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摂取される
②デバイスドライバやパッチと称して、マルウエアを配布される

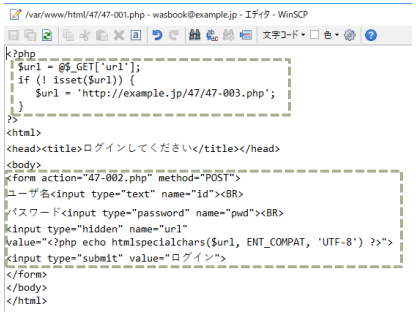
オープンリダイレクト脆弱性の対策

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）

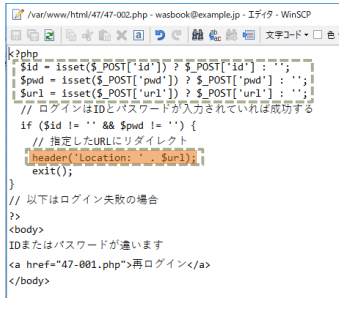
オープンリダイレクタ　47-001:正常系

【ブラウザ】

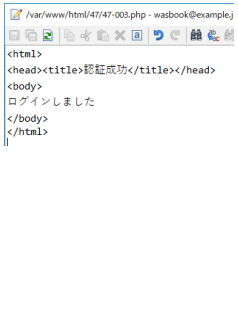
【サーバ：　47/47-001.php　】



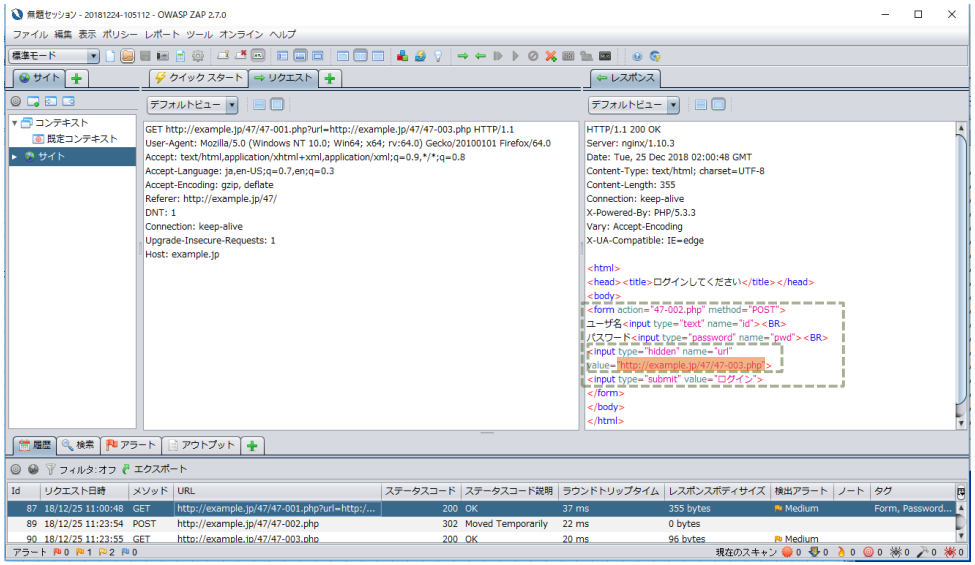
【サーバ：　47/47-002.php　】



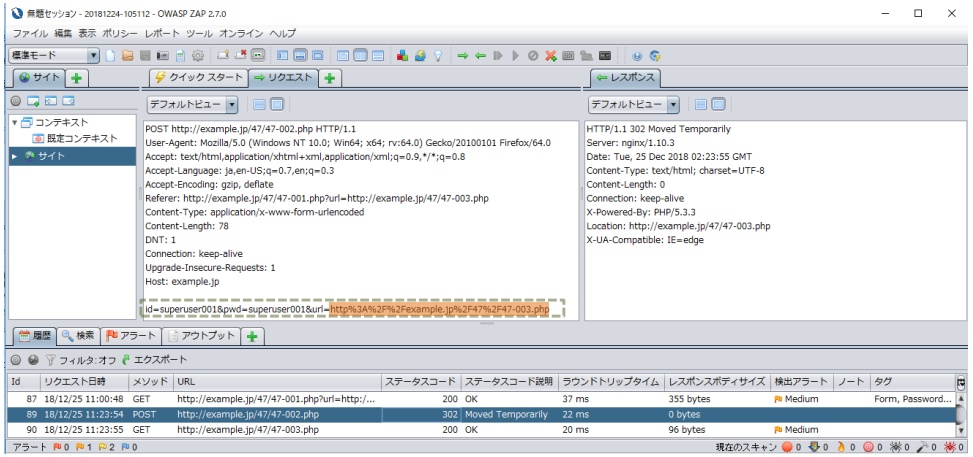
【サーバ：　47/47-003.php　】



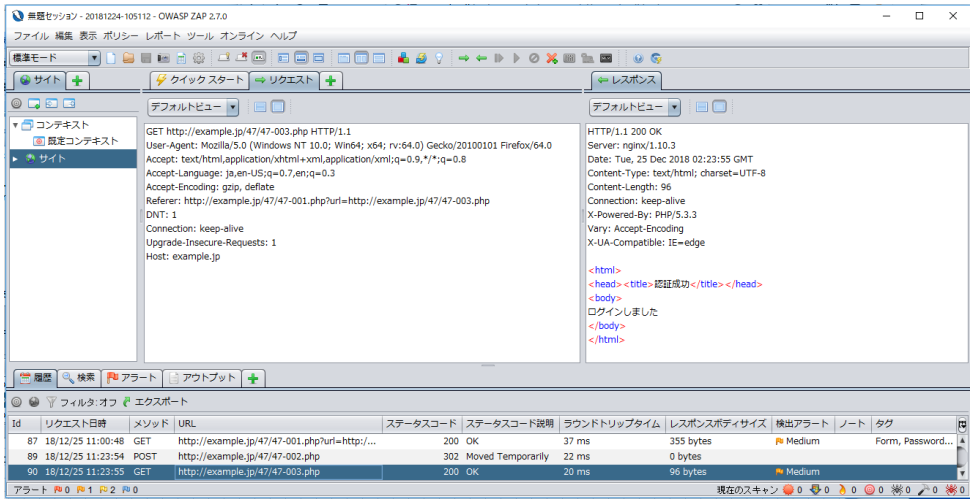
【ブラウザ→サーバ： リクエスト 47/47-001.php → レスポンス 】オープンリダイレクタ 正常系



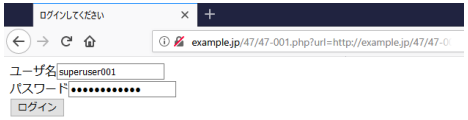
【ブラウザ→サーバ： リクエスト 47/47-002.php → レスポンス 】オープンリダイレクタ 正常系

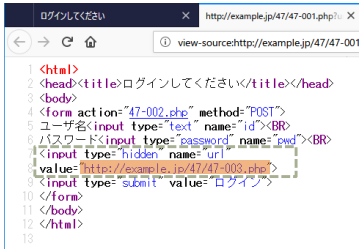


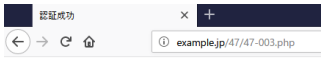
【ブラウザ→サーバ：リクエスト 47/47-003.php → レスポンス 】オープンリダイレクタ 正常系



【ブラウザ】

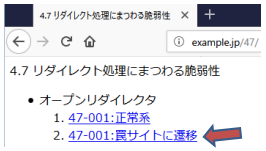


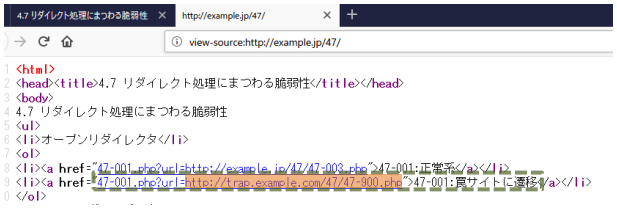




オープンリダイレクタ　47-001:罠サイトに遷移

【ブラウザ】





【サーバ：　47/47-001.php　】

/var/www/html/47/47-001.php - wasbook@example.jp - エディタ - WinSCP

```
<?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　】

/var/www/html/47/47-002.php - wasbook@example.jp - エディタ - WinSCP

```
<?php
  $id = isset($_POST['id']) ? $_POST['id'] : '';
  $pwd = isset($_POST['pwd']) ? $_POST['pwd'] : '';
  $url = isset($_POST['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>
IDまたはパスワードが違います
<a href="47-001.php">再ログイン</a>
</body>
```

【サーバ：　47/47-900.php　】

/var/www/html/47/47-900.php - wasbook@example.jp - エディタ - WinSCP

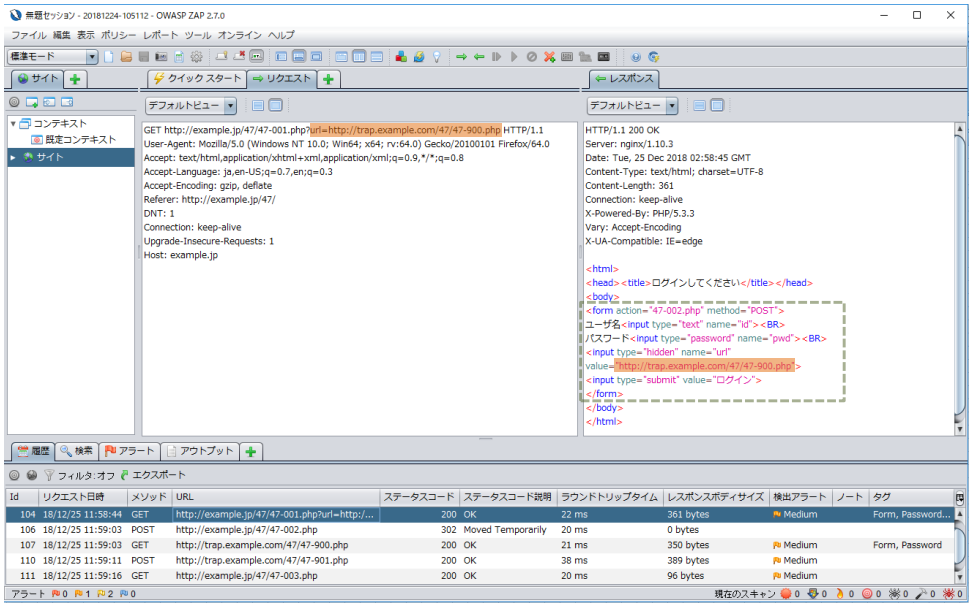
```
<html>
<head><title>ログインエラー</title></head>
<body>
IDまたはパスワードが違います。再度認証してください。
<form action="47-901.php" method="POST">
ユーザ名<input type="text" name="id"><BR>
パスワード<input type="password" name="pwd"><BR>
<input type="submit" value="ログイン">
</form>
</body>
</html>
```

【サーバ：　47/47-901.php　】

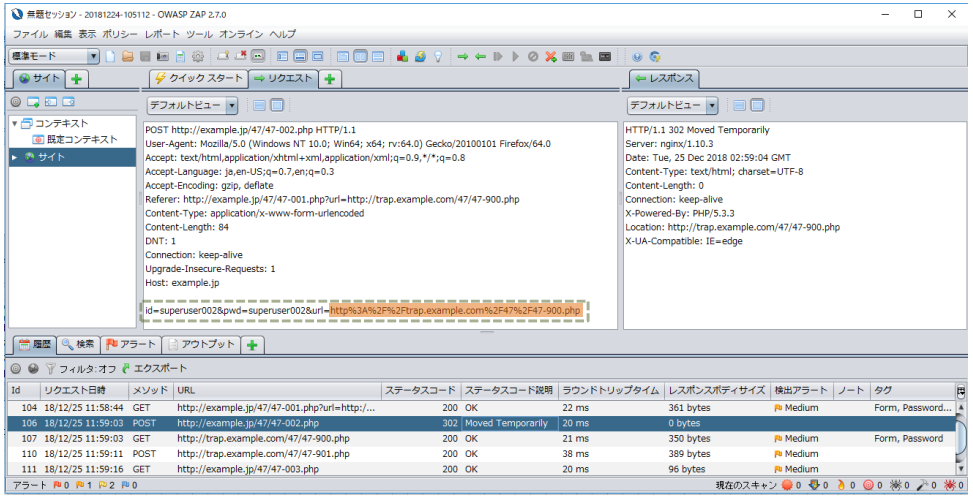
/var/www/html/47/47-901.php - wasbook@example.jp - エディタ - WinSCP

```
<?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>
```

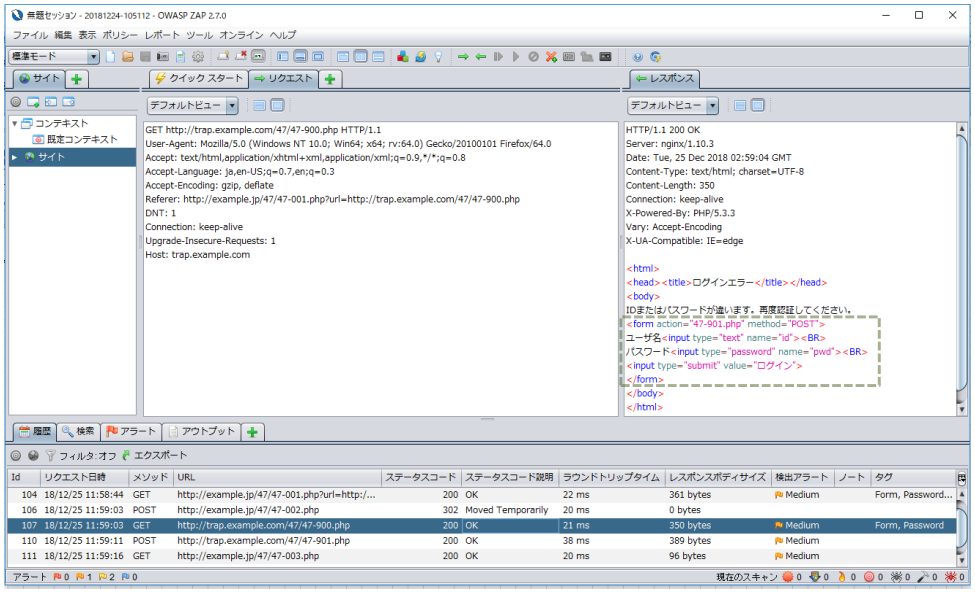
【ブラウザ→サーバ：リクエスト 47/47-001.php → レスポンス 】オープンリダイレクタ 裏サイトに遷移



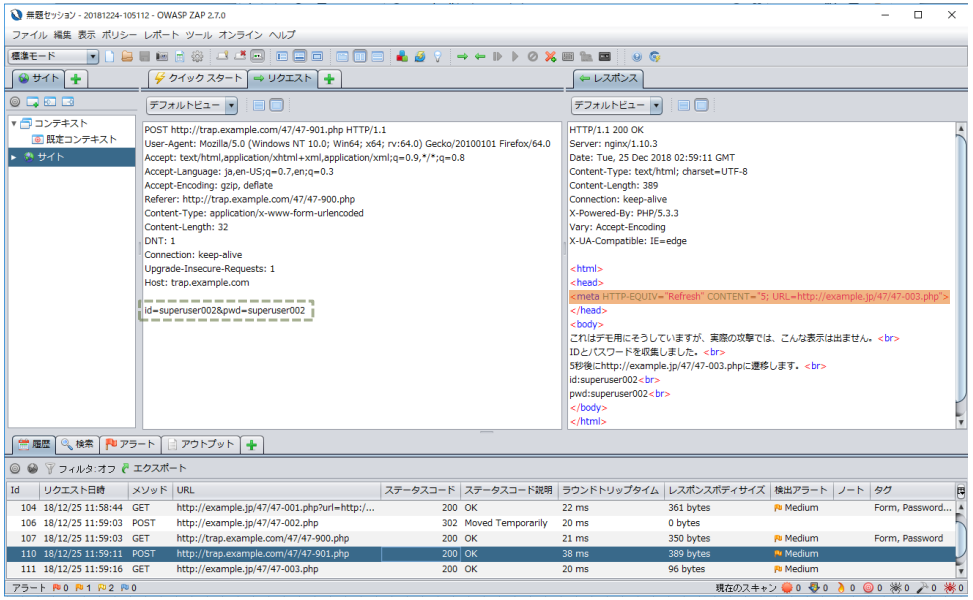
【ブラウザ→サーバ：リクエスト 47/47-002.php → レスポンス 】オープンリダイレクタ 裏サイトに遷移



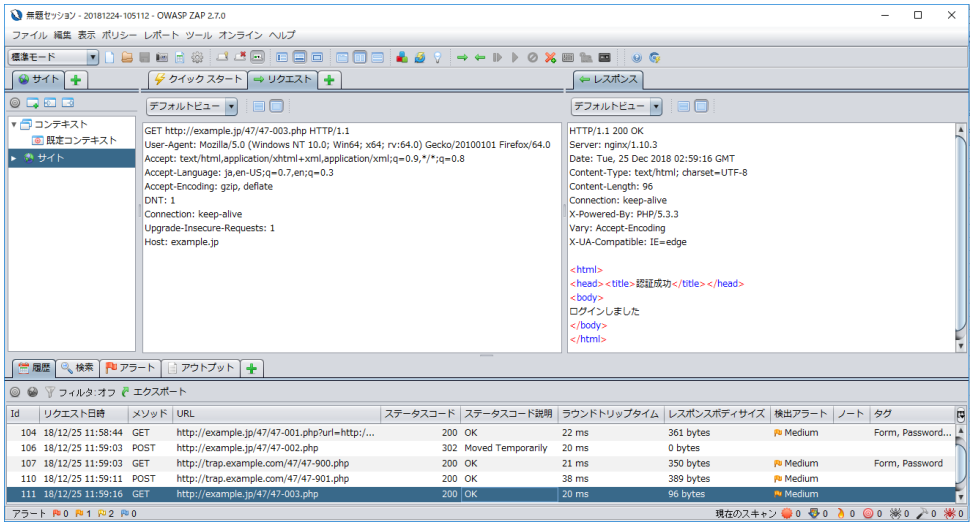
【ブラウザ→偽サーバ：リクエスト trap.example.com/47/47-900.php → レスポンス 】オープンリダイレクタ 罠サイトに遷移



【ブラウザ→偽サーバ：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 罠サイトに遷移



【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 裏サイトに遷移



【ブラウザ】