type-Options」ヘッダー (「nosniff」値を使用) によって、IE と Chrome では応答のコンテンツ・タイプを無視できなくなります。
このアクションは、信頼できないコンテンツ (ユーザーがアップロードしたコンテンツなど) が、(悪質な命名後などに) ユーザーのブラウザーで実行されることを防ぎます。

X-XSS-Protection ヘッダーが欠落しています

TOC

テスト・タイプ:

アプリケーション・レベル・テスト

脅威の分類:

情報漏えい

原因:

セキュリティーで保護されていない Web アプリケーション・プログラムまたは設定

セキュリティー・リスク:

- ユーザー名、パスワード、マシン名などの Web アプリケーションに関する秘密情報や、秘密のファイルの場所などの情報を取得することができます
- 知識の乏しいユーザーに、ユーザー名、パスワード、クレジット・カード番号、社会保険番号などの秘密情報を提供するように求めることができます

影響を受ける製品:

CWE:

200

参考資料:

便利な HTTP ヘッダーのリスト
IE XSS フィルター

技術的な説明:

「X-XSS-Protection」ヘッダーによって、クロスサイト・スクリプティング・フィルターが強制的に (ユーザーが無効にしている場合でも) 「有効」モードになります。
このフィルターは、最新の Web ブラウザー (IE 8+、Chrome 4+) 内にビルドされており、通常であればデフォルトで有効に

なっています。これは、クロスサイト・スクリプティングに対する唯一かつ初めての防御策として設計されたものではありませんが、保護のための追加層として機能します。

セッション Cookie に HttpOnly 属性がありません

TOC

テスト・タイプ:

アプリケーション・レベル・テスト

脅威の分類:

情報漏えい

原因:

Web アプリケーションが HttpOnly 属性のないセッション Cookie を設定しています

セキュリティー・リスク:

ハッカーが正規のユーザーになりすまし、ユーザーのレコードを表示または改変したり、ユーザーとしてトランザクションを実行するのに使用することができる、カスタマー・セッションおよび Cookie を盗み出したり操作することができる可能性があります

影響を受ける製品:

CWE:

653

X-Force:

85873

技術的な説明:

アプリケーション・テスト時に、テストした Web アプリケーションが HttpOnly 属性のないセッション Cookie を設定したことが検出されました。このセッション Cookie は HttpOnly 属性を含んでいないため、サイトに注入された悪意のあるスクリプトによってアクセスされるおそれがあり、その値が盗まれる可能性があります。セッション・トークンに保管された情報は盗まれる可能性があり、後で ID の盗用やユーザーのなりすましに利用される場合があります。

ボディー・パラメーターをクエリーで送信

TOC

テスト・タイプ:

アプリケーション・レベル・テスト

脅威の分類:

情報漏えい

原因:

セキュリティーで保護されていない Web アプリケーション・プログラムまたは設定

セキュリティー・リスク:

- ユーザー名、パスワード、マシン名などの Web アプリケーションに関する秘密情報や、秘密のファイルの場所などの情報を取得することができます
- 知識の乏しいユーザーに、ユーザー名、パスワード、クレジット・カード番号、社会保険番号などの秘密情報を提供するように求めることができます

影響を受ける製品:

CWE:

200

参考資料:

Hypertext Transfer Protocol (HTTP/1.1) セマンティクスおよびコンテンツ:
GET
POST

技術的な説明:

GET 要求は、サーバーを照会するように作成され、一方 POST 要求はデータを実行依頼するためのものです。
ただし、技術的な目的を除き、照会パラメーターの攻撃は本体パラメーターより容易です。これは、オリジナル・サイトへのリンクの送信や、ブログまたはコメント内へのリンクの貼り付けは簡単なので、本体パラメーター攻撃よりも効果的な結果が得られるためです。本体パラメーターが含まれる要求を攻撃するには、攻撃者は、被害者がアクセスした際に実行依頼されるフォームを含むページを作成する必要があります。
被害者にオリジナル・サイトにアクセスさせるよりも、よく知らないページにアクセスさせるほうが、はるかに困難です。そのため、照会ストリングに届く本体パラメーターのサポートは推奨されません。

一時ファイルのダウンロード

TOC

テスト・タイプ:

アプリケーション・レベル・テスト

脅威の分類:

予測可能なリソースの位置

原因:

テンポラリー・ファイルが製作環境に残されています

セキュリティー・リスク:

アプリケーション・ロジック、およびユーザー名やパスワードなどのその他の秘密情報を公開する可能性のある一時スクリプト・ファイルをダウンロードできます

影響を受ける製品:

CWE:
531

X-Force:
52887

参考資料:
WASC 脅威の分類: 予測可能なリソースの場所

技術的な説明:
Web サーバーは、通常 CGI (Common Gateway Interface) ファイル名の拡張子 (たとえば .pl) をハンドラー (たとえば Perl) と関連付けます。URL パスが .pl で終わる場合、パスで指定されたファイル名が Pel に送信されて実行されます。ファイルのコンテンツは、ブラウザーには返されません。ただし、スクリプト・ファイルがその場で編集されたときには、編集対象のスクリプトのバックアップ・コピーを、エディターが .bak、.sav、.old、~ などの別のファイル拡張子を付けて保存する場合があります。Web サーバーは、通常これらの拡張子に対する特定のハンドラーを持っていません。攻撃者がこれらのファイルを要求した場合、ファイルのコンテンツが直接ブラウザーに送信されます。
これらの一時ファイルは、デバッグ目的に使用される秘密情報を格納していたり、現在のロジックとは異なるものの悪用される可能性のあるアプリケーション・ロジックを公開している場合があるので、仮想ディレクトリーの配下から削除することが重要です。

秘密セッション情報を含むパーマネント Cookie

TOC

テスト・タイプ:
アプリケーション・レベル・テスト

脅威の分類:
不適切なセッション有効期限

原因:
Web アプリケーションがパーマネント Cookie に秘密のセッション情報を (ディスク上) を格納しています

セキュリティー・リスク:
パーマネント Cookie としてディスク上に保存されたセッション情報 (Cookie) を盗み出せる可能性があります

影響を受ける製品:

CWE:
539

X-Force:
52827

参考資料:
Financial Privacy: The Gramm-Leach Bliley Act
医療保険の積算と責任に関する法律 (HIPAA)
サーベンス・オクスリー法
California SB1386
HTTP State Management Mechanism (RFC 2109)

技術的な説明:
アプリケーション・テスト時に、ユーザー資格情報またはセッション・トークンなどの機密性の高いセッション情報がクライアントのコンピューターのパーマネント Cookie に保存されたことが検出されました。

[1] 他のユーザーもコンピューターを使用できるため、これらの情報が漏えいしたり、ID の盗用やユーザーのなりすましに利用されたりする可能性があります。

[2] コンピューターのセキュリティーが損なわれると、アカウント情報が盗まれて、後で悪意を持つユーザーにより利用される可能性があります。

また、複数のプライバシー規制法で、秘密情報にアクセスする前にユーザーが一意に識別されることが規定されています。パーマネント Cookie では、他のユーザーが認証なしに Web アプリケーションにログオンできるため、これらのプライバシー規制法に適合していない可能性があります。

非表示のディレクトリーを検出

TOC

テスト・タイプ:
インフラストラクチャー・テスト

脅威の分類:
情報漏えい

原因:
Web サーバーまたはアプリケーション・サーバーが安全でない方法で設定されています

セキュリティー・リスク:
攻撃者が Web サイトをマップするのに利用できるサイトのファイル・システム構造についての情報を取得することができます

影響を受ける製品:

CWE:
200

X-Force:
52599

技術的な説明:
Web アプリケーションが、サイト内のディレクトリーの存在を明らかにしています。ディレクトリーのコンテンツは表示されていませんが、この情報は攻撃者がサイトに対するさらなる攻撃を行うのに役立つ場合があります。たとえば、ディレクトリー名を知ることによって、攻撃者はコンテンツのタイプとその中にあるファイルやサブディレクトリーに使われている可能性のあるファイル名を知って、アクセスすることができる場合があります。ディレクトリーのコンテンツが重要であればあるほど、この問題の深刻度も高くなります。

アプリケーション・エラー

TOC

テスト・タイプ:
アプリケーション・レベル・テスト

脅威の分類:
情報漏えい

原因:
- 受信したパラメーター値について、適切な境界チェックが行われませんでした
- ユーザーの入力が必要なデータ型式に一致することを確認するための検証が行われませんでした

セキュリティー・リスク:
秘密のデバッグ情報を収集することができます

影響を受ける製品:

CWE:
550

X-Force:
52502

参考資料:
アポストロフィーを使用してサイトをハッキングする例は、次の RFP サイトの「How I hacked PacketStorm」(著者: Rain Forest Puppy) を参照してください。
「Web Application Disassembly with ODBC Error Messages」(著者: David Litchfield)」
CERT アドバイザリー (CA-1997-25): CGI スクリプトにおけるユーザー提供データのサニタイズ

技術的な説明:
攻撃者がアプリケーションで必要とされていないパラメーターまたはパラメーター値を格納する要求を偽造してアプリケーションを調査 (以下に例を示します) したとき、アプリケーションが攻撃に対して脆弱となる未定義のステータスになる場合があります。攻撃者は、要求に対するアプリケーションの応答から有用な情報を取得して、アプリケーションの弱点を突き止めます。

例えば、パラメーター・フィールドがアポストロフィーで囲まれた文字列である場合 (例えば ASP スクリプトや SQL クエリー)、注入されたアポストロフィー記号が文字列のストリームを早く停止させることにより、スクリプトの正常なフロー/構文を変更します。
エラー・メッセージで重要な情報が明らかになってしまうもうひとつの原因は、スクリプティング・エンジン、Web サーバー、またはデータベースの設定が誤っている場合です。

いくつかのさまざまなバリアントがあります:
[1] パラメーターの削除
[2] パラメーター値の削除
[3] パラメーター値を Null に設定
[4] パラメーター値を数値オーバーフローする値 (+/- 99999999) に設定
[5] パラメーター値を ' " \' \") ; などの危険性のある文字に変更
[6] 数値パラメーター値に文字列を追加
[7] パラメーター名に "." (ドット) または "[]" (不等号括弧) を追加

クライアント側 (JavaScript) Cookie 参照

TOC

テスト・タイプ:
アプリケーション・レベル・テスト

脅威の分類:
情報漏えい

原因:
クライアント側に Cookie を作成します

セキュリティー・リスク:
この攻撃による最悪のケースのシナリオは、コンテキストとクライアント側で作成された Cookie の役割によって異なります

影響を受ける製品:

CWE:
602

X-Force:
52514

参考資料:
WASC 脅威の分類: 情報漏洩

技術的な説明:
Cookie とは、通常、Web サーバーによって作成されて Web ブラウザーに保存される情報のことです。
Cookie には、Web アプリケーションが使用する情報が格納されます。Web アプリケーションは、主にユーザーを識別してそのユーザーの状態を保存する目的で、この情報を使用します (ただし、それだけではありません)。
AppScan は、クライアント側の JavaScript コードがサイトの Cookie の操作 (作成または変更) に使用されていることを検出

しました。
攻撃者がこのコードを表示してロジックを理解し、その知識に基づいて自分の Cookie を作成したり、既存の Cookie を変更したりするためにコードを使用する可能性があります。
攻撃者がどのような損害を引き起こすかは、アプリケーションが Cookie をどのように使用しているか、またはアプリケーションが Cookie に
どのような情報を格納しているかによって異なります。特に、Cookie の操作によってセッションの乗っ取りや権限の拡張につながる可能性があります。
Cookie の不正操作によって発生するその他の脆弱性としては、SQL インジェクションやクロスサイト・スクリプティングなどがあります。

内部 IP の開示パターンを発見

TOC

テスト・タイプ:

アプリケーション・レベル・テスト

脅威の分類:

情報漏えい

原因:

セキュリティーで保護されていない Web アプリケーション・プログラムまたは設定

セキュリティー・リスク:

ユーザー名、パスワード、マシン名などの Web アプリケーションに関する秘密情報や、秘密のファイルの場所などの情報を取得することができます

影響を受ける製品:

CWE:

200

X-Force:

52657

技術的な説明:

AppScan が、内部 IP アドレスを含むレスポンスを検出しました。内部 IP とは、次の IP 範囲で定義される IP です。
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

内部 IP は、内部ネットワークの IP アドレッシング・スキームを明らかにするため、攻撃者にとって有益な情報となります。内部ネットワークの IP アドレッシング・スキームを知ることで、攻撃者が内部ネットワークに対するさらなる攻撃をしかけやすくなる場合があります。

アプリケーション・データ

認識された URL 31

TOC

URL
http://10.228.148.130/app/org/
http://10.228.148.130/app/org
http://10.228.148.130/app/org/list
http://10.228.148.130/app/org/list?page=1
http://10.228.148.130/app/org/list?page=2
http://10.228.148.130/app/js/jquery-1.9.1.min.js
http://10.228.148.130/app/js/jquery.cookie.js
http://10.228.148.130/app/js/common.js
http://10.228.148.130/app/js/bootstrap.min.js
http://10.228.148.130/app/js/main.js
http://10.228.148.130/app/js/jquery-1.11.3.min.js
http://10.228.148.130/app/js/jquery-ui.min.js
http://10.228.148.130/app/js/functionCommon.js
http://10.228.148.130/app/home/trackLog
http://10.228.148.130/app/home/trackLog
http://10.228.148.130/app/org
http://10.228.148.130/app/org
http://10.228.148.130/app/org/list
http://10.228.148.130/app/org/list?page=2
http://10.228.148.130/app/org/detail/130102044
http://10.228.148.130/app/org/detail/130102044
http://10.228.148.130/app/home/trackLog
http://10.228.148.130/app/org
http://10.228.148.130/app/org
http://10.228.148.130/app/org
http://10.228.148.130/app/org/list
http://10.228.148.130/app/org/detail/130100001
http://10.228.148.130/app/home/trackLog
http://10.228.148.130/app/org/list
http://10.228.148.130/app/home/trackLog
http://10.228.148.130/app/org/list?page=2

パラメーター 15

TOC

名前	値	URL	タイプ
page	1 2	http://10.228.148.130/app/org/list?page=1	単純リンク
kankei_kikan		http://10.228.148.130/app/org	ラジオ
	130102044	http://10.228.148.130/app/org/detail/130102044	カスタム
key_keyword		http://10.228.148.130/app/org	テキスト
key_addr		http://10.228.148.130/app/org	テキスト
key_update	変更	http://10.228.148.130/app/org	非表示
key_publish	公開	http://10.228.148.130/app/org	非表示
key_pref	13 4	http://10.228.148.130/app/org	選択
key_track_log	クリア 戻る 相談窓口検索バナー	http://10.228.148.130/app/home/trackLog	本文
	130100001	http://10.228.148.130/app/org/detail/130100001	カスタム
key_screen	GC0010.相談窓口検索 GC0020.相談窓口一覧 GC0030.相談窓口詳細	http://10.228.148.130/app/home/trackLog	本文
submit	検索	http://10.228.148.130/app/org	サブミット
key_new	新規	http://10.228.148.130/app/org	非表示
_token	yuEor3ontYoqIVemgYB9Md6zAOEcgAoJnyhA89RA	http://10.228.148.130/app/org	非表示
_token	yuEor3ontYoqIVemgYB9Md6zAOEcgAoJnyhA89RA	http://10.228.148.130/app/home/trackLog	非表示

失敗した要求 0

TOC

URL	理由

フィルタリングされた URL 17

TOC

URL	理由
http://10.228.148.130/app/images/100555157.gif	ファイル拡張子
http://10.228.148.130/app/css/bootstrap.min.css	ファイル拡張子
http://10.228.148.130/app/css/hweb_layout.css	ファイル拡張子
http://10.228.148.130/app/css/hweb_style.css	ファイル拡張子
http://10.228.148.130/app/css/style_pc.css	ファイル拡張子
http://10.228.148.130/app/css/style_print.css	ファイル拡張子
http://10.228.148.130/app/images/logo_pc.gif	ファイル拡張子
http://10.228.148.130/app/images/head_text01.gif	ファイル拡張子
http://10.228.148.130/app/images/head_text02.gif	ファイル拡張子
http://10.228.148.130/app/images/c_icon_pankuzu.png	ファイル拡張子
http://10.228.148.130/app/images/spacer.gif	ファイル拡張子
http://10.228.148.130/app/images/foot_logo.gif	ファイル拡張子
http://10.228.148.130/app/images/foot_pagetop.png	ファイル拡張子
http://10.228.148.130/app/css/style.tableconverter.css	ファイル拡張子
http://10.228.148.130/app/images/con_img12.jpg	ファイル拡張子
http://10.228.148.130/app/images/con_img13.jpg	ファイル拡張子
http://10.228.148.130/app/images/con_img14.jpg	ファイル拡張子

コメント 14

TOC

URL	コメント
http://10.228.148.130/app/org/	scs_jyogai_start
http://10.228.148.130/app/org/	/header_wp
http://10.228.148.130/app/org/	△パンくずナビ△
http://10.228.148.130/app/org/	scs_jyogai_end
http://10.228.148.130/app/org/	▲ヘッダ▲
http://10.228.148.130/app/org/	▼テンプレート▼
http://10.228.148.130/app/org/	search-box
http://10.228.148.130/app/org/	▲テンプレート▲
http://10.228.148.130/app/org/	/div main-inner
http://10.228.148.130/app/org/	▼フッタ▼
http://10.228.148.130/app/org/	/div main
http://10.228.148.130/app/org/	/div wrap
http://10.228.148.130/app/org/	/div baseall
http://10.228.148.130/app/org/	/div basebg

JavaScript 16

TOC

URL / コード

http://10.228.148.130/app/org/

```
$(function () {
$("#blockskip a").focus(function () {
$(this)
.parent()
.animate({
height: '1.5em'
}, { duration: 'fast' })
.addClass("show");
});
$("#blockskip a").blur(function () {
$(this)
.parent()
.animate({
height: '1px'
}, {
duration: 'fast',
complete: function () {
$(this).removeClass("show");
}
})
});
});
```

http://10.228.148.130/app/org/

```
var __lang_MR0001 = "パスワードを変更して下さい。";
var __lang_MR0002 = "パスワードが誤っています。パスワードを確認し、再度入力して下さい。";
var __lang_GM0050_err_msg = "From～Toの期間を正しく指定してください";
var __lang_GM0050_err_msg_month = "From～Toの期間が25ヶ月を超えています。正しく指定してください";
var __lang_GM0060_err_msg = "From～Toの期間を正しく指定してください";
var urlTrackLog = 'http://10.228.148.130/app/home/trackLog';
var __token = 'yuEor3ontYoqIVemgYB9Md6zAOEcgAoJnyhA89RA';
var btnBack = '戻る';
var btnChoose = 'ファイルを選択';
var btnClear = 'クリア';
var banner_soudan = '相談窓口検索バナー';
var banner_faq = 'FAQ検索バナー';
var banner_anketo = 'アンケートフォームバナー';

// In case Faq Management screen
if ('soudan-index' == 'management-faq' || 'soudan-index' == 'management-faq-upload') {
    var messRequire = 'アップロードするファイルを選択してください。';
    var messMaxSize = 'This file have large size ';
    var messExtent = 'CSVファイルを指定してください。';
    var messExists = '対象ファイルがありません。再度選択してください。';
    var extensionFile = 'csv';
    var maxSizeFile = parseInt('67100000') * 1024;
}

var __lang_GM0060_err_msg = "From～Toの期間を正しく指定してください";

//In case soudan Management screen
if ('soudan-index' == 'soudanbunya-index') {
    var messRequire = 'アップロードするファイルを選択してください。';
    var messMaxSize = 'This file have large size ';
    var messExtent = 'CSVファイルを指定してください。';
    var messExists = '対象ファイルがありません。再度選択してください。';
    var extensionFile = 'csv';
    var maxSizeFile = parseInt('67100000') * 1024;
}

//In case soudan Management screen
if ('soudan-index' == 'soudanmadoguchi-index') {
```

```
        var messRequire = 'アップロードするファイルを選択してください。';
        var messMaxSize = 'This file have large size ';
        var messExtent = 'CSVファイルを指定してください。';
        var messExists = '対象ファイルがありません。再度選択してください。';
        var extensionFile = 'csv';
        var maxSizeFile = parseInt('67100000') * 1024;
    }

    //In case faq search screen
    if ('soudan-index' == 'faq-index') {
        var messSpecialCharacter = '検索不可能な文字(&,<,>,",\',©,®,\\,{,},$,%)が含まれています。';
        var messNoFilter = '検索条件を入力してください。';
    }

    //In case soudan search screen
    if ('soudan-index' == 'soudan-index') {
        var messSpecialCharacter = '検索不可能な文字(&,<,>,",\',©,®,\\,{,},$,%)が含まれています。';
        var messNoFilter = '検索条件を入力してください。';
    }
```

http://10.228.148.130/app/org/

```
  window._token = 'yuEor3ontYoqIVemgYB9Md6zAOEcgAoJnyhA89RA';
```

http://10.228.148.130/app/org/

```
        $(document).ready(function() {
          $('.clear-btn').click(function() {
          $('.clear-btn').attr('disabled', 'disabled');
          $('#counter').attr('disabled', 'disabled');
          $('input:checkbox').removeAttr('checked');
          $('input:radio').removeAttr('checked');
          $('#do-not-select').trigger('click');
          $('.w-full').val('');
          $('.w-half').val('');
          $('#prefectures').val('');
          $('#counter').val('');
          $('.error-msg').remove();
          var mess = $('.error-msg-client').html();
          if (mess != '') {
          $('.error-msg-client').addClass('error-msg-no-display');
          $('.error-msg-client').html('');
          }
          trackLog('GC0010.相談窓口検索', btnClear);
          $('.clear-btn').removeAttr('disabled');
          });

          $('.command-btn').click(function(e) {
          $('.error-msg').remove();
          $('.error-msg-client').html('');
          $('.error-msg-client').addClass('error-msg-no-display');
          var messErr = validateSearch();
          if (messErr != '') {
          $('.error-msg-client').html(messErr);
          $('.error-msg-client').removeClass('error-msg-no-display');
          $('html, body').animate({ scrollTop: 0 }, 'slow');
          return false;
          } else {
          getStringBytes();
          }
          });

          $('#madoguti').change(function() {
          disableLanguageDropdown();
          });
```

```
    var valueRadio = '';
    initCheckedRadio(valueRadio);
    disableLanguageDropdown();
    clearMessgeWhenBackBrowser('soudanList');
  });


  function getStringBytes() {
    var url = "http://10.228.148.130/app/get-string-bytes";
    var keyword = $("#input-assist").val();
    var key_address = $("#key_addr").val();
    var max_length = $("#input-assist").attr('maxLength');
    if ((keyword.length > parseInt(max_length)/2) ||  (key_address.length > parseInt(max_length)/2)) {
    $.ajax({
    url: url,
    type: 'POST',
    data:{
    _token : __token,
    keyword : keyword,
    city : key_address,
    max_length : max_length
    },
    success: function (res) {
    console.log(res);
    if( res['result']  == false) {
    $('.error-msg-client').html(res['msg']);
    $('.error-msg-client').removeClass('error-msg-no-display');
    } else {
    $("#command-submit").trigger('click');
    }

    }
    });
    } else {
    $("#command-submit").trigger('click');
    }

  }

 /*
   Checked radio if data search not record
  */
  function initCheckedRadio(valueRadio) {
    if (valueRadio != '') {
    $('input[type=radio]').each(function () {
    if ($(this).val() == valueRadio) {
    $(this).attr('checked', 'checked');
    return;
    }
    });
    }
  }

  /*
    Disabled dropdown language
   */
  function disableLanguageDropdown() {
    if ($('#madoguti').is(':checked')) {
    $('#counter').removeAttr('disabled');
    } else {
    $('#counter').val('');
    $('#counter').attr('disabled', 'disabled');
    }
  }

  /*
    Validate client search
   */
  function validateSearch() {
    var prefectures = $('#prefectures').val();
    var counter = $('#counter').val();
    var addr = $('.w-half').val();
    var keyWord = $('.w-full').val();

    // Check pattern
    if (!checkSpecialCharacter(keyWord) && keyWord != '') {
    return messSpecialCharacter;
    }
```

```
        // Check pattern
        if (!checkSpecialCharacter(addr) && addr != '') {
        return messSpecialCharacter;
        }

        // Check Require
        if (counter == '' && prefectures == '' && addr == '' && keyWord == '') {
        var isCheck = false;
        $('input[type=checkbox]').each(function () {
        if ($(this).is(":checked")) {
        isCheck = true;
        return;
        }
        });

        $('input[type=radio]').each(function () {
        if ($(this).is(":checked")) ...
```

http://10.228.148.130/app/js/jquery-1.9.1.min.js

```
/*! jQuery v1.9.1 | (c) 2005, 2012 jQuery Foundation, Inc. | jquery.org/license
//@ sourceMappingURL=jquery.min.map
*/(function(e,t){var n,r,i=typeof t,o=e.document,a=e.location,s=e.jQuery,u=e.$,l={},c=
[],p="1.9.1",f=c.concat,d=c.push,h=c.slice,g=c.indexOf,m=l.toString,y=l.hasOwnProperty,v=p.trim,b=function(e,
t){return new b.fn.init(e,t,r)},x=/[+-]?(?:\d*\.|)\d+(?:[eE][+-]?\d+|)/.source,w=/\S+/g,T=/^[\s\uFEFF\xA0]+|
[\s\uFEFF\xA0]+$/g,N=/^(?:(<[\w\W]+>)[^>]*|#([\w-]*))$/,C=/^<(\w+)\s*\/?>(?:<\/\1>|)$/,k=/^[\],:
{}\s]*$/,E=/(?:^|:|,)(?:\s*\[)+/g,S=/\\(?:["\\\/bfnrt]|u[\da-fA-F]{4})/g,A=/"[^"\\\r\n]*"|true|false|null|-?
(?:\d+\.|)\d+(?:[eE][+-]?\d+|)/g,j=/^-ms-/,D=/-([\da-z])/gi,L=function(e,t){return
t.toUpperCase()},H=function(e){(o.addEventListener||"load"===e.type||"complete"===o.readyState)&&
(q(),b.ready())},q=function(){o.addEventListener?
(o.removeEventListener("DOMContentLoaded",H,!1),e.removeEventListener("load",H,!1)):
(o.detachEvent("onreadystatechange",H),e.detachEvent("onload",H))};b.fn=b.prototype=
{jquery:p,constructor:b,init:function(e,n,r){var i,a;if(!e)return this;if("string"==typeof e){if(i="
<"===e.charAt(0)&&">"===e.charAt(e.length-1)&&e.length>=3?
[null,e,null]:N.exec(e),!i||!i[1]&&n)return!n||n.jquery?(n||r).find(e):this.constructor(n).find(e);if(i[1])
{if(n=n instanceof b?n[0]:n,b.merge(this,b.parseHTML(i[1],n&&n.nodeType?
n.ownerDocument||n:o,!0)),C.test(i[1])&&b.isPlainObject(n))for(i in n)b.isFunction(this[i])?this[i]
(n[i]):this.attr(i,n[i]);return this}if(a=o.getElementById(i[2]),a&&a.parentNode){if(a.id!==i[2])return
r.find(e);this.length=1,this[0]=a}return this.context=o,this.selector=e,this}return e.nodeType?
(this.context=this[0]=e,this.length=1,this):b.isFunction(e)?r.ready(e):(e.selector!==t&&
(this.selector=e.selector,this.context=e.context),b.makeArray(e,this))},selector:"",length:0,size:function()
{return this.length},toArray:function(){return h.call(this)},get:function(e){return null==e?
this.toArray():0>e?this[this.length+e]:this[e]},pushStack:function(e){var
t=b.merge(this.constructor(),e);return t.prevObject=this,t.context=this.context,t},each:function(e,t){return
b.each(this,e,t)},ready:function(e){return b.ready.promise().done(e),this},slice:function(){return
this.pushStack(h.apply(this,arguments))},first:function(){return this.eq(0)},last:function(){return this.eq(-
1)},eq:function(e){var t=this.length,n=+e+(0>e?t:0);return this.pushStack(n>=0&&t>n?[this[n]]:
[])},map:function(e){return this.pushStack(b.map(this,function(t,n){return e.call(t,n,t)}))},end:function()
{return this.prevObject||this.constructor(null)},push:d,sort:[].sort,splice:
[].splice},b.fn.init.prototype=b.fn,b.extend=b.fn.extend=function(){var e,n,r,i,o,a,s=arguments[0]||
{},u=1,l=arguments.length,c=!1;for("boolean"==typeof s&&(c=s,s=arguments[1]||{},u=2),"object"==typeof
s||b.isFunction(s)||(s={}),l===u&&(s=this,--u);l>u;u++)if(null!=(o=arguments[u]))for(i in
o)e=s[i],r=o[i],s!==r&&(c&&r&&(b.isPlainObject(r)||(n=b.isArray(r)))?(n?(n=!1,a=e&&b.isArray(e)?e:
[]):a=e&&b.isPlainObject(e)?e:{},s[i]=b.extend(c,a,r)):r!==t&&(s[i]=r));return
s},b.extend({noConflict:function(t){return e.$===b&&(e.$=u),t&&e.jQuery===b&&
(e.jQuery=s),b},isReady:!1,readyWait:1,holdReady:function(e){e?b.readyWait++:b.ready(!0)},ready:function(e)
{if(e===!0?!--b.readyWait:!b.isReady){if(!o.body)return setTimeout(b.ready);b.isReady=!0,e!==!0&&--
b.readyWait>0||(n.resolveWith(o,
[b]),b.fn.trigger&&b(o).trigger("ready").off("ready"))}},isFunction:function(e)
{return"function"===b.type(e)},isArray:Array.isArray||function(e)
{return"array"===b.type(e)},isWindow:function(e){return null!=e&&e==e.window},isNumeric:function(e)
{return!isNaN(parseFloat(e))&&isFinite(e)},type:function(e){return null==e?e+"":"object"==typeof
e||"function"==typeof e?l[m.call(e)]||"object":typeof e},isPlainObject:function(e)
{if(!e||"object"!==b.type(e)||e.nodeType||b.isWindow(e))return!1;try{if(e.constructor&&!y.call(e,"constructor
")&&!y.call(e.constructor.prototype,"isPrototypeOf"))return!1}catch(n){return!1}var r;for(r in e);return
r===t||y.call(e,r)},isEmptyObject:function(e){var t;for(t in e)return!1;return!0},error:function(e){throw
Error(e)},parseHTML:function(e,t,n){if(!e||"string"!=typeof e)return null;"boolean"==typeof t&&
(n=t,t=!1),t=t||o;var r=C.exec(e),i=!n&&[];return r?[t.createElement(r[1])]:
(r=b.buildFragment([e],t,i),i&&b(i).remove(),b.merge([],r.childNodes))},parseJSON:function(n){return
e.JSON&&e.JSON.parse?e.JSON.parse(n):null===n?n:"string"==typeof n&&
(n=b.trim(n),n&&k.test(n.replace(S,"@").replace(A,"]").replace(E,""))?Function("return "+n)():
(b.error("Invalid JSON: "+n),t)},parseXML:function(n){var r,i;if(!n||"string"!=typeof n)return
```

```
null;try{e.DOMParser?(i=new DOMParser,r=i.parseFromString(n,"text/xml")):(r=new
ActiveXObject("Microsoft.XMLDOM"),r.async="false",r.loadXML(n))}catch(o){r=t}return
r&&r.documentElement&&!r.getElementsByTagName("parsererror").length||b.error("Invalid XML:
"+n),r},noop:function(){},globalEval:function(t){t&&b.trim(t)&&(e.execScript||...
```

http://10.228.148.130/app/js/jquery.cookie.js

```
/*!
 * jQuery Cookie Plugin v1.3.1
 * https://github.com/carhartl/jquery-cookie
 *
 * Copyright 2013 Klaus Hartl
 * Released under the MIT license
 */
(function (factory) {
 if (typeof define === 'function' && define.amd) {
        // AMD. Register as anonymous module.
        define(['jquery'], factory);
 } else {
        // Browser globals.
        factory(jQuery);
       }
}(function ($) {

 var pluses = /\+/g;

 function raw(s) {
        return s;
       }

 function decoded(s) {
        return decodeURIComponent(s.replace(pluses, ' '));
       }

 function converted(s) {
        if (s.indexOf('"') === 0) {
                // This is a quoted cookie as according to RFC2068, unescape
                s = s.slice(1, -1).replace(/\\"/g, '"').replace(/\\\\/g, '\\');
               }
        try {
                return config.json ? JSON.parse(s) : s;
        } catch(er) {}
       }

 var config = $.cookie = function (key, value, options) {

        // write
        if (value !== undefined) {
                options = $.extend({}, config.defaults, options);

                if (typeof options.expires === 'number') {
                        var days = options.expires, t = options.expires = new Date();
                        t.setDate(t.getDate() + days);
                       }

                value = config.json ? JSON.stringify(value) : String(value);

                return (document.cookie = [
                        config.raw ? key : encodeURIComponent(key),
                        '='       ,
                        config.raw ? value : encodeURIComponent(value),
                        options.expires ? '; expires=' + options.expires.toUTCString() : '', // use
expires attribute, max-age is not supported by IE
                        options.path    ? '; path=' + options.path : '',
                        options.domain  ? '; domain=' + options.domain : '',
                        options.secure  ? '; secure' : ''
                ].join(''));
               }

        // read
        var decode = config.raw ? raw : decoded;
        var cookies = document.cookie.split('; ');
        var result = key ? undefined : {};
```

```
        for (var i = 0, l = cookies.length; i < l; i++) {
                var parts = cookies[i].split('=');
                var name = decode(parts.shift());
                var cookie = decode(parts.join('='));

                if (key && key === name) {
                        result = converted(cookie);
                        break;
                       }

                if (!key) {
                        result[name] = converted(cookie);
                       }
               }

        return result;
 };

 config.defaults = {};

 $.removeCookie = function (key, options) {
        if ($.cookie(key) !== undefined) {
                // Must not alter options, thus extending a fresh object...
                $.cookie(key, '', $.extend({}, options, { expires: -1 }));
                return true;
               }
        return false;
 };

}));
```

http://10.228.148.130/app/js/common.js

```
$(function(){
 //       プレースホルダーを設定
 $("input.searchBox").attr('placeholder', '       サイト内検索');

 //       グローバルナビ
 if(location.pathname != "/") {
     $('#gnavi li a[href^="/' + location.pathname.split("/")[1] +
'"]').parent('li').addClass('active');
         }
  // Add class 'focused' by tab key
   $('.menu-item-has-children a').focus( function () {
        $(this).siblings('.sub').addClass('focused');
 })

 .blur(function(){
        $(this).siblings('.sub').removeClass('focused');
 });

 // For children
 $('.sub-menu a').focus( function () {
        $(this).parents('.sub').addClass('focused');
        $(this).parents('.menu-item-has-children').addClass('active');
 })

 .blur(function(){
        $(this).parents('.sub').removeClass('focused');
        $(this).parents('.menu-item-has-children').removeClass('active');
 });

 $(".sub").hover(
        function() {
                $(this).parents('.menu-item-has-children').addClass('active');
        }       ,
        function() {
                $(this).parents('.menu-item-has-children').removeClass('active');
               }
 );


//      //スマホヘッダグローバルメニュー開閉
```

```
 $("#toggle01").click(function() {
         if ($(this).hasClass("menu-open")) {
                $("#toggle01").removeClass("menu-open");
                 $(".button_text").html('       メニュー');
                 $("#gnavi_menu").slideUp("slow");
                 $(this).children('img').attr("alt","       グローバルメニューを開く");;
                 return "";
         } else {
                $("#toggle01").addClass("menu-open");
                 $(".button_text").html('       閉じる');
                 $("#gnavi_menu").slideDown("slow");
                 $(this).children('img').attr("alt","       グローバルメニューを閉じる");;
      }
            return "close";
 });
});
```

http://10.228.148.130/app/js/bootstrap.min.js

```
/*!
 * Bootstrap v3.3.6 (http://getbootstrap.com)
 * Copyright 2011-2015 Twitter, Inc.
 * Licensed under the MIT license
 */
if("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript requires jQuery");+function(a){"use
strict";var b=a.fn.jquery.split(" ")[0].split(".");if(b[0]<2&&b[1]<9||1==b[0]&&9==b[1]&&b[2]<1||b[0]>2)throw
new Error("Bootstrap's JavaScript requires jQuery version 1.9.1 or higher, but lower than version 3")}
(jQuery),+function(a){"use strict";function b(){var a=document.createElement("bootstrap"),b=
{WebkitTransition:"webkitTransitionEnd",MozTransition:"transitionend",OTransition:"oTransitionEnd
otransitionend",transition:"transitionend"};for(var c in b)if(void
0!==a.style[c])return{end:b[c]};return!1}a.fn.emulateTransitionEnd=function(b){var
c=!1,d=this;a(this).one("bsTransitionEnd",function(){c=!0});var e=function()
{c||a(d).trigger(a.support.transition.end)};return setTimeout(e,b),this},a(function()
{a.support.transition=b(),a.support.transition&&(a.event.special.bsTransitionEnd=
{bindType:a.support.transition.end,delegateType:a.support.transition.end,handle:function(b){return
a(b.target).is(this)?b.handleObj.handler.apply(this,arguments):void 0}})})}(jQuery),+function(a){"use
strict";function b(b){return this.each(function(){var
c=a(this),e=c.data("bs.alert");e||c.data("bs.alert",e=new d(this)),"string"==typeof b&&e[b].call(c)})}var
c='[data-dismiss="alert"]',d=function(b)
{a(b).on("click",c,this.close)};d.VERSION="3.3.6",d.TRANSITION_DURATION=150,d.prototype.close=function(b)
{function c(){g.detach().trigger("closed.bs.alert").remove()}var e=a(this),f=e.attr("data-target");f||
(f=e.attr("href"),f=f&&f.replace(/.*(?=#[^\s]*$)/,""));var g=a(f);b&&b.preventDefault(),g.length||
(g=e.closest(".alert")),g.trigger(b=a.Event("close.bs.alert")),b.isDefaultPrevented()||
(g.removeClass("in"),a.support.transition&&g.hasClass("fade")?
g.one("bsTransitionEnd",c).emulateTransitionEnd(d.TRANSITION_DURATION):c())};var
e=a.fn.alert;a.fn.alert=b,a.fn.alert.Constructor=d,a.fn.alert.noConflict=function(){return
a.fn.alert=e,this},a(document).on("click.bs.alert.data-api",c,d.prototype.close)}(jQuery),+function(a){"use
strict";function b(b){return this.each(function(){var d=a(this),e=d.data("bs.button"),f="object"==typeof
b&&b;e||d.data("bs.button",e=new c(this,f)),"toggle"==b?e.toggle():b&&e.setState(b)})}var c=function(b,d)
{this.$element=a(b),this.options=a.extend({},c.DEFAULTS,d),this.isLoading=!1};c.VERSION="3.3.6",c.DEFAULTS=
{loadingText:"loading..."},c.prototype.setState=function(b){var
c="disabled",d=this.$element,e=d.is("input")?"val":"html",f=d.data();b+="Text",null==f.resetText&&d.data("res
etText",d[e]()),setTimeout(a.proxy(function(){d[e](null==f[b]?this.options[b]:f[b]),"loadingText"==b?
(this.isLoading=!0,d.addClass(c).attr(c,c)):this.isLoading&&
(this.isLoading=!1,d.removeClass(c).removeAttr(c))},this),0)},c.prototype.toggle=function(){var
a=!0,b=this.$element.closest('[data-toggle="buttons"]');if(b.length){var
c=this.$element.find("input");"radio"==c.prop("type")?(c.prop("checked")&&
(a=!1),b.find(".active").removeClass("active"),this.$element.addClass("active")):"checkbox"==c.prop("type")&&
(c.prop("checked")!==this.$element.hasClass("active")&&
(a=!1),this.$element.toggleClass("active")),c.prop("checked",this.$element.hasClass("active")),a&&c.trigger("
change")}else this.$element.attr("aria-
pressed",!this.$element.hasClass("active")),this.$element.toggleClass("active")};var
d=a.fn.button;a.fn.button=b,a.fn.button.Constructor=c,a.fn.button.noConflict=function(){return
a.fn.button=d,this},a(document).on("click.bs.button.data-api",'[data-toggle^="button"]',function(c){var
d=a(c.target);d.hasClass("btn")||
(d=d.closest(".btn")),b.call(d,"toggle"),a(c.target).is('input[type="radio"]')||a(c.target).is('input[type="c
heckbox"]')||c.preventDefault()}).on("focus.bs.button.data-api blur.bs.button.data-api",'[data-
toggle^="button"]',function(b){a(b.target).closest(".btn").toggleClass("focus",/^focus(in)?
$/.test(b.type))})}(jQuery),+function(a){"use strict";function b(b){return this.each(function(){var
d=a(this),e=d.data("bs.carousel"),f=a.extend({},c.DEFAULTS,d.data(),"object"==typeof b&&b),g="string"==typeof
b?b:f.slide;e||d.data("bs.carousel",e=new c(this,f)),"number"==typeof b?e.to(b):g?e[g]
():f.interval&&e.pause().cycle()})}var c=function(b,c)
```

```
{this.$element=a(b),this.$indicators=this.$element.find(".carousel-
indicators"),this.options=c,this.paused=null,this.sliding=null,this.interval=null,this.$active=null,this.$ite
ms=null,this.options.keyboard&&this.$element.on("keydown.bs.carousel",a.proxy(this.keydown,this)),"hover"==th
is.options.pause&&!("ontouchstart"in
document.documentElement)&&this.$element.on("mouseenter.bs.carousel",a.proxy(this.pause,this)).on("mouseleave
.bs.carousel",a.proxy(this.cycle,this))};c.VERSION="3.3.6",c.TRANSITION_DURATION=600,c.DEFAULTS=
{interval:5e3,pause:"hover",wrap:!0,keyboard:!0},c.prototype.keydown=function(a)
{if(!/input|textarea/i.test(a.target.tagName)){switch(a.which){cas...
```

http://10.228.148.130/app/js/main.js

```
$(document).ready(function () {

});
```

http://10.228.148.130/app/js/jquery-1.11.3.min.js

```
/*! jQuery v1.11.3 | (c) 2005, 2015 jQuery Foundation, Inc. | jquery.org/license */
!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?
b(a,!0):function(a){if(!a.document)throw new Error("jQuery requires a window with a document");return
b(a)}:b(a)}("undefined"!=typeof window?window:this,function(a,b){var c=
[],d=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toString,j=h.hasOwnProperty,k=
{},l="1.11.3",m=function(a,b){return new m.fn.init(a,b)},n=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,o=/^-ms-
/,p=/-([\da-z])/gi,q=function(a,b){return b.toUpperCase()};m.fn=m.prototype=
{jquery:l,constructor:m,selector:"",length:0,toArray:function(){return d.call(this)},get:function(a){return
null!=a?0>a?this[a+this.length]:this[a]:d.call(this)},pushStack:function(a){var
b=m.merge(this.constructor(),a);return b.prevObject=this,b.context=this.context,b},each:function(a,b){return
m.each(this,a,b)},map:function(a){return this.pushStack(m.map(this,function(b,c){return
a.call(b,c,b)}))},slice:function(){return this.pushStack(d.apply(this,arguments))},first:function(){return
this.eq(0)},last:function(){return this.eq(-1)},eq:function(a){var b=this.length,c=+a+(0>a?b:0);return
this.pushStack(c>=0&&b>c?[this[c]]:[])},end:function(){return
this.prevObject||this.constructor(null)},push:f,sort:c.sort,splice:c.splice},m.extend=m.fn.extend=function()
{var a,b,c,d,e,f,g=arguments[0]||{},h=1,i=arguments.length,j=!1;for("boolean"==typeof g&&
(j=g,g=arguments[h]||{},h++),"object"==typeof g||m.isFunction(g)||(g={}),h===i&&(g=this,h--
);i>h;h++)if(null!=(e=arguments[h]))for(d in e)a=g[d],c=e[d],g!==c&&(j&&c&&(m.isPlainObject(c)||
(b=m.isArray(c)))?(b?(b=!1,f=a&&m.isArray(a)?a:[]):f=a&&m.isPlainObject(a)?a:{},g[d]=m.extend(j,f,c)):void
0!==c&&(g[d]=c));return g},m.extend({expando:"jQuery"+
(l+Math.random()).replace(/\D/g,""),isReady:!0,error:function(a){throw new Error(a)},noop:function()
{},isFunction:function(a){return"function"===m.type(a)},isArray:Array.isArray||function(a)
{return"array"===m.type(a)},isWindow:function(a){return null!=a&&a==a.window},isNumeric:function(a)
{return!m.isArray(a)&&a-parseFloat(a)+1>=0},isEmptyObject:function(a){var b;for(b in
a)return!1;return!0},isPlainObject:function(a){var
b;if(!a||"object"!==m.type(a)||a.nodeType||m.isWindow(a))return!1;try{if(a.constructor&&!j.call(a,"constructo
r")&&!j.call(a.constructor.prototype,"isPrototypeOf"))return!1}catch(c){return!1}if(k.ownLast)for(b in
a)return j.call(a,b);for(b in a);return void 0===b||j.call(a,b)},type:function(a){return null==a?
a+"":"object"==typeof a||"function"==typeof a?h[i.call(a)]||"object":typeof a},globalEval:function(b)
{b&&m.trim(b)&&(a.execScript||function(b){a.eval.call(a,b)})(b)},camelCase:function(a){return
a.replace(o,"ms-").replace(p,q)},nodeName:function(a,b){return
a.nodeName&&a.nodeName.toLowerCase()===b.toLowerCase()},each:function(a,b,c){var
d,e=0,f=a.length,g=r(a);if(c){if(g){for(;f>e;e++)if(d=b.apply(a[e],c),d===!1)break}else for(e in
a)if(d=b.apply(a[e],c),d===!1)break}else if(g){for(;f>e;e++)if(d=b.call(a[e],e,a[e]),d===!1)break}else for(e
in a)if(d=b.call(a[e],e,a[e]),d===!1)break;return a},trim:function(a){return null==a?"":
(a+"").replace(n,"")},makeArray:function(a,b){var c=b||[];return null!=a&&(r(Object(a))?
m.merge(c,"string"==typeof a?[a]:a):f.call(c,a)),c},inArray:function(a,b,c){var d;if(b){if(g)return
g.call(b,a,c);for(d=b.length,c=c?0>c?Math.max(0,d+c):c:0;d>c;c++)if(c in b&&b[c]===a)return c}return-
1},merge:function(a,b){var c=+b.length,d=0,e=a.length;while(c>d)a[e++]=b[d++];if(c!==c)while(void
0!==b[d])a[e++]=b[d++];return a.length=e,a},grep:function(a,b,c){for(var d,e=
[],f=0,g=a.length,h=!c;g>f;f++)d=!b(a[f],f),d!==h&&e.push(a[f]);return e},map:function(a,b,c){var
d,f=0,g=a.length,h=r(a),i=[];if(h)for(;g>f;f++)d=b(a[f],f,c),null!=d&&i.push(d);else for(f in
a)d=b(a[f],f,c),null!=d&&i.push(d);return e.apply([],i)},guid:1,proxy:function(a,b){var
c,e,f;return"string"==typeof b&&(f=a[b],b=a,a=f),m.isFunction(a)?(c=d.call(arguments,2),e=function(){return
a.apply(b||this,c.concat(d.call(arguments)))},e.guid=a.guid=a.guid||m.guid++,e):void 0},now:function()
{return+new Date},support:k}),m.each("Boolean Number String Function Array Date RegExp Object Error".split("
"),function(a,b){h["[object "+b+"]"]=b.toLowerCase()});function r(a){var b="length"in
a&&a.length,c=m.type(a);return"function"===c||m.isWindow(a)?!1:1===a.nodeType&&b?!0:"array"===c||0===b||"numb
er"==typeof b&&b>0&&b-1 in a}var s=function(a){var b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u="sizzle"+1*new
Date,v=a.document,w=0,x=0,y=ha(),z=ha(),A=ha(),B=function(a,b){return a===b&&(l=!0),0},C=1<<31,D=
{}.hasOwnProperty,E=[],F=E.pop,G=E.push,H=E.push,I=E.slice,J=function(a,b){for(var
```

```
c=0,d=a.length;d>c;c++)if(a[c]===b)return c;return-
1},K="checked|selected|async|autofocus|autoplay|controls|defer|disabled|hidden|ismap|loop|multiple|open|reado
nly|required|scoped",L="[\\x20\\t\\r\\n\\f]",M="(?:\\\\.|[\\w-]|[^\\x00-
\\xa0])+",N=M.replace("w","w#"),O="\...
```

http://10.228.148.130/app/js/jquery-ui.min.js

```
/*! jQuery UI - v1.11.3 - 2015-02-12
* http://jqueryui.com
* Includes: core.js, widget.js, mouse.js, position.js, accordion.js, autocomplete.js, button.js,
datepicker.js, dialog.js, draggable.js, droppable.js, effect.js, effect-blind.js, effect-bounce.js, effect-
clip.js, effect-drop.js, effect-explode.js, effect-fade.js, effect-fold.js, effect-highlight.js, effect-
puff.js, effect-pulsate.js, effect-scale.js, effect-shake.js, effect-size.js, effect-slide.js, effect-
transfer.js, menu.js, progressbar.js, resizable.js, selectable.js, selectmenu.js, slider.js, sortable.js,
spinner.js, tabs.js, tooltip.js
* Copyright 2015 jQuery Foundation and other contributors; Licensed MIT */

(function(e){"function"==typeof define&&define.amd?define(["jquery"],e):e(jQuery)})(function(e){function
t(t,s){var n,a,o,r=t.nodeName.toLowerCase();return"area"===r?
(n=t.parentNode,a=n.name,t.href&&a&&"map"===n.nodeName.toLowerCase()?(o=e("img[usemap='#"+a+"']")
[0],!!o&&i(o)):!1):(/^(input|select|textarea|button|object)$/.test(r)?!t.disabled:"a"===r?
t.href||s:s)&&i(t)}function i(t){return
e.expr.filters.visible(t)&&!e(t).parents().addBack().filter(function()
{return"hidden"===e.css(this,"visibility")}).length}function s(e){for(var t,i;e.length&&e[0]!==document;)
{if(t=e.css("position"),("absolute"===t||"relative"===t||"fixed"===t)&&
(i=parseInt(e.css("zIndex"),10),!isNaN(i)&&0!==i))return i;e=e.parent()}return 0}function n()
{this._curInst=null,this._keyEvent=!1,this._disabledInputs=
[],this._datepickerShowing=!1,this._inDialog=!1,this._mainDivId="ui-datepicker-div",this._inlineClass="ui-
datepicker-inline",this._appendClass="ui-datepicker-append",this._triggerClass="ui-datepicker-
trigger",this._dialogClass="ui-datepicker-dialog",this._disableClass="ui-datepicker-
disabled",this._unselectableClass="ui-datepicker-unselectable",this._currentClass="ui-datepicker-current-
day",this._dayOverClass="ui-datepicker-days-cell-over",this.regional=[],this.regional[""]=
{closeText:"Done",prevText:"Prev",nextText:"Next",currentText:"Today",monthNames:
["January","February","March","April","May","June","July","August","September","October","November","December
"],monthNamesShort:["Jan","Feb","Mar","Apr","May","Jun","Jul","Aug","Sep","Oct","Nov","Dec"],dayNames:
["Sunday","Monday","Tuesday","Wednesday","Thursday","Friday","Saturday"],dayNamesShort:
["Sun","Mon","Tue","Wed","Thu","Fri","Sat"],dayNamesMin:
["Su","Mo","Tu","We","Th","Fr","Sa"],weekHeader:"Wk",dateFormat:"mm/dd/yy",firstDay:0,isRTL:!1,showMonthAfter
Year:!1,yearSuffix:""},this._defaults={showOn:"focus",showAnim:"fadeIn",showOptions:
{},defaultDate:null,appendText:"",buttonText:"...",buttonImage:"",buttonImageOnly:!1,hideIfNoPrevNext:!1,navi
gationAsDateFormat:!1,gotoCurrent:!1,changeMonth:!1,changeYear:!1,yearRange:"c-
10:c+10",showOtherMonths:!1,selectOtherMonths:!1,showWeek:!1,calculateWeek:this.iso8601Week,shortYearCutoff:"
+10",minDate:null,maxDate:null,duration:"fast",beforeShowDay:null,beforeShow:null,onSelect:null,onChangeMonth
Year:null,onClose:null,numberOfMonths:1,showCurrentAtPos:0,stepMonths:1,stepBigMonths:12,altField:"",altForma
t:"",constrainInput:!0,showButtonPanel:!1,autoSize:!1,disabled:!1},e.extend(this._defaults,this.regional[""])
,this.regional.en=e.extend(!0,{},this.regional[""]),this.regional["en-US"]=e.extend(!0,
{},this.regional.en),this.dpDiv=a(e("<div id='"+this._mainDivId+"' class='ui-datepicker ui-widget ui-widget-
content ui-helper-clearfix ui-corner-all'></div>"))}function a(t){var i="button, .ui-datepicker-prev, .ui-
datepicker-next, .ui-datepicker-calendar td a";return t.delegate(i,"mouseout",function()
{e(this).removeClass("ui-state-hover"),-1!==this.className.indexOf("ui-datepicker-
prev")&&e(this).removeClass("ui-datepicker-prev-hover"),-1!==this.className.indexOf("ui-datepicker-
next")&&e(this).removeClass("ui-datepicker-next-hover")}).delegate(i,"mouseover",o)}function o()
{e.datepicker._isDisabledDatepicker(v.inline?v.dpDiv.parent()[0]:v.input[0])||(e(this).parents(".ui-
datepicker-calendar").find("a").removeClass("ui-state-hover"),e(this).addClass("ui-state-hover"),-
1!==this.className.indexOf("ui-datepicker-prev")&&e(this).addClass("ui-datepicker-prev-hover"),-
1!==this.className.indexOf("ui-datepicker-next")&&e(this).addClass("ui-datepicker-next-hover"))}function
r(t,i){e.extend(t,i);for(var s in i)null==i[s]&&(t[s]=i[s]);return t}function h(e){return function(){var
t=this.element.val();e.apply(this,arguments),this._refresh(),t!==this.element.val()&&this._trigger("change")}
}e.ui=e.ui||{},e.extend(e.ui,{version:"1.11.3",keyCode:
{BACKSPACE:8,COMMA:188,DELETE:46,DOWN:40,END:35,ENTER:13,ESCAPE:27,HOME:36,LEFT:37,PAGE_DOWN:34,PAGE_UP:33,PE
RIOD:190,RIGHT:39,SPACE:32,TAB:9,UP:38}}),e.fn.extend({scrollParent:function(t){var
i=this.css("position"),s="absolute"===i,n=t?/(auto|scroll|hidden)/:/(auto|scroll)/,a=this.parents().filter(fu
nction(){var t=e(this);return s&&"static"===t.css("position")?!1:n.test(t.css("overflow")+t.css("overflow-
y")+t.css("overflow-x"))}).eq(0);return"fixed"!==i&&a...
```

http://10.228.148.130/app/js/functionCommon.js

```
// Back browser when button clicked
```

```
init();
function init(){
 $('.openNav').on('click', function () {
         openNav();
 })
 $('.closebtn').on('click', function () {
         closeNav();
 })
}
function goBack() {
    window.history.back();
}

function checkValidateFile(idForm, idFile) {
    $('.clsMess').remove();

    // Check require
    var fileName = $(idFile).val();
    if (fileName == null || fileName == '') {
        $('.clsMessageErr').removeClass('noDisplay');
        $('.clsMessageErr').html(messRequire);
        return;
    }

    // Check extention file
    var extension = fileName.substr( (fileName.lastIndexOf('.') +1));
    if (extension.toLowerCase() != extensionFile) {
        $('.clsMessageErr').removeClass('noDisplay');
        $('.clsMessageErr').html(messExtent);
        return;
    }

    // Check file exists
    var size = $(idFile)[0].files[0].size;
    if (size === 0) {
        $('.clsMessageErr').removeClass('noDisplay');
        $('.clsMessageErr').html(messExists);
        return ;
    }

    // Check size File
    var maxSizeCheck = Number(maxSizeFile);
    if (Number($(idFile)[0].files[0].size) > maxSizeCheck) {
        $('.clsMessageErr').removeClass('noDisplay');
        $('.clsMessageErr').html(messMaxSize);
        return;
    }

    $(idForm).submit();
}

function checkSpecialCharacter(value) {
    var priceRegex = /^[^\\'"&©®%$<>{}]+$/;
    return priceRegex.test(value);
}

function clearMess() {
    $('.clsMess').remove();
    if (!$('.clsMessageErr').hasClass('noDisplay')) {
        $('.clsMessageErr').html('');
        $('.clsMessageErr').addClass('noDisplay');
    }

}

function trackLog(screen, trackName) {
    $.ajax({
        url: urlTrackLog,
        type: 'POST',
        data:{ '_token' : __token, 'key_screen' : screen, 'key_track_log' : trackName},
        dataType: 'text',
        async: false,
        success: function (res) {
        }
    });
}

function openNav() {
```

```
    document.getElementById("mySidenav").style.width = "100%";
    // document.getElementById("base").style.marginLeft = "110";
}

/* Set the width of the side navigation to 0 and the left margin of the page content to 0 */
function closeNav() {
    document.getElementById("mySidenav").style.width = "0";
    // document.getElementById("base").style.marginLeft = "0";
}

function clearMessgeWhenBackBrowser(key) {
    if (typeof readCookie(key) != 'undefined' && readCookie(key) != ''){
        $('.error-msg').remove();
        $('.error-msg-client').addClass('error-msg-no-display');
        eraseCookie(key);
    }
}

function createCookie(name,value,days) {
    if (days) {
        var date = new Date();
        date.setTime(date.getTime()+(days*24*60*60*1000));
        var expires = "; expires="+date.toGMTString();
    }
    else var expires = "";
    document.cookie = name+"="+value+expires+"; path=/";
}

function readCookie(name) {
    var nameEQ = name + "=";
    var ca = document.cookie.split(';');
    for(var i=0;i < ca.length;i++) {
        var c = ca[i];
        while (c.charAt(0)==' ') c = c.substring(1,c.length);
        if (c.indexOf(nameEQ) == 0) return c.substring(nameEQ.length,c.length);
    }
    return null;
}

function eraseCookie(name) {
    createCookie(name, '', false);
}
function monthDiff(d1, d2) {
 var months;
     months = (d2.getFullYear() - d1.getFullYear()) * 12;
     months -= d1.getMonth() + 1;
     months += d2.getMonth();
 return months <= 0 ? 0 : months;
}
```

http://10.228.148.130/app/org/list

```
  var __lang_MR0001 = "パスワードを変更して下さい。";
  var __lang_MR0002 = "パスワードが誤っています。パスワードを確認し、再度入力して下さい。";
  var __lang_GM0050_err_msg = "From～Toの期間を正しく指定してください";
  var __lang_GM0050_err_msg_month = "From～Toの期間が25ヶ月を超えています。正しく指定してください";
  var __lang_GM0060_err_msg = "From～Toの期間を正しく指定してください";
  var urlTrackLog = 'http://10.228.148.130/app/home/trackLog';
  var __token = 'yuEor3ontYoqIVemgYB9Md6zAOEcgAoJnyhA89RA';
  var btnBack = '戻る';
  var btnChoose = 'ファイルを選択';
  var btnClear = 'クリア';
  var banner_soudan = '相談窓口検索バナー';
  var banner_faq = 'FAQ検索バナー';
  var banner_anketo = 'アンケートフォームバナー';

  // In case Faq Management screen
  if ('soudan-showSoudanList' == 'management-faq' || 'soudan-showSoudanList' == 'management-faq-upload') {
      var messRequire = 'アップロードするファイルを選択してください。';
      var messMaxSize = 'This file have large size ';
      var messExtent = 'CSVファイルを指定してください。';
```

```
        var messExists = '対象ファイルがありません。再度選択してください。';
        var extensionFile = 'csv';
        var maxSizeFile = parseInt('67100000') * 1024;
    }

    var __lang_GM0060_err_msg = "From〜Toの期間を正しく指定してください";

   //In case soudan Management screen
    if ('soudan-showSoudanList' == 'soudanbunya-index') {
        var messRequire = 'アップロードするファイルを選択してください。';
        var messMaxSize = 'This file have large size ';
        var messExtent = 'CSVファイルを指定してください。';
        var messExists = '対象ファイルがありません。再度選択してください。';
        var extensionFile = 'csv';
        var maxSizeFile = parseInt('67100000') * 1024;
    }

    //In case soudan Management screen
    if ('soudan-showSoudanList' == 'soudanmadoguchi-index') {
        var messRequire = 'アップロードするファイルを選択してください。';
        var messMaxSize = 'This file have large size ';
        var messExtent = 'CSVファイルを指定してください。';
        var messExists = '対象ファイルがありません。再度選択してください。';
        var extensionFile = 'csv';
        var maxSizeFile = parseInt('67100000') * 1024;
    }

    //In case faq search screen
    if ('soudan-showSoudanList' == 'faq-index') {
        var messSpecialCharacter = '検索不可能な文字(&,<,>,",\',©,®,\\,{,},$,%)が含まれています。';
        var messNoFilter = '検索条件を入力してください。';
    }

    //In case soudan search screen
    if ('soudan-showSoudanList' == 'soudan-index') {
        var messSpecialCharacter = '検索不可能な文字(&,<,>,",\',©,®,\\,{,},$,%)が含まれています。';
        var messNoFilter = '検索条件を入力してください。';
    }
```

http://10.228.148.130/app/org/list

```
            $(document).ready(function() {
            $('.back').click(function(e) {
            trackLog('GC0020.相談窓口一覧', btnBack);
            });
            createCookie('soudanList', "1", true);
            });
```

http://10.228.148.130/app/org/detail/130102044

```
    var __lang_MR0001 = "パスワードを変更して下さい。";
    var __lang_MR0002 = "パスワードが誤っています。パスワードを確認し、再度入力して下さい。";
    var __lang_GM0050_err_msg = "From〜Toの期間を正しく指定してください";
    var __lang_GM0050_err_msg_month = "From〜Toの期間が25ヶ月を超えています。正しく指定してください";
    var __lang_GM0060_err_msg = "From〜Toの期間を正しく指定してください";
    var urlTrackLog = 'http://10.228.148.130/app/home/trackLog';
    var __token = 'yuEor3ontYoqIVemgYB9Md6zAOEcgAoJnyhA89RA';
    var btnBack = '戻る';
    var btnChoose = 'ファイルを選択';
    var btnClear = 'クリア';
    var banner_soudan = '相談窓口検索バナー';
    var banner_faq = 'FAQ検索バナー';
    var banner_anketo = 'アンケートフォームバナー';
```

```
   // In case Faq Management screen
   if ('soudan-showDetailSoudan' == 'management-faq' || 'soudan-showDetailSoudan' == 'management-faq-upload')
 {
       var messRequire = 'アップロードするファイルを選択してください。';
       var messMaxSize = 'This file have large size ';
       var messExtent = 'CSVファイルを指定してください。';
       var messExists = '対象ファイルがありません。再度選択してください。';
       var extensionFile = 'csv';
       var maxSizeFile = parseInt('67100000') * 1024;
   }

   var __lang_GM0060_err_msg = "From〜Toの期間を正しく指定してください";

  //In case soudan Management screen
   if ('soudan-showDetailSoudan' == 'soudanbunya-index') {
       var messRequire = 'アップロードするファイルを選択してください。';
       var messMaxSize = 'This file have large size ';
       var messExtent = 'CSVファイルを指定してください。';
       var messExists = '対象ファイルがありません。再度選択してください。';
       var extensionFile = 'csv';
       var maxSizeFile = parseInt('67100000') * 1024;
   }

   //In case soudan Management screen
   if ('soudan-showDetailSoudan' == 'soudanmadoguchi-index') {
       var messRequire = 'アップロードするファイルを選択してください。';
       var messMaxSize = 'This file have large size ';
       var messExtent = 'CSVファイルを指定してください。';
       var messExists = '対象ファイルがありません。再度選択してください。';
       var extensionFile = 'csv';
       var maxSizeFile = parseInt('67100000') * 1024;
   }

   //In case faq search screen
   if ('soudan-showDetailSoudan' == 'faq-index') {
       var messSpecialCharacter = '検索不可能な文字(&,<,>,",\',©,®,\\,{,},$,%)が含まれています。';
       var messNoFilter = '検索条件を入力してください。';
   }

   //In case soudan search screen
   if ('soudan-showDetailSoudan' == 'soudan-index') {
       var messSpecialCharacter = '検索不可能な文字(&,<,>,",\',©,®,\\,{,},$,%)が含まれています。';
       var messNoFilter = '検索条件を入力してください。';
   }
```

http://10.228.148.130/app/org/detail/130102044

```
       $(document).ready(function() {
         $('.back').click(function(e) {
         trackLog('GC0030.相談窓口詳細', btnBack);
         });
         $('.push-faq').click(function(e) {
         trackLog('GC0030.相談窓口詳細', banner_faq);
         });
         $('.push-soudan').click(function(e) {
         trackLog('GC0030.相談窓口詳細', banner_soudan);
         });
         $('.push-anketo').click(function(e) {
         trackLog('GC0030.相談窓口詳細', banner_anketo);
         });
       });
```

Cookie 8

TOC

名前 値	最初のセット 要求 URL	ドメイン	セキュア 期限切れ
PHPSESSID	http://10.228.148.130/app/org/	10.228.148.130	偽
6ebsdplhncev03jjcb2lk1cia0	http://10.228.148.130/app/org		
XSRF-TOKEN	http://10.228.148.130/app/org/	10.228.148.130	偽
eyJpdiI6Ikl1RldrYk9xZWlXazhaQWZvQVVBVkE9PSIsInZhbHVlIjoic1J5WUFTaTdhVjc0eXBBU0l3WTArWEsyK3NKdFBnT1huQ3hGNmFDTjN5aUlqcFNicHdoajBPelF3a0hsSnBiK1NXbDFTaFlvdm9UalltNkg1dkNKdVE9PSIsIm1hYyI6ImEzNjUyZTdhNmI2N2ZjYzhlMGUzY2ZmMDJhMTk3ZmEyZjgwYjVkNTkxMDU1MjM4MDU4NDAzNzhlNGZjYzE2YzgifQ%3D%3D	http://10.228.148.130/app/org		2018/06/12 10:47:13
laravel_session	http://10.228.148.130/app/org/	10.228.148.130	偽
eyJpdiI6InNsNTZuZzBmYzIyZmgxZlhLN2V0N2c9PSIsInZhbHVlIjoiN1pmWkdkd1NWMWFSb2dnTm5RS1NoZzNKS2ZrcEZpYmxHK3E5dGZqMUlndXZMZnI1QjVtWmdpbWtNcTMzSWh0ZHNCb3BKVDRFdjFGSDJlcVROMnE0cGc9PSIsIm1hYyI6ImU4ODMyYzE2ODg2YjJkMmNjNTJlZDVlNzM2NDZmMThjMGM1NzllN2U4NTZiZGU0ZmYxZTRmNWQ1YzVkODE1ZDgifQ%3D%3D	http://10.228.148.130/app/org		2018/06/12 10:47:13
soudanList	http://10.228.148.130/app/home/trackLog		偽
soudanList	http://10.228.148.130/app/org		偽
soudanList 1	http://10.228.148.130/app/org/		偽

	detail/130102044	
soudanList		偽
1	http://10.228.148.130/app/org/detail/130100001	
soudanList		偽
1	http://10.228.148.130/app/org/list?page=1	