

## 4.10 ファイルアクセスにまつわる問題

### ディレクトリ・トラバーサル脆弱性の脆弱性

Webアプリケーションには、外部からサーバ上のファイル名を指定できるものがあります  
この場合に、ファイル名に対するチェックが不十分であると、アプリケーションの意図しないファイルに対して、閲覧や改竄、削除ができることがあります

#### ディレクトリ・トラバーサル脆弱性の影響

- ① 秘密情報の漏洩、データの改竄・削除
- ② 任意のスキプトの実行 (OSコマンド・インジェクションと同様の影響)
- ③ アプリケーションの機能停止

#### ディレクトリ・トラバーサル脆弱性の対策

- ① 外部からファイル名を指定できる仕様を避ける
  - ② ファイル名にディレクトリ名が含まれないようにする
  - ③ ファイル名を英数字に限定する
- PHPの場合には、basename関数で、ディレクトリ階層を反映させずにファイル名指定できますが、関数にバイナリセーフではない問題があります

### 意図しないファイル公開

秘密情報を公開ディレクトリに配置していると、秘密情報が漏洩します

#### 意図しないファイル公開の対策

- ① 重要な情報を公開領域に置かない
- ② ディレクトリ・リスティングを無効化します

Apache HTTP Server の場合には、httpd.conf を以下のように設定します

```
<Directory バス指定>
Options -Indexes その他のオプション
その他の設定
</Directory>
```

レンタルサーバなどで、httpd.conf の設定ができない場合には、公開ディレクトリに .htaccess を置いて、以下のように設定します。(レンタルサーバによっては設定不可)

```
Options -Indexes
```

Apache HTTP Server の場合に、外部から参照できないように、.htaccess を以下のように設定します

```
<files *.txt >
deny from all
</files>
```

拡張子[txt]を参照不可にする

## 4a-001:ディレクトリ・トラバーサル(正常系)

### 【ブラウザ】

4.10 ファイルアクセスにまつわる問題

- [1. 4a-001:ディレクトリ・トラバーサル \(正常系\)](#)
- [2. 4a-001:ディレクトリ・トラバーサル \(/etc/hosts表示\)](#)
- [3. 4a-001:ディレクトリ・トラバーサル \(スクリプト:ソース表示\)](#)
- [4. 4a-001b:ディレクトリ・トラバーサル対策\(basename関数利用\) \(正常系\)](#)
- [5. 4a-001b:ディレクトリ・トラバーサル対策\(basename関数利用\) \(正常系\) \(/etc/hosts表示…失敗\)](#)
- [6. 4a-001c:ディレクトリ・トラバーサル対策\(ファイル名を英数字に限定\) \(正常系\)](#)
- [7. 4a-001c:ディレクトリ・トラバーサル対策\(ファイル名を英数字に限定\) \(/etc/hosts表示…失敗\)](#)
- [8. 4a/data/:意図しないファイル公開](#)

[phpinfo](#)  
[ホームに戻る](#)

```
<html>
<head><title>4.10 ファイルアクセスにまつわる問題</title></head>
<body>
4.10 ファイルアクセスにまつわる問題
<ol>
<li><a href="/4a-001.php?template=spring" >4a-001:ディレクトリ・トラバーサル (正常系) </a></li>
<li><a href="/4a-001.php?template=../../../../../../../../etc/hosts$00" >4a-001:ディレクトリ・トラバーサル (/etc/hosts表示) </a></li>
<li><a href="/4a-001.php?template=../../../../4a-001.php$00" >4a-001:ディレクトリ・トラバーサル (スクリプト:ソース表示) </a></li>
<li><a href="/4a-001b.php?template=spring" >4a-001b:ディレクトリ・トラバーサル対策(basename関数利用) (正常系) </a></li>
<li><a href="/4a-001b.php?template=../../../../../../../../etc/hosts$00" >4a-001b:ディレクトリ・トラバーサル対策(basename関数利用) (正常系) (/etc/hosts表示…失敗) </a></li>
<li><a href="/4a-001c.php?template=spring" >4a-001c:ディレクトリ・トラバーサル対策(ファイル名を英数字に限定) (正常系) </a></li>
<li><a href="/4a-001c.php?template=../../../../../../../../etc/hosts$00" >4a-001c:ディレクトリ・トラバーサル対策(ファイル名を英数字に限定) (/etc/hosts表示…失敗) </a></li>
<li><a href="/data/" >4a/data/:意図しないファイル公開</li>
</ol>
<br>
<a href="/phpinfo.php" >phpinfo</a><br>
<a href="/" >ホームに戻る</a>
</body>
</html>
```

## 【サーバ: 4a/4a-001.php 】

```
/var/www/html/4a/4a-001.php - wasbook@example.jp - エディタ - Wi  
k?php  
define('TPLDIR', '/var/www/html/4a/tmp1/');  
$tmpl = filter_input(INPUT_GET, 'template');  
>>  
<body>  
<?php readfile(TPLDIR . $tmpl . '.html'); >>  
メニュー (以下略)  
</body>
```

## 【ブラウザ→サーバ: リクエスト 4a/4a-001.php → レスポンス 】

The screenshot shows the OWASP ZAP interface. The left pane displays the request details for a GET request to `http://example.jp/4a/4a-001.php?template=spring`. The right pane displays the response details, which is an HTTP 200 OK with headers including `Server: nginx/1.10.3`, `Date: Sun, 30 Dec 2018 04:16:03 GMT`, and `Content-Type: text/html; charset=UTF-8`. The response body contains the HTML output: `<body>春のキャンペーン開催中!<br>メニュー (以下略)</body>`. The bottom pane shows a table of request logs with the following entry:

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	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	タグ
3	18/12/30 13:16...	GET	http://example.jp/4a/4a-001.php?templ...	200	OK	233 ms	82 bytes	Medium	

## 【ブラウザ】

The screenshot shows a browser window with the address bar containing `example.jp/4a/4a-001.php?template=spring`. The page content is: `春のキャンペーン開催中!` followed by `メニュー (以下略)`.

The screenshot shows a browser window with the address bar containing `view-source:http://example.jp/4a/4a-001.php?template=spring`. The source code is displayed as follows:

```
1 <body>  
2 春のキャンペーン開催中!<br>  
3 メニュー (以下略)  
4 </body>  
5
```

## 4a-001:ディレクトリ・トラバーサル(/etc/hosts表示)

### 【ブラウザ】

4.10 ファイルアクセスにまつわる問題

- [4a-001:ディレクトリ・トラバーサル \(正常系\)](#)
- [4a-001:ディレクトリ・トラバーサル \(/etc/hosts表示\)](#)
- [4a-001:ディレクトリ・トラバーサル \(スクリプト:ソース表示\)](#)
- [4a-001b:ディレクトリ・トラバーサル対策\(basename関数利用\) \(正常系\)](#)
- [4a-001b:ディレクトリ・トラバーサル対策\(basename関数利用\) \(正常系\) \(/etc/hosts表示…失敗\)](#)
- [4a-001c:ディレクトリ・トラバーサル対策\(ファイル名を英数字に限定\) \(正常系\)](#)
- [4a-001c:ディレクトリ・トラバーサル対策\(ファイル名を英数字に限定\) \(/etc/hosts表示…失敗\)](#)
- [4a/data/:意図しないファイル公開](#)

[phpinfo](#)  
[ホームに戻る](#)

```
1 <html>
2 <head><title>4.10 ファイルアクセスにまつわる問題</title></head>
3 <body>
4 4.10 ファイルアクセスにまつわる問題
5 <ol>
6 <li><a href="/4a-001.php?template=spring">4a-001:ディレクトリ・トラバーサル (正常系) </a></li>
7 <li><a href="/4a-001.php?template=../../../../etc/hosts%00">4a-001:ディレクトリ・トラバーサル (/etc/hosts表示) </a></li>
8 <li><a href="/4a-001.php?template=../../../../4a-001.php%00">4a-001:ディレクトリ・トラバーサル (スクリプト:ソース表示) </a></li>
9 <li><a href="/4a-001b.php?template=spring">4a-001b:ディレクトリ・トラバーサル対策(basename関数利用) (正常系) </a></li>
10 <li><a href="/4a-001b.php?template=../../../../etc/hosts%00">4a-001b:ディレクトリ・トラバーサル対策(basename関数利用) (正常系) (/etc/hosts表示…失敗) </a></li>
11 <li><a href="/4a-001c.php?template=spring">4a-001c:ディレクトリ・トラバーサル対策(ファイル名を英数字に限定) (正常系) </a></li>
12 <li><a href="/4a-001c.php?template=../../../../etc/hosts%00">4a-001c:ディレクトリ・トラバーサル対策(ファイル名を英数字に限定) (/etc/hosts表示…失敗) </a></li>
13 </li><a href="/data/">4a/data/:意図しないファイル公開</li>
14 </ol>
15 <a href="/phpinfo.php">phpinfo</a><br>
16 <a href="/">ホームに戻る</a>
17 </body>
18 </html>
19
```

### 【サーバ: 4a/4a-001.php】

```
/var/www/html/4a/4a-001.php - wasbook@example.jp - エディタ・Wi
k?php
define('TMPLDIR', '/var/www/html/4a/tmp1/');
$tpl = filter_input(INPUT_GET, 'template');
?>
<body>
<?php readfile(TMPLDIR . $tpl . '.html'); ?>
メニュー (以下略)
</body>
```

## 【ブラウザ→サーバ: リクエスト 4a/4a-001.php → レスポンス】

The screenshot shows the OWASP ZAP 2.7.0 interface. The left pane displays the request details for a GET request to `http://example.jp/4a/4a-001.php?template=../../../../etc/hosts%00`. The right pane displays the response details, which is an HTTP 200 OK from a server running nginx/1.10.3. The response body contains the contents of the `/etc/hosts` file, including entries for `127.0.0.1` and IPv6 addresses, followed by a comment about IPv6 capable hosts and a menu option.

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...	ラウンドトリップタ...	レスポンスボディサ...	検出アラ...	ノ...	タグ
6	18/12/30 13:23...	GET	http://example.jp/4a/4a-001.php?templat...	200	OK	26 ms	294 bytes	Medium		

## 【ブラウザ】

The browser window shows the rendered page content. The text is as follows:

```
127.0.0.1 localhost example.jp trap.example.com api.example.net internal.example.jp
127.0.1.1 wasbook # The following lines are desirable for IPv6 capable hosts ::1
localhost ip6-localhost ip6-loopback ff02::1 ip6-allnodes ff02::2 ip6-allrouters
メニュー (以下略)
```

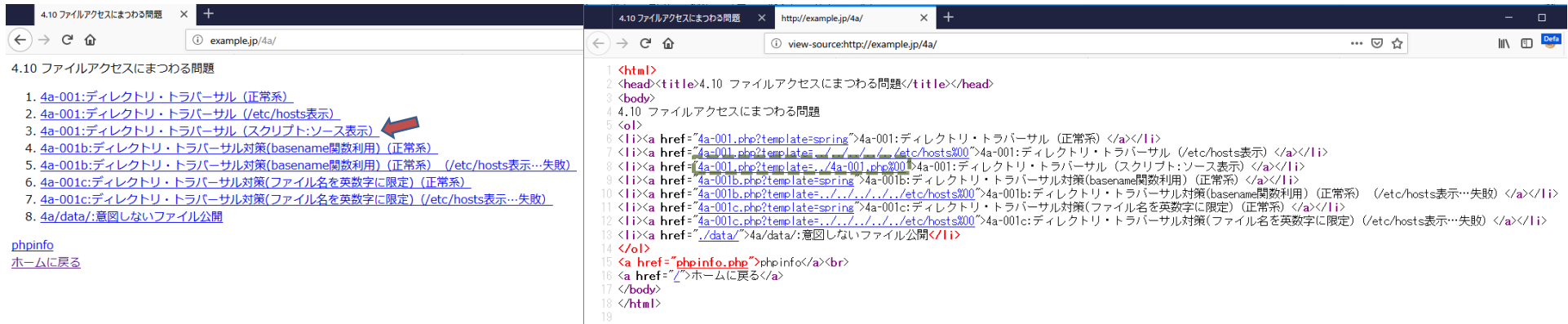
Below the rendered content, there is a note: `/etc/hosts` の内容が漏洩している

The browser window shows the source code of the page. The text is as follows:

```
1 <body>
2 127.0.0.1 localhost example.jp trap.example.com api.example.net internal.example.jp
3 127.0.1.1 wasbook
4
5 # The following lines are desirable for IPv6 capable hosts
6 ::1 localhost ip6-localhost ip6-loopback
7 ff02::1 ip6-allnodes
8 ff02::2 ip6-allrouters
9 メニュー (以下略)
10 </body>
11
```

## 4a-001:ディレクトリ・トラバーサル(スクリプト:ソース表示)

### 【ブラウザ】



4.10 ファイルアクセスにまつわる問題

- [4a-001:ディレクトリ・トラバーサル \(正常系\)](#)
- [4a-001:ディレクトリ・トラバーサル \(/etc/hosts表示\)](#)
- [4a-001b:ディレクトリ・トラバーサル \(スクリプト:ソース表示\)](#)
- [4a-001b:ディレクトリ・トラバーサル対策\(basename関数利用\) \(正常系\)](#)
- [4a-001b:ディレクトリ・トラバーサル対策\(basename関数利用\) \(正常系\) \(/etc/hosts表示…失敗\)](#)
- [4a-001c:ディレクトリ・トラバーサル対策\(ファイル名を英数字に限定\) \(正常系\)](#)
- [4a-001c:ディレクトリ・トラバーサル対策\(ファイル名を英数字に限定\) \(/etc/hosts表示…失敗\)](#)
- [4a/data/:意図しないファイル公開](#)

[phpinfo](#)  
[ホームに戻る](#)

```
1 <html>
2 <head><title>4.10 ファイルアクセスにまつわる問題</title></head>
3 <body>
4 4.10 ファイルアクセスにまつわる問題
5 <ol>
6 <li><a href="/4a-001.php?template=spring">4a-001:ディレクトリ・トラバーサル (正常系) </a></li>
7 <li><a href="/4a-001.php?template=../../../../etc/hosts800">4a-001:ディレクトリ・トラバーサル (/etc/hosts表示) </a></li>
8 <li><a href="/4a-001.php?template=../../../../4a-001.php800">4a-001:ディレクトリ・トラバーサル (スクリプト:ソース表示) </a></li>
9 <li><a href="/4a-001b.php?template=spring">4a-001b:ディレクトリ・トラバーサル対策(basename関数利用) (正常系) </a></li>
10 <li><a href="/4a-001b.php?template=../../../../etc/hosts800">4a-001b:ディレクトリ・トラバーサル対策(basename関数利用) (正常系) (/etc/hosts表示…失敗) </a></li>
11 <li><a href="/4a-001c.php?template=spring">4a-001c:ディレクトリ・トラバーサル対策(ファイル名を英数字に限定) (正常系) </a></li>
12 <li><a href="/4a-001c.php?template=../../../../etc/hosts800">4a-001c:ディレクトリ・トラバーサル対策(ファイル名を英数字に限定) (/etc/hosts表示…失敗) </a></li>
13 <li><a href="/data/">4a/data/:意図しないファイル公開</li>
14 </ol>
15 <a href="/phpinfo.php">phpinfo</a><br>
16 <a href="/">ホームに戻る</a>
17 </body>
18 </html>
19
```

### 【サーバ: 4a/4a-001.php】

```
/var/www/html/4a/4a-001.php - wasbook@example.jp - エディタ - Wi
k?php
define('TMPLDIR', '/var/www/html/4a/tmp1/');
$tpl = filter_input(INPUT_GET, 'template');
?>
<body>
<?php readfile(TMPLDIR . $tpl . '.html'); ?>
メニュー (以下略)
</body>
```

## 【ブラウザ→サーバ: リクエスト 4a/4a-001.php → レスポンス】

The screenshot shows the OWASP ZAP interface. The left pane displays the request details for a GET request to `http://example.jp/4a/4a-001.php?template=../4a-001.php%00`. The right pane displays the response details, which is an HTTP 200 OK with headers including `Server: nginx/1.10.3` and `Content-Type: text/html; charset=UTF-8`. The response body contains PHP code for a template filter and a file read operation, with the body content highlighted by a dashed green box.

```
GET http://example.jp/4a/4a-001.php?template=../4a-001.php%00 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0
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/4a/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Sun, 30 Dec 2018 04:31:02 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 235
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
<?php
define('TPLDIR', '/var/www/html/4a/tmpl/');
$tpl = filter_input(INPUT_GET, 'template');
?>
<body>
<?php readfile(TPLDIR . $tpl . '.html'); ?>
メニュー (以下略)
</body>
メニュー (以下略)
</body>
```

## 【ブラウザ】

The screenshot shows a browser window with the URL `example.jp/4a/4a-001.php?template=../4a-001.php%00`. The page content is `メニュー (以下略) メニュー (以下略)`.

Webブラウザから「ソース表示」機能を使うとサーバのスキプトの内容が表示できています

The screenshot shows the browser's source code view for the URL `http://example.jp/4a/4a-001.php?template=../4a-001.php%00`. The source code is as follows:

```
1 <body>
2 <?php
3   define(' TPLDIR', '/var/www/html/4a/tmpl/');
4   $tpl = filter_input(INPUT_GET, 'template');
5   ?>
6 <body>
7 <?php readfile(TPLDIR . $tpl . '.html'); ?>
8 メニュー (以下略)
9 </body>
10 メニュー (以下略)
11 </body>
12
```

## 4a-001b:ディレクトリ・トラバーサル対策(basename関数利用)(正常系)

### 【ブラウザ】

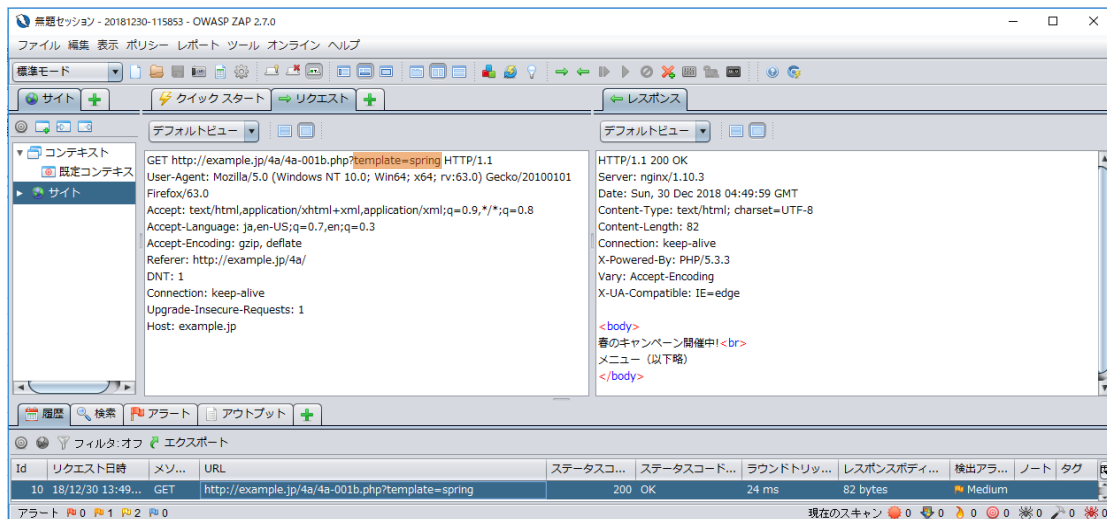


The screenshot shows a web browser window with the address bar at `example.jp/4a/`. The page content includes a list of links under the heading "4.10 ファイルアクセスにまつわる問題". A red arrow points to the link "4a-001b:ディレクトリ・トラバーサル対策(basename関数利用)(正常系)". To the right, a "view-source" window is open, displaying the HTML source code of the page. The source code shows a list of links with href attributes pointing to various PHP files, including the one highlighted in the browser window.

### 【サーバ: 4a/4a-001b.php】

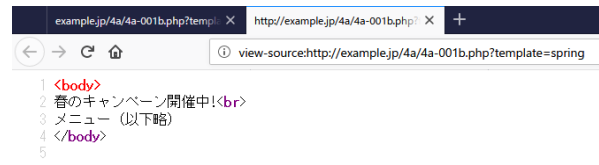
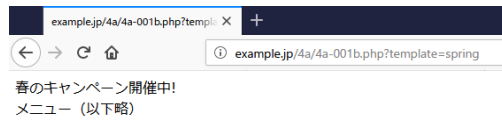
```
/var/www/html/4a/4a-001b.php - wasbook@example.jp - エディタ - WinSCP  
k?php  
define('TMPLDIR', './var/www/html/4a/tmp1/');  
$tmpl = basename(filter_input(INPUT_GET, 'template'));  
>>  
<body>  
<?php readfile(TMPLDIR . $tmpl . '.html'); >>  
メニュー (以下略)  
</body>
```

### 【ブラウザ→サーバ: リクエスト 4a/4a-001b.php → レスポンス】



The screenshot shows the developer tools of a web browser. The "Network" tab is active, showing a request to `http://example.jp/4a/4a-001b.php?template=spring`. The request headers include `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0` and `Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8`. The response headers include `HTTP/1.1 200 OK`, `Server: nginx/1.10.3`, and `Date: Sun, 30 Dec 2018 04:49:59 GMT`. The response body contains the HTML content of the page, including the link "メニュー (以下略)".

## 【ブラウザ】





## 4a-001b:ディレクトリ・トラバーサル対策(basename関数利用)(正常系)(/etc/hosts表示…失敗)

### 【ブラウザ】

4.10 ファイルアクセスにまつわる問題

- 4a-001:ディレクトリ・トラバーサル (正常系)
- 4a-001:ディレクトリ・トラバーサル (/etc/hosts表示)
- 4a-001:ディレクトリ・トラバーサル (スクリプト:ソース表示)
- 4a-001b:ディレクトリ・トラバーサル対策(basename関数利用) (正常系)
- 4a-001b:ディレクトリ・トラバーサル対策(basename関数利用) (正常系) (/etc/hosts表示…失敗)
- 4a-001c:ディレクトリ・トラバーサル対策(ファイル名を英数字に限定) (正常系)
- 4a-001c:ディレクトリ・トラバーサル対策(ファイル名を英数字に限定) (/etc/hosts表示…失敗)
- 4a/data/:意図しないファイル公開

[phpinfo](#)  
[ホームに戻る](#)

【サーバ: 4a/4a-001b.php 】

```

/var/www/html/4a/4a-001b.php - wasbook@example.jp - エディタ - WinSCP
<?php
define('TMPLDIR', './var/www/html/4a/tmp/');
$tpl = basename(filter_input(INPUT_GET, 'template'));
?>
<body>
<?php readfile(TMPLDIR . $tpl . '.html'); ?>
メニュー (以下略)
</body>

```

basename関数で、ディレクトリ階層を反映させずにファイル名指定します  
関数にはバイナリセーフではない問題があります

```

1 <html>
2 <head><title>4.10 ファイルアクセスにまつわる問題</title></head>
3 <body>
4 4.10 ファイルアクセスにまつわる問題
5 <ol>
6 <li><a href="/4a-001.php?template=spring">4a-001:ディレクトリ・トラバーサル (正常系) </a></li>
7 <li><a href="/4a-001.php?template=../../../../etc/hosts%00">4a-001:ディレクトリ・トラバーサル (/etc/hosts表示) </a></li>
8 <li><a href="/4a-001.php?template=../../../../4a-001c.php%00">4a-001:ディレクトリ・トラバーサル (スクリプト:ソース表示) </a></li>
9 <li><a href="/4a-001b.php?template=spring">4a-001b:ディレクトリ・トラバーサル対策(basename関数利用) (正常系) </a></li>
10 <li><a href="/4a-001b.php?template=../../../../etc/hosts%00">4a-001b:ディレクトリ・トラバーサル対策(basename関数利用) (正常系) (/etc/hosts表示…失敗) </a></li>
11 <li><a href="/4a-001c.php?template=spring">4a-001c:ディレクトリ・トラバーサル対策(ファイル名を英数字に限定) (正常系) </a></li>
12 <li><a href="/4a-001c.php?template=../../../../etc/hosts%00">4a-001c:ディレクトリ・トラバーサル対策(ファイル名を英数字に限定) (/etc/hosts表示…失敗) </a></li>
13 <li><a href="/data/">4a/data/:意図しないファイル公開</li>
14 </ol>
15 <a href="/phpinfo.php">phpinfo</a><br>
16 <a href="/">ホームに戻る</a>
17 </body>
18 </html>
19

```

### 【ブラウザ→サーバ: リクエスト 4a/4a-001b.php → レスポンス】

無題セッション - 20181230-115853 - 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

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/4a/4a-001b.php?template=../../../../etc/hosts%00 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0
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/4a/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp

```

デフォルトビュー

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Sun, 30 Dec 2018 04:54:23 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 183
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>

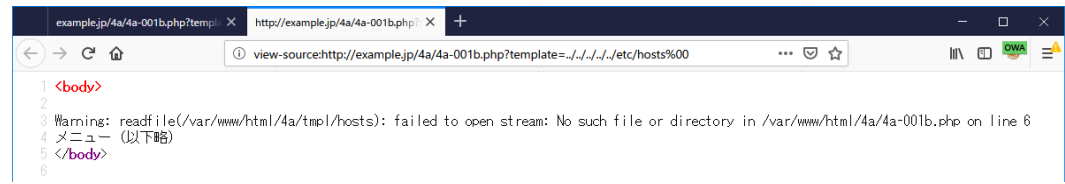
Warning: readfile(/var/www/html/4a/tmp/hosts): failed to open stream: No such file or directory in
/var/www/html/4a/4a-001b.php on line 6
メニュー (以下略)
</body>

```

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...	レスポンスボディサイズ	検出アラート	ノート	タグ
13	18/12/30 13:54:23	GET	http://example.jp/4a/4a-001b.php?template=../../../../etc/hosts%...	200	OK	21 ms	183 bytes	Medium		

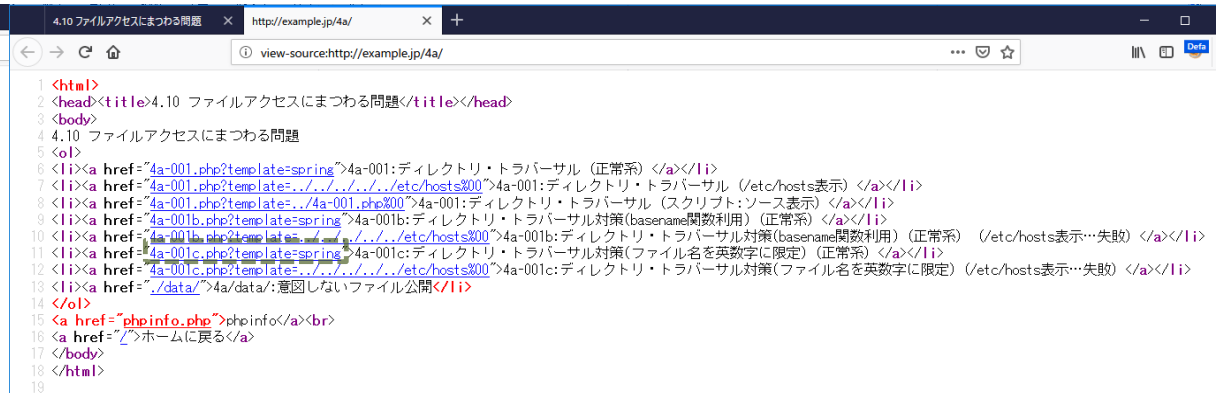
現在のスキャン

## 【ブラウザ】

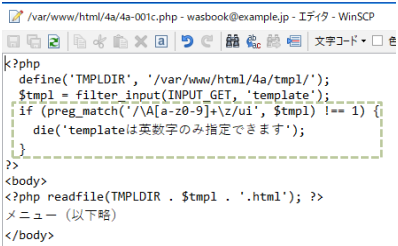


## 4a-001c:ディレクトリ・トラバーサル対策(ファイル名を英数字に限定)(正常系)

### 【ブラウザ】



### 【サーバ: 4a/4a-001c.php】



ファイル名を英数字のみに限定するチェックを入れます

## 【ブラウザ→サーバ: リクエスト 4a/4a-001c.php → レスポンス】

The screenshot shows the OWASP ZAP interface. The left pane shows the context tree with 'サイト' selected. The main pane displays the request and response details for the URL `http://example.jp/4a/4a-001c.php?template=spring`.

**Request:**

```
GET http://example.jp/4a/4a-001c.php?template=spring HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0
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/4a/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp
```

**Response:**

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Sun, 30 Dec 2018 05:08:56 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 82
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
春のキャンペーン開催中!<br>
メニュー (以下略)
</body>
```

Below the main pane is a table of request logs:

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...	レスポンスボディサイズ	検出アラート	ノート	タグ
14	18/12/30 14:08:56	GET	http://example.jp/4a/4a-001c.php?template=spring	200	OK	27 ms	82 bytes	Medium		

## 【ブラウザ】

The browser window shows the rendered page content for the URL `http://example.jp/4a/4a-001c.php?template=spring`. The page content is:

春のキャンペーン開催中!  
メニュー (以下略)

The browser window shows the source code for the URL `view-source:http://example.jp/4a/4a-001c.php?template=spring`. The source code is:

```
1 <body>
2 春のキャンペーン開催中!<br>
3 メニュー (以下略)
4 </body>
5
```

# 4a-001c:ディレクトリ・トラバーサル対策(ファイル名を英数字に限定)(/etc/hosts表示…失敗)

## 【ブラウザ】

4.10 ファイルアクセスにまつわる問題

- 4a-001:ディレクトリ・トラバーサル (正常系)
- 4a-001:ディレクトリ・トラバーサル (/etc/hosts表示)
- 4a-001:ディレクトリ・トラバーサル (スクリプト:ソース表示)
- 4a-001b:ディレクトリ・トラバーサル対策(basename関数利用) (正常系)
- 4a-001b:ディレクトリ・トラバーサル対策(basename関数利用) (/etc/hosts表示…失敗)
- 4a-001c:ディレクトリ・トラバーサル対策(ファイル名を英数字に限定) (正常系)
- 4a-001c:ディレクトリ・トラバーサル対策(ファイル名を英数字に限定) (/etc/hosts表示…失敗)
- 4a/data/:意図しないファイル公開

phpinfo  
ホームに戻る

【サーバ: 4a/4a-001c.php】

```
#!/var/www/html/4a/4a-001c.php - wasbook@example.jp - エディタ - WinSCP
```

```
<?php
define('TMPLDIR', '/var/www/html/4a/tmp1/');
$tpl = filter_input(INPUT_GET, 'template');
if (preg_match('/^[a-z0-9]+\z/ui', $tpl) !== 1) {
    die('templateは英数字のみ指定できます');
}
>>
<body>
<?php readfile(TMPLDIR . $tpl . '.html'); >>
メニュー (以下略)
</body>
```

ファイル名を英数字のみに限定するチェックを入れます

view-source:http://example.jp/4a/

```
1 <html>
2 <head><title>4.10 ファイルアクセスにまつわる問題</title></head>
3 <body>
4 4.10 ファイルアクセスにまつわる問題
5 <ol>
6 <li><a href="/4a-001.php?template=spring">4a-001:ディレクトリ・トラバーサル (正常系) </a></li>
7 <li><a href="/4a-001.php?template=../../../../etc/hosts%00">4a-001:ディレクトリ・トラバーサル (/etc/hosts表示) </a></li>
8 <li><a href="/4a-001.php?template=../../../../4a-001.php%00">4a-001:ディレクトリ・トラバーサル (スクリプト:ソース表示) </a></li>
9 <li><a href="/4a-001b.php?template=spring">4a-001b:ディレクトリ・トラバーサル対策(basename関数利用) (正常系) </a></li>
10 <li><a href="/4a-001b.php?template=../../../../etc/hosts%00">4a-001b:ディレクトリ・トラバーサル対策(basename関数利用) (/etc/hosts表示…失敗) </a></li>
11 <li><a href="/4a-001c.php?template=spring">4a-001c:ディレクトリ・トラバーサル対策(ファイル名を英数字に限定) (正常系) </a></li>
12 <li><a href="/4a-001c.php?template=../../../../etc/hosts%00">4a-001c:ディレクトリ・トラバーサル対策(ファイル名を英数字に限定) (/etc/hosts表示…失敗) </a></li>
13 <li><a href="/data/">4a/data/:意図しないファイル公開</li>
14 </ol>
15 <a href="/phpinfo.php">phpinfo</a><br>
16 <a href="/">ホームに戻る</a>
17 </body>
18 </html>
```

## 【ブラウザ→サーバ: リクエスト 4a/4a-001c.php → レスポンス】

無題セッション - 20181230-115853 - OWASP ZAP 2.7.0

GET http://example.jp/4a/4a-001c.php?template=../../../../etc/hosts%00 HTTP/1.1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0  
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/4a/  
DNT: 1  
Connection: keep-alive  
Upgrade-Insecure-Requests: 1  
Host: example.jp

HTTP/1.1 200 OK  
Server: nginx/1.10.3  
Date: Sun, 30 Dec 2018 05:14:28 GMT  
Content-Type: text/html; charset=UTF-8  
Connection: keep-alive  
X-Powered-By: PHP/5.3.3  
X-UA-Compatible: IE=edge

templateは英数字のみ指定できます

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...	レスポンスボディサイズ	検出アラート	ノート	タグ
15	18/12/30 14:14:28	GET	http://example.jp/4a/4a-001c.php?template=../../../../etc/hosts%...	200	OK	22 ms	44 bytes	Medium		

## 【ブラウザ】

example.jp/4a/4a-001c.php?template=../../../../etc/hosts%00

templateは英数字のみ指定できます

view-source:http://example.jp/4a/4a-001c.php?template=../../../../etc/hosts%00

templateは英数字のみ指定できます

/etc/hosts の表示に失敗

## 4a/data/:意図しないファイル公開

### 【ブラウザ】

The screenshot shows a web browser with two tabs. The left tab is at 'example.jp/4a/' and displays a list of links under the heading '4.10 ファイルアクセスにまつわる問題'. The right tab is at 'view-source:http://example.jp/4a/' and shows the HTML source code of the page. A red arrow points from the link '4a/data/:意図しないファイル公開' in the list to the corresponding HTML element in the source code: `<li><a href="/data/">4a/data/:意図しないファイル公開</a></li>`.

4.10 ファイルアクセスにまつわる問題

1. [4a-001:ディレクトリ・トラバーサル \(正常系\)](#)
2. [4a-001:ディレクトリ・トラバーサル \(/etc/hosts表示\)](#)
3. [4a-001:ディレクトリ・トラバーサル \(スクリプト:ソース表示\)](#)
4. [4a-001b:ディレクトリ・トラバーサル対策\(basename関数利用\) \(正常系\)](#)
5. [4a-001b:ディレクトリ・トラバーサル対策\(basename関数利用\) \(/etc/hosts表示…失敗\)](#)
6. [4a-001c:ディレクトリ・トラバーサル対策\(ファイル名を英数字に限定\) \(正常系\)](#)
7. [4a-001c:ディレクトリ・トラバーサル対策\(ファイル名を英数字に限定\) \(/etc/hosts表示…失敗\)](#)
8. [4a/data/:意図しないファイル公開](#)

[phpinfo](#)  
[ホームに戻る](#)

```
1 <html>
2 <head><title>4.10 ファイルアクセスにまつわる問題</title></head>
3 <body>
4 4.10 ファイルアクセスにまつわる問題
5 <ol>
6 <li><a href="/4a-001.php?template=spring">4a-001:ディレクトリ・トラバーサル (正常系) </a></li>
7 <li><a href="/4a-001.php?template=../../../../etc/hosts800">4a-001:ディレクトリ・トラバーサル (/etc/hosts表示) </a></li>
8 <li><a href="/4a-001.php?template=../../../../4a-001.php800">4a-001:ディレクトリ・トラバーサル (スクリプト:ソース表示) </a></li>
9 <li><a href="/4a-001b.php?template=spring">4a-001b:ディレクトリ・トラバーサル対策(basename関数利用) (正常系) </a></li>
10 <li><a href="/4a-001b.php?template=../../../../etc/hosts800">4a-001b:ディレクトリ・トラバーサル対策(basename関数利用) (正常系) (/etc/hosts表示…失敗) </a></li>
11 <li><a href="/4a-001c.php?template=spring">4a-001c:ディレクトリ・トラバーサル対策(ファイル名を英数字に限定) (正常系) </a></li>
12 <li><a href="/4a-001c.php?template=../../../../etc/hosts800">4a-001c:ディレクトリ・トラバーサル対策(ファイル名を英数字に限定) (/etc/hosts表示…失敗) </a></li>
13 <li><a href="/data/">4a/data/:意図しないファイル公開</li>
14 </ol>
15 <a href="/phpinfo.php">phpinfo</a><br>
16 <a href="/">ホームに戻る</a>
17 </body>
18 </html>
19
```

