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>
```

example.jp/4h/4h-020.html#http://example.jp/4h/4h-021.html

処理を行います 実行

example.jp/4h/4h-020.html#http:// | http://example.jp/4h/4h-020.html#

view-source:http://example.jp/4h/4h-020.html#http://example.jp/4h/4h-021.html

```
1 <body>
2 処理を行います <input type="button" value="実行" onclick="go()">
3 <script>
4 function go() {
5   // 様々な処理
6   var url = location.hash.slice(1);
7   if (url.match(/^https?:¥/¥//)) {
8     location.href = url;
9   } else {
10    alert('遷移先URLが不適切');
11  }
12 }
13 </script>
14 </body>
```

example.jp/4h/4h-021.html

実行しました

example.jp/4h/4h-021.html | http://example.jp/4h/4h-021.html

view-source:http://example.jp/4h/4h-021.html

```
1 <body>
2 実行しました
3 </body>
```

【サーバ： 4h/4h-020.html 】

/var/www/html/4h/4h-020.html - wasbook@example.jp - エディタ - WinSCP

文字コード 色

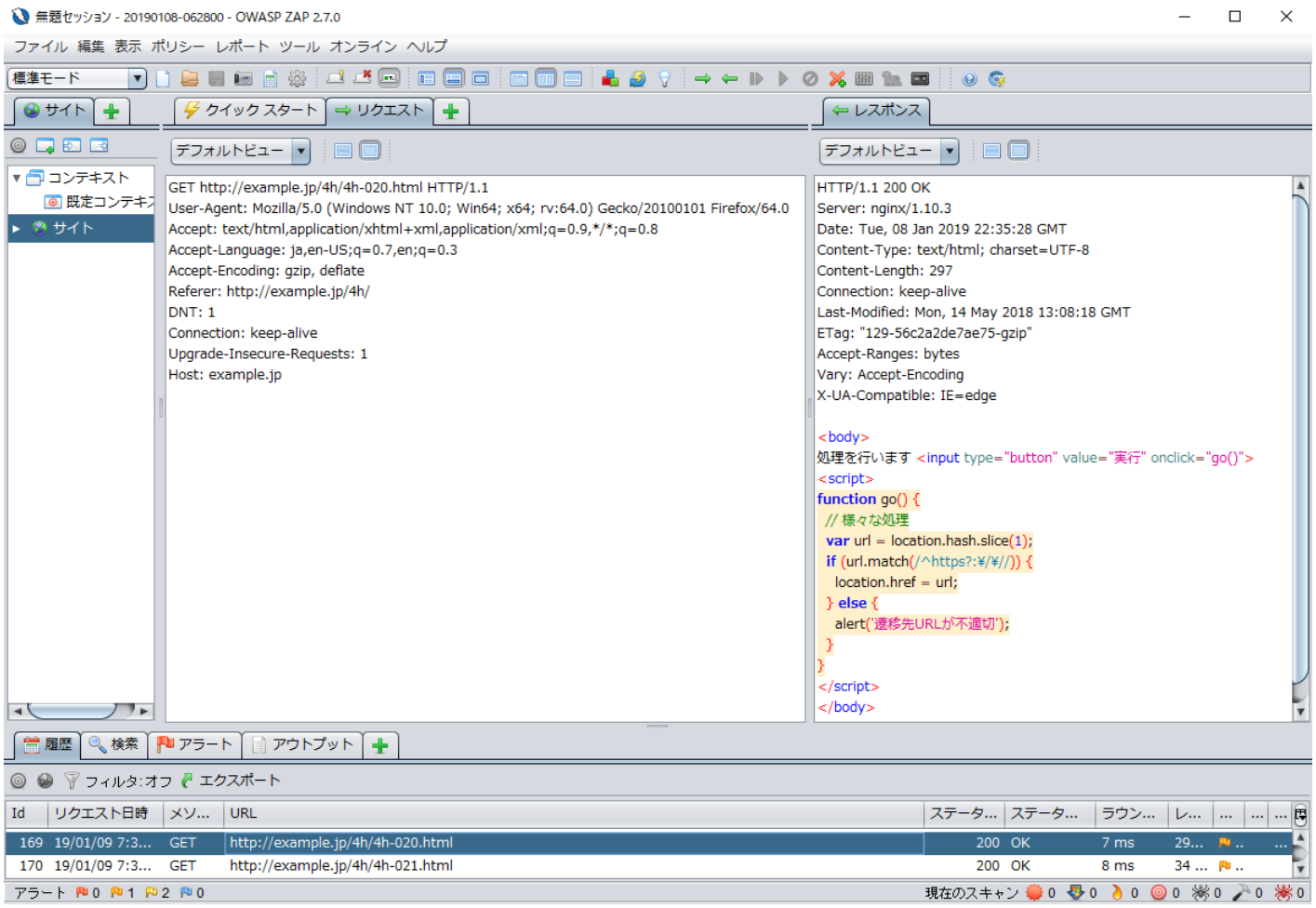
```
<body>
処理を行います <input type="button" value="実行" onclick="go()">
<script>
function go() {
  // 様々な処理
  var url = location.hash.slice(1);
  if (url.match(/^https?:\/\//)) {
    location.href = url;
  } else {
    alert('遷移先URLが不適切');
  }
}
</script>
</body>
```

【サーバ： 4h/4h-021.html 】

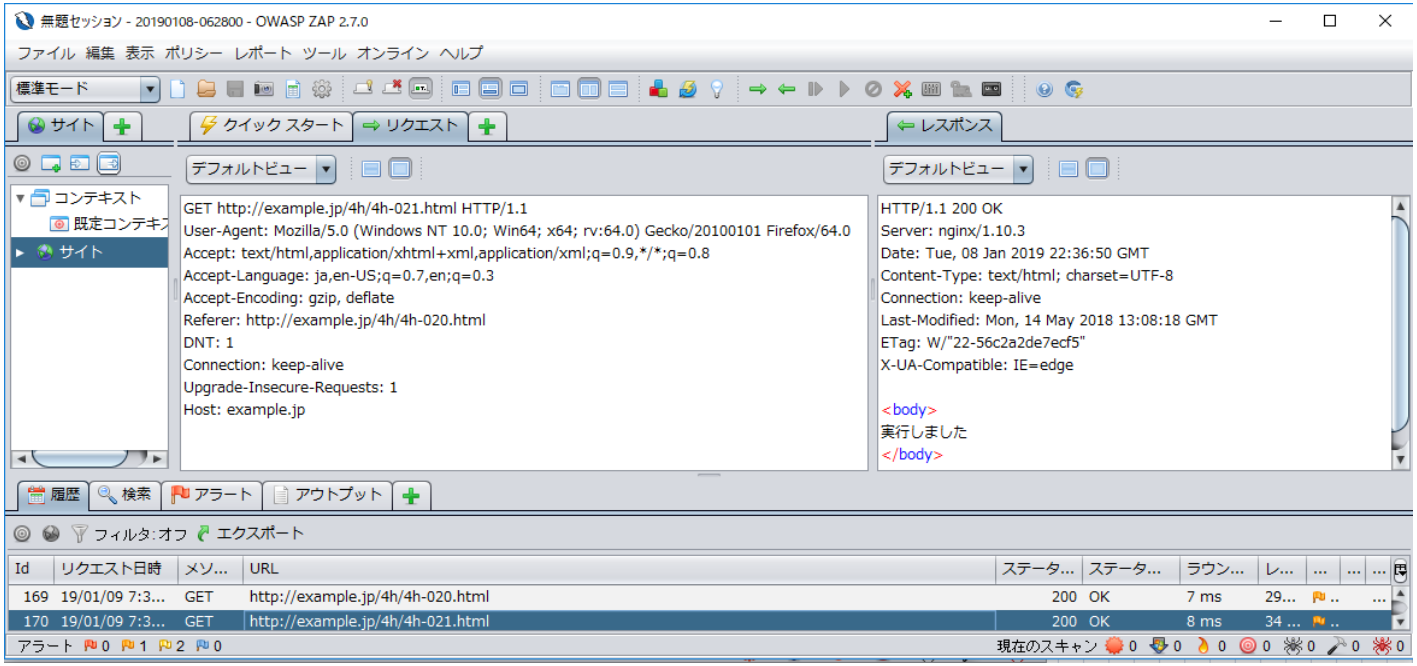
/var/www/html/4h/4h-021.html -

```
<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 】



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



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
  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)

```
<li>4.17.4 オープンリダイレクト</li>
<ol>
<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>
<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>
<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>
<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>
</ol>
```

example.jp/4h/4h-020.html#http://trap.example.com/4h/4h-901.html

処理を行います 実行

view-source:http://example.jp/4h/4h-020.html#http://trap.example.com/4h/4h-901.html

```
<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>
```

trap.example.com/4h/4h-901.html

ログインタイムアウトにより処理に失敗しました。
ID
パスワード
ログイン

view-source:http://trap.example.com/4h/4h-901.html

```
<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>
```

trap.example.com/4h/4h-902.php

IDとパスワードを盗みました
ID: miko
パスワード: HIMITSU1234
10秒後に本来のURLに遷移します。

view-source:http://trap.example.com/4h/4h-902.php

```
<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>
```

example.jp/4h/4h-021.html

実行しました

view-source:http://example.jp/4h/4h-021.html

```
<body>
実行しました
</body>
```

【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-021.html 】

/var/www/html/4h/4h-021.html -

```
<body>
実行しました
</body>
```

【サーバ： 4h/4h-901.html 】

/var/www/html/4h/4h-901.html - wasbook@example.jp - エディタ - WinSC

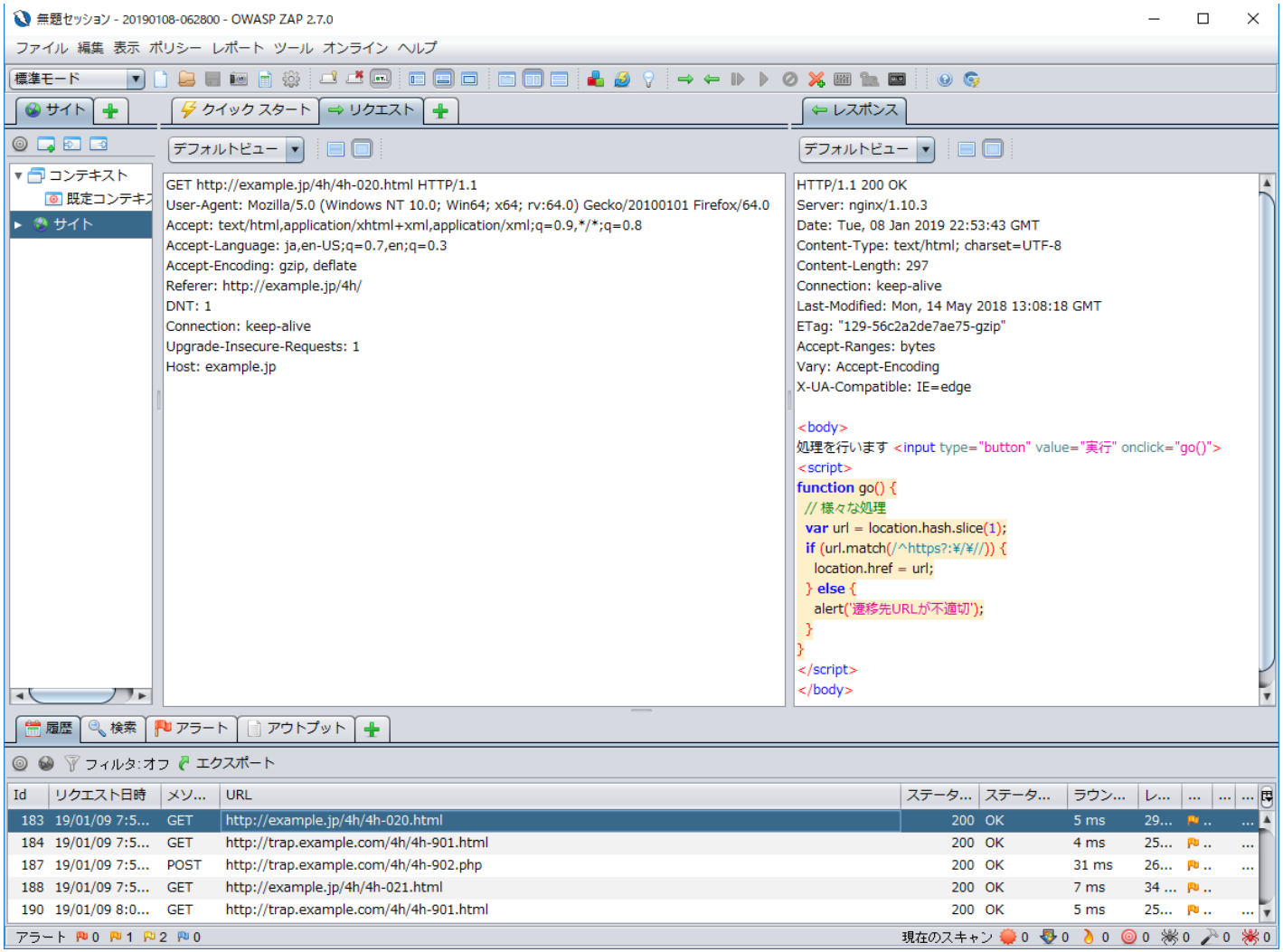
```
<body>
ログインタイムアウトにより処理に失敗しました。<br>
<form action="4h-902.php" method="post">
ID <input name="id"><br>
パスワード <input name="pwd" type="password"><br>
<input type="submit" value="ログイン">
</form>
```

【サーバ： 4h/4h-902.php 】

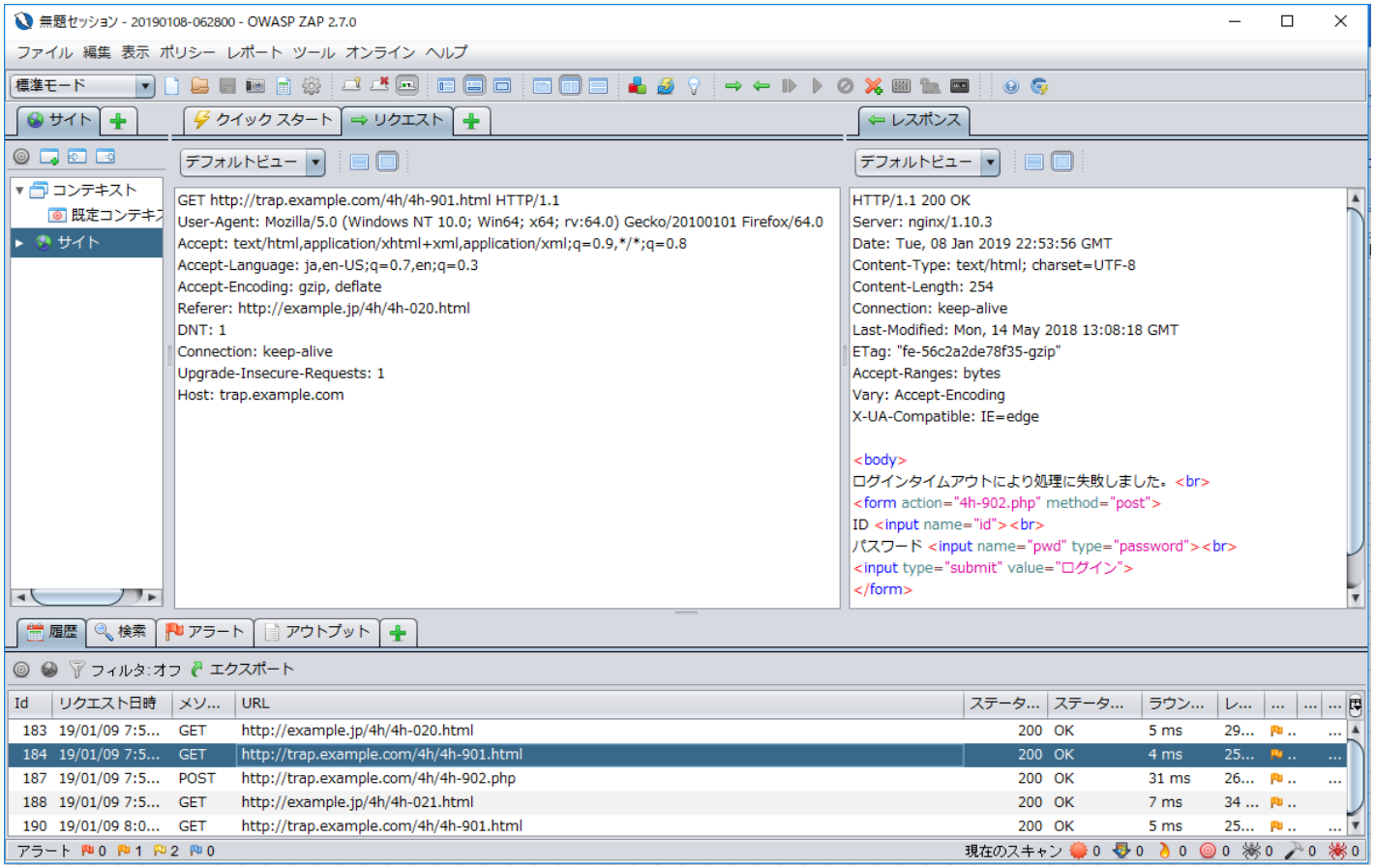
/var/www/html/4h/4h-902.php - wasbook@example.jp - エディタ - WinSCP

```
<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>
```

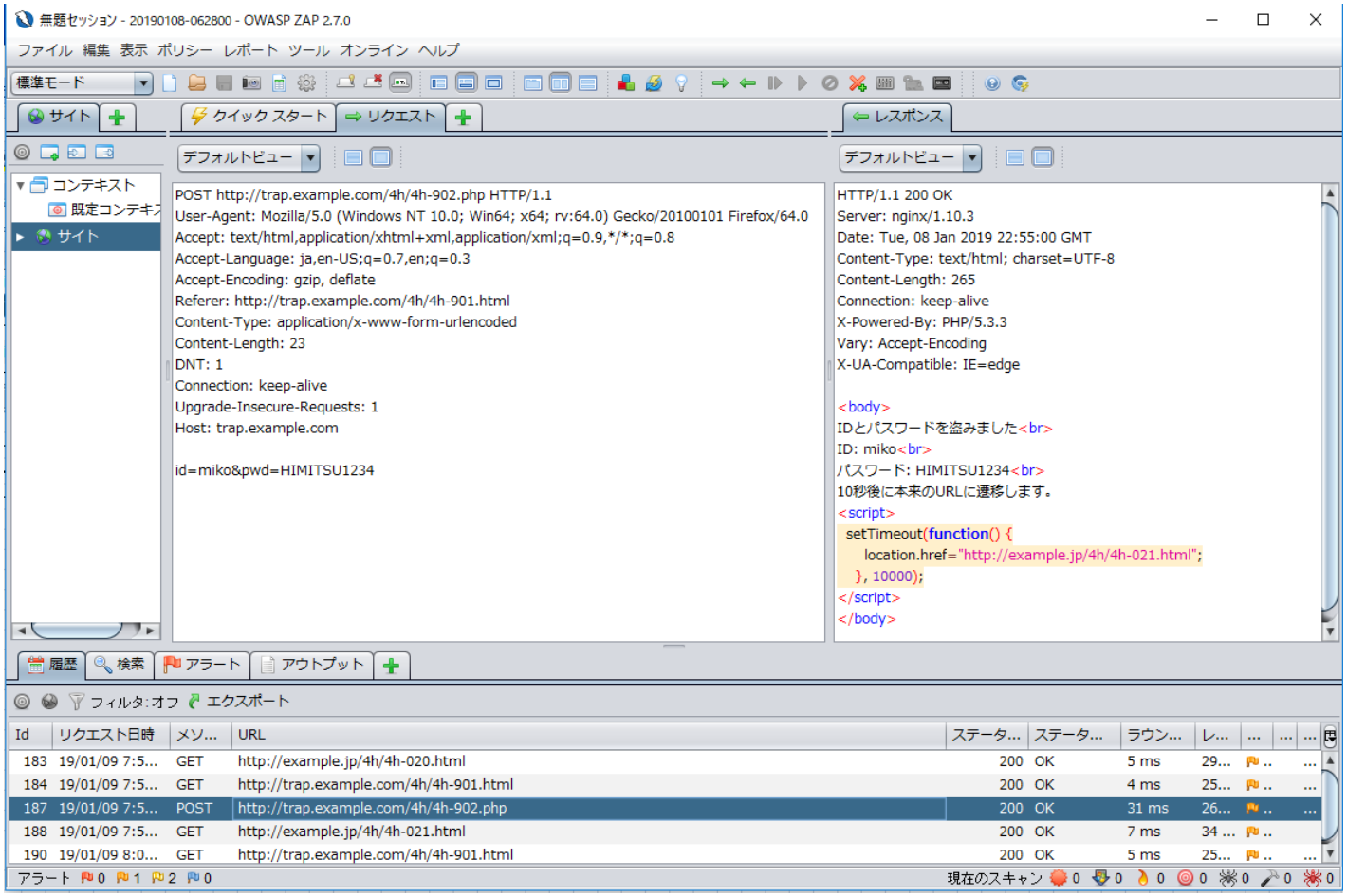
【ブラウザ→サーバ： リクエスト 4h/4h-020.html → レスポンス 】



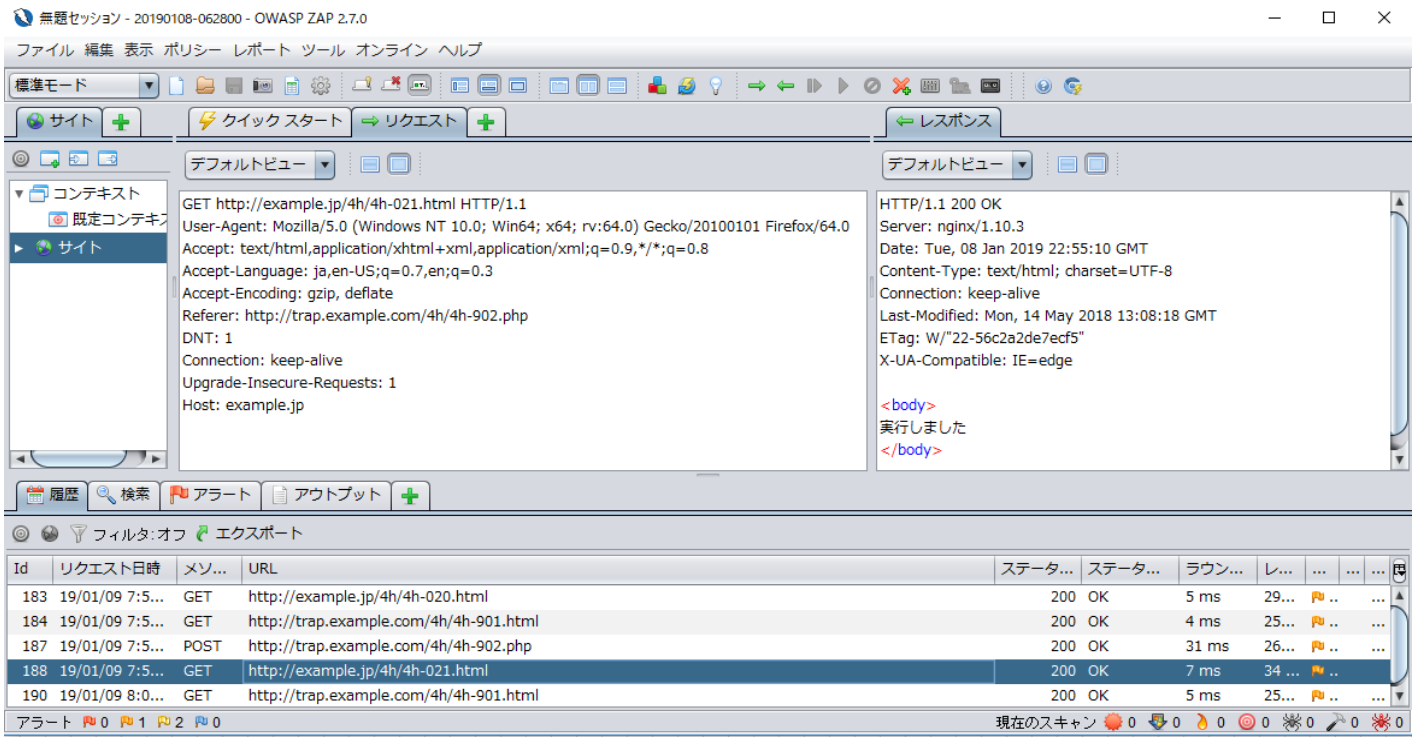
【ブラウザ→サーバ： リクエスト trap.example.com/4h/4h-901.html → レスポンス 】



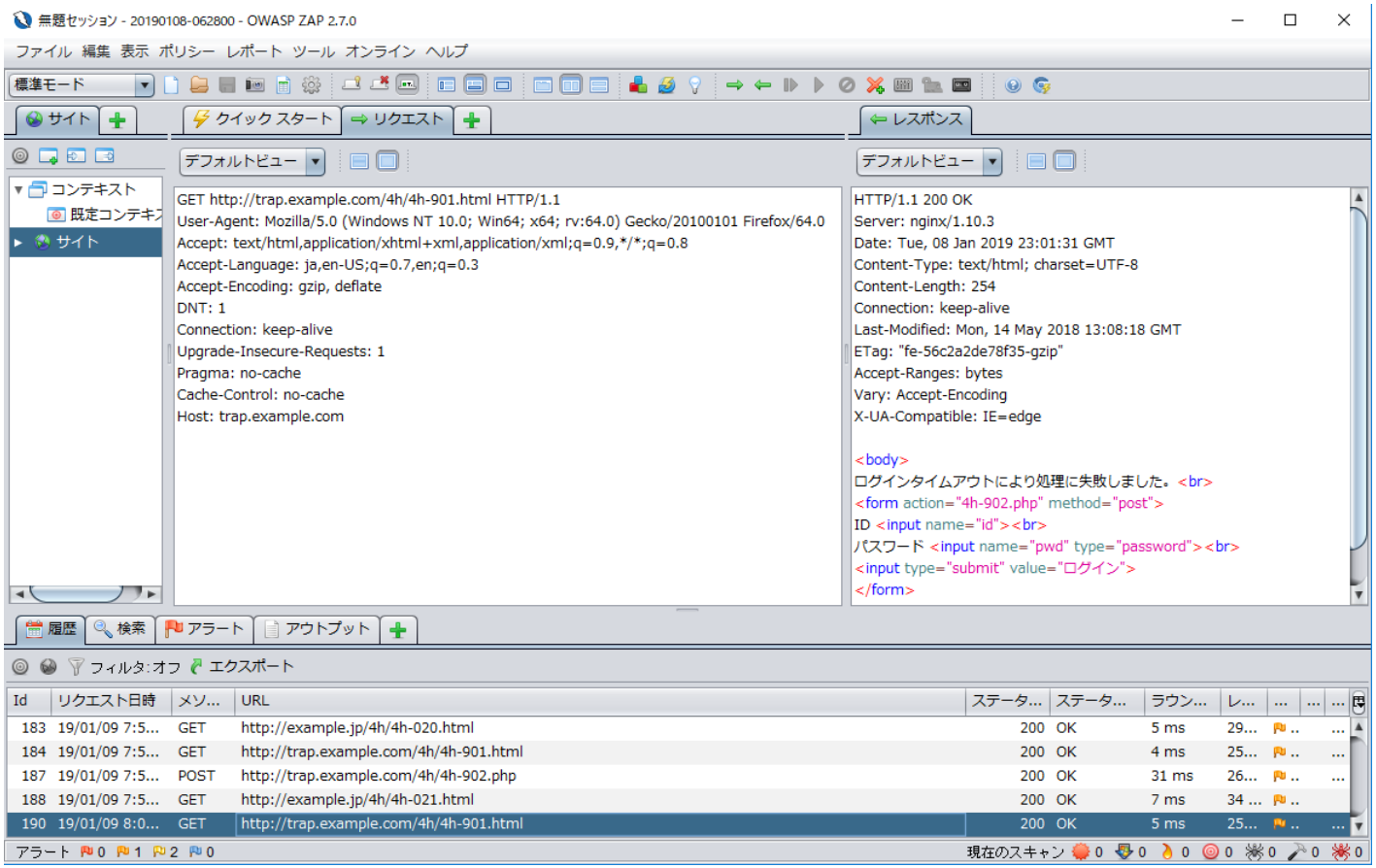
【ブラウザ→サーバ： リクエスト trap.example.com/4h/4h-902.php → レスポンス 】



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



【ブラウザ→サーバ： リクエスト trap.example.com/4h/4h-901.php → レスポンス 】

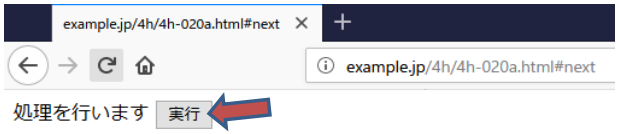


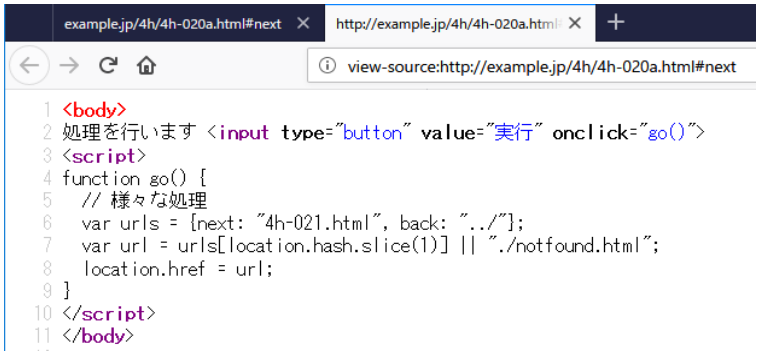
4h-020a:オープンリダイレクト対策版(正常系)

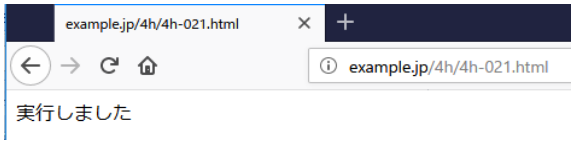
【ブラウザ】

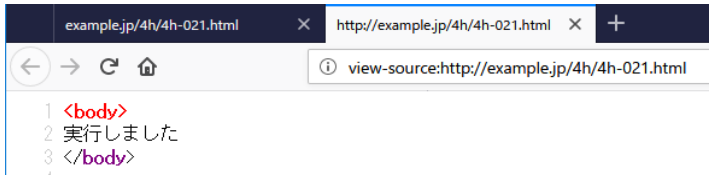
- 4.17.4 オープンリダイレクト
  1. 4h-020 :オープンリダイレクト(正常系)
  2. 4h-020 :オープンリダイレクト(攻撃)
  3. 4h-020a:オープンリダイレクト対策版(正常系)
  4. 4h-020a:オープンリダイレクト対策版(攻撃)

```
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>
```



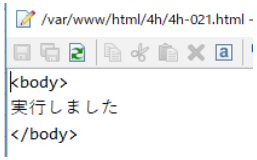




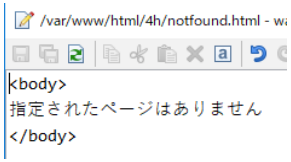


【サーバ: 4h/4h-020a.html 】

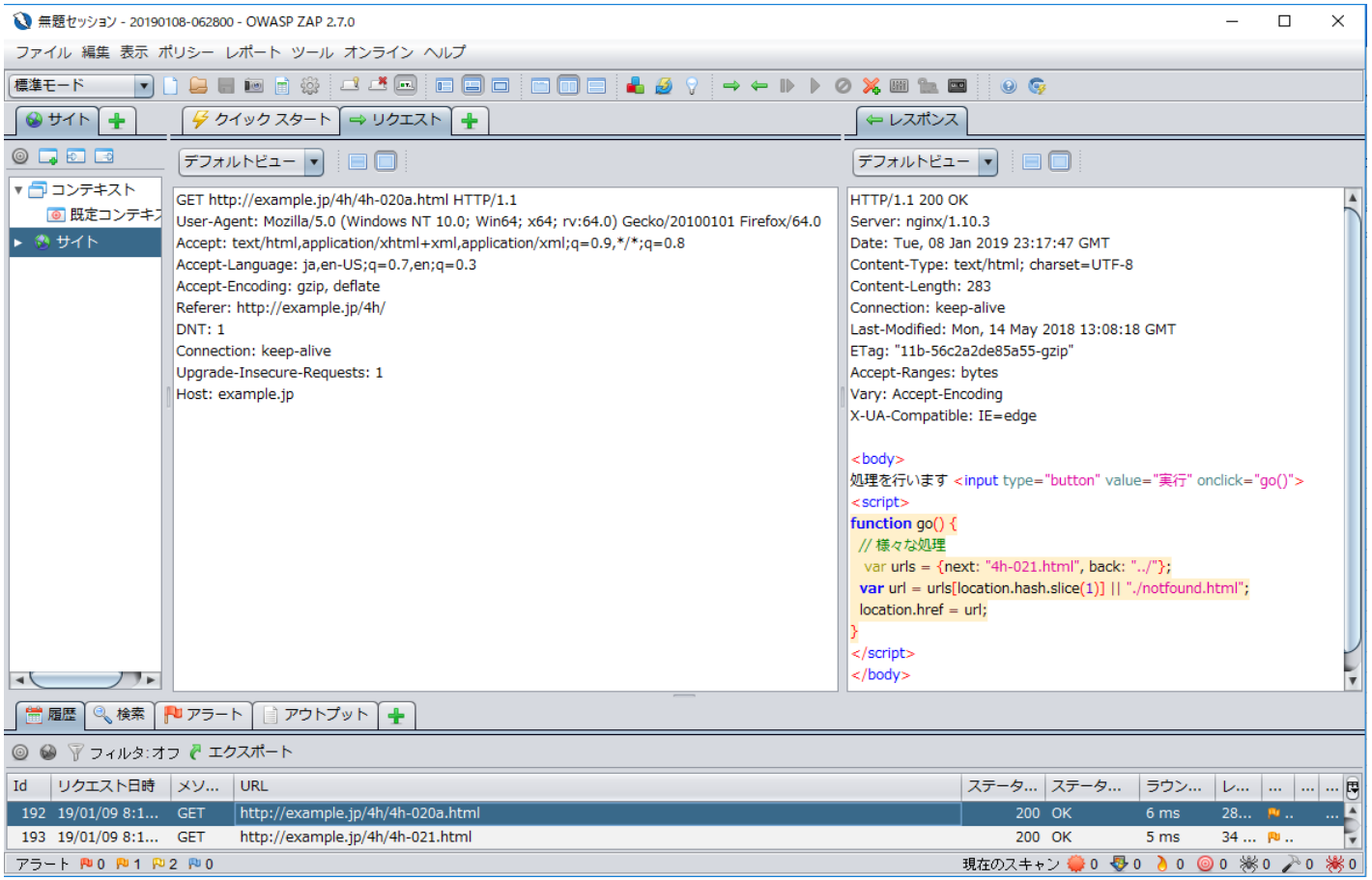
【サーバ: 4h/4h-021.html 】



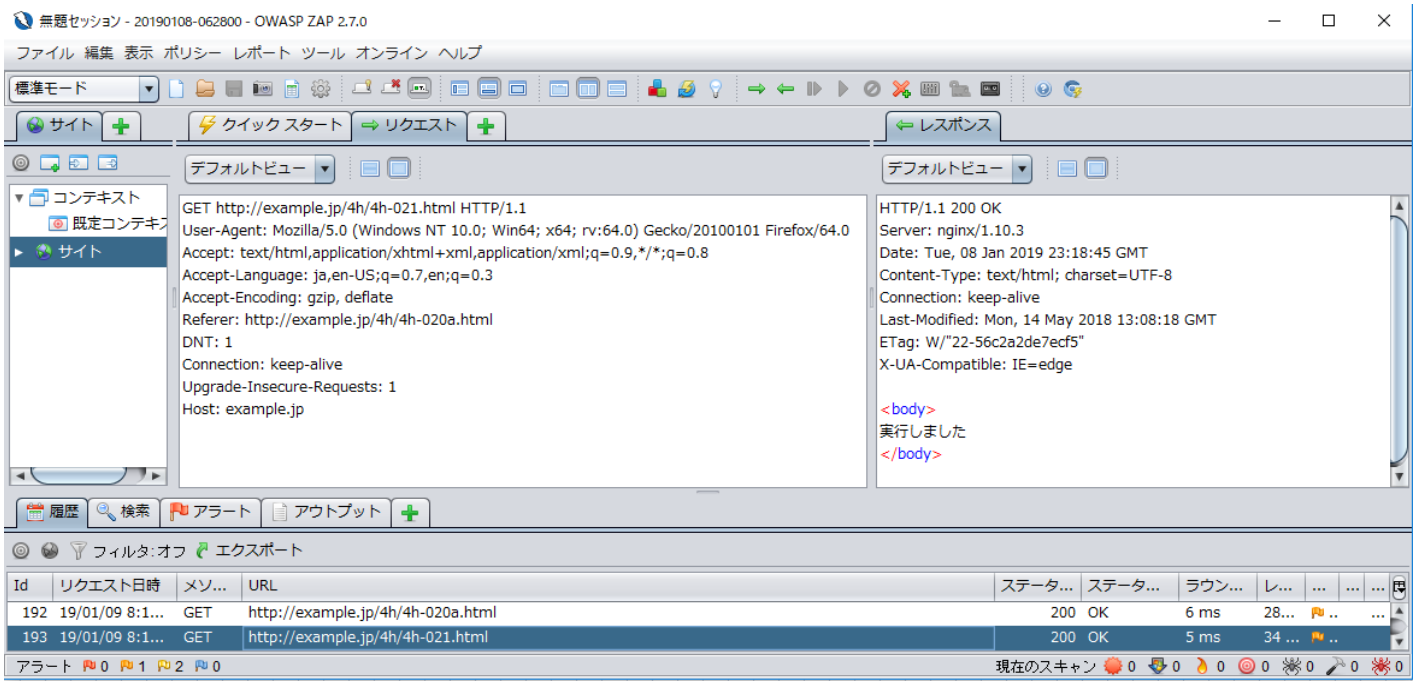
【サーバ: 4h/notfound.html 】



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



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

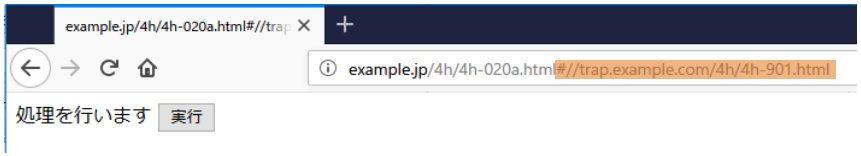


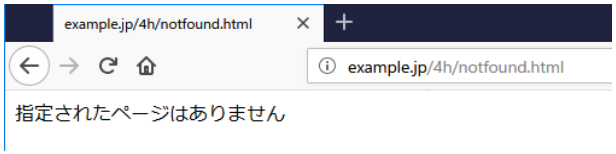
4h-020a:オープンリダイレクト対策版(正常系)

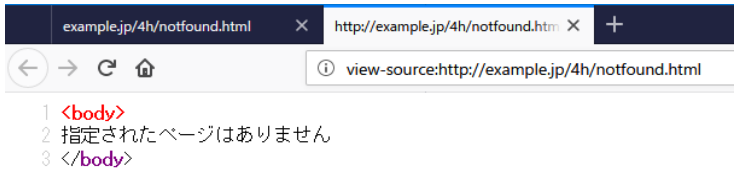
【ブラウザ】

- 4.17.4 オープンリダイレクト
  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)

```
<li>4.17.4 オープンリダイレクト</li>
<ol>
<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>
<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>
<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>
<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>
</ol>
```







【サーバ: 4h/4h-020a.html 】

```
<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 】

```
<body>
実行しました
</body>
```

【サーバ: 4h/notfound.html 】

```
<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

文字コード

```
<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

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
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

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...
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

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