

## 4.6 セッション管理の不備

### 46-001:RefererからのセッションID漏洩

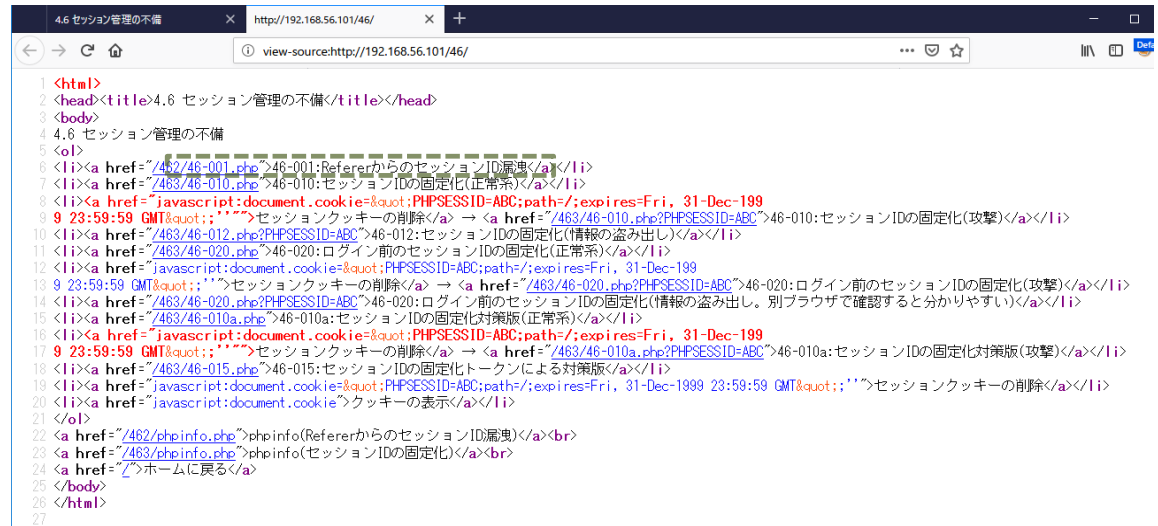
#### 【ブラウザ】



4.6 セッション管理の不備

- 46-001:RefererからのセッションID漏洩
- 46-010:セッションIDの固定化(正常系)
- セッションクッキーの削除 → 46-010:セッションIDの固定化(攻撃)
- 46-012:セッションIDの固定化(情報の盗み出し)
- 46-020:ログイン前のセッションIDの固定化(正常系)
- セッションクッキーの削除 → 46-020:ログイン前のセッションIDの固定化(攻撃)
- 46-020a:セッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)
- 46-010a:セッションIDの固定化対策版(正常系)
- セッションクッキーの削除 → 46-010a:セッションIDの固定化対策版(攻撃)
- 46-015:セッションIDの固定化トークンによる対策版
- セッションクッキーの削除
- クッキーの表示

[phpinfo\(RefererからのセッションID漏洩\)](#)  
[phpinfo\(セッションIDの固定化\)](#)  
[ホームに戻る](#)



```
1 <html>
2 <head><title>4.6 セッション管理の不備</title></head>
3 <body>
4 4.6 セッション管理の不備
5 <ol>
6 <li><a href="/462/46-001.php">46-001:RefererからのセッションID漏洩</a></li>
7 <li><a href="/463/46-010.php">46-010:セッションIDの固定化(正常系)</a></li>
8 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC&quot;;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;'">セッションクッキーの削除</a> → <a href="/463/46-010.php?PHPSESSID=ABC">46-010:セッションIDの固定化(攻撃)</a></li>
9 <li><a href="/463/46-012.php?PHPSESSID=ABC">46-012:セッションIDの固定化(情報の盗み出し)</a></li>
10 <li><a href="/463/46-020.php">46-020:ログイン前のセッションIDの固定化(正常系)</a></li>
11 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC&quot;;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;'">セッションクッキーの削除</a> → <a href="/463/46-020.php?PHPSESSID=ABC">46-020:ログイン前のセッションIDの固定化(攻撃)</a></li>
12 <li><a href="/463/46-020a.php?PHPSESSID=ABC">46-020a:セッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)</a></li>
13 <li><a href="/463/46-010a.php">46-010a:セッションIDの固定化対策版(正常系)</a></li>
14 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC&quot;;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;'">セッションクッキーの削除</a> → <a href="/463/46-010a.php?PHPSESSID=ABC">46-010a:セッションIDの固定化対策版(攻撃)</a></li>
15 <li><a href="/463/46-015.php">46-015:セッションIDの固定化トークンによる対策版</a></li>
16 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC&quot;;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;'">セッションクッキーの削除</a></li>
17 <li><a href="javascript:document.cookie">クッキーの表示</a></li>
18 </ol>
19 <a href="/462/phpinfo.php">phpinfo(RefererからのセッションID漏洩)</a><br>
20 <a href="/463/phpinfo.php">phpinfo(セッションIDの固定化)</a><br>
21 <a href="#">ホームに戻る</a>
22 </body>
23 </html>
```

#### 【サーバ: 462/46-001.php】

```
/var/www/html/462/46-001.php - wasbook@example.jp - エディタ - WinSCP
k?php
  session_start();
?>
<body> <a href="/46-002.php">Next</a> </body>
```

#### 【サーバ: 462/46-002.php】

```
/var/www/html/462/46-002.php - wasbook@example.jp - エディタ - WinSCP
k?php
  session_start();
?>
<body>
  <a href="http://trap.example.com/462/46-900.cgi">外部サイトへのリンク</a>
</body>
```

#### 【サーバ: 462/46-900.cgi】

```
/var/www/html/462/46-900.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/;

my $e_referer = escapeHTML(referer());

print encode('UTF-8', <<END_OF_HTML>);
Content-Type: text/html; charset=UTF-8

<body>
  こちらはセッションID収集サイト。Refererは以下の通り<BR>
  $e_referer
</body>
END_OF_HTML
```

【ブラウザ→サーバ: リクエスト 462/46-001.php → レスポンス】RefererからのセッションID漏洩

無題セッション - 20181223-235505 - 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

```
GET http://example.jp/462/46-001.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/46/
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: Mon, 24 Dec 2018 01:51:15 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 82
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
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body> <a href="http://example.jp/462/46-002.php?PHPSESSID=1ehuqkic0doidr46n4jqg71v17">Next</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
7	18/12/24 1:51:14	GET	http://example.jp/462/46-001.php	200	OK	23 ms	82 bytes	Medium		
9	18/12/24 1:52:19	GET	http://example.jp/462/46-002.php?PHPSESS...	200	OK	24 ms	101 bytes	Medium		
10	18/12/24 1:53:31	GET	http://trap.example.com/462/46-900.cgi	200	OK	101 ms	162 bytes	Medium		

アラート 0 2 3 0 現在のスキャン 0 0 0 0 0 0 0 0 0 0

【ブラウザ→サーバ: リクエスト 462/46-002.php → レスポンス】RefererからのセッションID漏洩

無題セッション - 20181223-235505 - 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

```
GET http://example.jp/462/46-002.php?PHPSESSID=1ehuqkic0doidr46n4jqg71v17 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/462/46-001.php
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: Mon, 24 Dec 2018 01:52:20 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 101
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
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
<a href="http://trap.example.com/462/46-900.cgi">外部サイトへのリンク</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
7	18/12/24 1:51:14	GET	http://example.jp/462/46-001.php	200	OK	23 ms	82 bytes	Medium		
9	18/12/24 1:52:19	GET	http://example.jp/462/46-002.php?PHPSESS...	200	OK	24 ms	101 bytes	Medium		
10	18/12/24 1:53:31	GET	http://trap.example.com/462/46-900.cgi	200	OK	101 ms	162 bytes	Medium		

アラート 0 2 3 0 現在のスキャン 0 0 0 0 0 0 0 0 0 0

## 【ブラウザ→偽サーバ: リクエスト http://trap.example.com/462/46-900.cgi → レスポンス】RefererからのセッションID漏洩

無題セッション - 20181223-235505 - 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://trap.example.com/462/46-900.cgi 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/462/46-002.php?PHPSESSID=1ehuqklc0doidr46n4jqg71v17
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: trap.example.com
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 24 Dec 2018 01:53:32 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 162
Connection: keep-alive
Vary: Accept-Encoding
X-UA-Compatible: IE=edge
```

<body>  
こちらはセッションID収集サイト。Refererは以下の通り<BR>  
http://example.jp/462/46-002.php?PHPSESSID=1ehuqklc0doidr46n4jqg71v17  
</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
7	18/12/24 1:51:14	GET	http://example.jp/462/46-001.php	200	OK	23 ms	82 bytes	Medium		
9	18/12/24 1:52:19	GET	http://example.jp/462/46-002.php?PHPSESS...	200	OK	24 ms	101 bytes	Medium		
10	18/12/24 1:53:31	GET	http://trap.example.com/462/46-900.cgi	200	OK	101 ms	162 bytes	Medium		

アラート 0 2 3 0 現在のスキャン 0 0 0 0 0 0 0 0 0 0 0 0

## 【ブラウザ】

example.jp/462/46-001.php

example.jp/462/46-001.php

Next

example.jp/462/46-002.php?PHPSESSID=1ehuqklc0doidr46n4jqg71v17

外部サイトへのリンク

trap.example.com/462/46-900.cgi

こちらはセッションID収集サイト。Refererは以下の通り  
http://example.jp/462/46-002.php?PHPSESSID=1ehuqklc0doidr46n4jqg71v17

## 46-010:セッションIDの固定化(正常系)

### 【ブラウザ】



4.6 セッション管理の不備

1. 46-001:RefererからのセッションID漏洩
2. 46-010:セッションIDの固定化(正常系) 
3. セッションクッキーの削除 → 46-010:セッションIDの固定化(攻撃)
4. 46-012:セッションIDの固定化(情報の盗み出し)
5. 46-020:ログイン前のセッションIDの固定化(正常系)
6. セッションクッキーの削除 → 46-020:ログイン前のセッションIDの固定化(攻撃)
7. 46-020:ログイン前のセッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)
8. 46-010a:セッションIDの固定化対策版(正常系)
9. セッションクッキーの削除 → 46-010a:セッションIDの固定化対策版(攻撃)
10. 46-015:セッションIDの固定化トークンによる対策版
11. セッションクッキーの削除
12. クッキーの表示

[phpinfo\(RefererからのセッションID漏洩\)](#)  
[phpinfo\(セッションIDの固定化\)](#)  
[ホームに戻る](#)



```
1 <html>
2 <head><title>4.6 セッション管理の不備</title></head>
3 <body>
4 4.6 セッション管理の不備
5 <ol>
6 <li><a href="/462/46-001.php">46-001:RefererからのセッションID漏洩</a></li>
7 <li><a href="/463/46-010.php">46-010:セッションIDの固定化(正常系)</a></li>
8 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-199
9 23:59:59 GMT&quot;;"">セッションクッキーの削除</a> → <a href="/463/46-010a.php?PHPSESSID=ABC">46-010a:セッションIDの固定化対策版(攻撃)</a></li>
10 <li><a href="/463/46-012.php?PHPSESSID=ABC">46-012:セッションIDの固定化(情報の盗み出し)</a></li>
11 <li><a href="/463/46-020.php">46-020:ログイン前のセッションIDの固定化(正常系)</a></li>
12 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-199
13 23:59:59 GMT&quot;;"">セッションクッキーの削除</a> → <a href="/463/46-020.php?PHPSESSID=ABC">46-020:ログイン前のセッションIDの固定化(攻撃)</a></li>
14 <li><a href="/463/46-020.php?PHPSESSID=ABC">46-020:ログイン前のセッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)</a></li>
15 <li><a href="/463/46-010a.php">46-010a:セッションIDの固定化対策版(正常系)</a></li>
16 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-199
17 23:59:59 GMT&quot;;"">セッションクッキーの削除</a> → <a href="/463/46-010a.php?PHPSESSID=ABC">46-010a:セッションIDの固定化対策版(攻撃)</a></li>
18 <li><a href="/463/46-015.php">46-015:セッションIDの固定化トークンによる対策版</a></li>
19 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;"">セッションクッキーの削除</a></li>
20 <li><a href="javascript:document.cookie">クッキーの表示</a></li>
21 </ol>
22 <a href="/462/phpinfo.php">phpinfo(RefererからのセッションID漏洩)</a><br>
23 <a href="/463/phpinfo.php">phpinfo(セッションIDの固定化)</a><br>
24 <a href="/">ホームに戻る</a>
25 </body>
26 </html>
27
```

### 【サーバ: 463/45-010.php】

```
/var/www/html/463/46-010.php - wasbook@example.jp - エディタ
k?php
session_start();
?>
<html>
<body>
<form action="/46-011.php" method="POST">
ユーザID:<input name="id" type="text"><br>
<input type="submit" value="ログイン">
</form>
</body>
</html>
```

### 【サーバ: 463/45-011.php】

```
/var/www/html/463/46-011.php - wasbook@example.jp - WinSCP
k?php
session_start();
$id = filter_input(INPUT_POST, 'id'); // 必ずログインに成功する (仕様)
$_SESSION['id'] = $id; // ユーザIDをセッションに保存
?>
<html>
<body>
<?php echo htmlspecialchars($id, ENT_COMPAT, 'UTF-8'); ?>
さん、ログイン成功です<br>
<a href="/46-012.php">個人情報</a>
</body>
</html>
```

### 【サーバ: 463/45-012.php】

```
/var/www/html/463/46-012.php - wasbook@example.jp - WinSCP
k?php
session_start();
?>
<html>
<body>
現在のユーザID:<?php echo htmlspecialchars($_SESSION['id'], ENT_COMPAT, 'UTF-8'); ?><br>
</body>
</html>
```

【ブラウザ→サーバ: リクエスト 463/46-010.php → レスポンス】セッションIDの固定化(正常系)

The screenshot shows the OWASP ZAP interface with a request and response view. The request is a GET to http://example.jp/463/46-010.php. The response is an HTML page with a form containing a hidden PHPSESSID field. The response body is highlighted with a dashed green box.

```
GET http://example.jp/463/46-010.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/46/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 24 Dec 2018 02:11:21 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 243
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=esc17lsobt9o60k4j3lrq6d3; path=/
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<html>
<body>
<form action="/46-011.php" method="POST"> <input type="hidden" name="PHPSESSID" value="esc17lsobt9o60k4j3lrq6d3" />
ユーザID: <input name="id" type="text"> <br>
<input type="submit" value="ログイン">
</form>
</body>
</html>
```

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	18/12/24 2:11:20	GET	http://example.jp/463/46-010.php	200	OK	27 ms	243 bytes	Medium		Form, Hidden, ...
17	18/12/24 2:14:35	POST	http://example.jp/463/46-011.php	200	OK	27 ms	112 bytes	Medium		
18	18/12/24 2:15:22	GET	http://example.jp/463/46-012.php	200	OK	31 ms	62 bytes	Medium		

アラート 0 2 4 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 463/46-010.php → レスポンス】セッションIDの固定化(正常系)

無題セッション - 20181223-235505 - 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

```
POST http://example.jp/463/46-011.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/463/46-010.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 46
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=esc17sobt9o60k4j3rjrgp6d3&id=yamada
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: Mon, 24 Dec 2018 02:14:35 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 112
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
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<html>
<body>
yamadaさん、ログイン成功です<BR>
<a href="/46-012.php">個人情報</a>
</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
15	18/12/24 2:11:20	GET	http://example.jp/463/46-010.php	200	OK	27 ms	243 bytes	Medium	Form, Hidden, ...	
17	18/12/24 2:14:35	POST	http://example.jp/463/46-011.php	200	OK	27 ms	112 bytes	Medium		
18	18/12/24 2:15:22	GET	http://example.jp/463/46-012.php	200	OK	31 ms	62 bytes	Medium		

アラート 0 2 4 0 現在のスキャン 0 0 0 0 0 0 0 0



## セッションクッキーの削除 → 46-010:セッションIDの固定化(攻撃)

### 【ブラウザ】

「CTRL」+「SHIFT」+「I」 → 「ストレージ」 → 「cookie」から「http://example.jpオリジン」を選択して、クッキーを削除する

4.6 セッション管理の不備

- 46-001:RefererからのセッションID漏洩
- 46-010:セッションIDの固定化(正常系)
- セッションクッキーの削除 → 46-010:セッションIDの固定化(攻撃) ← ②
- 46-012:セッションIDの固定化(情報の盗み出し)
- 46-020:ログイン前のセッションIDの固定化(正常系)
- セッションクッキーの削除 → 46-020:ログイン前のセッションIDの固定化(攻撃)
- 46-020:ログイン前のセッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)
- 46-010a:セッションIDの固定化対策版(正常系)
- セッションクッキーの削除 → 46-010a:セッションIDの固定化対策版(攻撃)
- 46-015:セッションIDの固定化トークンによる対策版
- セッションクッキーの削除
- クッキーの表示

[phpinfo\(RefererからのセッションID漏洩\)](#)  
[phpinfo\(セッションIDの固定化\)](#)  
[ホームに戻る](#)

Cookie

名前	ドメイン	パス	有効期限	アクセス日時	値	Htt
PHPSESSID	example.jp	/		2018 11:44:32	esc17b0q9o9k...	false

① アイテムを追加  
"PHPSESSID-example.jp/" を削除  
"example.jp" のすべてのアイテムを削除  
すべてを削除  
すべてのセッション Cookie を削除

```
<html>
<head><title>4.6 セッション管理の不備</title></head>
<body>
4.6 セッション管理の不備
<ol>
<li><a href="/462/46-001.php">46-001:RefererからのセッションID漏洩</a></li>
<li><a href="/463/46-010.php">46-010:セッションIDの固定化(正常系)</a></li>
<li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC&quot;;path=/;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;">セッションクッキーの削除</a> → <a href="/463/46-010.php?PHPSESSID=ABC">46-010:セッションIDの固定化(攻撃)</a></li>
<li><a href="/463/46-012.php?PHPSESSID=ABC">46-012:セッションIDの固定化(情報の盗み出し)</a></li>
<li><a href="/463/46-020.php">46-020:ログイン前のセッションIDの固定化(正常系)</a></li>
<li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC&quot;;path=/;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;">セッションクッキーの削除</a> → <a href="/463/46-020.php?PHPSESSID=ABC">46-020:ログイン前のセッションIDの固定化(攻撃)</a></li>
<li><a href="/463/46-020.php?PHPSESSID=ABC">46-020:ログイン前のセッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)</a></li>
<li><a href="/463/46-010a.php">46-010a:セッションIDの固定化対策版(正常系)</a></li>
<li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC&quot;;path=/;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;">セッションクッキーの削除</a> → <a href="/463/46-010a.php?PHPSESSID=ABC">46-010a:セッションIDの固定化対策版(攻撃)</a></li>
<li><a href="/463/46-015.php">46-015:セッションIDの固定化トークンによる対策版</a></li>
<li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC&quot;;path=/;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;">セッションクッキーの削除</a></li>
<li><a href="javascript:document.cookie">クッキーの表示</a></li>
</ol>
<a href="/462/phpinfo.php">phpinfo(RefererからのセッションID漏洩)</a><br>
<a href="/463/phpinfo.php">phpinfo(セッションIDの固定化)</a><br>
<a href="/">ホームに戻る</a>
</body>
</html>
```

### 【サーバ: 463/45-010.php】

```
/var/www/html/463/46-010.php - wasbook@example.jp - エディタ
k?php
session_start();
?>
<html>
<body>
<form action="/46-011.php" method="POST">
ユーザID:<input name="id" type="text"><br>
<input type="submit" value="ログイン">
</form>
</body>
</html>
```

### 【サーバ: 463/45-011.php】

```
/var/www/html/463/46-011.php - wasbook@example.jp - エディタ - WinSCP
k?php
session_start();
?id = filter_input(INPUT_POST, 'id'); // 必ずログインに成功する (仕様)
$_SESSION['id'] = $id; // ユーザIDをセッションに保存
?>
<html>
<body>
<?php echo htmlspecialchars($id, ENT_COMPAT, 'UTF-8'); ?>
さん、ログイン成功です<br>
<a href="/46-012.php">個人情報</a>
</body>
</html>
```

### 【サーバ: 463/45-012.php】

```
/var/www/html/463/46-012.php - wasbook@example.jp - エディタ - WinSCP
k?php
session_start();
?>
<html>
<body>
現在のユーザID:<?php echo htmlspecialchars($_SESSION['id'], ENT_COMPAT, 'UTF-8'); ?><br>
</body>
</html>
```



【ブラウザ→サーバ: リクエスト 463/46-010.php → レスポンス】セッションクッキーの削除 → 46-010:セッションIDの固定化(攻撃)

セッションID: PHPSESSID=ABC に固定

```

GET http://example.jp/463/46-010.php?PHPSESSID=ABC HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/xml,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/46/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 24 Dec 2018 03:05:08 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 220
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
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<html>
<body>
<form action="/46-011.php" method="POST"> <input type="hidden" name="PHPSESSID" value="ABC" />
ユーザ名:<input type="text" value="" />
<input type="submit" value="ログイン">
</form>
</body>
</html>
    
```

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
27	18/12/24 3:05:07	GET	http://example.jp/463/46-010.php?PHPSESS...	200	OK	25 ms	220 bytes	Medium	Form, Hidden	
28	18/12/24 3:05:34	POST	http://example.jp/463/46-011.php	200	OK	23 ms	126 bytes	Medium		
29	18/12/24 3:05:59	GET	http://example.jp/463/46-012.php?PHPSESS...	200	OK	21 ms	62 bytes	Medium		

【ブラウザ→サーバ: リクエスト 463/46-011.php → レスポンス】セッションクッキーの削除 → 46-010:セッションIDの固定化(攻撃)

```

POST http://example.jp/463/46-011.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/463/46-010.php?PHPSESSID=ABC
Content-Type: application/x-www-form-urlencoded
Content-Length: 23
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp

PHPSESSID=ABC&id=tanaka

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 24 Dec 2018 03:05:34 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 126
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
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<html>
<body>
tanakaさん、ログイン成功です<BR>
<a href="/46-01a.php?PHPSESSID=ABC">個人情報</a>
</body>
</html>
    
```

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
27	18/12/24 3:05:07	GET	http://example.jp/463/46-010.php?PHPSESS...	200	OK	25 ms	220 bytes	Medium	Form, Hidden	
28	18/12/24 3:05:34	POST	http://example.jp/463/46-011.php	200	OK	23 ms	126 bytes	Medium		
29	18/12/24 3:05:59	GET	http://example.jp/463/46-012.php?PHPSESS...	200	OK	21 ms	62 bytes	Medium		

【ブラウザ→サーバ: リクエスト 463/46-012.php → レスポンス】セッションクッキーの削除 → 46-010:セッションIDの固定化(攻撃)

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

- Request (Left Panel):**
  - Method: GET
  - URL: http://example.jp/463/46-012.php?PHPSESSID=ABC
  - 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/463/46-011.php
  - DNT: 1
  - Connection: keep-alive
  - Upgrade-Insecure-Requests: 1
  - Host: example.jp
- Response (Right Panel):**
  - HTTP/1.1 200 OK
  - Server: nginx/1.10.3
  - Date: Mon, 24 Dec 2018 03:05:59 GMT
  - Content-Type: text/html; charset=UTF-8
  - 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
  - X-UA-Compatible: IE=edge
  - Body:
 

```
<html>
<body>
現在のユーザID:tanaka<BR>
</body>
</html>
```
- Log Table (Bottom):**

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
27	18/12/24 3:05:07	GET	http://example.jp/463/46-010.php?PHPSESS...	200	OK	25 ms	220 bytes	Medium		Form, Hidden
28	18/12/24 3:05:34	POST	http://example.jp/463/46-011.php	200	OK	23 ms	126 bytes	Medium		
29	18/12/24 3:05:59	GET	http://example.jp/463/46-012.php?PHPSESS...	200	OK	21 ms	62 bytes	Medium		

【ブラウザ】

The browser address bar shows the URL: `example.jp/463/46-010.php?PHPSESSID=ABC`. The page content includes a text input field for the user ID containing "tanaka" and a "ログイン" (Login) button.

The browser address bar shows the URL: `example.jp/463/46-011.php`. The page content displays a message: "tanakaさん、ログイン成功です" (Hello tanaka, login successful) with a link to "個人情報" (Personal Information).

The browser address bar shows the URL: `example.jp/463/46-012.php?PHPSESSID=ABC`. The page content displays the message: "現在のユーザID:tanaka" (Current user ID: tanaka).

## 46-012:セッションIDの固定化(情報の盗み出し)

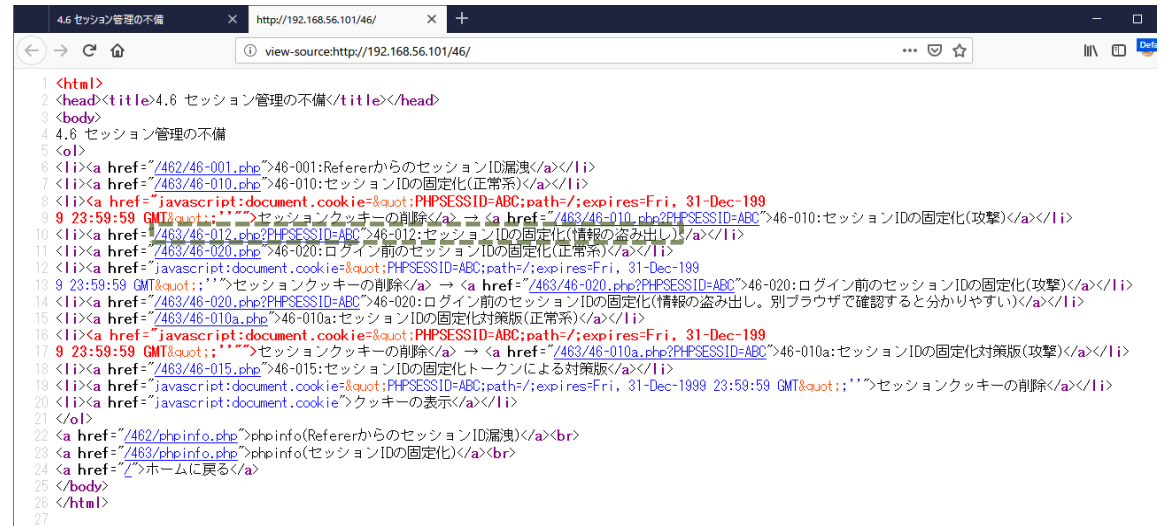
### 【ブラウザ】



4.6 セッション管理の不備

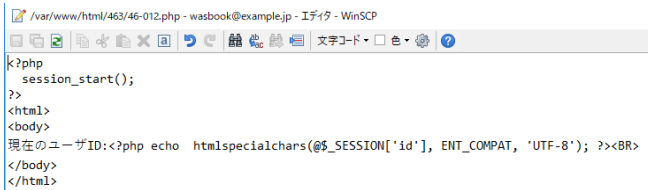
- 46-001:RefererからのセッションID漏洩
- 46-010:セッションIDの固定化(正常系)
- セッションクッキーの削除 → 46-010:セッションIDの固定化(攻撃)
- 46-012:セッションIDの固定化(情報の盗み出し) ←
- 46-020:ログイン前のセッションIDの固定化(正常系)
- セッションクッキーの削除 → 46-020:ログイン前のセッションIDの固定化(攻撃)
- 46-020:ログイン前のセッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)
- 46-010a:セッションIDの固定化対策版(正常系)
- セッションクッキーの削除 → 46-010a:セッションIDの固定化対策版(攻撃)
- 46-015:セッションIDの固定化トークンによる対策版
- セッションクッキーの削除
- クッキーの表示

[phpinfo\(RefererからのセッションID漏洩\)](#)  
[phpinfo\(セッションIDの固定化\)](#)  
[ホームに戻る](#)



```
1 <html>
2 <head><title>4.6 セッション管理の不備</title></head>
3 <body>
4 4.6 セッション管理の不備
5 <ol>
6 <li><a href="/462/46-001.php">46-001:RefererからのセッションID漏洩</a></li>
7 <li><a href="/463/46-010.php">46-010:セッションIDの固定化(正常系)</a></li>
8 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-199
9 23:59:59 GMT&quot;;"">セッションクッキーの削除</a> → <a href="/463/46-010.php?PHPSESSID=ABC">46-010:セッションIDの固定化(攻撃)</a></li>
10 <li><a href="/463/46-012.php?PHPSESSID=ABC">46-012:セッションIDの固定化(情報の盗み出し)</a></li>
11 <li><a href="/463/46-020.php">46-020:ログイン前のセッションIDの固定化(正常系)</a></li>
12 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-199
13 23:59:59 GMT&quot;;"">セッションクッキーの削除</a> → <a href="/463/46-020.php?PHPSESSID=ABC">46-020:ログイン前のセッションIDの固定化(攻撃)</a></li>
14 <li><a href="/463/46-020.php?PHPSESSID=ABC">46-020:ログイン前のセッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)</a></li>
15 <li><a href="/463/46-010a.php">46-010a:セッションIDの固定化対策版(正常系)</a></li>
16 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-199
17 23:59:59 GMT&quot;;"">セッションクッキーの削除</a> → <a href="/463/46-010a.php?PHPSESSID=ABC">46-010a:セッションIDの固定化対策版(攻撃)</a></li>
18 <li><a href="/463/46-015.php">46-015:セッションIDの固定化トークンによる対策版</a></li>
19 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;"">セッションクッキーの削除</a></li>
20 <li><a href="javascript:document.cookie">クッキーの表示</a></li>
21 </ol>
22 <a href="/462/phpinfo.php">phpinfo(RefererからのセッションID漏洩)</a><br>
23 <a href="/463/phpinfo.php">phpinfo(セッションIDの固定化)</a><br>
24 <a href="/">ホームに戻る</a>
25 </body>
26 </html>
27
```

### 【サーバ: 463/46-012.php】



```
/var/www/html/463/46-012.php - wasbook@example.jp - エディタ - WinSCP
k?php
  session_start();
?>
<html>
<body>
現在のユーザID:<?php echo htmlspecialchars($_SESSION['id'], ENT_COMPAT, 'UTF-8'); ?><br>
</body>
</html>
```

### 【ブラウザ→サーバ: リクエスト 463/46-012.php → レスポンス】 46-012:セッションIDの固定化(情報の盗み出し)

無題セッション - 20181223-235505 - 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/463/46-012.php?PHPSESSID=ABC 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/46/  
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: Mon, 24 Dec 2018 03:45:22 GMT  
Content-Type: text/html; charset=UTF-8  
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  
X-UA-Compatible: IE=edge

<html>  
<body>  
現在のユーザID:tanaka<BR>  
</body>  
</html>

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
33	18/12/24 3:45:21	GET	http://example.jp/463/46-012.php?PHPSESS...	200	OK	25 ms	62 bytes	Medium		

アラート 0

現在のスキャン

OWASP ZAPからPHPSESSID=ABC  
をスニファー

### 【ブラウザ】

4.6 セッション管理の不備

- 46-001:RefererからのセッションID漏洩
- 46-010:セッションIDの固定化(正常系)
- セッションクッキーの削除 → 46-010:セッションIDの固定化(攻撃)
- 46-012:セッションIDの固定化(情報の盗み出し)
- 46-020:ログイン前のセッションIDの固定化(正常系)
- セッションクッキーの削除 → 46-020:ログイン前のセッションIDの固定化(攻撃)
- 46-020:ログイン前のセッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)
- 46-010a:セッションIDの固定化対策版(正常系)
- セッションクッキーの削除 → 46-010a:セッションIDの固定化対策版(攻撃)
- 46-015:セッションIDの固定化トークンによる対策版
- セッションクッキーの削除
- クッキーの表示

[phpinfo\(RefererからのセッションID漏洩\)](#)  
[phpinfo\(セッションIDの固定化\)](#)  
[ホームに戻る](#)

他の端末から攻撃者がPHPSESSID=ABCを確認する  
というストーリーで、ChromeからWebブラウズ

example.jp/463/46-012.php?PHP x +

保護されていない通信 | example.jp/463/46-012.php?PHPSESSID=ABC

現在のユーザID:tanaka

ユーザID:tanaka を盗み見できる

## 46-020:ログイン前のセッションIDの固定化(正常系)

### 【ブラウザ】

4.6 セッション管理の不備

- 46-001:RefererからのセッションID漏洩
- 46-010:セッションIDの固定化(正常系)
- セッションクッキーの削除 → 46-010:セッションIDの固定化(攻撃)
- 46-012:セッションIDの固定化(情報の盗み出し)
- 46-020:ログイン前のセッションIDの固定化(正常系)
- セッションクッキーの削除 → 46-020:ログイン前のセッションIDの固定化(攻撃)
- 46-020:ログイン前のセッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)
- 46-010a:セッションIDの固定化対策版(正常系)
- セッションクッキーの削除 → 46-010a:セッションIDの固定化対策版(攻撃)
- 46-015:セッションIDの固定化トークンによる対策版
- セッションクッキーの削除
- クッキーの表示

[phpinfo\(RefererからのセッションID漏洩\)](#)  
[phpinfo\(セッションIDの固定化\)](#)  
[ホームに戻る](#)

```
1 <html>
2 <head<title>4.6 セッション管理の不備</title></head>
3 <body>
4 4.6 セッション管理の不備
5 <ol>
6 <li><a href="/462/46-001.php">46-001:RefererからのセッションID漏洩</a></li>
7 <li><a href="/463/46-010.php">46-010:セッションIDの固定化(正常系)</a></li>
8 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-199
9 23:59:59 GMT&quot;;"">セッションクッキーの削除</a> → <a href="/463/46-010.php?PHPSESSID=ABC">46-010:セッションIDの固定化(攻撃)</a></li>
10 <li><a href="/463/46-012.php?PHPSESSID=ABC">46-012:セッションIDの固定化(情報の盗み出し)</a></li>
11 <li><a href="/463/46-020.php">46-020:ログイン前のセッションIDの固定化(正常系)</a></li>
12 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-199
13 23:59:59 GMT&quot;;"">セッションクッキーの削除</a> → <a href="/463/46-020.php?PHPSESSID=ABC">46-020:ログイン前のセッションIDの固定化(攻撃)</a></li>
14 <li><a href="/463/46-020.php?PHPSESSID=ABC">46-020:ログイン前のセッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)</a></li>
15 <li><a href="/463/46-010a.php">46-010a:セッションIDの固定化対策版(正常系)</a></li>
16 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-199
17 23:59:59 GMT&quot;;"">セッションクッキーの削除</a> → <a href="/463/46-010a.php?PHPSESSID=ABC">46-010a:セッションIDの固定化対策版(攻撃)</a></li>
18 <li><a href="/463/46-015.php">46-015:セッションIDの固定化トークンによる対策版</a></li>
19 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;"">セッションクッキーの削除</a></li>
20 <li><a href="javascript:document.cookie">クッキーの表示</a></li>
21 </ol>
22 <a href="/462/phpinfo.php">phpinfo(RefererからのセッションID漏洩)</a><br>
23 <a href="/463/phpinfo.php">phpinfo(セッションIDの固定化)</a><br>
24 <a href="/">ホームに戻る</a>
25 </body>
26 </html>
27
```

### 【サーバ: 463/46-020.php】

```
/var/www/html/463/46-020.php - wasbook@example.jp - エディタ - WinSCP
k?php
session_start();
$name = @$_SESSION['name'];
$mail = @$_SESSION['mail'];
?>
<head><title>個人情報の入力</title></head>
<body>
<form action="46-021.php" method="POST">
氏名:<input name="name" value=""?php
echo htmlspecialchars($name, ENT_COMPAT, 'UTF-8'); ?>><br>
メール:<input name="mail" value=""?php
echo htmlspecialchars($mail, ENT_COMPAT, 'UTF-8'); ?>><br>
<input type="submit" value="確認">
</form>
</body>
</html>
```

### 【サーバ: 463/46-021.php】

```
/var/www/html/463/46-021.php - wasbook@example.jp - エディタ - WinSCP
k?php
session_start();
$name = $_SESSION['name'] = filter_input(INPUT_POST, 'name');
$mail = $_SESSION['mail'] = filter_input(INPUT_POST, 'mail');
?>
<head><title>個人情報の確認</title></head>
<body>
<form action="46-022.php" method="POST">
氏名:<?php echo htmlspecialchars($name, ENT_COMPAT, 'UTF-8'); ?><br>
メール:<?php echo htmlspecialchars($mail, ENT_COMPAT, 'UTF-8'); ?><br>
<input type="submit" value="登録"><br>
<a href="46-020.php">戻る</a>
</form>
</body>
</html>
```

### 【サーバ: 463/46-022.php】

```
/var/www/html/463/46-022.php - wasbook@example.jp - エディタ - WinSCP
k?php
session_start();
$name = $_SESSION['name'];
$mail = $_SESSION['mail'];
?>
<head><title>個人情報の登録</title></head>
<body>
登録しました<br>
氏名:<?php echo htmlspecialchars($name, ENT_COMPAT, 'UTF-8'); ?><br>
メール:<?php echo htmlspecialchars($mail, ENT_COMPAT, 'UTF-8'); ?><br>
</body>
</html>
```

【ブラウザ→サーバ: リクエスト 463/46-020.php → レスポンス】ログイン前のセッションIDの固定化(正常系)

The screenshot shows the Burp Suite interface with the following details:

- Request (GET http://example.jp/463/46-020.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/46/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp
            
```
- Response (HTTP/1.1 200 OK):**

```

Server: nginx/1.10.3
Date: Mon, 24 Dec 2018 04:04:02 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 317
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=k2ci8gdjcl2fh2jpm4e8h1k3; path=/
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<head><title>個人情報の入力</title></head>
<body>
<form action="/46-021.php" method="POST">
  <input type="hidden" name="PHPSESSID" value="k2ci8gdjcl2fh2jpm4e8h1k3" />
  氏名:<input name="name" value=""><br>
  メール:<input name="mail" value=""><br>
  <input type="submit" value="確認">
</form>
</body>
</html>
            
```
- Table of Requests:**

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
38	18/12/24 4:04:01	GET	http://example.jp/463/46-020.php	200	OK	36 ms	317 bytes	Medium		Form, Hidden, ...
40	18/12/24 4:04:56	POST	http://example.jp/463/46-021.php	200	OK	26 ms	245 bytes	Medium		Form
41	18/12/24 4:05:45	POST	http://example.jp/463/46-022.php	200	OK	22 ms	146 bytes	Medium		

【ブラウザ→サーバ: リクエスト 463/46-021.php → レスポンス】ログイン前のセッションIDの固定化(正常系)

無題セッション - 20181223-235505 - 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

サイト

```
POST http://example.jp/463/46-021.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/463/46-020.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 85
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=k2o8gdjcl2lfh2jpm4e8h1k38name=%E9%88%B4%E6%9C%A8&mail=suzuki%40example.jp
Upgrade-Insecure-Requests: 1
Host: example.jp
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 24 Dec 2018 04:04:57 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 245
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
Vary: Accept-Encoding
X-UA-Compatible: IE=edge
```

```
<head><title>個人情報の確認</title></head>
<body>
<form action="/46-022.php" method="POST">
氏名: 鈴木<br>
メール: suzuki@example.jp<br>
<input type="submit" value="登録"><br>
<a href="/46-020.php">戻る</a>
</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
38	18/12/24 4:04:01	GET	http://example.jp/463/46-020.php	200	OK	36 ms	317 bytes	Medium		Form, Hidden, ...
40	18/12/24 4:04:56	POST	http://example.jp/463/46-021.php	200	OK	26 ms	245 bytes	Medium		Form
41	18/12/24 4:05:45	POST	http://example.jp/463/46-022.php	200	OK	22 ms	146 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 463/46-022.php → レスポンス】ログイン前のセッションIDの固定化(正常系)

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

- Request (Left Panel):**
  - Method: POST
  - URL: http://example.jp/463/46-022.php
  - Headers:
    - 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/463/46-021.php
    - Content-Type: application/x-www-form-urlencoded
    - Content-Length: 0
    - DNT: 1
    - Connection: keep-alive
    - Cookie: PHPSESSID=k2c8gdjic2lfh2ijpm4e8h1k3
    - Upgrade-Insecure-Requests: 1
    - Host: example.jp
- Response (Right Panel):**
  - Method: HTTP/1.1 200 OK
  - Server: nginx/1.10.3
  - Date: Mon, 24 Dec 2018 04:05:46 GMT
  - Content-Type: text/html; charset=UTF-8
  - Content-Length: 146
  - 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
  - Vary: Accept-Encoding
  - X-UA-Compatible: IE=edge
- HTML Body (Right Panel):**

```
<head><title>個人情報の登録</title></head>
<body>
登録しました<br>
氏名:鈴木<br>
メール:suzuki@example.jp<br>
</body>
</html>
```
- Log Table (Bottom):**

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
38	18/12/24 4:04:01	GET	http://example.jp/463/46-020.php	200	OK	36 ms	317 bytes	Medium		Form, Hidden, ...
40	18/12/24 4:04:56	POST	http://example.jp/463/46-021.php	200	OK	26 ms	245 bytes	Medium		Form
41	18/12/24 4:05:45	POST	http://example.jp/463/46-022.php	200	OK	22 ms	146 bytes	Medium		

【ブラウザ】

The browser window shows the URL `example.jp/463/46-020.php`. The form contains the following fields:

- 氏名: 鈴木
- メール: suzuki@example.jp
- 確認 button (highlighted with a red arrow)

The browser window shows the URL `example.jp/463/46-021.php`. The page displays the following information:

- 氏名: 鈴木
- メール: suzuki@example.jp
- 登録 button (highlighted with a red arrow)
- 戻る button

The browser window shows the URL `example.jp/463/46-022.php`. The page displays the following information:

- 登録しました
- 氏名: 鈴木
- メール: suzuki@example.jp



## セッションクッキーの削除 → 46-020:ログイン前のセッションIDの固定化(攻撃)

### 【ブラウザ】

「CTRL」+「SHIFT」+「I」 → 「ストレージ」 → 「cookie」から「http://example.jpオリジン」を選択して、クッキーを削除する

4.6 セッション管理の不備

- 46-001:RefererからのセッションID漏洩
- 46-010:セッションIDの固定化(正常系)
- セッションクッキーの削除 → 46-010:セッションIDの固定化(攻撃)
- 46-012:セッションIDの固定化(情報の盗み出し)
- 46-020:ログイン前のセッションIDの固定化(正常系)
- セッションクッキーの削除 → 46-020:ログイン前のセッションIDの固定化(攻撃) ②
- 46-020:ログイン前のセッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)
- 46-010a:セッションIDの固定化対策版(正常系)
- セッションクッキーの削除 → 46-010a:セッションIDの固定化対策版(攻撃)
- 46-015:セッションIDの固定化トークンによる対策版
- セッションクッキーの削除
- クッキーの表示

phpinfo(RefererからのセッションID漏洩)  
phpinfo(セッションIDの固定化)  
ホームに戻る

名前	ドメイン	パス	有効期限	アクセス日時	値	Htt
PHPSESSID	example.jp	/		2018 17:44:32...	esc17b0kt9o6k...	false

① アイテムを追加  
"PHPSESSID-example.jp" を削除  
"example.jp" のすべてのアイテムを削除  
すべてを削除  
すべてのセッション Cookie を削除

### 【サーバ: 463/46-020.php】

```
#!/var/www/html/463/46-020.php - wasbook@example.jp - エディタ - WinSCP
k?php
session_start();
$name = @$_SESSION['name'];
$mail = @$_SESSION['mail'];
?>
<head><title>個人情報の入力</title></head>
<body>
<form action="46-021.php" method="POST">
氏名:<input name="name" value=""?>php
echo htmlspecialchars($name, ENT_COMPAT, 'UTF-8'); ?><br>
メール:<input name="mail" value=""?>php
echo htmlspecialchars($mail, ENT_COMPAT, 'UTF-8'); ?><br>
<input type="submit" value="確認">
</form>
</body>
</html>
```

### 【サーバ: 463/46-021.php】

```
#!/var/www/html/463/46-021.php - wasbook@example.jp - エディタ - WinSCP
k?php
session_start();
$name = filter_input(INPUT_POST, 'name');
$mail = filter_input(INPUT_POST, 'mail');
?>
<head><title>個人情報の確認</title></head>
<body>
<form action="46-022.php" method="POST">
氏名:<?php echo htmlspecialchars($name, ENT_COMPAT, 'UTF-8'); ?><br>
メール:<?php echo htmlspecialchars($mail, ENT_COMPAT, 'UTF-8'); ?><br>
<input type="submit" value="登録"><br>
<a href="46-020.php">戻る</a>
</form>
</body>
</html>
```

### 【サーバ: 463/46-022.php】

```
#!/var/www/html/463/46-022.php - wasbook@example.jp - エディタ - WinSCP
k?php
session_start();
$name = $_SESSION['name'];
$mail = $_SESSION['mail'];
?>
<head><title>個人情報の登録</title></head>
<body>
登録しました<br>
氏名:<?php echo htmlspecialchars($name, ENT_COMPAT, 'UTF-8'); ?><br>
メール:<?php echo htmlspecialchars($mail, ENT_COMPAT, 'UTF-8'); ?><br>
</body>
</html>
```

【ブラウザ→サーバ: リクエスト 463/46-020.php → レスポンス】ログイン前のセッションIDの固定化(攻撃)

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

セッションID: PHPSESSID=ABC に固定化

コンテキスト: GET http://example.jp/463/46-020.php?PHPSESSID=ABC 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/46/  
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: Mon, 24 Dec 2018 13:02:25 GMT  
Content-Type: text/html; charset=UTF-8  
Content-Length: 294  
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  
Vary: Accept-Encoding  
X-UA-Compatible: IE=edge

```
<head><title>個人情報の入力</title></head>
<body>
<form action="/46-021.php" method="POST"><input type="hidden" name="
PHPSESSID" value="ABC"/>
氏名:<input name="name" value=""><br>
メール:<input name="mail" value=""><br>
<input type="submit" value="確認">
</form>
</body>
</html>
```

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
7	18/12/24 22:02:25	GET	http://example.jp/463/46-020.php?PHPSESS...	200	OK	29 ms	294 bytes	Medium	Form, Hidden	
10	18/12/24 22:04:21	POST	http://example.jp/463/46-021.php	200	OK	25 ms	314 bytes	Medium	Form, Hidden	
11	18/12/24 22:05:09	POST	http://example.jp/463/46-022.php	200	OK	22 ms	149 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 463/46-021.php → レスポンス】ログイン前のセッションIDの固定化(攻撃)

The screenshot displays the OWASP ZAP interface with a request and response view. The request (ID 10) is a POST to http://example.jp/463/46-021.php with a session ID of ABC. The response (ID 11) is a 200 OK with HTML content containing a form with a hidden session ID field.

```
POST http://example.jp/463/46-021.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/463/46-020.php?PHPSESSID=ABC
Content-Type: application/x-www-form-urlencoded
Content-Length: 65
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp

PHPSESSID=ABC&name=%E9%AB%98%E6%A9%8B&mail=takahashi%40example.jp

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 24 Dec 2018 13:04:21 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 314
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
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<head><title>個人情報の確認</title></head>
<body>
<form action="/46-022.php" method="POST"><input type="hidden" name="
PHPSESSID" value="ABC" />
氏名:高橋<br>
メール:takahashi@example.jp<br>
<input type="submit" value="登録"><br>
<a href="/46-020.php?PHPSESSID=ABC">戻る</a>
</form>
</body>
</html>
```

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
7	18/12/24 22:02:25	GET	http://example.jp/463/46-020.php?PHPSESS...	200	OK	29 ms	294 bytes	Medium	Form, Hidden	
10	18/12/24 22:04:21	POST	http://example.jp/463/46-021.php	200	OK	25 ms	314 bytes	Medium	Form, Hidden	
11	18/12/24 22:05:09	POST	http://example.jp/463/46-022.php	200	OK	22 ms	149 bytes	Medium		

【ブラウザ→サーバ: リクエスト 463/46-022.php → レスポンス】ログイン前のセッションIDの固定化(攻撃)

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

```
POST http://example.jp/463/46-022.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/463/46-021.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 13
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp

PHPSESSID=ABC
```

デフォルトビュー

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 24 Dec 2018 13:05:09 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 149
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
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<head><title>個人情報の登録</title></head>
<body>
登録しました<br>
氏名:高橋<br>
メール:takahashi@example.jp<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
7	18/12/24 22:02:25	GET	http://example.jp/463/46-020.php?PHPSESS...	200	OK	29 ms	294 bytes	Medium		Form, Hidden
10	18/12/24 22:04:21	POST	http://example.jp/463/46-021.php	200	OK	25 ms	314 bytes	Medium		Form, Hidden
11	18/12/24 22:05:09	POST	http://example.jp/463/46-022.php	200	OK	22 ms	149 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】

個人情報を入力 × +

example.jp/463/46-020.php?PHPSESSID=ABC

氏名: 高橋  
メール: takahashi@example.jp

確認

個人情報を入力 × http://example.jp/463/46-020.php × +

view-source:http://example.jp/463/46-020.php?PHPSESSID=ABC

```
1 <head><title>個人情報の入力</title></head>
2 <body>
3 <form action="46-021.php" method="POST"><input type="hidden" name="PHPSESSID" value="ABC" />
4 氏名:<input name="name" value=""><br>
5 メール:<input name="mail" value=""><br>
6 <input type="submit" value="確認">
7 </form>
8 </body>
9 </html>
10
```

個人情報の確認 × +

example.jp/463/46-021.php

氏名: 高橋  
メール: takahashi@example.jp

登録  
戻る

個人情報の確認 × http://example.jp/463/46-021.php × +

view-source:http://example.jp/463/46-021.php

```
1 <head><title>個人情報の確認</title></head>
2 <body>
3 <form action="46-022.php" method="POST"><input type="hidden" name="PHPSESSID" value="ABC" />
4 氏名: 高橋<br>
5 メール: takahashi@example.jp<br>
6 <input type="submit" value="登録"><br>
7 <a href="46-020.php?PHPSESSID=ABC">戻る</a>
8 </form>
9 </body>
10 </html>
11
```

個人情報の登録 × +

example.jp/463/46-022.php

登録しました  
氏名: 高橋  
メール: takahashi@example.jp

個人情報の登録 × http://example.jp/463/46-022.php × +

view-source:http://example.jp/463/46-022.php

```
1 <head><title>個人情報の登録</title></head>
2 <body>
3 登録しました<br>
4 氏名: 高橋<br>
5 メール: takahashi@example.jp<br>
6 </body>
7 </html>
8
```

## 46-020:ログイン前のセッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)

### 【ブラウザ】

4.6 セッション管理の不備

- 46-001:RefererからのセッションID漏洩
- 46-010:セッションIDの固定化(正常系)
- セッションクッキーの削除 → 46-010:セッションIDの固定化(攻撃)
- 46-012:セッションIDの固定化(情報の盗み出し)
- 46-020:ログイン前のセッションIDの固定化(正常系)
- セッションクッキーの削除 → 46-020:ログイン前のセッションIDの固定化(攻撃)
- 46-020:ログイン前のセッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)**
- 46-010a:セッションIDの固定化対策版(正常系)
- セッションクッキーの削除 → 46-010a:セッションIDの固定化対策版(攻撃)
- 46-015:セッションIDの固定化トークンによる対策版
- セッションクッキーの削除
- クッキーの表示

[phpinfo\(RefererからのセッションID漏洩\)](#)  
[phpinfo\(セッションIDの固定化\)](#)  
[ホームに戻る](#)

```
1 <html>
2 <head><title>4.6 セッション管理の不備</title></head>
3 <body>
4 4.6 セッション管理の不備
5 <ol>
6 <li><a href="/462/46-001.php">46-001:RefererからのセッションID漏洩</a></li>
7 <li><a href="/463/46-010.php">46-010:セッションIDの固定化(正常系)</a></li>
8 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-199
9 23:59:59 GMT&quot;;"">セッションクッキーの削除</a> → <a href="/463/46-010a.php?PHPSESSID=ABC">46-010a:セッションIDの固定化対策版(攻撃)</a></li>
10 <li><a href="/463/46-012.php?PHPSESSID=ABC">46-012:セッションIDの固定化(情報の盗み出し)</a></li>
11 <li><a href="/463/46-020.php">46-020:ログイン前のセッションIDの固定化(正常系)</a></li>
12 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-199
13 23:59:59 GMT&quot;;"">セッションクッキーの削除</a> → <a href="/463/46-020.php?PHPSESSID=ABC">46-020:ログイン前のセッションIDの固定化(攻撃)</a></li>
14 <li><a href="/463/46-020.php?PHPSESSID=ABC">46-020:ログイン前のセッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)</a></li>
15 <li><a href="/463/46-010a.php">46-010a:セッションIDの固定化対策版(正常系)</a></li>
16 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-199
17 23:59:59 GMT&quot;;"">セッションクッキーの削除</a> → <a href="/463/46-010a.php?PHPSESSID=ABC">46-010a:セッションIDの固定化対策版(攻撃)</a></li>
18 <li><a href="/463/46-015.php">46-015:セッションIDの固定化トークンによる対策版</a></li>
19 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;"">セッションクッキーの削除</a></li>
20 <li><a href="javascript:document.cookie">クッキーの表示</a></li>
21 </ol>
22 <a href="/462/phpinfo.php">phpinfo(RefererからのセッションID漏洩)</a><br>
23 <a href="/463/phpinfo.php">phpinfo(セッションIDの固定化)</a><br>
24 <a href="/">ホームに戻る</a>
25 </body>
26 </html>
27
```

### 【サーバ: 463/46-020.php】

```
/var/www/html/463/46-020.php - wasbook@example.jp - エディタ - WinSCP
k?php
session_start();
$name = @$_SESSION['name'];
$mail = @$_SESSION['mail'];
?>
<head><title>個人情報の入力</title></head>
<body>
<form action="46-021.php" method="POST">
氏名:<input name="name" value="">?php
echo htmlspecialchars($name, ENT_COMPAT, 'UTF-8'); ?><br>
メール:<input name="mail" value="">?php
echo htmlspecialchars($mail, ENT_COMPAT, 'UTF-8'); ?><br>
<input type="submit" value="確認">
</form>
</body>
</html>
```

### 【サーバ: 463/46-021.php】

```
/var/www/html/463/46-021.php - wasbook@example.jp - エディタ - WinSCP
k?php
session_start();
$name = $_SESSION['name'] = filter_input(INPUT_POST, 'name');
$mail = $_SESSION['mail'] = filter_input(INPUT_POST, 'mail');
?>
<head><title>個人情報の確認</title></head>
<body>
<form action="46-022.php" method="POST">
氏名:<?php echo htmlspecialchars($name, ENT_COMPAT, 'UTF-8'); ?><br>
メール:<?php echo htmlspecialchars($mail, ENT_COMPAT, 'UTF-8'); ?><br>
<input type="submit" value="登録"><br>
<a href="46-020.php">戻る</a>
</form>
</body>
</html>
```

### 【サーバ: 463/46-022.php】

```
/var/www/html/463/46-022.php - wasbook@example.jp - エディタ - WinSCP
k?php
session_start();
$name = $_SESSION['name'];
$mail = $_SESSION['mail'];
?>
<head><title>個人情報の登録</title></head>
<body>
登録しました<br>
氏名:<?php echo htmlspecialchars($name, ENT_COMPAT, 'UTF-8'); ?><br>
メール:<?php echo htmlspecialchars($mail, ENT_COMPAT, 'UTF-8'); ?><br>
</body>
</html>
```

【ブラウザ→サーバ: リクエスト 463/46-020.php → レスポンス】ログイン前のセッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)

The screenshot shows the OWASP ZAP interface. The left pane shows the request details for a GET request to `http://example.jp/463/46-020.php?PHPSESSID=ABC`. The right pane shows the response, which is an HTML page with a form. The form contains a hidden input field for `PHPSESSID` with the value `ABC`, and other fields for name, email, and a submit button. The response status is `HTTP/1.1 200 OK`.

```
GET http://example.jp/463/46-020.php?PHPSESSID=ABC 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/46/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 24 Dec 2018 13:24:27 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 320
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
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<head><title>個人情報を入力</title></head>
<body>
<form action="/46-021.php" method="POST"><input type="hidden" name="
PHPSESSID" value="ABC" />
氏名:<input name="name" value="高橋"><br>
メール:<input name="mail" value="takahashi@example.jp"><br>
<input type="submit" value="確認">
</form>
</body>
</html>
```

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	18/12/24 22:24:27	GET	http://example.jp/463/46-020.php?PHPSESS...	200	OK	22 ms	320 bytes	Medium		Form, Hidden
16	18/12/24 22:29:55	POST	http://example.jp/463/46-021.php	200	OK	23 ms	314 bytes	Medium		Form, Hidden
17	18/12/24 22:33:59	POST	http://example.jp/463/46-022.php	200	OK	26 ms	149 bytes	Medium		

【ブラウザ→サーバ: リクエスト 463/46-021.php → レスポンス】ログイン前のセッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)

The screenshot shows the Burp Suite interface with the following details:

- Request (Left Panel):**

```
POST http://example.jp/463/46-021.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/463/46-020.php?PHPSESSID=ABC
Content-Type: application/x-www-form-urlencoded
Content-Length: 65
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp
```
- Response (Right Panel):**

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 24 Dec 2018 13:29:55 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 314
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
Vary: Accept-Encoding
X-UA-Compatible: IE=edge
```

The HTML body of the response is as follows:

```
<head><title>個人情報の確認</title></head>
<body>
<form action="/46-022.php" method="POST"><input type="hidden" name="
PHPSESSID" value="ABC" />
氏名:高橋<br>
メール:takahashi@example.jp<br>
<input type="submit" value="登録"><br>
<a href="/46-020.php?PHPSESSID=ABC">戻る</a>
</form>
</body>
</html>
```
- Request Log (Bottom Panel):**

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	18/12/24 22:24:27	GET	http://example.jp/463/46-020.php?PHPSESS...	200	OK	22 ms	320 bytes	Medium	Form, Hidden	
16	18/12/24 22:29:55	POST	http://example.jp/463/46-021.php	200	OK	23 ms	314 bytes	Medium	Form, Hidden	
17	18/12/24 22:33:59	POST	http://example.jp/463/46-022.php	200	OK	26 ms	149 bytes	Medium		

アラート: 0 1 2 0 現在のスキャン: 0 0 0 0 0 0



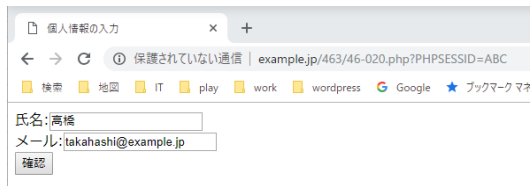
【ブラウザ→サーバ: リクエスト 463/46-022.php → レスポンス】ログイン前のセッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)

The screenshot displays the OWASP ZAP interface. The left pane shows the context tree with 'サイト' selected. The main pane is split into 'リクエスト' (Request) and 'レスポンス' (Response) views. The request is a POST to 'http://example.jp/463/46-022.php' with headers including 'User-Agent: Mozilla/5.0' and 'Host: example.jp'. The response is an HTTP 200 OK from 'nginx/1.10.3' with headers like 'Date: Mon, 24 Dec 2018 13:33:59 GMT' and 'Content-Type: text/html; charset=UTF-8'. The response body contains HTML for a login confirmation page: '<head><title>個人情報の登録</title></head><br>登録しました<br>氏名:高橋<br>メール:takahashi@example.jp<br>'. 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	18/12/24 22:24:27	GET	http://example.jp/463/46-020.php?PHPSESS...	200	OK	22 ms	320 bytes	Medium	Form, Hidden	
16	18/12/24 22:29:55	POST	http://example.jp/463/46-021.php	200	OK	23 ms	314 bytes	Medium	Form, Hidden	
17	18/12/24 22:33:59	POST	http://example.jp/463/46-022.php	200	OK	26 ms	149 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】



個人情報を入力

保護されていない通信 | example.jp/463/46-020.php?PHPSESSID=ABC

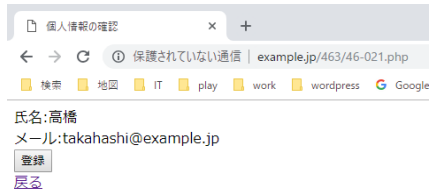
検索 地図 IT play work wordpress Google ブックマークマネージャ

氏名: 高橋

メール: takahashi@example.jp

確認

他の端末から攻撃者がPHPSESSID=ABCを確認するというストーリーで、ChromeからWebブラウズ



個人情報の確認

保護されていない通信 | example.jp/463/46-021.php

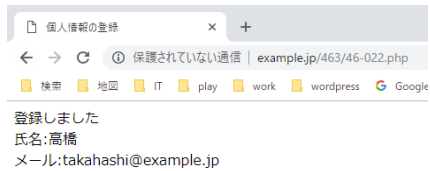
検索 地図 IT play work wordpress Google

氏名: 高橋

メール: takahashi@example.jp

登録

戻る



個人情報の登録

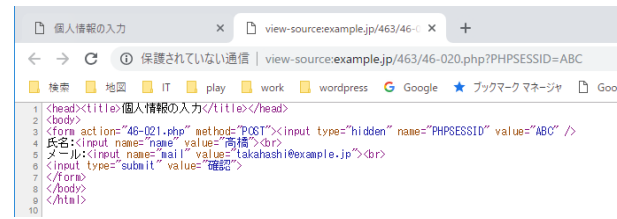
保護されていない通信 | example.jp/463/46-022.php

検索 地図 IT play work wordpress Google

登録しました

氏名: 高橋

メール: takahashi@example.jp



個人情報を入力

view-source:example.jp/463/46-020.php?PHPSESSID=ABC

```
1 <head><title>個人情報の入力</title></head>
2 <body>
3 <form action="46-021.php" method="POST"><input type="hidden" name="PHPSESSID" value="ABC" />
4 氏名:<input name="name" value="高橋"><br>
5 メール:<input name="mail" value="takahashi@example.jp"><br>
6 <input type="submit" value="確認">
7 </form>
8 </body>
9 </html>
10
```



個人情報の確認

http://example.jp/463/46-021.php

view-source:http://example.jp/463/46-021.php

```
1 <head><title>個人情報の確認</title></head>
2 <body>
3 <form action="46-022.php" method="POST"><input type="hidden" name="PHPSESSID" value="ABC" />
4 氏名: 高橋<br>
5 メール: takahashi@example.jp<br>
6 <input type="submit" value="登録"><br>
7 <a href="46-020.php?PHPSESSID=ABC">戻る</a>
8 </form>
9 </body>
10 </html>
11
```



個人情報の登録

http://example.jp/463/46-022.php

view-source:http://example.jp/463/46-022.php

```
1 <head><title>個人情報の登録</title></head>
2 <body>
3 登録しました<br>
4 氏名: 高橋<br>
5 メール: takahashi@example.jp<br>
6 </body>
7 </html>
8
```

## 46-010a:セッションIDの固定化対策版(正常系)

### 【ブラウザ】

4.6 セッション管理の不備

- 46-001:RefererからのセッションID漏洩
- 46-010:セッションIDの固定化(正常系)
- セッションクッキーの削除 → 46-010:セッションIDの固定化(攻撃)
- 46-012:セッションIDの固定化(情報の盗み出し)
- 46-020:ログイン前のセッションIDの固定化(正常系)
- セッションクッキーの削除 → 46-020:ログイン前のセッションIDの固定化(攻撃)
- 46-020:ログイン前のセッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)
- 46-010a:セッションIDの固定化対策版(正常系) ←
- セッションクッキーの削除 → 46-010a:セッションIDの固定化対策版(攻撃)
- 46-015:セッションIDの固定化トークンによる対策版
- セッションクッキーの削除
- クッキーの表示

[phpinfo\(RefererからのセッションID漏洩\)](#)  
[phpinfo\(セッションIDの固定化\)](#)  
[ホームに戻る](#)

```
1 <html>
2 <head><title>4.6 セッション管理の不備</title></head>
3 <body>
4 4.6 セッション管理の不備
5 <ol>
6 <li><a href="/462/46-001.php">46-001:RefererからのセッションID漏洩</a></li>
7 <li><a href="/463/46-010.php">46-010:セッションIDの固定化(正常系)</a></li>
8 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC&quot;;expires=Fri, 31-Dec-199
9 23:59:59 GMT&quot;;"">セッションクッキーの削除</a> → <a href="/463/46-010.php?PHPSESSID=ABC">46-010:セッションIDの固定化(攻撃)</a></li>
10 <li><a href="/463/46-012.php?PHPSESSID=ABC">46-012:セッションIDの固定化(情報の盗み出し)</a></li>
11 <li><a href="/463/46-020.php">46-020:ログイン前のセッションIDの固定化(正常系)</a></li>
12 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC&quot;;path=/;expires=Fri, 31-Dec-199
13 9 23:59:59 GMT&quot;;"">セッションクッキーの削除</a> → <a href="/463/46-020.php?PHPSESSID=ABC">46-020:ログイン前のセッションIDの固定化(攻撃)</a></li>
14 <li><a href="/463/46-020.php?PHPSESSID=ABC">46-020:ログイン前のセッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)</a></li>
15 <li><a href="/463/46-010a.php">46-010a:セッションIDの固定化対策版(正常系)</a></li>
16 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC&quot;;path=/;expires=Fri, 31-Dec-199
17 9 23:59:59 GMT&quot;;"">セッションクッキーの削除</a> → <a href="/463/46-010a.php?PHPSESSID=ABC">46-010a:セッションIDの固定化対策版(攻撃)</a></li>
18 <li><a href="/463/46-015.php">46-015:セッションIDの固定化トークンによる対策版</a></li>
19 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC&quot;;path=/;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;"">セッションクッキーの削除</a></li>
20 <li><a href="javascript:document.cookie">クッキーの表示</a></li>
21 </ol>
22 <a href="/462/phpinfo.php">phpinfo(RefererからのセッションID漏洩)</a><br>
23 <a href="/463/phpinfo.php">phpinfo(セッションIDの固定化)</a><br>
24 <a href="/">ホームに戻る</a>
25 </body>
26 </html>
27
```

### 【サーバ: 463/46-010a.php】

```
/var/www/html/463/46-010a.php - wasbook@example.jp - エディタ - WinSCP
k?php
session_start();
?>
<html>
<body>
<form action="/46-011a.php" method="POST">
ユーザーID:<input name="id" type="text"><br>
<input type="submit" value="ログイン">
</form>
</body>
</html>
```

### 【サーバ: 463/46-011a.php】

```
/var/www/html/463/46-011a.php - wasbook@example.jp - エディタ - WinSCP
k?php
session_start();
$id = filter_input(INPUT_POST, 'id'); // 必ずログインに成功する (仕様)
session_regenerate_id(true); // セッションIDの変更
$_SESSION['id'] = $id; // ユーザIDをセッションに保存
?>
<body>
<?php echo htmlspecialchars($id, ENT_COMPAT, 'UTF-8'); ?>さん、ログイン成功です<br>
<a href="/46-012.php">個人情報</a>
</body>
```

### 【サーバ: 463/46-012.php】

```
/var/www/html/463/46-012.php - wasbook@example.jp - エディタ - WinSCP
k?php
session_start();
?>
<html>
<body>
現在のユーザID:<?php echo htmlspecialchars($_SESSION['id'], ENT_COMPAT, 'UTF-8'); ?><br>
</body>
</html>
```

【ブラウザ→サーバ: リクエスト 463/46-010a.php → レスポンス】セッションIDの固定化対策版(正常系)

The screenshot displays the OWASP ZAP 2.7.0 interface. The top toolbar includes buttons for '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 window is split into two panes: 'コンテキスト' (Context) on the left and 'レスポンス' (Response) on the right. The 'コンテキスト' pane shows the request details for 'http://example.jp/463/46-010a.php'. The 'レスポンス' pane shows the response details, including headers and HTML body content. The response body contains a form with a hidden input for 'PHPSESSID' and a text input for 'ユーザID'. The status bar at the bottom shows 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	18/12/24 22:59:10	GET	http://example.jp/463/46-010a.php	200	OK	22 ms	244 bytes	Medium	Form, Hidden, ...	
22	18/12/24 23:04:39	POST	http://example.jp/463/46-011a.php	200	OK	27 ms	94 bytes	Medium	SetCookie	
23	18/12/24 23:06:01	GET	http://example.jp/463/46-012.php	200	OK	27 ms	59 bytes	Medium		

【ブラウザ→サーバ: リクエスト 463/46-011a.php → レスポンス】セッションIDの固定化対策版(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

```

POST http://example.jp/463/46-011a.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/463/46-010a.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 43
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=p6rmttuk372393ntq4p7tamt1
Upgrade-Insecure-Requests: 1
Host: example.jp

PHPSESSID=p6rmttuk372393ntq4p7tamt1&sid=uno
    
```

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 24 Dec 2018 14:04:40 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 94
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=8h20pr37ni3pmq32f2fnmlsvqt; path=/
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
unoさん、ログイン成功です<BR>
<a href="/46-012.php">個人情報</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	18/12/24 22:59:10	GET	http://example.jp/463/46-010a.php	200	OK	22 ms	244 bytes	Medium		Form, Hidden, ...
22	18/12/24 23:04:39	POST	http://example.jp/463/46-011a.php	200	OK	27 ms	94 bytes	Medium	SetCookie	
23	18/12/24 23:06:01	GET	http://example.jp/463/46-012.php	200	OK	27 ms	59 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 463/46-012.php → レスポンス】セッションIDの固定化対策版(正常系)

The screenshot shows the Burp Suite interface with the following details:

**Request (GET http://example.jp/463/46-012.php):**

```

HTTP/1.1
Host: example.jp
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/463/46-011a.php
Connection: keep-alive
DNT: 1
Cookie: PHPSESSID=8h20pr37nl3pmq32f2fm1svq4
Upgrade-Insecure-Requests: 1
  
```

**Response (HTTP/1.1 200 OK):**

```

Server: nginx/1.10.3
Date: Mon, 24 Dec 2018 14:06:01 GMT
Content-Type: text/html; charset=UTF-8
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
X-UA-Compatible: IE=edge
<html>
<body>
現在のユーザID:uno<BR>
</body>
</html>
  
```

**Request Log Table:**

ID	Request Date	Method	URL	Status Code	Status Code Description	Round Trip Time	Response Body Size	Output Alert	Note	Tag
19	18/12/24 22:59:10	GET	http://example.jp/463/46-010a.php	200	OK	22 ms	244 bytes	Medium	Form, Hidden, ...	
22	18/12/24 23:04:39	POST	http://example.jp/463/46-011a.php	200	OK	27 ms	94 bytes	Medium	SetCookie	
23	18/12/24 23:06:01	GET	http://example.jp/463/46-012.php	200	OK	27 ms	59 bytes	Medium		

## 【ブラウザ】

example.jp/463/46-010a.php × +

← → ↻ 🏠 example.jp/463/46-010a.php

ユーザID: uno

ログイン

example.jp/463/46-011a.php × +

← → ↻ 🏠 example.jp/463/46-011a.php

unoさん、ログイン成功です

[個人情報](#)

example.jp/463/46-012.php × +

← → ↻ 🏠 example.jp/463/46-012.php

現在のユーザID: uno

example.jp/463/46-010a.php × http://example.jp/463/46-010a.php × +

← → ↻ 🏠 view-source:http://example.jp/463/46-010a.php

```
1 <html>
2 <body>
3 <form action="/46-011a.php" method="POST"><input type="hidden" name="PHPSESSID" value="p6rmttk372393nt04p7tamt1" />
4 ユーザID:<input name="id" type="text"><br>
5 <input type="submit" value="ログイン">
6 </form>
7 </body>
8 </html>
9
```

example.jp/463/46-011a.php × http://example.jp/463/46-011a.php × +

← → ↻ 🏠 view-source:http://example.jp/463/46-011a.php

```
1 <body>
2 unoさん、 ログイン成功です<BR>
3 <a href="/46-012.php">個人情報</a>
4 </body>
5
```

example.jp/463/46-012.php × http://example.jp/463/46-012.php × +

← → ↻ 🏠 view-source:http://example.jp/463/46-012.php

```
1 <html>
2 <body>
3 現在のユーザID:uno<BR>
4 </body>
5 </html>
6
```

## セッションクッキーの削除 → 46-010a:セッションIDの固定化対策版(攻撃)

### 【ブラウザ】

4.6 セッション管理の不備

- 46-001:RefererからのセッションID漏洩
- 46-010:セッションIDの固定化(正常系)
- セッションクッキーの削除 → 46-010:セッションIDの固定化(攻撃)
- 46-012:セッションIDの固定化(情報の盗み出し)
- 46-020:ログイン前のセッションIDの固定化(正常系)
- セッションクッキーの削除 → 46-020:ログイン前のセッションIDの固定化(攻撃)
- 46-020:ログイン前のセッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)
- 46-010a:セッションIDの固定化対策版(正常系)
- セッションクッキーの削除 → 46-010a:セッションIDの固定化対策版(攻撃) ← ②
- 46-015:セッションIDの固定化トークンによる対策版
- セッションクッキーの削除
- クッキーの表示

phpinfo(RefererからのセッションID漏洩)  
phpinfo(セッションIDの固定化)  
ホームに戻る

名前	ドメイン	パス	有効期限	アクセス日時	値	Htt
PHPSessionID-example.jp...	example.jp	/	17:44:32...	esc17b0d90e6k...	false	

① アイテムを追加  
"PHPSessionID-example.jp..." を削除 ←  
"example.jp" のすべてのアイテムを削除  
すべてを削除  
すべてのセッション Cookie を削除

```
1 <html>
2 <head><title>4.6 セッション管理の不備</title></head>
3 <body>
4 4.6 セッション管理の不備
5 <ol>
6 <li><a href="/462/46-001.php">46-001:RefererからのセッションID漏洩</a></li>
7 <li><a href="/463/46-010.php">46-010:セッションIDの固定化(正常系)</a></li>
8 <li><a href="javascript:document.cookie=&quot;PHPSessionID=ABC&quot;;path=/;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;;">セッションクッキーの削除</a> → <a href="/463/46-010.php?PHPSessionID=ABC">46-010:セッションIDの固定化(攻撃)</a></li>
9 <li><a href="/463/46-012.php?PHPSessionID=ABC">46-012:セッションIDの固定化(情報の盗み出し)</a></li>
10 <li><a href="/463/46-020.php">46-020:ログイン前のセッションIDの固定化(正常系)</a></li>
11 <li><a href="javascript:document.cookie=&quot;PHPSessionID=ABC&quot;;path=/;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;;">セッションクッキーの削除</a> → <a href="/463/46-020.php?PHPSessionID=ABC">46-020:ログイン前のセッションIDの固定化(攻撃)</a></li>
12 <li><a href="/463/46-015.php">46-015:セッションIDの固定化トークンによる対策版</a></li>
13 <li><a href="javascript:document.cookie=&quot;PHPSessionID=ABC&quot;;path=/;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;;">セッションクッキーの削除</a> → <a href="/463/46-010a.php?PHPSessionID=ABC">46-010a:セッションIDの固定化対策版(攻撃)</a></li>
14 <li><a href="/463/46-015.php">46-015:セッションIDの固定化トークンによる対策版</a></li>
15 <li><a href="javascript:document.cookie=&quot;PHPSessionID=ABC&quot;;path=/;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;;">セッションクッキーの削除</a></li>
16 <li><a href="javascript:document.cookie=&quot;PHPSessionID=ABC&quot;;path=/;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;;">クッキーの表示</a></li>
17 </ol>
18 <li><a href="/462/phpinfo.php">phpinfo(RefererからのセッションID漏洩)</a><br>
19 <li><a href="/463/phpinfo.php">phpinfo(セッションIDの固定化)</a><br>
20 <li><a href="/">ホームに戻る</a>
21 </body>
22 </html>
```

### 【サーバ: 463/46-010a.php】

```
/var/www/html/463/46-010a.php - wasbook@example.jp - エディタ
k?php
    session_start();
    >>
<html>
<body>
<form action="/46-011a.php" method="POST">
  ユーザID:<input name="id" type="text"><br>
  <input type="submit" value="ログイン">
</form>
</body>
</html>
```

### 【サーバ: 463/46-011a.php】

```
/var/www/html/463/46-011a.php - wasbook@example.jp - エディタ - WinSCP
k?php
    session_start();
    $id = filter_input(INPUT_POST, 'id'); // 必ずログインに成功する (仕様)
    session_regenerate_id(true); // セッションIDの変更
    $_SESSION['id'] = $id; // ユーザIDをセッションに保存
    >>
<body>
<?php echo htmlspecialchars($id, ENT_COMPAT, 'UTF-8'); >>さん、ログイン成功です<br>
<a href="/46-012.php">個人情報</a>
</body>
```

### 【サーバ: 463/46-012.php】

```
/var/www/html/463/46-012.php - wasbook@example.jp - エディタ - WinSCP
k?php
    session_start();
    >>
<html>
<body>
現在のユーザID:<?php echo htmlspecialchars($_SESSION['id'], ENT_COMPAT, 'UTF-8'); >><br>
</body>
</html>
```



【ブラウザ→サーバ: リクエスト 463/46-010a.php → レスポンス】セッションクッキーの削除 → 46-010a:セッションIDの固定化対策版(攻撃)

The screenshot displays the OWASP ZAP 2.7.0 interface. The left pane shows the context tree with 'サイト' selected. The main area is split into 'リクエスト' (Request) and 'レスポンス' (Response) views.

**Request Details:**

```

GET http://example.jp/463/46-010a.php?PHPSESSID=ABC 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/46/
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: Mon, 24 Dec 2018 23:27:40 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 221
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
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<html>
<body>
<form action="/46-011a.php" method="POST"><input type="hidden" name="PHPSESSID" value="ABC"/>
ユーザID:<input name="id" type="text"><br>
<input type="submit" value="ログイン">
</form>
</body>
</html>
    
```

The response body shows a form with a hidden session ID parameter and a login button. A dashed box highlights the session ID value 'ABC' in the hidden input field.

**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
45	18/12/25 8:27:40	GET	http://example.jp/463/46-010a.php?PHPSES...	200	OK	27 ms	221 bytes	Medium	Form, Hidden	
48	18/12/25 8:28:53	POST	http://example.jp/463/46-011a.php	200	OK	25 ms	138 bytes	Medium	SetCookie	
49	18/12/25 8:29:54	GET	http://example.jp/463/46-012.php?PHPSESS...	200	OK	26 ms	66 bytes	Medium		

アラート: 0 2 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 463/46-011a.php → レスポンス】セッションクッキーの削除 → 46-010a:セッションIDの固定化対策版(攻撃)

The screenshot displays the Burp Suite interface with the following details:

- Request (Left Panel):**

```
POST http://example.jp/463/46-011a.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/463/46-010a.php?PHPSESSID=ABC
Content-Type: application/x-www-form-urlencoded
Content-Length: 27
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp
```

The request body contains: `PHPSESSID=ABC&id=DAVIDBOWIE`
- Response (Right Panel):**

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 24 Dec 2018 23:28:53 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 138
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=fc9bhb2j5bj4tjtbb4jocvj1; path=/
Vary: Accept-Encoding
X-UA-Compatible: IE=edge
```

The response body contains: `<body> DAVIDBOWIEさん、ログイン成功です<BR> <a href="/46-012.php?PHPSESSID=fc9bhb2j5bj4tjtbb4jocvj1">個人情報</a> </body>`
- History Table (Bottom):**

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
45	18/12/25 8:27:40	GET	http://example.jp/463/46-010a.php?PHPSES...	200	OK	27 ms	221 bytes	Medium	Form, Hidden	
48	18/12/25 8:28:53	POST	http://example.jp/463/46-011a.php	200	OK	25 ms	138 bytes	Medium	SetCookie	
49	18/12/25 8:29:54	GET	http://example.jp/463/46-012.php?PHPSESS...	200	OK	26 ms	66 bytes	Medium		

アラート: 0 2 3 0

【ブラウザ→サーバ: リクエスト 463/46-012.php → レスポンス】セッションクッキーの削除 → 46-010a:セッションIDの固定化対策版(攻撃)

The screenshot displays the OWASP ZAP 2.7.0 interface. The top toolbar includes buttons for '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 window 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 'リクエスト' pane shows a GET request to 'http://example.jp/463/46-012.php?PHPSESSID=fc90hb2j5b4jtbb4jocvj1'. The 'レスポンス' pane shows an HTTP/1.1 200 OK response with headers including 'Server: nginx/1.10.3', 'Date: Mon, 24 Dec 2018 23:29:54 GMT', and 'Content-Type: text/html; charset=UTF-8'. The response body contains HTML tags and the text '現在のユーザID: DAVIDBOWIE <BR>'. Below the main 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
45	18/12/25 8:27:40	GET	http://example.jp/463/46-010a.php?PHPSES...	200	OK	27 ms	221 bytes	Medium	Form, Hidden	
48	18/12/25 8:28:53	POST	http://example.jp/463/46-011a.php	200	OK	25 ms	138 bytes	Medium	SetCookie	
49	18/12/25 8:29:54	GET	http://example.jp/463/46-012.php?PHPSESS...	200	OK	26 ms	66 bytes	Medium		

アラート: 0 2 3 0 現在のスキャン: 0 0 0 0 0 0 0 0

## 【ブラウザ】

example.jp/463/46-010a.php?PHPSESSID=ABC

← → ↻ 🏠 example.jp/463/46-010a.php?PHPSESSID=ABC

ユーザーID: DAVIDBOWIE

ログイン

example.jp/463/46-011a.php

← → ↻ 🏠 example.jp/463/46-011a.php

DAVIDBOWIEさん、ログイン成功です

[個人情報](#)

example.jp/463/46-012.php?PHPSESSID=fc9bb2j5bj4tjtitbb4jocvj1

← → ↻ 🏠 example.jp/463/46-012.php?PHPSESSID=fc9bb2j5bj4tjtitbb4jocvj1

現在のユーザーID: DAVIDBOWIE

example.jp/463/46-010a.php?PHPSESSID=ABC

view-source:http://example.jp/463/46-010a.php?PHPSESSID=ABC

```
1 <html>
2 <body>
3 <form action="46-011a.php" method="POST"><input type="hidden" name="PHPSESSID" value="ABC" />
4 ユーザーID:<input name="id" type="text"><br>
5 <input type="submit" value="ログイン">
6 </form>
7 </body>
8 </html>
9
```

example.jp/463/46-011a.php

view-source:http://example.jp/463/46-011a.php

```
1 <body>
2 DAVIDBOWIEさん、ログイン成功です<br>
3 <a href="46-012.php?PHPSESSID=fc9bb2j5bj4tjtitbb4jocvj1">個人情報</a>
4 </body>
5
```

example.jp/463/46-012.php?PHPSESSID=fc9bb2j5bj4tjtitbb4jocvj1

view-source:http://example.jp/463/46-012.php?PHPSESSID=fc9bb2j5bj4tjtitbb4jocvj1

```
1 <html>
2 <body>
3 現在のユーザーID: DAVIDBOWIE<br>
4 </body>
5 </html>
6
```

## 46-015:セッションIDの固定化トークンによる対策版

### 【ブラウザ】

4.6 セッション管理の不備

- 46-001:RefererからのセッションID漏洩
- 46-010:セッションIDの固定化(正常系)
- セッションクッキーの削除 → 46-010:セッションIDの固定化(攻撃)
- 46-012:セッションIDの固定化(情報の盗み出し)
- 46-020:ログイン前のセッションIDの固定化(正常系)
- セッションクッキーの削除 → 46-020:ログイン前のセッションIDの固定化(攻撃)
- 46-020:ログイン前のセッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)
- 46-010a:セッションIDの固定化対策版(正常系)
- セッションクッキーの削除 → 46-010a:セッションIDの固定化対策版(攻撃)
- 46-015:セッションIDの固定化トークンによる対策版
- セッションクッキーの削除
- クッキーの表示

[phpinfo\(RefererからのセッションID漏洩\)](#)  
[phpinfo\(セッションIDの固定化\)](#)  
[ホームに戻る](#)

```
1 <html>
2 <head><title>4.6 セッション管理の不備</title></head>
3 <body>
4 4.6 セッション管理の不備
5 <ol>
6 <li><a href="/462/46-001.php">46-001:RefererからのセッションID漏洩</a></li>
7 <li><a href="/463/46-010.php">46-010:セッションIDの固定化(正常系)</a></li>
8 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-199
9 23:59:59 GMT&quot;;"">セッションクッキーの削除</a> → <a href="/463/46-010.php?PHPSESSID=ABC">46-010:セッションIDの固定化(攻撃)</a></li>
10 <li><a href="/463/46-012.php?PHPSESSID=ABC">46-012:セッションIDの固定化(情報の盗み出し)</a></li>
11 <li><a href="/463/46-020.php">46-020:ログイン前のセッションIDの固定化(正常系)</a></li>
12 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-199
13 23:59:59 GMT&quot;;"">セッションクッキーの削除</a> → <a href="/463/46-020.php?PHPSESSID=ABC">46-020:ログイン前のセッションIDの固定化(攻撃)</a></li>
14 <li><a href="/463/46-020.php?PHPSESSID=ABC">46-020:ログイン前のセッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)</a></li>
15 <li><a href="/463/46-010a.php">46-010a:セッションIDの固定化対策版(正常系)</a></li>
16 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-199
17 23:59:59 GMT&quot;;"">セッションクッキーの削除</a> → <a href="/463/46-010a.php?PHPSESSID=ABC">46-010a:セッションIDの固定化対策版(攻撃)</a></li>
18 <li><a href="/463/46-015.php">46-015:セッションIDの固定化トークンによる対策版</a></li>
19 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;"">セッションクッキーの削除</a></li>
20 <li><a href="javascript:document.cookie">クッキーの表示</a></li>
21 </ol>
22 <a href="/462/phpinfo.php">phpinfo(RefererからのセッションID漏洩)</a><br>
23 <a href="/463/phpinfo.php">phpinfo(セッションIDの固定化)</a><br>
24 <a href="/">ホームに戻る</a>
25 </body>
26 </html>
27
```

### 【サーバ: 462/46-015.php】

```
k?php
// /dev/urandomによる疑似乱数生成器
function getToken() {
    // /dev/urandomから24バイト読み込み
    $s = file_get_contents('/dev/urandom', false, NULL, 0, 24);
    return base64_encode($s); // base64エンコードして返す
}

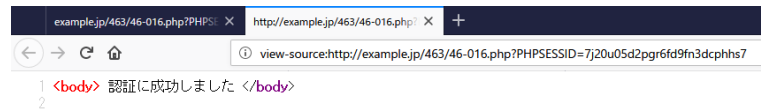
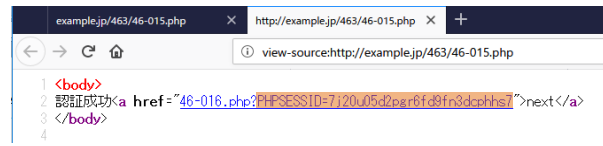
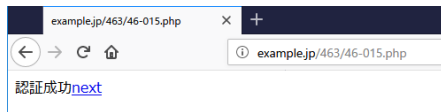
// ここまでで認証成功
session_start();
$token = getToken(); // トークンの生成
// トークンとcookieとセッションに保存
setcookie('token', $token, 0, '/'); // トークンcookie
$_SESSION['token'] = $token;
?>
<body>
認証成功<a href="/46-016.php">next</a>
</body>
```

### 【サーバ: 462/46-016.php】

```
k?php
session_start();
// ユーザIDの確認
$token = $_COOKIE['token'];
if (! $token || $token != $_SESSION['token']) {
    die('認証エラー');
}
?>
<body> 認証に成功しました </body>
```



## 【ブラウザ】



# セッションクッキーの削除

## 【ブラウザ】

4.6 セッション管理の不備

- 1. 46-001:RefererからのセッションID漏洩
- 2. 46-010:セッションIDの固定化(正常系)
- 3. **セッションクッキーの削除** → 46-010:セッションIDの固定化(攻撃) ← ①
- 4. 46-012:セッションIDの固定化(情報の盗み出し)
- 5. 46-020:ログイン前のセッションIDの固定化(正常系)
- 6. セッションクッキーの削除 → 46-020:ログイン前のセッションIDの固定化(攻撃)
- 7. 46-020:ログイン前のセッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)
- 8. 46-010a:セッションIDの固定化対策版(正常系)
- 9. セッションクッキーの削除 → 46-010a:セッションIDの固定化対策版(攻撃)
- 10. 46-015:セッションIDの固定化トークンによる対策版
- 11. **セッションクッキーの削除** ← ②
- 12. クッキーの表示

phpinfo(RefererからのセッションID漏洩)  
phpinfo(セッションIDの固定化)  
ホームに戻る

PHPSESSID=ABCを割り当てておきます

「SHIFT」+「CTRL」+「I」

名前	ドメイン	パス	有効期限	アクセス日時	値	HttpOnly	同一サイト
token	example.jp	/	セッション	Tue, 25 Dec 2018 00:29:30 GMT	n5omb9DqZf3HecC9vDk%2BREB...	false	Unset

```
4.6 セッション管理の不備 x http://192.168.56.101/46/ x +
view-source:http://192.168.56.101/46/
1 <html>
2 <head><title>4.6 セッション管理の不備</title></head>
3 <body>
4 4.6 セッション管理の不備
5 <ol>
6 <li><a href="/462/46-001.php">46-001:RefererからのセッションID漏洩</a></li>
7 <li><a href="/463/46-010.php">46-010:セッションIDの固定化(正常系)</a></li>
8 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;"">セッションクッキーの削除</a> → <a href="/463/46-010a.php?PHPSESSID=ABC">46-010a:セッションIDの固定化対策版(攻撃)</a></li>
9 23:59:59 GMT&quot;;"">セッションクッキーの削除</a> → <a href="/463/46-012.php?PHPSESSID=ABC">46-012:セッションIDの固定化(情報の盗み出し)</a></li>
10 <li><a href="/463/46-020.php">46-020:ログイン前のセッションIDの固定化(正常系)</a></li>
11 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;"">セッションクッキーの削除</a> → <a href="/463/46-020.php?PHPSESSID=ABC">46-020:ログイン前のセッションIDの固定化(攻撃)</a></li>
12 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;"">セッションクッキーの削除</a> → <a href="/463/46-020a.php?PHPSESSID=ABC">46-020a:ログイン前のセッションIDの固定化対策版(攻撃)</a></li>
13 <li><a href="/463/46-020.php?PHPSESSID=ABC">46-020:ログイン前のセッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)</a></li>
14 <li><a href="/463/46-010a.php">46-010a:セッションIDの固定化対策版(正常系)</a></li>
15 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;"">セッションクッキーの削除</a> → <a href="/463/46-010a.php?PHPSESSID=ABC">46-010a:セッションIDの固定化対策版(攻撃)</a></li>
16 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;"">セッションクッキーの削除</a> → <a href="/463/46-015.php">46-015:セッションIDの固定化トークンによる対策版</a></li>
17 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;"">セッションクッキーの削除</a></li>
18 <li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;"">セッションクッキーの表示</a></li>
19 </ol>
20 <a href="/462/phpinfo.php">phpinfo(RefererからのセッションID漏洩)</a><br>
21 <a href="/463/phpinfo.php">phpinfo(セッションIDの固定化)</a><br>
22 <a href="/">ホームに戻る</a>
23 </body>
24 </html>
25
26
27
```

javascriptdocument.cookie="PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-1999 23:59:59 GMT;"

クッキーに過去期限が設定されたので、削除された

名前	ドメイン	パス	有効期限	アクセス日時	値	HttpOnly	同一サイト
GMT;";							

選択されたホストには表示できるデータがありません



## クッキーの表示

### 【ブラウザ】

4.6 セッション管理の不備

- 46-001:RefererからのセッションID漏洩
- 46-010:セッションIDの固定化(正常系)
- セッションクッキーの削除 → 46-010:セッションIDの固定化(攻撃)
- 46-012:セッションIDの固定化(情報の盗み出し)
- 46-020:ログイン前のセッションIDの固定化(正常系)
- セッションクッキーの削除 → 46-020:ログイン前のセッションIDの固定化(攻撃)
- 46-020:ログイン前のセッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)
- 46-010a:セッションIDの固定化対策版(正常系)
- セッションクッキーの削除 → 46-010a:セッションIDの固定化対策版(攻撃)
- 46-015:セッションIDの固定化トークンによる対策版
- セッションクッキーの削除
- クッキーの表示

phpinfo(RefererからのセッションID漏洩)  
phpinfo(セッションIDの固定化)  
ホームに戻る

名前	ドメイン	パス	有効期限	アクセス日時	値	HttpOnly	同サイト
token	example.jp	/	セッション	Tue, 25 Dec 2018 00:29:30 GMT	nSqm9DqZjF3kle6C9vuDk%2BREBQXDRBg	false	Unset

```
<html>
<head><title>4.6 セッション管理の不備</title></head>
<body>
4.6 セッション管理の不備
<ol>
<li><a href="/462/46-001.php">46-001:RefererからのセッションID漏洩</a></li>
<li><a href="/463/46-010.php">46-010:セッションIDの固定化(正常系)</a></li>
<li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;"">セッションクッキーの削除</a> → <a href="/463/46-010a.php?PHPSESSID=ABC">46-010a:セッションIDの固定化対策版(攻撃)</a></li>
<li><a href="/463/46-012.php?PHPSESSID=ABC">46-012:セッションIDの固定化(情報の盗み出し)</a></li>
<li><a href="/463/46-020.php">46-020:ログイン前のセッションIDの固定化(正常系)</a></li>
<li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;"">セッションクッキーの削除</a> → <a href="/463/46-020.php?PHPSESSID=ABC">46-020:ログイン前のセッションIDの固定化(攻撃)</a></li>
<li><a href="/463/46-020.php?PHPSESSID=ABC">46-020:ログイン前のセッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)</a></li>
<li><a href="/463/46-010a.php">46-010a:セッションIDの固定化対策版(正常系)</a></li>
<li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;"">セッションクッキーの削除</a> → <a href="/463/46-010a.php?PHPSESSID=ABC">46-010a:セッションIDの固定化対策版(攻撃)</a></li>
<li><a href="/463/46-015.php">46-015:セッションIDの固定化トークンによる対策版</a></li>
<li><a href="javascript:document.cookie=&quot;PHPSESSID=ABC;path=/;expires=Fri, 31-Dec-1999 23:59:59 GMT&quot;;"">セッションクッキーの削除</a></li>
<li><a href="javascript:document.cookie">クッキーの表示</a></li>
</ol>
<li><a href="/462/phpinfo.php">phpinfo(RefererからのセッションID漏洩)</a><br>
<a href="/463/phpinfo.php">phpinfo(セッションIDの固定化)</a><br>
<a href="/">ホームに戻る</a>
</body>
</html>
```

javascript:document.cookie

名前	ドメイン	パス	有効期限	アクセス日時	値	HttpOnly	同サイト
----	------	----	------	--------	---	----------	------

選択されたホストには表示できるデータがありません

4.6 セッション管理の不備

- 1. [46-001:RefererからのセッションID漏洩](#)
- 2. [46-010:セッションIDの固定化\(正常系\)](#)
- 3. [セッションクッキーの削除](#) → [46-010:セッションIDの固定化\(攻撃\)](#)
- 4. [46-012:セッションIDの固定化\(情報の盗み出し\)](#)
- 5. [46-020:ログイン前のセッションIDの固定化\(正常系\)](#)
- 6. [セッションクッキーの削除](#) → [46-020:ログイン前のセッションIDの固定化\(攻撃\)](#)
- 7. [46-020:ログイン前のセッションIDの固定化\(情報の盗み出し。別ブラウザで確認すると分かりやすい\)](#)
- 8. [46-010a:セッションIDの固定化対策版\(正常系\)](#)
- 9. [セッションクッキーの削除](#) → [46-010a:セッションIDの固定化対策版\(攻撃\)](#)
- 10. [46-015:セッションIDの固定化トークンによる対策版](#)
- 11. [セッションクッキーの削除](#)
- 12. [クッキーの表示](#)

[phpinfo\(RefererからのセッションID漏洩\)](#)      

[phpinfo\(セッションIDの固定化\)](#)

[ホームに戻る](#)

phpinfo()

example.jp/462/phpinfo

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' '--enable-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)
PHP API	20090626
PHP Extension	20090626
Zend Extension	220090626
Zend Extension Build	API220090626,NTS
PHP Extension Build	API20090626,NTS
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled

manager	
Zend Multibyte Support	disabled
IPv6 Support	enabled
Registered PHP Streams	https, ftps, php, file, glob, data, http, ftp
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls
Registered Stream Filters	string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk

This program makes use of the Zend Scripting Language Engine:  
 Zend Engine v2.3.0, Copyright (c) 1998-2010 Zend Technologies



## PHP Credits

### Configuration

#### cgi-fcgi

Directive	Local Value	Master Value
cgi.check_shebang_line	1	1
cgi.discard_path	0	0
cgi.fix_pathinfo	1	1
cgi.force_redirect	1	1
cgi.nph	0	0
cgi.redirect_status_env	no value	no value
cgi.rfc2616_headers	0	0
fastcgi.logging	1	1

#### Core

PHP Version	5.3.3
-------------	-------

Directive	Local Value	Master Value
allow_call_time_pass_reference	Off	Off
allow_url_fopen	On	On
allow_url_include	On	On
always_populate_raw_post_data	Off	Off
arg_separator.input	&	&
arg_separator.output	&	&
asp_tags	Off	Off
auto_append_file	no value	no value
auto_globals_jit	On	On
auto_prepend_file	no value	no value
browscap	no value	no value
default_charset	no value	no value
default_mimetype	text/html	text/html
define_syslog_variables	Off	Off
disable_classes	no value	no value
disable_functions	no value	no value
display_errors	On	On
display_startup_errors	Off	Off
doc_root	no value	no value
docref_ext	no value	no value
docref_root	no value	no value

enable_dl	Off	Off
error_append_string	no value	no value
error_log	no value	no value
error_prepend_string	no value	no value
error_reporting	22527	22527
exit_on_timeout	Off	Off
expose_php	On	On
extension_dir	/usr/local/lib/php/extensions /no-debug-non-zts-20090626	/usr/local/lib/php/extensions /no-debug-non-zts-20090626
file_uploads	On	On
highlight.bg	#FFFFFF	#FFFFFF
highlight.comment	#FF8000	#FF8000
highlight.default	#0000BB	#0000BB
highlight.html	#000000	#000000
highlight.keyword	#007700	#007700
highlight.string	#DD0000	#DD0000
html_errors	Off	Off
ignore_repeated_errors	Off	Off
ignore_repeated_source	Off	Off
ignore_user_abort	Off	Off
implicit_flush	Off	Off
include_path	::	::
log_errors	On	On
log_errors_max_len	1024	1024
magic_quotes_gpc	Off	Off
magic_quotes_runtime	Off	Off
magic_quotes_sybase	Off	Off
mail_add_x_header	On	On
mail.force_extra_parameters	no value	no value
mail.log	no value	no value
max_execution_time	30	30
max_file_uploads	20	20
max_input_nesting_level	64	64
max_input_time	60	60
memory_limit	128M	128M
open_basedir	no value	no value
output_buffering	4096	4096
output_handler	no value	no value
post_max_size	8M	8M
precision	14	14
realpath_cache_size	16K	16K
realpath_cache_ttl	120	120
register_argc_argv	Off	Off
register_globals	Off	Off
register_long_arrays	Off	Off
report_memleaks	On	On
report_zend_debug	On	On
request_order	GP	GP
safe_mode	Off	Off
safe_mode_exec_dir	no value	no value
safe_mode_gid	Off	Off
safe_mode_include_dir	no value	no value
sendmail_from	no value	no value
sendmail_path	/usr/sbin/sendmail -t -i	/usr/sbin/sendmail -t -i
serialize_precision	100	100
short_open_tag	Off	Off
SMTP	localhost	localhost
smtp_port	25	25
sql.safe_mode	Off	Off
track_errors	Off	Off

unserialize_callback_func	no value	no value
upload_max_filesize	2M	2M
upload_tmp_dir	no value	no value
user_dir	no value	no value
user_ini.cache_ttl	300	300
user_ini.filename	.user.ini	.user.ini
variables_order	GPCS	GPCS
xmlrpc_error_number	0	0
xmlrpc_errors	Off	Off
y2k_compliance	On	On
zend.enable_gc	On	On

### date

date/time support	enabled
"Olson" Timezone Database Version	2010.9
Timezone Database	internal
Default timezone	Asia/Tokyo

Directive	Local Value	Master Value
date.default_latitude	31.7667	31.7667
date.default_longitude	35.2333	35.2333
date.sunrise_zenith	90.583333	90.583333
date.sunset_zenith	90.583333	90.583333
date.timezone	Asia/Tokyo	Asia/Tokyo

### dom

DOM/XML	enabled
DOM/XML API Version	20031129
libxml Version	2.7.8
HTML Support	enabled
XPath Support	enabled
XPointer Support	enabled
Schema Support	enabled
RelaxNG Support	enabled

### ereg

Regex Library	Bundled library enabled
---------------	-------------------------

### filter

Input Validation and Filtering	enabled
Revision	\$Revision: 298196 \$

Directive	Local Value	Master Value
filter.default	unsafe_raw	unsafe_raw
filter.default_flags	no value	no value

### json

json support	enabled
json version	1.2.1

### libxml

## libXML

libXML support	active
libXML Compiled Version	2.7.8
libXML Loaded Version	20708
libXML streams	enabled

## mbstring

Multibyte Support	enabled
Multibyte string engine	libmbfl
HTTP input encoding translation	disabled

mbstring extension makes use of "streamable kanji code filter and converter", which is distributed under the GNU Lesser General Public License version 2.1.

Multibyte (japanese) regex support	enabled
Multibyte regex (oniguruma) backtrack check	On
Multibyte regex (oniguruma) version	4.7.1

Directive	Local Value	Master Value
mbstring.detect_order	<i>no value</i>	<i>no value</i>
mbstring.encoding_translation	Off	Off
mbstring.func_overload	0	0
mbstring.http_input	pass	pass
mbstring.http_output	pass	pass
mbstring.http_output_conv_mimetypes	^(text/application/xhtml +xml)	^(text/application/xhtml +xml)
mbstring.internal_encoding	UTF-8	UTF-8
mbstring.language	Japanese	Japanese
mbstring.strict_detection	Off	Off
mbstring.substitute_character	<i>no value</i>	<i>no value</i>

## mysql

MySQL Support	enabled
Active Persistent Links	0
Active Links	0
Client API version	5.0.15
MYSQL_MODULE_TYPE	external
MYSQL_SOCKET	/var/run/mysqld/mysqld.sock
MYSQL_INCLUDE	-I/usr/local/mysql-5.0.15/include/mysql
MYSQL_LIBS	-L/usr/local/mysql-5.0.15/lib/mysql -mysqlclient

Directive	Local Value	Master Value
mysql.allow_local_infile	On	On
mysql.allow_persistent	On	On
mysql.connect_timeout	60	60
mysql.default_host	<i>no value</i>	<i>no value</i>
mysql.default_password	<i>no value</i>	<i>no value</i>
mysql.default_port	<i>no value</i>	<i>no value</i>
mysql.default_socket	/var/run/mysqld/mysqld.sock	/var/run/mysqld/mysqld.sock
mysql.default_user	<i>no value</i>	<i>no value</i>
mysql.max_links	Unlimited	Unlimited
mysql.max_persistent	Unlimited	Unlimited
mysql.trace_mode	Off	Off

## openssl

OpenSSL support	enabled
OpenSSL Library Version	OpenSSL 1.0.1t 3 May 2016
OpenSSL Header Version	OpenSSL 1.0.1t 3 May 2016

### pcre

PCRE (Perl Compatible Regular Expressions) Support	enabled
PCRE Library Version	8.0.2 2010-03-19

Directive	Local Value	Master Value
pcre.backtrack_limit	100000	100000
pcre.recursion_limit	100000	100000

### PDO

PDO support	enabled
PDO drivers	mysql

### pdo\_mysql

PDO Driver for MySQL	enabled
Client API version	5.0.15

### Reflection

Reflection	enabled
Version	\$Revision: 300393 \$

### session

Session Support	enabled
Registered save handlers	files user
Registered serializer handlers	php php_binary

Directive	Local Value	Master Value
session.auto_start	Off	Off
session.bug_compat_42	Off	Off
session.bug_compat_warn	Off	Off
session.cache_expire	180	180
session.cache_limiter	nocache	nocache
session.cookie_domain	no value	no value
session.cookie_httponly	Off	Off
session.cookie_lifetime	0	0
session.cookie_path	/	/
session.cookie_secure	Off	Off
session.entropy_file	no value	no value
session.entropy_length	0	0
session.gc_divisor	1000	1000
session.gc_maxlifetime	1440	1440
session.gc_probability	1	1
session.hash_bits_per_character	5	5
session.hash_function	0	0
session.name	PHPSESSID	PHPSESSID
session.referer_check	no value	no value
session.save_handler	files	files
session.save_path	/var/lib/php/sessions	/var/lib/php/sessions

session.serialize_handler	php	php
session.use_cookies	Off	On
session.use_only_cookies	Off	On
session.use_trans_sid	1	0

## SPL

<b>SPL support</b>	<b>enabled</b>
<b>Interfaces</b>	Countable, OuterIterator, RecursiveIterator, SeekableIterator, SplObserver, SplSubject
<b>Classes</b>	AppendIterator, ArrayIterator, ArrayObject, BadFunctionCallException, BadMethodCallException, CachingIterator, DirectoryIterator, DomainException, EmptyIterator, FilesystemIterator, FilterIterator, GlobIterator, InfiniteIterator, InvalidArgumentException, IteratorIterator, LengthException, LimitIterator, LogicException, MultipleIterator, NoRewindIterator, OutOfBoundsException, OutOfRangeException, OverflowException, ParentIterator, RangeException, RecursiveArrayIterator, RecursiveCachingIterator, RecursiveDirectoryIterator, RecursiveFilterIterator, RecursiveIteratorIterator, RecursiveRegexIterator, RecursiveTreeIterator, RegexIterator, RuntimeException, SplDoublyLinkedList, SplFileInfo, SplFileObject, SplFixedArray, SplHeap, SplMinHeap, SplMaxHeap, SplObjectStorage, SplPriorityQueue, SplQueue, SplStack, SplTempFileObject, UnderflowException, UnexpectedValueException

## standard

<b>Dynamic Library Support</b>	enabled
<b>Path to sendmail</b>	/usr/sbin/sendmail -t -i

Directive	Local Value	
assert.active	1	1
assert.bail	0	0
assert.callback	<i>no value</i>	<i>no value</i>
assert.quiet_eval	0	0
assert.warning	1	1
auto_detect_line_endings	0	0
default_socket_timeout	60	60
safe_mode_allowed_env_vars	PHP_	PHP_
safe_mode_protected_env_vars	LD_LIBRARY_PATH	LD_LIBRARY_PATH
url_rewriter.tags	a=href,area=href,frame=src,input=src,form=fakeentry	a=href,area=href,frame=src,input=src,form=fakeentry
user_agent	<i>no value</i>	<i>no value</i>

## Additional Modules

Module Name
-------------

## Environment

Variable	Value
GATEWAY_INTERFACE	CGI/1.1
HTTP_DNT	1
REMOTE_ADDR	127.0.0.1
QUERY_STRING	<i>no value</i>
HTTP_USER_AGENT	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
DOCUMENT_ROOT	/var/www/html
REMOTE_PORT	46796
HTTP_UPGRADE_INSECURE_REQUESTS	1
HTTP_ACCEPT	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
SERVER_SIGNATURE	<address>Apache/2.4.25 (Debian) Server at example.jp Port 88</address>



CONTEXT_DOCUMENT_ROOT	/usr/lib/cgi-bin/
SCRIPT_FILENAME	/var/www/html/462/phpinfo.php
HTTP_HOST	example.jp
HTTP_X_REMOTE_ADDR	192.168.56.1
REDIRECT_HANDLER	application/x-httpd-php-5.3.3
HTTP_X_FORWARDED_FOR	192.168.56.1
REQUEST_URI	/462/phpinfo.php
SERVER_SOFTWARE	Apache/2.4.25 (Debian)
HTTP_CONNECTION	close
REQUEST_SCHEME	http
PATH	/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
REDIRECT_URL	/462/phpinfo.php
HTTP_ACCEPT_LANGUAGE	ja,en-US;q=0.7,en;q=0.3
HTTP_REFERER	http://example.jp/46/
SERVER_PROTOCOL	HTTP/1.0
HTTP_ACCEPT_ENCODING	gzip, deflate
REDIRECT_STATUS	200
HTTP_X_REAL_IP	192.168.56.1
REQUEST_METHOD	GET
SERVER_ADDR	127.0.0.1
SERVER_ADMIN	webmaster@localhost
CONTEXT_PREFIX	/cgi-bin/
PWD	/usr/lib/cgi-bin
SERVER_PORT	88
SCRIPT_NAME	/462/phpinfo.php
SERVER_NAME	example.jp
ORIG_SCRIPT_FILENAME	/usr/lib/cgi-bin/php-5.3.3
ORIG_PATH_INFO	/462/phpinfo.php
ORIG_PATH_TRANSLATED	/var/www/html/462/phpinfo.php
ORIG_SCRIPT_NAME	/cgi-bin/php-5.3.3

### PHP Variables

Variable	Value
\$_SERVER["GATEWAY_INTERFACE"]	CGI/1.1
\$_SERVER["HTTP_DNT"]	1
\$_SERVER["REMOTE_ADDR"]	127.0.0.1
\$_SERVER["QUERY_STRING"]	<i>no value</i>
\$_SERVER["HTTP_USER_AGENT"]	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
\$_SERVER["DOCUMENT_ROOT"]	/var/www/html
\$_SERVER["REMOTE_PORT"]	46796
\$_SERVER["HTTP_UPGRADE_INSECURE_REQUESTS"]	1
\$_SERVER["HTTP_ACCEPT"]	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
\$_SERVER["SERVER_SIGNATURE"]	<address>Apache/2.4.25 (Debian) Server at example.jp Port 88</address>
\$_SERVER["CONTEXT_DOCUMENT_ROOT"]	/usr/lib/cgi-bin/
\$_SERVER["SCRIPT_FILENAME"]	/var/www/html/462/phpinfo.php
\$_SERVER["HTTP_HOST"]	example.jp
\$_SERVER["HTTP_X_REMOTE_ADDR"]	192.168.56.1
\$_SERVER["REDIRECT_HANDLER"]	application/x-httpd-php-5.3.3
\$_SERVER["HTTP_X_FORWARDED_FOR"]	192.168.56.1
\$_SERVER["REQUEST_URI"]	/462/phpinfo.php
\$_SERVER["SERVER_SOFTWARE"]	Apache/2.4.25 (Debian)
\$_SERVER["HTTP_CONNECTION"]	close
\$_SERVER["REQUEST_SCHEME"]	http

\$_SERVER["PATH"]	/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
\$_SERVER["REDIRECT_URL"]	/462/phpinfo.php
\$_SERVER["HTTP_ACCEPT_LANGUAGE"]	ja,en-US;q=0.7,en;q=0.3
\$_SERVER["HTTP_REFERER"]	http://example.jp/46/
\$_SERVER["SERVER_PROTOCOL"]	HTTP/1.0
\$_SERVER["HTTP_ACCEPT_ENCODING"]	gzip, deflate
\$_SERVER["REDIRECT_STATUS"]	200
\$_SERVER["HTTP_X_REAL_IP"]	192.168.56.1
\$_SERVER["REQUEST_METHOD"]	GET
\$_SERVER["SERVER_ADDR"]	127.0.0.1
\$_SERVER["SERVER_ADMIN"]	webmaster@localhost
\$_SERVER["CONTEXT_PREFIX"]	/cgi-bin/
\$_SERVER["PWD"]	/usr/lib/cgi-bin
\$_SERVER["SERVER_PORT"]	88
\$_SERVER["SCRIPT_NAME"]	/462/phpinfo.php
\$_SERVER["SERVER_NAME"]	example.jp
\$_SERVER["ORIG_SCRIPT_FILENAME"]	/usr/lib/cgi-bin/php-5.3.3
\$_SERVER["ORIG_PATH_INFO"]	/462/phpinfo.php
\$_SERVER["ORIG_PATH_TRANSLATED"]	/var/www/html/462/phpinfo.php
\$_SERVER["ORIG_SCRIPT_NAME"]	/cgi-bin/php-5.3.3
\$_SERVER["PHP_SELF"]	/462/phpinfo.php
\$_SERVER["REQUEST_TIME"]	1545701030

## PHP License

This program is free software; you can redistribute it and/or modify it under the terms of the PHP License as published by the PHP Group and included in the distribution in the file: LICENSE

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

If you did not receive a copy of the PHP license, or have any questions about PHP licensing, please contact [license@php.net](mailto:license@php.net).