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任意のスクリプトの実行（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ファイル名にデレクトリ名が含まれないようにする　　PHPの場合には、basename関数で、デ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、関数にバイナリセイフではない問題があります
③ファイル名を英数字に限定する

意図しないファイル公開

秘密情報を公開デ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 パス指定>
  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
```

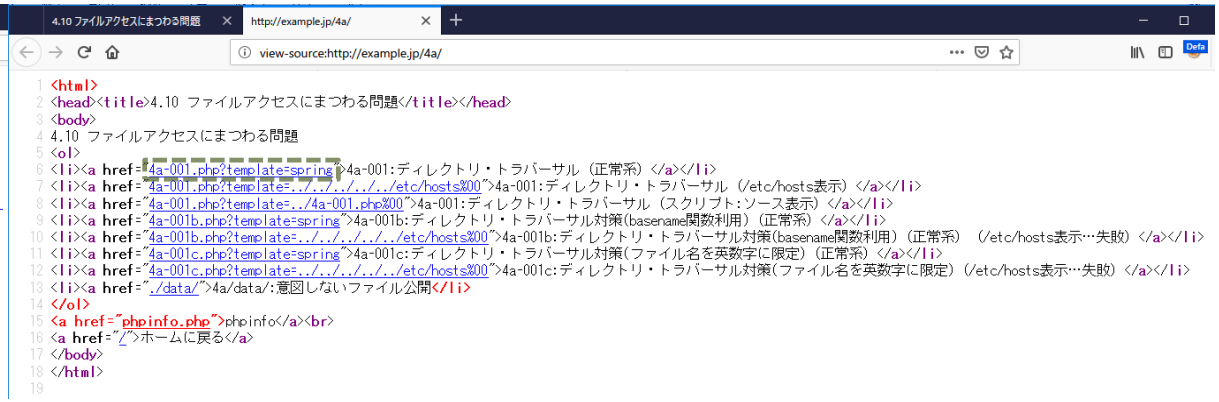
Apache HTTP Server の場合に、外部から参照できないように、 .htaccess を以下のように設定します

```
<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】

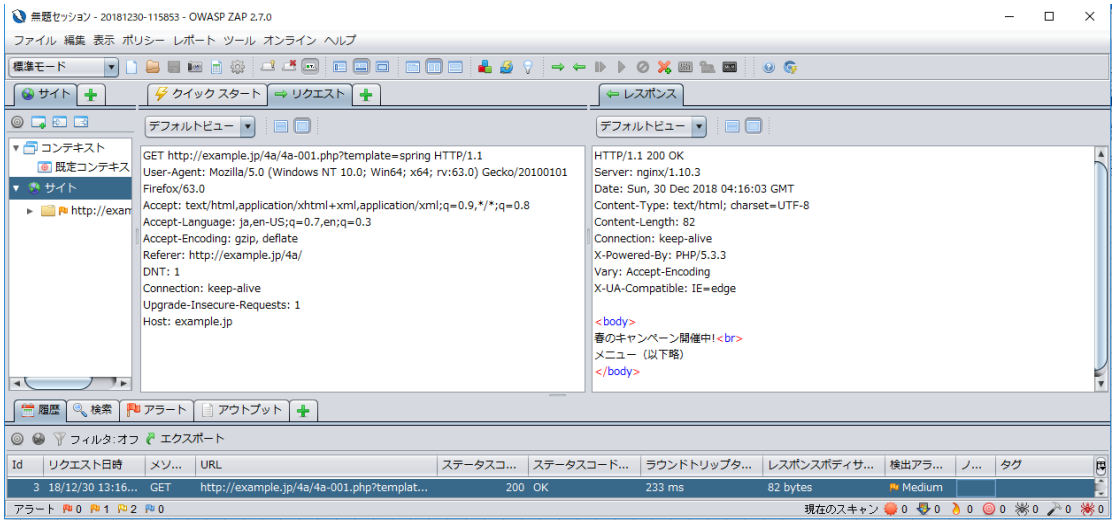


【サーバ： 4a/4a-001.php 】

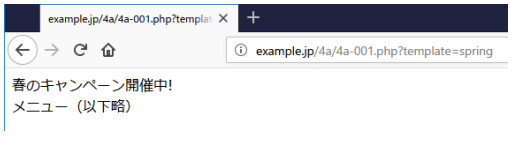
/var/www/html/4a/4a-001.php - wasbook@example.jp - エディタ - Wi

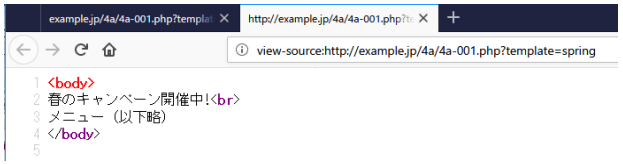
```
<?php
  define('TMPLDIR', '/var/www/html/4a/tmpl/');
  $tmpl = filter_input(INPUT_GET, 'template');
?>
<body>
<?php readfile(TMPLDIR . $tmpl . '.html'); ?>
メニュー（以下略）
</body>
```

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



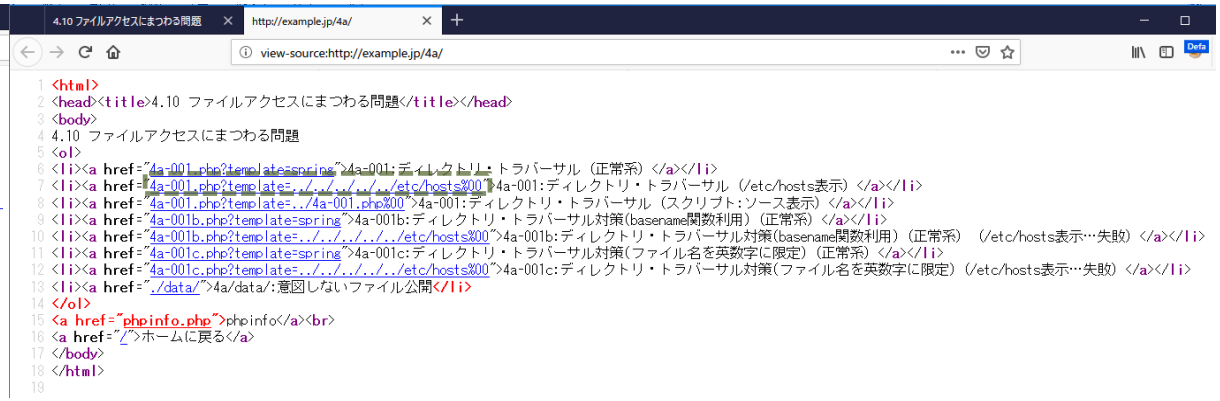
【ブラウザ】



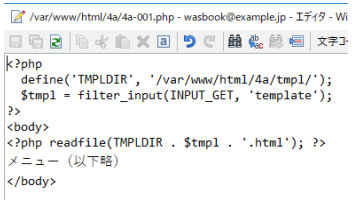


4a-001:ディレクトリ・トラバーサル（/etc/hosts表示）

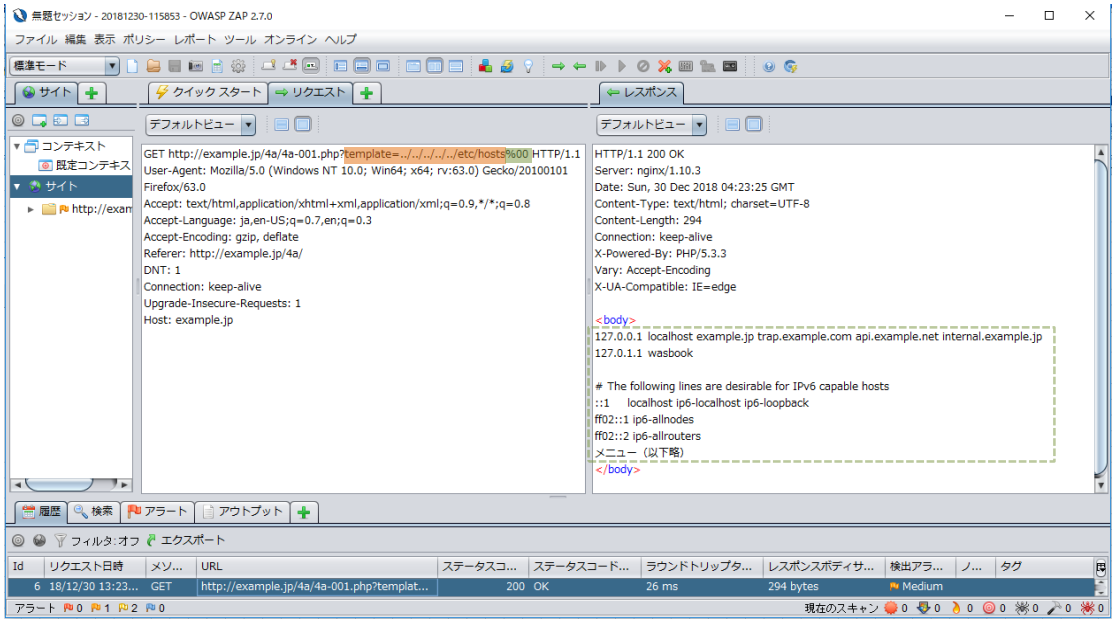
【ブラウザ】



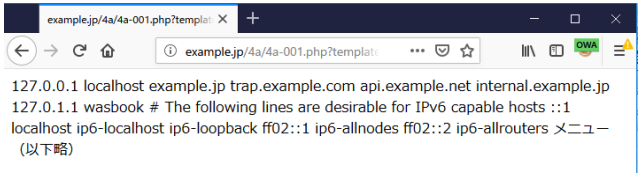
【サーバ： 4a/4a-001.php 】



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



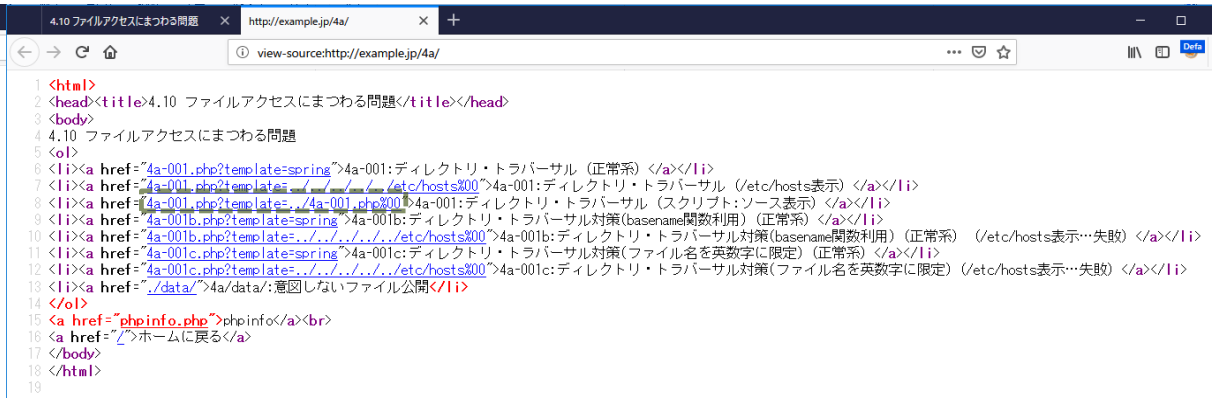
【ブラウザ】



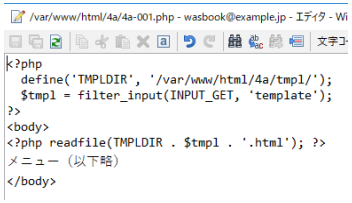
/etc/hosts の内容が漏洩している

4a-001:ディレクトリ・トラバーサル（スクリプト:ソース表示）

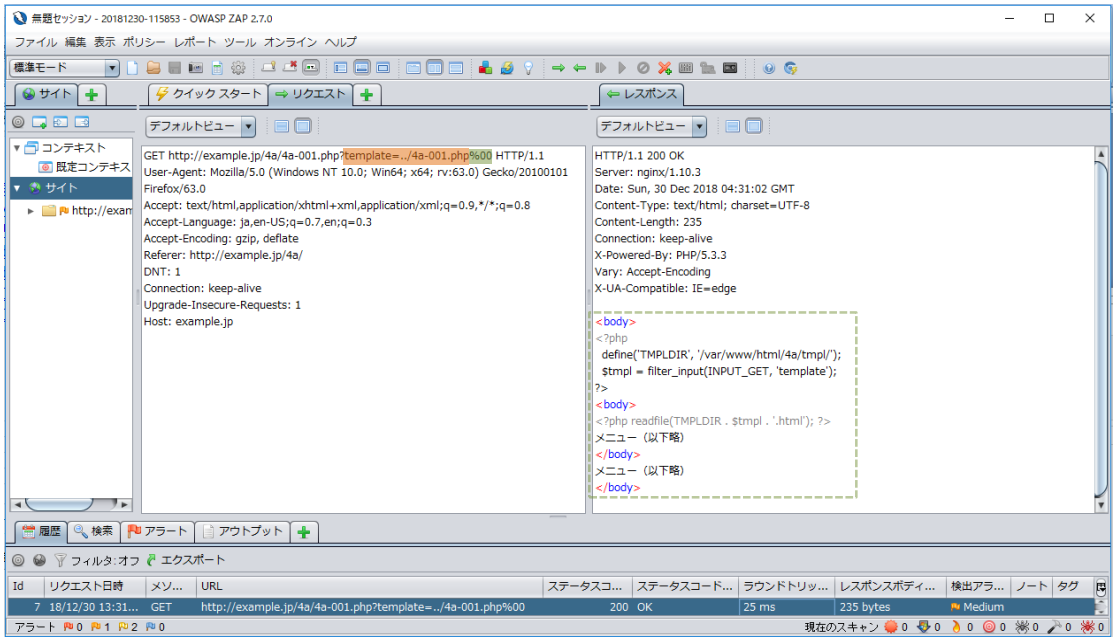
【ブラウザ】



【サーバ： 4a/4a-001.php 】



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

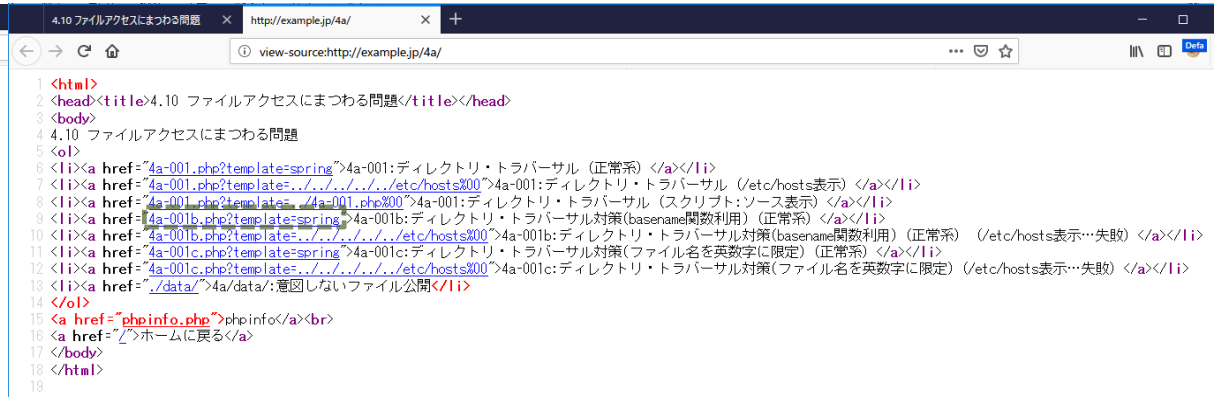


【ブラウザ】

Webブラウザから「ソース表示」機能を使うと
サーバのスクリプトの内容が表示できていません

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】

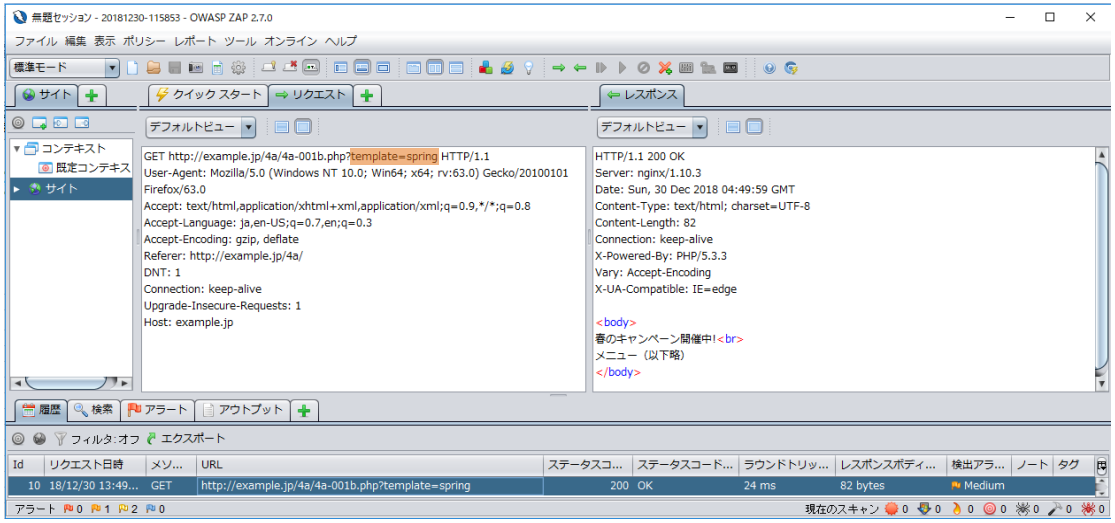


【サーバ： 4a/4a-001b.php 】

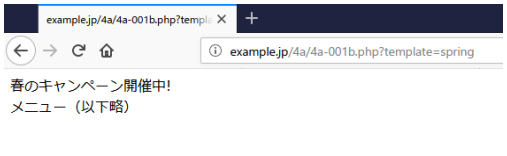
/var/www/html/4a/4a-001b.php - wasbook@example.jp - エディタ - WinSCP

```
<?php
  define('TMPLDIR', '/var/www/html/4a/tmpl/');
  $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 】



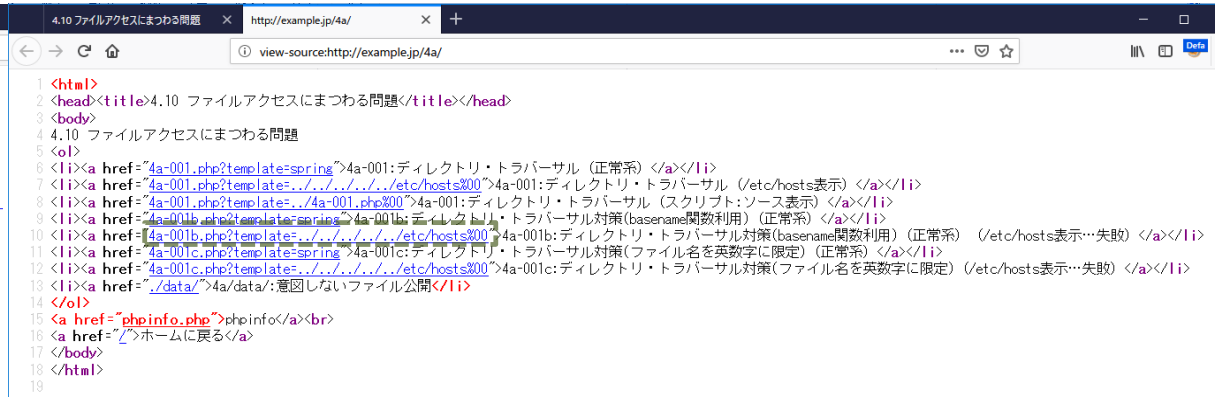
【ブラウザ】


example.jp/4a/4a-001b.php?templa
example.jp/4a/4a-001b.php?template=spring
春のキャンペーン開催中!
メニュー（以下略）


example.jp/4a/4a-001b.php?templ
http://example.jp/4a/4a-001b.php?
view-source:http://example.jp/4a/4a-001b.php?template=spring
<body>
春のキャンペーン開催中!
メニュー（以下略）
</body>

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】



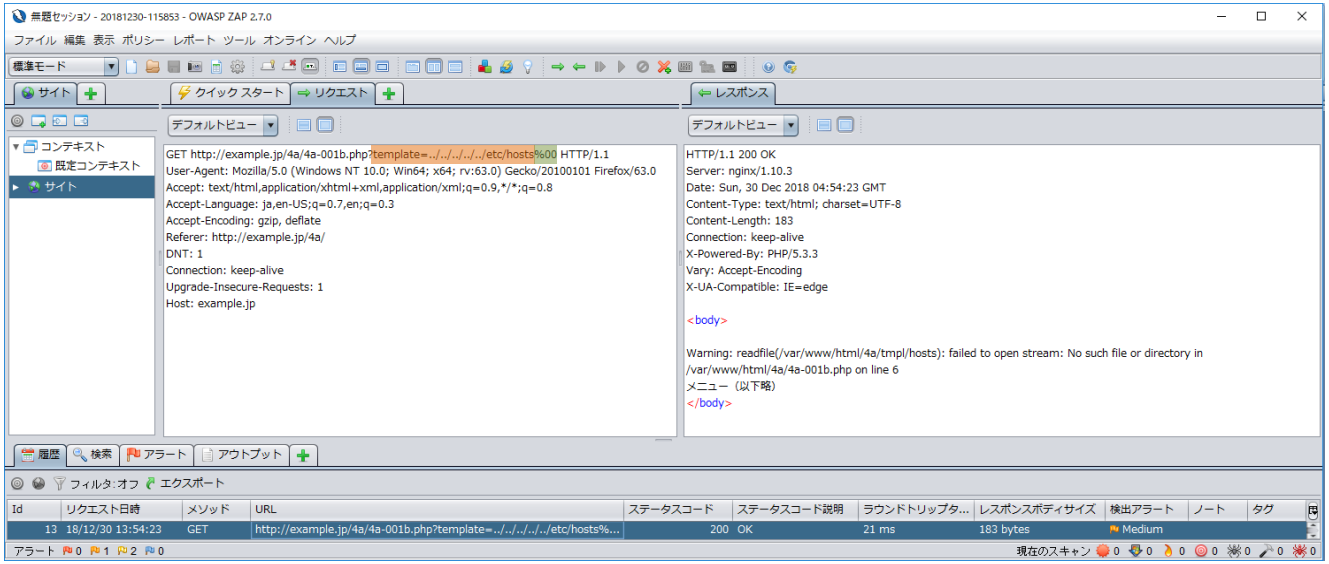
【サーバ： 4a/4a-001b.php 】

/var/www/html/4a/4a-001b.php - wasbook@example.jp - エディタ - WinSCP

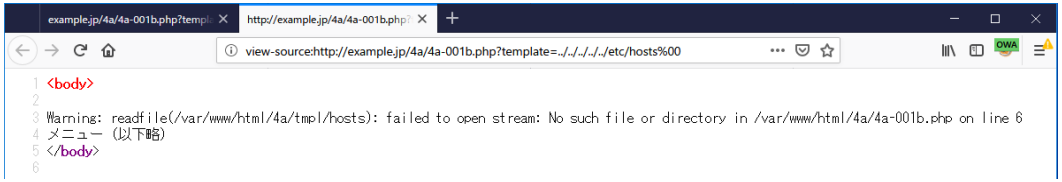
```
k?php
  define('TMPLDIR', '/var/www/html/4a/tmpl/');
  $tmpl = basename(filter_input(INPUT_GET, 'template'));
?>
<body>
<?php readfile(TMPLDIR . $tmpl . '.html'); ?>
メニュー（以下略）
</body>
```

basename関数で、デ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イフではない問題があります

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



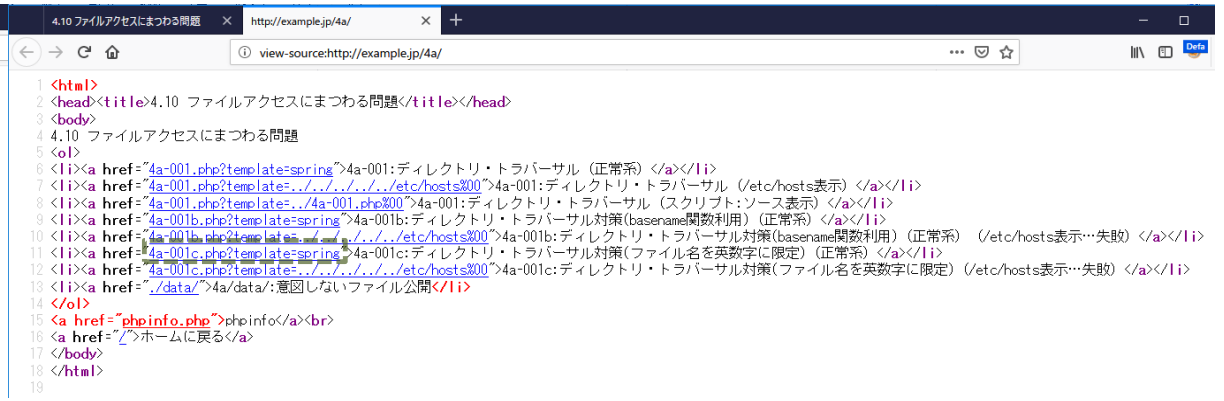
【ブラウザ】



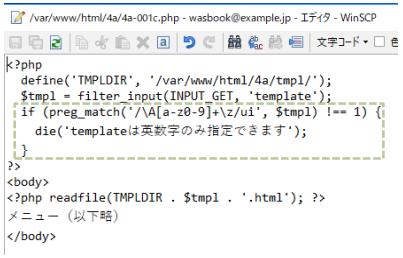
/etc/hosts の表示に失敗

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)

【ブラウザ】

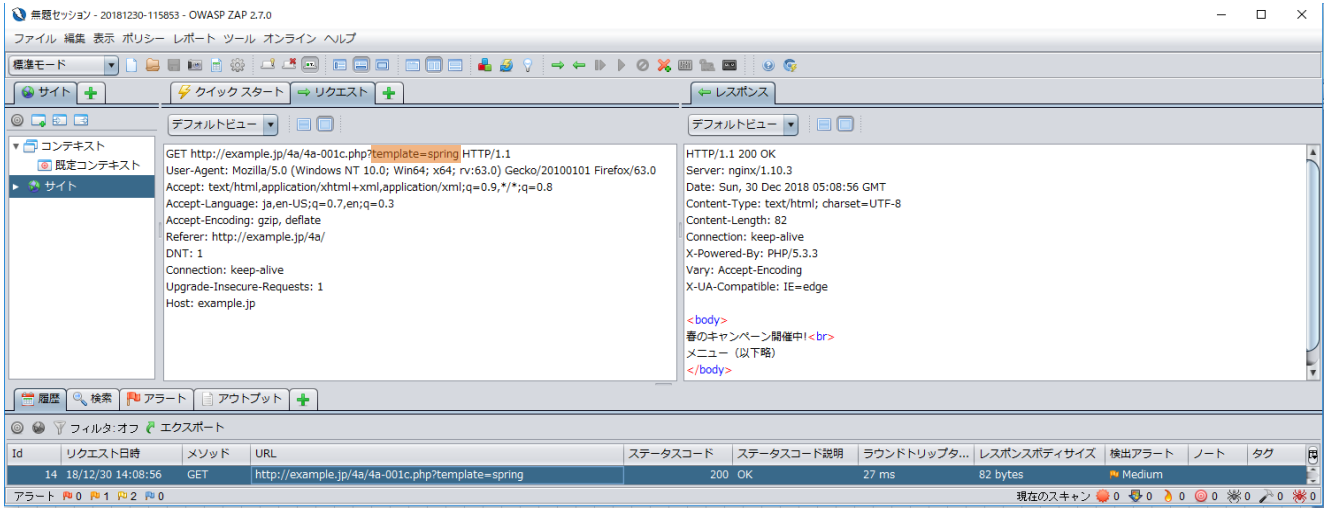


【サーバ： 4a/4a-001c.php 】

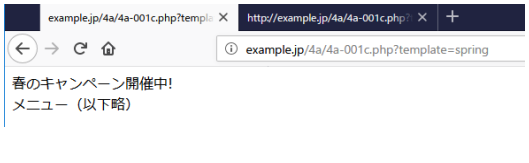


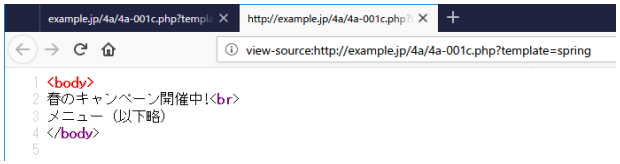
ファイル名を英数字のみに限定するチェックを入れます

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



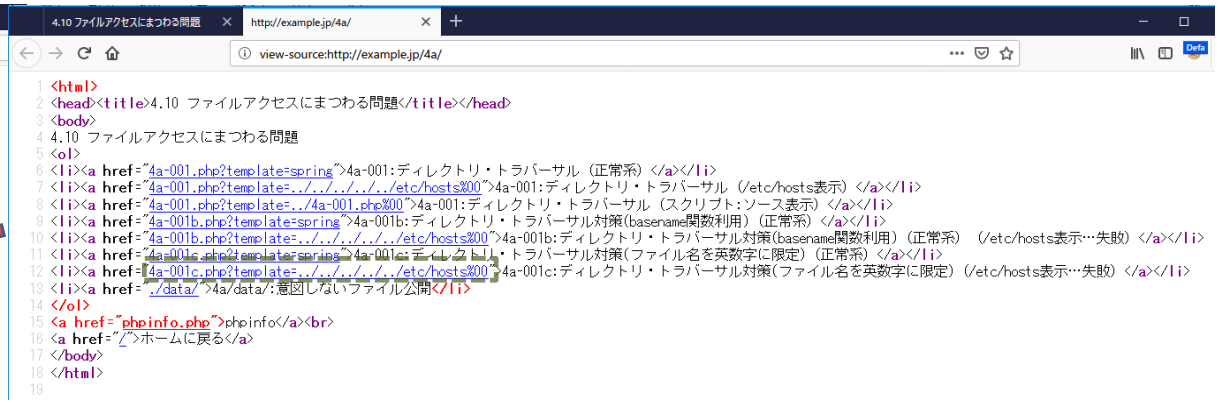
【ブラウザ】



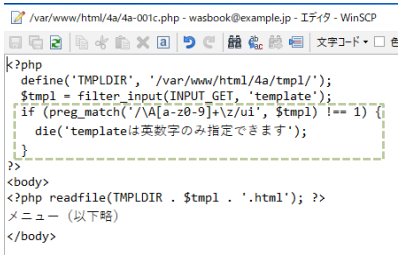


4a-001c:ディレクトリ・トラバーサル対策(ファイル名を英数字に限定)(/etc/hosts表示…失敗)

【ブラウザ】

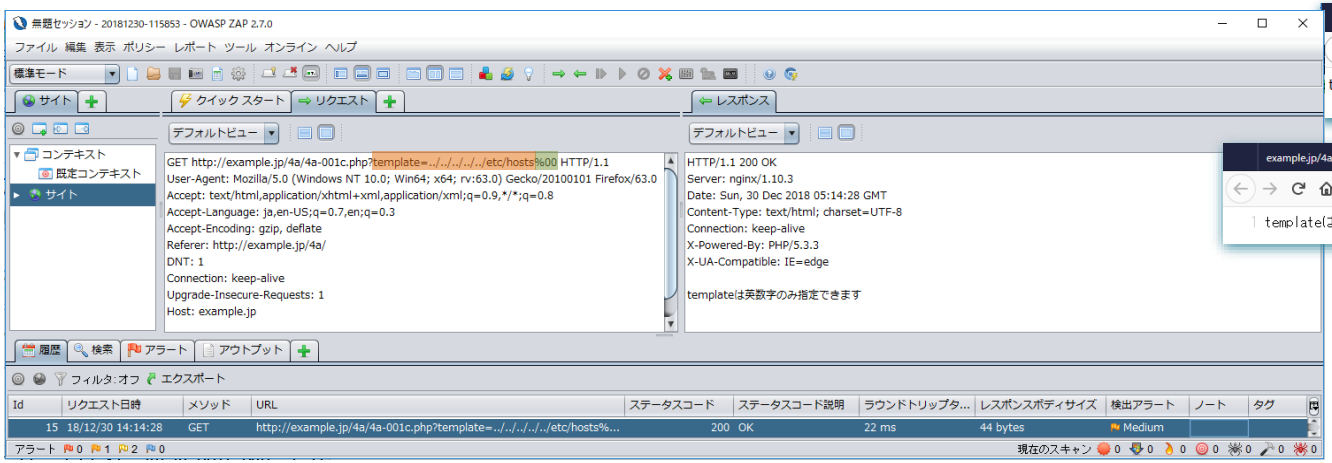


【サーバ： 4a/4a-001c.php 】

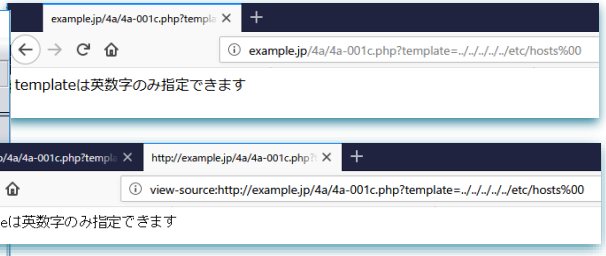


ファイル名を英数字のみに限定するチェックを入れます

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



【ブラウザ】

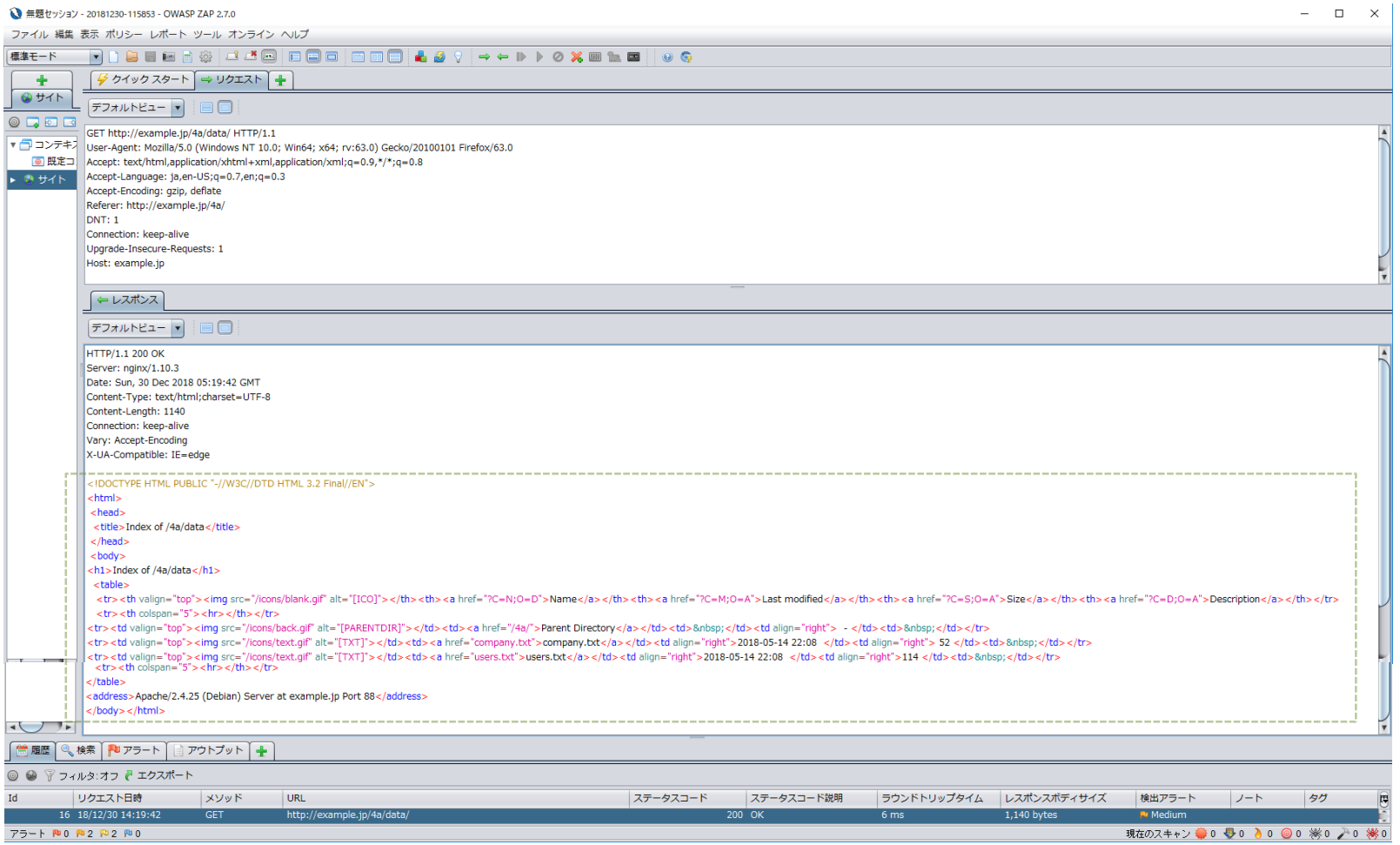


/etc/hosts の表示に失敗

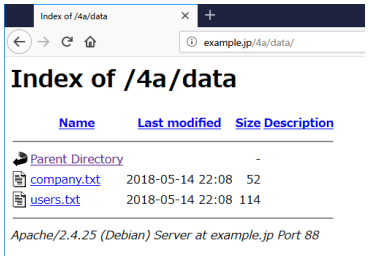
4a/data/:意図しないファイル公開

【ブラウザ】

【ブラウザ→サーバ：リクエスト 4a/data/ → レスポンス 】



【ブラウザ】



ディレクトリ・リスティングの状態