

## 4.7 クッキー出力にまつわる脆弱性

セッション変数は外部から変更できないのに対して、クッキー値はアプリ利用者によって、書き換えができます

	クッキー	セッション変数
使いやすさ	APIにより設定、取得	変数とほぼ同じように使える
配列やオブジェクトの格納	アプリ側で文字列に変換する必要あり	通常の変数と同様に使える場合が多い
サイズの制限	厳しい制限あり	実用上は無制限
利用者による格納情報の直接参照	容易	不可能
クッキー脆弱時の情報漏洩しやすさ	クッキー漏洩すればデータも漏洩	漏洩のしにくさを制御可能
利用者によるデータ改変	容易	不可能
第三者によるデータ改変	XSSやHTTPヘッダインジェクションなどの脆弱性があれば可能	不可能
情報の寿命の制限	容易	セッションの寿命
異なるサーバとの情報共有	ドメインが同じであれば可能	基本的に不可能

### クッキーのセキュア属性の不備

HTTPとHTTPSが混在するサイトで、セッションIDを保持するクッキーにセキュア属性をつけると、HTTPページでセッション管理機能が使えなくなるので、アプリが動かなくなります。

### クッキーのセキュア属性不備に対する対策

- ①サイト全体を常時TLSにして、クッキーに secure属性をつける

PHPの場合には、php.ini に以下を設定する

```
session.cookie_secure = On
```

Apache Tomcat の場合は、HTTPS接続された状況でリクエストされる際には、セッションIDのクッキーに対しては自動的にセッション属性をつけることができます

ASP.NETの場合には、web.configファイルに以下を設定します

```
<configuration>
  <system.web>
    <httpcookies requireSSL="true" />
  </system.web>
</configuration>
```

- ②セッションIDとは別にセキュア属性付きのクッキーとして、トークンを発行し、ページごとにトークンを確認する

48-001:トークン生成(TLS)

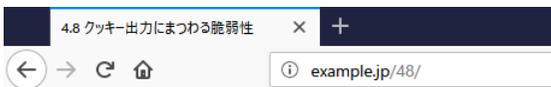
## 4.8.2 クッキーのセキュア属性不備

HTTPSにてクッキーをセット(セキュア属性なし)

HTTPにてクッキーを表示

48-900:罠サイトを閲覧

【ブラウザ】



4.8 クッキー出力にまつわる脆弱性  
4.8.2 クッキーのセキュア属性不備

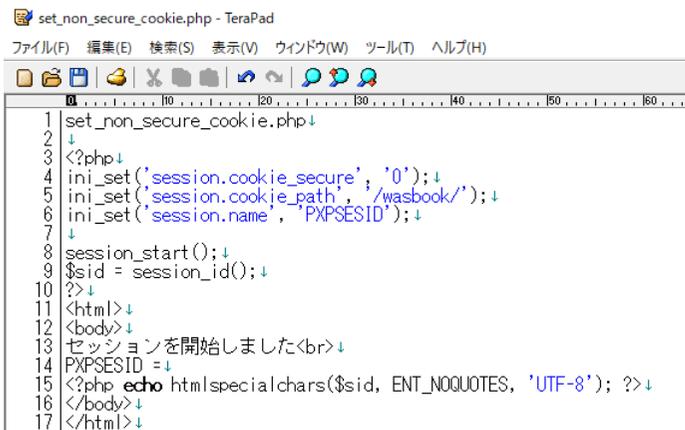
1. [HTTPSにてクッキーをセット \(セキュア属性なし\)](#)
2. [HTTPにてクッキーを表示](#)
3. [48-900:罠サイトを閲覧](#)
4. [48-001:トークン生成\(TLS\)](#)
5. [48-001:トークン生成\(非TLS\)](#)

[phpinfo](#)

[ホームに戻る](#)



【httpsサーバ: wasbook.org/set\_non\_secure\_cookie.php】



## 【ブラウザ】

wasbook.org/set\_non\_secure\_cookie X +

← → ↻ 🏠 [https://wasbook.org/set\\_non\\_secure\\_cookie.php](https://wasbook.org/set_non_secure_cookie.php)

セッションを開始しました  
PXPSESID = 2bvq0j0uq05hb89o7udgpgm6nk

wasbook.org/set\_non\_secure\_cookie X [https://wasbook.org/set\\_non\\_secure\\_cookie.php](https://wasbook.org/set_non_secure_cookie.php) X +

← → ↻ 🏠 [view-source:https://wasbook.org/set\\_non\\_secure\\_cookie.php](view-source:https://wasbook.org/set_non_secure_cookie.php)

```
1 <html>
2 <body>
3 セッションを開始しました<br>
4 PXPSESID =
5 2bvq0j0uq05hb89o7udgpgm6nk</body>
6 </html>
7
```

4.8 クッキー出力にまつわる脆弱性 X +

← → ↻ 🏠 [example.jp/48/](http://example.jp/48/)

4.8 クッキー出力にまつわる脆弱性  
4.8.2 クッキーのセキュア属性不備

1. [HTTPSにてクッキーをセット \(セキュア属性なし\)](#)
2. [HTTPにてクッキーを表示](#)
3. [48-900:罠サイトを閲覧](#)
4. [48-001:トークン生成\(TLS\)](#)
5. [48-001:トークン生成\(非TLS\)](#)

[phpinfo](#)  
[ホームに戻る](#)

4.8 クッキー出力にまつわる脆弱性 X <http://example.jp/48/> X +

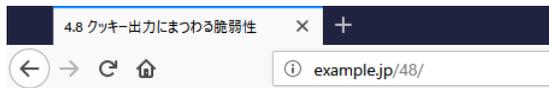
← → ↻ 🏠 <view-source:http://example.jp/48/> ... 📄 ☆ 🖨

```
1 <html>
2 <head><title>4.8 クッキー出力にまつわる脆弱性</title></head>
3 <body>
4 4.8 クッキー出力にまつわる脆弱性<br>
5 4.8.2 クッキーのセキュア属性不備
6 <ol>
7 <li><a href="https://wasbook.org/set_non_secure_cookie.php">HTTPSにてクッキーをセット (セキュア属性なし) </a></li>
8 <li><a href="http://wasbook.org/display_cookie.php">HTTPにてクッキーを表示</a></li>
9 <li><a href="http://trap.example.com/48/48-900.html">48-900:罠サイトを閲覧</a></li>
10 <li><a href="https://example.jp/48/48-001.php">48-001:トークン生成(TLS)</a></li>
11 <li><a href="48-001.php">48-001:トークン生成(非TLS)</a></li>
12 </ol>
13 <a href="phpinfo.php">phpinfo</a><br>
14 <a href="/">ホームに戻る</a>
15 </body>
16 </html>
17
```

wasbook.org/display\_cookie.php X +

← → ↻ 🏠 [wasbook.org/display\\_cookie.php](wasbook.org/display_cookie.php)

```
Array
(
    [PXPSESID] => 2bvq0j0uq05hb89o7udgpgm6nk
)
```



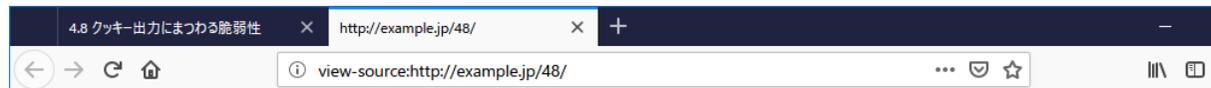
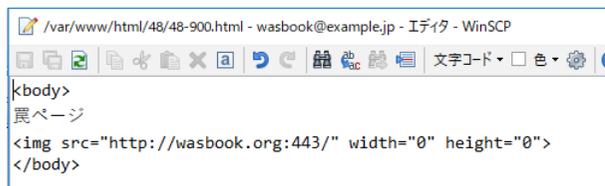
#### 4.8 クッキー出力にまつわる脆弱性 4.8.2 クッキーのセキュア属性不備

1. [HTTPSにてクッキーをセット \(セキュア属性なし\)](#)
2. [HTTPにてクッキーを表示](#)
3. [48-900:罠サイトを閲覧](#) 
4. [48-001:トークン生成\(TLS\)](#)
5. [48-001:トークン生成\(非TLS\)](#)

[phpinfo](#)

[ホームに戻る](#)

#### 【サーバ: 48/48-900.html】



```
1 <html>
2 <head><title>4.8 クッキー出力にまつわる脆弱性</title></head>
3 <body>
4 4.8 クッキー出力にまつわる脆弱性<br>
5 4.8.2 クッキーのセキュア属性不備
6 <ol>
7 <li><a href="https://wasbook.org/set_non_secure_cookie.php">HTTPSにてクッキーをセット (セキュア属性なし) </a></li>
8 <li><a href="http://wasbook.org/display_cookie.php">HTTPにてクッキーを表示</a></li>
9 <li><a href="http://trap.example.com/48/48-900.html">48-900:罠サイトを閲覧</a></li>
10 <li><a href="https://example.jp/48/48-001.php">48-001:トークン生成(TLS)</a></li>
11 <li><a href="48-001.php">48-001:トークン生成(非TLS)</a></li>
12 </ol>
13 <a href="phpinfo.php">phpinfo</a><br>
14 <a href="/">ホームに戻る</a>
15 </body>
16 </html>
17
```

【ブラウザ→偽サーバ : リクエスト trap.example.com/48/48-900.html → レスポンス】

The screenshot displays the OWASP ZAP 2.7.0 interface. The top menu bar includes 'ファイル', '編集', '表示', 'ポリシー', 'レポート', 'ツール', 'オンライン', and 'ヘルプ'. The main workspace is divided into three panes: 'コンテキスト' (Contexts) on the left, 'リクエスト' (Request) in the center, and 'レスポンス' (Response) on the right. The 'リクエスト' pane shows a GET request to 'http://trap.example.com/48/48-900.html' with various headers including User-Agent, Accept, Accept-Language, Accept-Encoding, Referer, DNT, Connection, Upgrade-Insecure-Requests, and Host. The 'レスポンス' pane shows an HTTP/1.1 200 OK response with headers for Server, Date, Content-Type, Content-Length, Connection, Last-Modified, ETag, Accept-Ranges, Vary, and X-UA-Compatible. The body contains HTML code: '<body>罾ページ<br></body>'. Below the workspace is a toolbar with '履歴', '検索', 'アラート', and 'アウトプット'. At the bottom, a table lists the request details, and a status bar shows '現在のスキャン' with various icons and counts.

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
12	18/12/29 12:31:22	GET	http://trap.example.com/48/48-900.html	200	OK	4 ms	85 bytes	Medium		

現在のスキャン: 0 0 0 0 0 0 0 0 0 0

## 【ブラウザ】

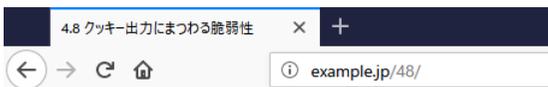
「CTRL」+「SHIFT」+「E」 → 「ネットワーク」 → 「wasbook.org:443」を選択して、クッキーPXPSESIDを確認する



「wasbook.org:443」はHTTPS通信を待ち受けているので、HTTPリクエストに対して、エラー400になっているが、HTTPリクエスト自体は平文で流れ、ネットワーク上で漏洩する危険性があることがわかる

## 48-001:トークン生成(TLS)

### 【ブラウザ】

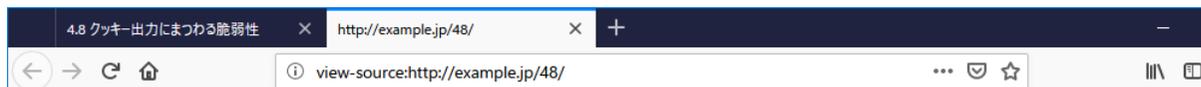


4.8 クッキー出力にまつわる脆弱性  
4.8.2 クッキーのセキュア属性不備

1. [HTTPSにてクッキーをセット \(セキュア属性なし\)](#)
2. [HTTPにてクッキーを表示](#)
3. [48-900:罠サイトを閲覧](#)
4. [48-001:トークン生成\(TLS\)](#)
5. [48-001:トークン生成\(非TLS\)](#)

[phpinfo](#)

[ホームに戻る](#)



```
1 <html>
2 <head><title>4.8 クッキー出力にまつわる脆弱性</title></head>
3 <body>
4 4.8 クッキー出力にまつわる脆弱性<br>
5 4.8.2 クッキーのセキュア属性不備
6 <ol>
7 <li><a href="https://wasbook.org/set_non_secure_cookie.php">HTTPSにてクッキーをセット (セキュア属性なし) </a></li>
8 <li><a href="http://wasbook.org/display_cookie.php">HTTPにてクッキーを表示</a></li>
9 <li><a href="http://trap.example.com/48/48-900.html">48-900:罠サイトを閲覧</a></li>
10 <li><a href="https://example.jp/48/48-001.php">48-001:トークン生成(TLS)</a></li>
11 <li><a href="48-001.php">48-001:トークン生成(非TLS)</a></li>
12 </ol>
13 <a href="phpinfo.php">phpinfo</a><br>
14 <a href="/">ホームに戻る</a>
15 </body>
16 </html>
17
```

### 【サーバ: 48/48-001.php】

```
/var/www/html/48/48-001.php - wasbook@example.jp - エディタ - WinSCP
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();
session_regenerate_id(true); // セッションIDの再生成
$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, '', '', true, true);
$_SESSION['token'] = $token;
?>
<body>
認証成功<a href="48-002.php">next</a>
</body>
```

### 【サーバ: 48/48-002.php】

```
/var/www/html/48/48-002.php - wasbook@example.jp - エディタ - WinSCP
k?php
session_start();
// ユーザIDの確認
$token = filter_input(INPUT_COOKIE, 'token');
if (empty($token) || $token !== $_SESSION['token']) {
    die('認証エラー。トークンが不正です。');
}
?>
<body> トークンをチェックし、認証状態を確認しました </body>
```

## 【ブラウザ】

安全ではない接続

https://example.jp/48/48-001.php

### 安全な接続ではありません

example.jp の所有者によるウェブサイトの設定が不適切です。あなたの情報が盗まれることを防ぐため、このウェブサイトへの接続は確立されません。

[詳細...](#)

エラーを報告すると、悪意のあるサイトの特定とブロックに役立ちます

[戻る](#) [エラー内容](#)

example.jp は不正なセキュリティ証明書を使用しています。

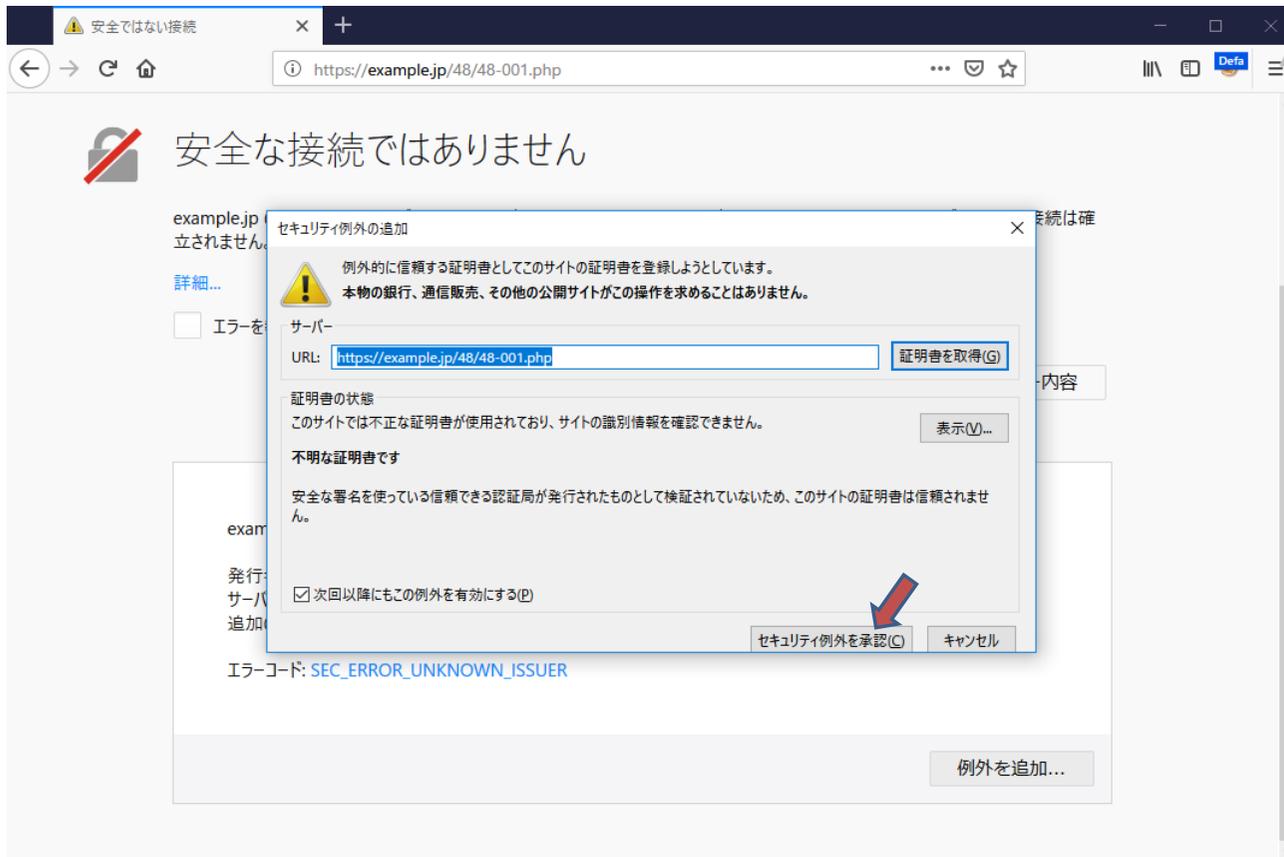
発行者の証明書が不明であるためこの証明書は信頼されません。  
サーバーが適正な中間証明書を送信しない可能性があります。  
追加のルート証明書をインポートする必要があるでしょう。

エラーコード: [SEC\\_ERROR\\_UNKNOWN\\_ISSUER](#)

[例外を追加...](#)

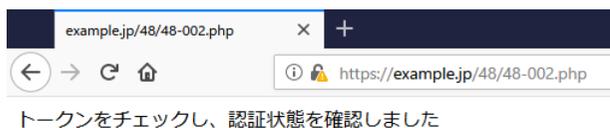
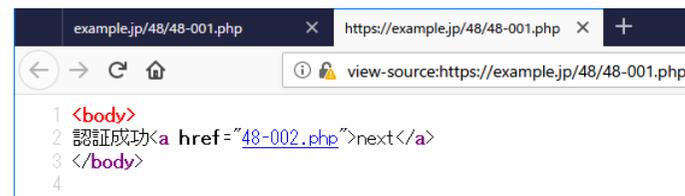
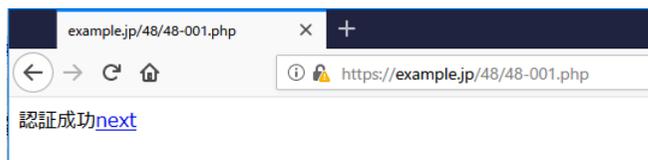
「エラー内容」をクリックすると、画面下部に証明書が信頼できない旨、表示される

「例外を追加」をクリック



テスト環境として、自己署名証明書が設定されているので、テストとして許容することにする。

「セキュリティ例外を承認」をクリック



【ブラウザ→サーバ : リクエスト 48/48-001.php → レスポンス】

無題セッション - 20181229-114638 - 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  
https://example.jp  
http://trap.examp

GET https://example.jp/48/48-001.php HTTP/1.1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Language: ja,en-US;q=0.7,en;q=0.3  
Accept-Encoding: gzip, deflate, br  
Referer: http://example.jp/48/  
DNT: 1  
Connection: keep-alive  
Upgrade-Insecure-Requests: 1  
Host: example.jp

HTTP/1.1 200 OK  
Server: nginx/1.10.3  
Date: Sat, 29 Dec 2018 05:22:21 GMT  
Content-Type: text/html; charset=UTF-8  
Connection: keep-alive  
Set-Cookie: PHPSESSID=fqe22dcksfodcljsmej758f7h6; path=/  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Cache-Control: no-store, no-cache, must-revalidate  
Pragma: no-cache  
Set-Cookie: PHPSESSID=lbdhg3748h7lsoa8mhjc85juq4; path=/  
Set-Cookie: token=1jMirVWRXktfkZ%2FCSV0oKc%2FxiGXVNGKX; secure; HttpOnly  
X-UA-Compatible: IE=edge

<body>  
認証成功<a href="48-002.php">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
14	18/12/29 14:22:21	GET	https://example.jp/48/48-001.php	200	OK	84 ms	58 bytes	Medium		SetCookie

アラート 0 0 0 4 0 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 48/48-002.php → レスポンス】

無題セッション - 20181229-114638 - 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  
https://example.jp  
http://trap.examp

デフォルトビュー

```
GET https://example.jp/48/48-002.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate, br
Referer: https://example.jp/48/48-001.php
DNT: 1
Connection: keep-alive
Cookie: token=1jMirVVRXktfkZ%2FCSV0oKC%2FxiGXVNGKX; PHPSESSID=ibddg3748h7soa8mhjc85juq4
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: Sat, 29 Dec 2018 05:29:09 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 82
Connection: keep-alive
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body> トークンをチェックし、認証状態を確認しました </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

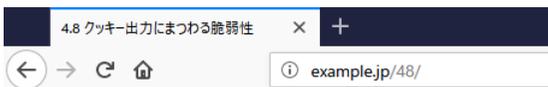
Id	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
17	18/12/29 14:29:09	GET	https://example.jp/48/48-002.php	200	OK	70 ms	82 bytes	Medium		

アラート 0 1 4 0

現在のスキャン 0 0 0 0 0 0 0 0

## 48-001:トークン生成(非TLS)

### 【ブラウザ】

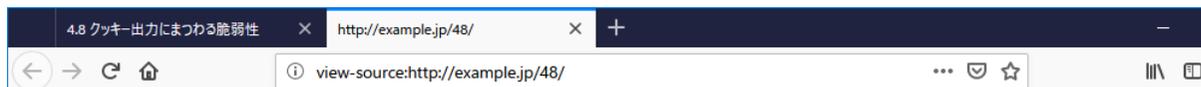


4.8 クッキー出力にまつわる脆弱性  
4.8.2 クッキーのセキュア属性不備

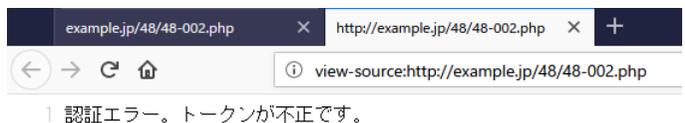
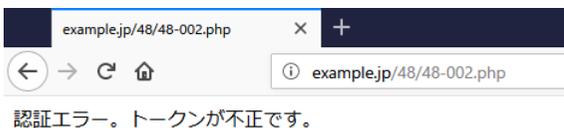
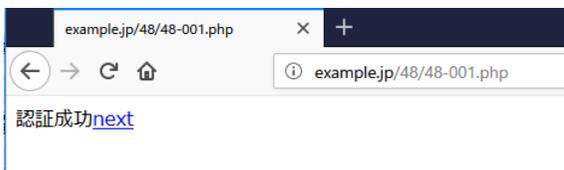
1. [HTTPSにてクッキーをセット \(セキュア属性なし\)](#)
2. [HTTPにてクッキーを表示](#)
3. [48-900:罠サイトを閲覧](#)
4. [48-001:トークン生成\(TLS\)](#)
5. [48-001:トークン生成\(非TLS\)](#) 

[phpinfo](#)

[ホームに戻る](#)



```
1 <html>
2 <head><title>4.8 クッキー出力にまつわる脆弱性</title></head>
3 <body>
4 4.8 クッキー出力にまつわる脆弱性<br>
5 4.8.2 クッキーのセキュア属性不備
6 <ol>
7 <li><a href="https://wasbook.org/set_non_secure_cookie.php">HTTPSにてクッキーをセット (セキュア属性なし) </a></li>
8 <li><a href="http://wasbook.org/display_cookie.php">HTTPにてクッキーを表示</a></li>
9 <li><a href="http://trap.example.com/48/48-900.html">48-900:罠サイトを閲覧</a></li>
10 <li><a href="https://example.jp/48/48-001.php">48-001:トークン生成(TLS)</a></li>
11 <li><a href="48-001.php">48-001:トークン生成(非TLS)</a></li>
12 </ol>
13 <a href="phpinfo.php">phpinfo</a><br>
14 <a href="/">ホームに戻る</a>
15 </body>
16 </html>
17
```



【ブラウザ→サーバ : リクエスト 48/48-001.php → レスポンス】

The screenshot displays the OWASP ZAP 2.7.0 interface. The top menu bar includes 'ファイル', '編集', '表示', 'ポリシー', 'レポート', 'ツール', 'オンライン', and 'ヘルプ'. The main workspace is divided into three panes: 'コンテキスト' (Contexts), 'リクエスト' (Request), and 'レスポンス' (Response). The 'リクエスト' pane shows a GET request to 'http://example.jp/48/48-001.php' with headers such as 'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0', 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8', 'Accept-Language: ja,en-US;q=0.7,en;q=0.3', 'Accept-Encoding: gzip, deflate', 'Referer: http://example.jp/48/', 'DNT: 1', 'Connection: keep-alive', 'Cookie: PHPSESSID=7hpgcr3toq60toqplqsgu0qu0', 'Upgrade-Insecure-Requests: 1', and 'Host: example.jp'. The 'レスポンス' pane shows an 'HTTP/1.1 200 OK' response with headers including 'Server: nginx/1.10.3', 'Date: Sat, 29 Dec 2018 05:33:52 GMT', 'Content-Type: text/html; charset=UTF-8', 'Connection: keep-alive', 'Expires: Thu, 19 Nov 1981 08:52:00 GMT', 'Cache-Control: no-store, no-cache, must-revalidate', 'Pragma: no-cache', 'Set-Cookie: PHPSESSID=lkffeknjmu7gjvh2c02pfph7l2; path=/' and 'Set-Cookie: token=FEwZbMwwEyqOjHW6%2BbQ3Egin5RChSjcR; secure; HttpOnly'. The response body contains the HTML snippet: '<body>認証成功<a href="48-002.php">next</a></body>'. At the bottom, a table lists the request details:

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
22	18/12/29 14:33:52	GET	http://example.jp/48/48-001.php	200	OK	5 ms	58 bytes	Medium		SetCookie

## 【ブラウザ→サーバ : リクエスト 48/48-002.php → レスポンス】

48-001.php で発行したトークンがセキュア属性付きクッキーだったので、HTTPS ではない 48-002.php でトークンが受け取れなかった。

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

- Request:** GET http://example.jp/48/48-002.php HTTP/1.1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Language: ja,en-US;q=0.7,en;q=0.3  
Accept-Encoding: gzip, deflate  
Referer: http://example.jp/48/48-001.php  
DNT: 1  
Connection: keep-alive  
Cookie: PHPSESSID=|kffeknjmu7gjh2c02pfp712  
Upgrade-Insecure-Requests: 1  
Host: example.jp
- Response:** HTTP/1.1 200 OK  
Server: nginx/1.10.3  
Date: Sat, 29 Dec 2018 05:33:53 GMT  
Content-Type: text/html; charset=UTF-8  
Connection: keep-alive  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Cache-Control: no-store, no-cache, must-revalidate  
Pragma: no-cache  
X-UA-Compatible: IE=edge
- Message:** 認証エラー。トークンが不正です。

Id	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
23	18/12/29 14:33:53	GET	http://example.jp/48/48-002.php	200	OK	5 ms	48 bytes	Medium		

現在のスキャン: 0 0 0 0 0 0 0 0