

---

# Security of HTTPHeader

2007 年 03 月 05 日

Ver. 1.0

---

# 目次

<b>1</b>	<b>WebAppli で使う HTTP ヘッダ作成関数の安全な使い方</b>	<b>2</b>
1.1	本文書の目的	3
<b>2</b>	<b>HTTP ヘッダ・インジェクションの概要</b>	<b>4</b>
2.1	HTTP ヘッダ・インジェクションの概要	5
2.2	HTTP ヘッダ・インジェクションへの対策	6
<b>3</b>	<b>HTTP ヘッダ・インジェクションの具体的な安全策</b>	<b>7</b>
3.1	CGI の場合	8
3.2	IIS + ASP の場合	8
3.3	ASP.NET の場合	10
3.4	JavaServlet の場合	12
3.5	PHP5.2.0 の場合	14
<b>4</b>	<b>執筆者など</b>	<b>17</b>
4.1	本文書の免責事項	18
4.2	執筆者	18
4.3	更新履歴	18
4.4	本文書の最新バージョン	18
4.5	HTTP ヘッダ名	18

# 1 WebAppli で使う HTTP ヘッダ作成関数の安全な使い方

## 1.1 本文書の目的

本文書は、Web アプリケーションで利用されている各種 HTTP ヘッダ作成関数の安全な使い方について検討する。

本文書で対象としている脅威は、主に以下である。

- HTTP ヘッダ・インジェクション (HTTP Response Splitting[ 1 ])

HTTP ヘッダ・インジェクションというより、「HTTP Response-Splitting 攻撃」の方が有名であろう。

しかしながら、どの関数が改行コードを許しているのかを調査している文献が見受けられなかった。一方で、[システム開発者|プログラマ]にとっては、このような情報が必要な情報であると感じ、本文書を作成した。

[ 1 ] 「HTTP Response Splitting, Web Cache Poisoning Attacks, and Related Topics」

<https://www.watchfire.com/securearea/whitepapers.aspx?id=8>

## 2 HTTP ヘッダ・インジェクション の概要

---

## 2.1 HTTP ヘッダ・インジェクションの概要

Web で使用している HTTP は、テキスト形式の通信プロトコルであり、空行を挟み、前段を「HTTP ヘッダ」、後段を「HTTP ボディ」と分ける構造となっている。

また「HTTP ヘッダ」は、ヘッダ情報を一行に一つを基本形式としている。

Web ブラウザと Web アプリケーション間でのクッキー情報の交換や、Web ページのリダイレクト先を示す URI の情報交換などに HTTP ヘッダは用いられている。

そして、ほとんどの Web アプリケーションには、HTTP ヘッダを操作する関数が用意されている。Web アプリケーションプログラマが一般的に利用するのは以下の 3 つであると思われる。

- クッキーを Web ブラウザへ送信する関数
- Web ページのリダイレクトを命令する関数
- 任意の HTTP ヘッダを[追加|上書]する関数

これらの関数に汚染データ[ ]を渡した場合、汚染データ中に改行コード(ヘッダ情報の区切りが改行コードであるため)を挿入することによって、任意の HTTP ヘッダを挿入されてしまうというのが、HTTP ヘッダ・インジェクションである。

また、クッキー情報の各プロパティは「;(セミコロン)」をデリミタとしているため、「;」をはさんで、任意のプロパティを指定される危険性もある。

脅威は、

- 任意の HTTP ヘッダを挿入される
- クッキー情報に任意のプロパティを挿入される
- HTTP Response Splitting

などであるが、現実的な深刻度はそれほど高くない。

しかし、Web アプリケーションを開発する[システム開発者|プログラマ]の方々には、このようなそれほど深刻度が低いセキュリティ問題といえども放置せずに、適切なプログラミングを行うことを希望する。

[ ] 汚染データ

ここでは、利用者から Web アプリケーションへ入力された安全な書式であると検証されていないデータと定義する。「汚染されているかも知れないデータ」とした方がより正確であるような気がする。

## 2.2 HTTP ヘッダ・インジェクションへの対策

HTTP ヘッダを操作する関数に汚染データを与える場合、改行コードについてサニタイズ処理を実施する。

ASP/ASP.NET や PHP では、URL エンコードを実施している。

もし、読者が利用している Web アプリケーション用の開発環境の HTTP ヘッダ作成関数内部でサニタイズ処理を行っていないのであれば、ASP/ASP.NET や PHP の方法を模倣して、Web アプリケーションプログラマがそれらの関数を用いる前に、URL エンコードを実施すればよいだろう。

また、クッキー情報の各プロパティは「;(セミコロン)」をデリミタとしている。利用する関数内部でサニタイズ処理していなければ、Web アプリケーションプログラマ自身が事前に「;(セミコロン)」を URL エンコードすればよいだろう。

以下の章で明らかとなるが、ASP/PHP と Java とでは、異なるサニタイズ処理がおこなわれていた。

どちらが正しいのだろうか。

### 3 HTTP ヘッダ・インジェクション の具体的な安全策

### 3.1 CGI の場合

CGI では、HTTP ヘッダも含めて HTTP リクエスト全体(HTTP ヘッダ+HTTP ボディ)を CGI プログラムが作成する必要がある。

よって、HTTP ヘッダを作成中に汚染データを使う場合、汚染データ中の改行コードに注意する必要がある。

また、クッキー情報の各プロパティは、「;(セミコロン)」をデリミタとしているため、クッキー情報の HTTP ヘッダを作成する際は「;(セミコロン)」もサニタイズ処理する必要がある。

### 3.2 IIS + ASP の場合

IIS + ASP での HTTP ヘッダ操作は、以下の関数がよく使われる。

関数名	操作内容
Response.Redirect	Web ページのリダイレクト要求
Response.Cookies	クッキー情報の送信
Response.AddHeader	任意ヘッダの追加

これらの関数に汚染データが配置されるようなテストプログラム(図 3.2-1)を作成し、Netcat を使ってどのような HTTP レスポンスが返るかを観察した。

MS-WindowsServer2003 SP1(日本語版)を実験環境として使用した。

```
<%
Option Explicit
Dim str
str = Request.QueryString("inputData")
Response.AddHeader "TestHeader",str
Response.Cookies("TestCookie") = str
Response.Redirect str
%>
```

図3.2-1 : ASP のヘッダ送信関数の実験プログラム



```
コマンド プロンプト
C:\>type in.txt
GET /httpHeaderTest.asp?inputData=TEST%0d%0atest;abc HTTP/1.0

C:\>nc -nvw 127.0.0.1 80 < in.txt
(UNKNOWN) [127.0.0.1] 80 (?) open
HTTP/1.1 302 Object moved
Connection: close
Date: Fri, 15 Dec 2006 14:15:13 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-Powered-By2: PHP 5
TestHeader: TEST
test;abc
Location: TEST%0D%0Atest%3Babc
Content-Length: 141
Content-Type: text/html
Set-Cookie: TestCookie=TEST%0D%0Atest%3Babc; path=/
Set-Cookie: ASPSESSIONIDCCBRATTS=N1PFPGFBEOKIFKEHDCFKJDP; path=/
Cache-control: private

<head><title>Object moved</title></head>
<body><h1>Object Moved</h1>This object may be found <a HREF="TEST%0D%0Atest%3Babc" here</a>.</body>
```

図3.2-2： 図 3.2-1の結果

結果は、図 3.2-2のように、AddHeader() 関数以外は関数内部で改行コードのサニタイズ処理が行われていることが確認された。

よって、ASP で上記の関数を使う場合、AddHeader() 関数以外は HTTP ヘッダ・インジェクションに気を使わずにコーディングを行うことができる。

また、AddHeader() 関数を使用する際には、ASP プログラム内で改行コードをサニタイズ処理(他の関数との関係も考えれば、URL エンコードが妥当だろう)することがセキュリティ対策上必要な対策である、ということである。

蛇足:

- 図 3.2-2のように、ASP では、改行コード(Cr と Lf)などが、URL エンコードされている。
- Location ヘッダには、汚染データそのものが与えられている。汚染データに別サイトの URL を指定される必要がない場合は、その対策が別途必要である。
- クッキー情報の箇所では「;」がサニタイズ処理されている(「;」が URL エンコードされ「%3B」になっている)。よって、ASP.NET とは異なり、クッキー情報の値をセットする際には、とくにセキュリティ対策を考慮しなくてもよい。ということになる。

### 3.3 ASP.NET の場合

ASP.NET での HTTP ヘッダ操作は、以下の関数がよく使われるだろう。

関数名	操作内容
Response.RedirectLocation	Web ページのリダイレクト要求
Response.Cookies.Add	クッキー情報の送信
Response.AddHeader Response.AppendHeader	任意ヘッダの追加

これらの関数に汚染データが渡るようなテストプログラム(図 3.3-1)を作成し、Netcat を使ってどのような HTTP レスポンスが返るかを観察した。

MS-Windows2000 SP4(日本語版)上の WebMatrix0.6.812 + .Net Framework1.1SP1(1.1.4322) を実験環境として使用した。

```
// ヘッダ追加用メソッド
Response.AddHeader("myAddHeader", TextBox1.Text);
Response.AppendHeader("myAppendHeader", TextBox1.Text);

// クッキー送信用メソッド
HttpCookie MyCookie = new HttpCookie("myAddCookie");
MyCookie.Value = TextBox1.Text;
Response.Cookies.Add(MyCookie);

// リダイレクト用メソッド
Response.RedirectLocation = TextBox1.Text;
```

図3.3-1 : ASP.NET のヘッダ送信関数の実験プログラム (C#)

```

C:\>type in.txt
POST /AppendHeader/AppendHeaderCS.aspx HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 107

TextBox1=TEST%0d%0atest%3Babc&Button1=Button&__VIEWSTATE=dDwtMjA0ODIyNzQyMjs7Psy
iB66T137EeXSIYy%2BR7g7hQMsb
C:\>nc -nv 127.0.0.1 80 < in.txt
(UNKNOWN) [127.0.0.1] 80 (?) open
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Fri, 15 Dec 2006 14:34:57 GMT
X-Powered-By: ASP.NET
X-AspNet-Version: 1.1.4322
myAddHeader: TEST%0d%0atest;abc
myAppendHeader: TEST%0d%0atest;abc
Location: TEST%0d%0atest;abc
Set-Cookie: myAddCookie=TEST%0d%0atest;abc; path=/
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 723

```

図3.3-2： 図 3.3-1の結果

結果は、図 3.3-2のように、関数内部で改行コードのサニタイズ処理が行われていることが確認された。

よって、ASP.NET で上記の関数を使う場合は、HTTP ヘッダ・インジェクションに気を使わずにコーディングを行うことができる。

蛇足:

- 図 3.3-2のように、ASP.NET では、改行コード(Cr と Lf)が、URL エンコードされている。
- Location ヘッダには、汚染データそのものが与えられている。汚染データに別サイトの URL が指定される必要がない場合は、その対策が別途必要である。
- クッキー情報の箇所では「;」がサニタイズ処理されていない。よって、クッキー情報の値以外のプロパティ(Domain や Expires など)を汚染データによってセットされる危険性がある。他の関数との関係も考えれば、「;」 「%3b」に置換する URL エンコード処理を ASP.NET プログラムは行う必要がある。

### 3.4 JavaServlet の場合

JavaServlet での HTTP ヘッダ操作は、以下の関数がよく使われるだろう。

関数名	操作内容
response.sendRedirect	Web ページのリダイレクト要求
response.addCookie	クッキー情報の送信
response.addHeader	任意ヘッダの追加

これらの関数に汚染データが渡るようなテストプログラム(図 3.4-1)を作成し、Netcat を使ってどのような HTTP レスポンスが返るかを観察した。

MS-WindowsXP SP2(日本語版)上の Tomcat5.5.17、JDK1.5.0\_06、Eclipse3.1.2 を実験環境として使用した。

```
protected void doGet(HttpServletRequest request, HttpServletResponse response) throws ServletException,
IOException {
    String myAddStr;
    String lsRedirect;
    request.setCharacterEncoding("Windows-31J");
    myAddStr = request.getParameter("addStr");
    lsRedirect = request.getParameter("lsRedirect");
    // HTTP ヘッダの追加
    response.addHeader("myAddHeader", myAddStr);
    // クッキーの追加
    Cookie myCookie = new Cookie("myCookie", myAddStr);
    response.addCookie(myCookie);
    // location ヘッダの追加
    // redirect to JSP
    if(lsRedirect.equals("1") == true){
        getServletConfig().getServletContext().getRequestDispatcher("/result.jsp").forward(
request, response);
    }else{
        response.sendRedirect(myAddStr);
    }
}
```

図3.4-1 : JavaServlet のヘッダ送信関数の実験プログラム

```

C:\>type in.txt
GET /AppendHeader/servlet/AppendHeaderServlet?addStr=test%0d%0aTEST:xyz"abc¥lmn&
IsRedirect=2 HTTP/1.0

C:\>nc -nv 127.0.0.1 8080 < in.txt
(UNKNOWN) [127.0.0.1] 8080 (?) open
HTTP/1.1 302 Moved Temporarily
Server: Apache-Coyote/1.1
myAddHeader: test TEST:xyz"abc¥lmn
Set-Cookie: myCookie="test TEST:xyz¥"abc¥lmn"
Location: http://localhost:8080/AppendHeader/servlet/test TEST:xyz"abc¥lmn
Content-Length: 0
Date: Mon, 11 Dec 2006 01:48:46 GMT
Connection: close

sent 105, rcvd 298: NOTSOCK
C:\>

```

図3.4-2： 図 3.4-1の結果

(パケットキャプチャを行うと、改行コードが「0x20」に置換されていることが分かる)

結果は、図 3.4-2のように、関数内部で改行コードのサニタイズ処理が行われていることが確認された。

よって、JavaServlet で上記の関数を使う場合は、HTTP ヘッダ・インジェクションに気を使わずにコーディングを行うことができる。

蛇足:

- 改行コード(Cr と Lf)がどのコードに置換されるかというものは、パケットキャプチャをした結果、「半角スペース(0x20)」に置換されることを確認した。
- Location ヘッダの左側の赤線にあるように、自動で自サイトの URL を先頭に挿入するようである。この現象は汚染データを使った URL リダイレクトを自 Web アプリケーション内に限定できる、ということである。
- クッキー情報の HTTP ヘッダでは、入力データを「”」で囲むことが、図 3.4-2で確認できる。また、「”」は「¥」でエスケープするようであるが、エスケープ文字「¥」はエスケープしなくてもいいようである。

### 3.5 PHP5.2.0 の場合

PHP での HTTP ヘッダ操作は、以下の関数がよく使われるだろう。

関数名	操作内容
header("Location: <<入力データ>>")	Web ページのリダイレクト要求
setcookie setrawcookie	クッキー情報の送信
header	任意ヘッダの追加

リダイレクトには、header() 関数を使って、Location ヘッダを作成するという方法を用いる。setrawcookie()関数は、URL エンコードしないという点で setcookie() 関数と同一であるとマニュアルには記載されている。

これらの関数に汚染データが渡るようなテストプログラム(図 3.5-1)を作成し、Netcat を使ってどのような HTTP レスポンスが返るかを観察した。

MS-WindowsServer2003 SP1(日本語版)上の PHP5.2.0 を実験環境として使用した。

```
<?
    $str = $_REQUEST["inputData"];
    setcookie('cookieName', $str, time() + 60);
    setrawcookie('RAWcookieName', $str, time() + 60);
    header("myHeader: $str");
?>
```

図3.5-1 : PHP のヘッダ送信関数の実験プログラム

```

コマンド プロンプト
C:\>type in.txt
GET /httpHeaderTest.php?inputData=TEST%0d%0atest;abc HTTP/1.0

C:\>nc -nvw 127.0.0.1 80 < in.txt
(UNKNOWN) [127.0.0.1] 80 (?) open
HTTP/1.1 200 OK
Connection: close
Date: Fri, 15 Dec 2006 15:18:30 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-Powered-By2: PHP 5
X-Powered-By: PHP/5.2.0
Set-Cookie: cookiename=TEST%0D%0Atest%3Babc; expires=Fri, 15-Dec-2006 15:19:30 GMT
Content-type: text/html

<br />
<b>Warning</b>: Cookie values can not contain any of the following ' ; %t%r%n%013%014 ' (TEST
test;abc) in <b>D:\datas\web\httpHeaderTest.php</b> on line <b>5</b><br />
<br />
<b>Warning</b>: Cannot modify header information - headers already sent by (out
put started at D:\datas\web\httpHeaderTest.php:5) in <b>D:\datas\web\httpHeaderT
est.php</b> on line <b>6</b><br />
sent 65, rcvd 661: NOTSOCK

```

図3.5-2： 図 3.5-1の結果

クッキーへの出力は URL エンコードされている(setcookie)。setrawcookie() 関数ではエラーになる

```

コマンド プロンプト
C:\>type in.txt
GET /httpHeaderTest.php?inputData=TEST%0d%0atest;abc HTTP/1.0

C:\>nc -nvw 127.0.0.1 80 < in.txt
(UNKNOWN) [127.0.0.1] 80 (?) open
HTTP/1.1 200 OK
Connection: close
Date: Fri, 15 Dec 2006 15:21:13 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-Powered-By2: PHP 5
X-Powered-By: PHP/5.2.0
Set-Cookie: cookiename=TEST%0D%0Atest%3Babc; expires=Fri, 15-Dec-2006 15:22:13 GMT
Content-type: text/html

<br />
<b>Warning</b>: Header may not contain more than a single header, new line dete
cted. in <b>D:\datas\web\httpHeaderTest.php</b> on line <b>6</b><br />
sent 65, rcvd 439: NOTSOCK

```

図3.5-3： 図 3.5-1の結果

header() 関数に改行コードを与えるとエラーになる

結果は、図 3.5-2～図 3.5-3のように、setcookie() 関数では URL エンコードされ、またそれ以外の setrawcookie() 関数、header() 関数では、エラーとなることが確認された。よって、PHP で上記の関数を使う場合は、HTTP ヘッダ・インジェクションに気を使わずにコーディングを行うことができる。

蛇足:

- setrawcookie() 関数、header() 関数に改行コードを与えることでエラーとなる。  
エラーにならないようにするには、PHP プログラム中で、改行コードを事前に URL エンコードするなど PHP プログラマが明示的に処理することで対処する必要がある。
- setcookie() 関数は改行コードだけでなく、クッキー情報のプロパティのデリミタである「;(セミコロン)」も URL エンコードされることが確認できる。

## 4 執筆者など

## 4.1 本文書の免責事項

本文書に記述されてる情報の利用は、読者の責任に帰するものとする。

本文書で行った実験は、執筆者の実験環境で確認したものである。モジュールの細かいバージョンなどの状況によっては、現象が異なる可能性がある。

## 4.2 執筆者

- active@window.goukaku.com

## 4.3 更新履歴

最初のバージョン : 2007 年 03 月 05 日

## 4.4 本文書の最新バージョン

<http://rocketeer.dip.jp/secProg/index.htm>

## 4.5 HTTP ヘッダ名

本文書では除外しているが、HTTP ヘッダ名に汚染データを割り当てる場合は、ヘッダ名とヘッダ値のデリミタが「:(コロン)」である。そのような場面では「:(コロン)」のサニタイズ処理が必要である。

また、クッキー情報では、クッキー名とクッキーの値が「=(イコール)」で区切られている。クッキー名に汚染データが入るような場合は、「=(イコール)」がどのように処理されるかシステム開発前に事前に観察しておく必要がある。

以 上