

メッセージダイジェストによるパスワード保護のために必要なハッシュ関数の要件

- | | | |
|------------|-------|---|
| ・現像計算困難性 | 一方向性 | ※ GPUを使った総当たり攻撃の結果、
8桁で英数字・数字・記号を使った総当たり攻撃は、MD5で約14分、SHA-1で約39分で完了する |
| ・第2現像計算困難性 | 弱衝突耐性 | |
| ・衝突困難性 | 強衝突耐性 | |

パスワードのメッセージダイジェストに対する攻撃

- オフラインブルートフォース攻撃 GPUを使った総当たり攻撃の結果、8桁で英数字・数字・記号を使った総当たり攻撃は、MD5で約14分、SHA-1で約39分で完了する。
- レインボーテーブル RainbowCrack ProjectのWebサイトには、8文字までのUS-ASCII文字全部に対応したMD5用テーブルや10文字までの英小文字と数字に対応したSHA-1用テーブルが売られています。単純なハッシュ関数による保存パスワードは市販レインボーテーブルで解読されます。
- ユーザDB内にパスワード辞書を作られる Webアプリに多数のユーザ、パスワードを登録し、同じハッシュ値を持つデータから元パスワードを突き止める。

パスワードのメッセージダイジェスト攻撃に対する対策

- ・ ソルト
- ・ ストレッチング
- ・ 処理速度の遅いハッシュ関数を使用する

自動ログインの安全な実装

- ・ セッションの寿命を延ばす
- ・ トークンを利用する(セッション寿命を延ばせない場合)
- ・ 認証チケットを利用する(Kerberos認証、ASP.NETのフォーム認証、複数サーバまたがった認証の場合には、SSO製品、OpenID Connectなどのオープンな認証基盤の利用)

ログアウト機能の要件

- ・ ログアウト処理は副作用があるので、POSTメソッドでリクエストする
- ・ ログアウト処理ではセッションを破棄する
- ・ 必要な場合、CSRF対策を実施する

5.2 アカウント管理

認証

メールアカウントの受信確認(実際にメールを送信して確認)

- ① メールにトークンつきURLを添付して、そのURLから処理を継続する
 - ② メールアドレスを入力後、トークン(確認番号)入力画面に遷移する
(トークンは指定したメールアドレスにメール送信する)
- メール送信→メールのURLをクリック→URLのページから登録を再開 (利用者にメールURLを閲覧させるのは好ましくない習慣)
メールアドレス入力→トークン番号入力→その他の登録内容入力 (推奨)
(トークン番号・メール送信)

ユーザIDの重複

- ・ パスワードが違えば同じIDで登録できるサイト
- ・ ユーザIDに一意制約をつけられないサイト

ユーザIDの自動登録への対処

- ・ CAPTCHA reCAPTCHA

パスワード変更

- パスワード変更時に、現在のパスワードを入力し確認する
 - パスワード変更時にはメールで通知する
 - パスワード変更機能に生じやすい脆弱性
- ①セッションハイジャック対策 ②CSRF脆弱性対策
①SQLインジェクション脆弱性 ②CSRF脆弱性

メールアドレス変更

- メールアドレス変更時には、新旧両方のメールアドレスに通知します。
- ・ 旧アドレスに送るのは、不正変更では正規ユーザのアドレスは元アドレスになるから
 - ・ 旧アドレスは既に受信できない場合があるので、受信確認までは行わない

パスワードリセット

パスワードリマインダー←現在のパスワードを教える パスワードリセット←リセットしたものを教えるか、パスワード変更を利用者にさせる

- 管理者向けパスワードリセット機能
 - 利用者向けパスワードリセット機能
- ①問合せを受け、利用者の本人確認を行う ②パスワード変更だけができる仮パスワードをメールで発行
- ①現在のパスワードをメールで通知 盗聴リスク
- ②パスワード変更画面のURLをメールで通知 フィッシング被害に会いやすい習慣
- ③ メールアドレス入力→スマホアプリ数値の2段階認証→登録メールアドレスに仮パスワードを送信
パスワード変更通知で不正利用された場合にも気が付く。
スマホアプリ数値の2段階認証によって、不正にパスワード無効されることを防ぐ。
仮パスワードと本番パスワードは別管理で、仮パスワード発行後も元パスワードでログインできるようにすべき。
- ④ メールアドレス入力→トークン確認番号を登録メールアドレスに送信→トークン確認番号を画面から入力→スマホアプリ数値の2段階認証→新しいパスワードを画面から入力
トークンのブルートフォース攻撃のために、回数制限を設け、アカウントロックするか、パスワードリセット機能を一定期間ロックする旨、メール通知します

53 認可

認可

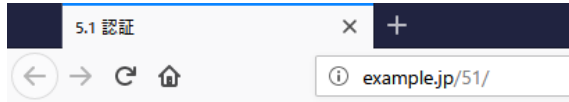
認可不備

情報リソースのURLを知っていると認証なしで情報を閲覧できる。
情報リソースのIDを変更すると権限外の情報が参照できる。
メニューの表示・非表示だけで制御している。
hiddenパラメータ、クッキーに権限情報を保持している。
⇒ URLやhiddenパラメータ、クッキーを書き換えると権限を不正利用できてしまう。

認可不備の対策

権限情報をセッション変数に保持することで、書き換えできないようにし、処理や表示の直前に権限の確認を行う。

51-001:パスワードのメッセージダイジェスト

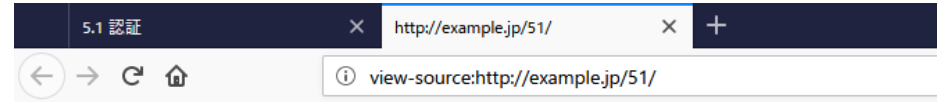


5.1 認証

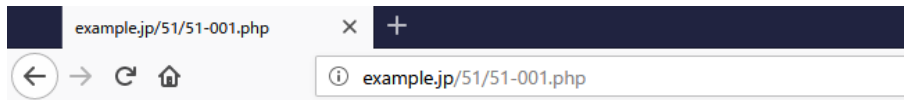
1. [51-001:パスワードのメッセージダイジェスト](#)
2. [51-002:自動ログイン](#)
3. [51-010:ログアウト確認のためのログイン画面](#)

[phpinfo](#)

[ホームに戻る](#)



```
1 <html>
2 <head><title>5.1 認証</title></head>
3 <body>
4 5.1 認証
5 <ol>
6 <li><a href="51-001.php">51-001:パスワードのメッセージダイジェスト</a></li>
7 <li><a href="51-002.php?autologin=on">51-002:自動ログイン</a></li>
8 <li><a href="51-010.php">51-010:ログアウト確認のためのログイン画面</a></li>
9 </ol>
10 <a href="phpinfo.php">phpinfo</a><br>
11 <a href="/">ホームに戻る</a>
12 </body>
13 </html>
..
```



```
string(64) "a44812a099b40ee49ffe2bd6c5de7403a1854e009ba9e2b417b9770d4ffac54b"
string(64) "cc2c26c9a22d7318f48ed99e8915c6861559ade98e4df3dab64e51c7ea476389"
string(64) "3fca4aab6f7bf9ed2ac855dbc0e22c148e7e23a137c49777e1e9269902571c8"
```

【サーバ: 51/51-001.php 】

```
/var/www/html/51/51-001.php - wasbook@example.jp - エディタ - WinSCP
kpre>
<?php
// FIXEDSALTはサイト毎に変更してください
define('FIXEDSALT', 'bc578d1503b4602a590d8f8ce4a8e634a55bec0d');
define('STRETCHCOUNT', 1000);

// ソルトを生成する
function get_salt($id) {
    return $id . pack('H*', FIXEDSALT); // ユーザIDと固定文字列を連結
}

function get_password_hash($id, $pwd) {
    $salt = get_salt($id);
    $hash = ''; // ハッシュの初期値
    for ($i = 0; $i < STRETCHCOUNT; $i++) {
        $hash = hash('sha256', $hash . $pwd . $salt); //
    }
    return $hash;
}
// 呼び出し例
var_dump(get_password_hash('user1', 'pass1'));
var_dump(get_password_hash('user1', 'pass2'));
var_dump(get_password_hash('user2', 'pass1'));
```

【ブラウザ→サーバ: リクエスト 51/51-001.php → レスポンス】

The screenshot shows 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 toolbar contains buttons for '標準モード', 'サイト', 'クイックスタート', 'リクエスト', and 'レスポンス'. The left sidebar shows a tree view with 'コンテキスト' and 'サイト' folders. The main area is split into two panes: 'リクエスト' and 'レスポンス'. The 'リクエスト' pane shows the following details:

```
GET http://example.jp/51/51-001.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/51/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp
```

The 'レスポンス' pane shows the following details:

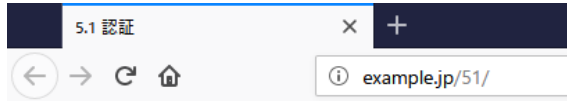
```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 09 Jan 2019 13:41:52 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 240
Connection: keep-alive
Vary: Accept-Encoding
X-UA-Compatible: IE=edge
```

Below the panes is a toolbar with '履歴', '検索', 'アラート', and 'アウトプット' buttons. At the bottom, there is a table with the following columns: 'Id', 'リクエスト日時', 'メソ...', 'URL', 'ステータスコ...', 'ステータスコード...', 'ラウンドトリップタ...', 'レスポンスボディサ...', '検出アラ...', 'ノ...', and 'タグ'. The table contains one row with the following data:

Id	リクエスト日時	メソ...	URL	ステータスコ...	ステータスコード...	ラウンドトリップタ...	レスポンスボディサ...	検出アラ...	ノ...	タグ
15	19/01/09 22:4...	GET	http://example.jp/51/51-001.php	200	OK	21 ms	240 bytes	Medium		

At the bottom right, there is a status bar with the text '現在のスキャン' and several icons representing different scan results.

51-002:自動ログイン

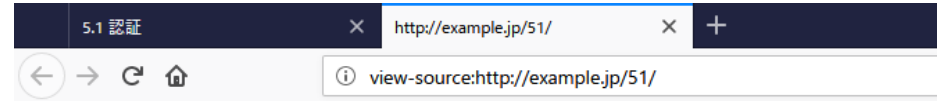


5.1 認証

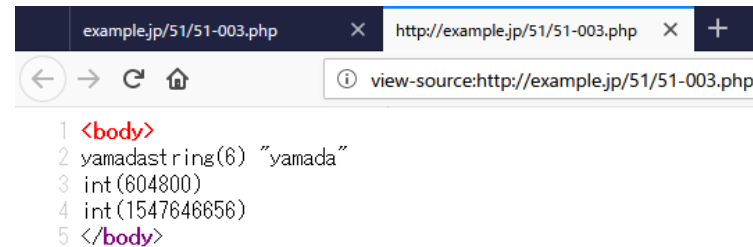
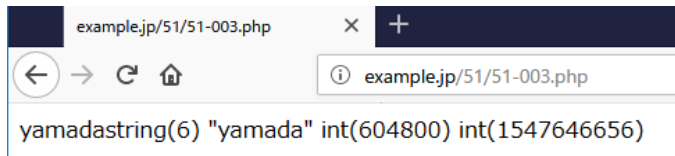
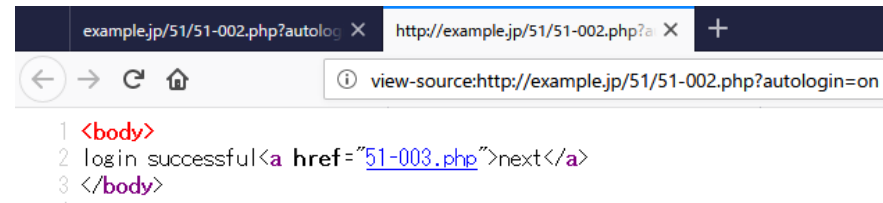
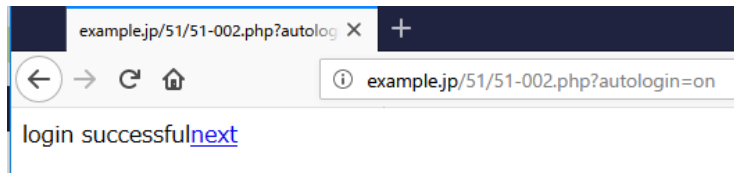
1. [51-001:パスワードのメッセージダイジェスト](#)
2. [51-002:自動ログイン](#)
3. [51-010:ログアウト確認のためのログイン画面](#)

[phpinfo](#)

[ホームに戻る](#)



```
1 <html>
2 <head><title>5.1 認証</title></head>
3 <body>
4 5.1 認証
5 <ol>
6 <li><a href="51-001.php">51-001:パスワードのメッセージダイジェスト</a></li>
7 <li><a href="51-002.php?autologin=on">51-002:自動ログイン</a></li>
8 <li><a href="51-010.php">51-010:ログアウト確認のためのログイン画面</a></li>
9 </ol>
10 <a href="phpinfo.php">phpinfo</a><br>
11 <a href="/">ホームに戻る</a>
12 </body>
13 </html>
```



【サーバ: 51/51-002.php 】

```
/var/www/html/51/51-002.php - wasbook@example.jp - エディタ - WinSCP
k?php
$autologin = (@$_GET['autologin'] === 'on');
$timeout = 30 * 60;
if ($autologin) {
    $timeout = 7 * 24 * 60 * 60;
    session_set_cookie_params($timeout);
}
session_start();
session_regenerate_id(true);
$_SESSION['id'] = 'yamada'; // ログイン機能がないので yamada で仮置き
$_SESSION['timeout'] = $timeout;
$_SESSION['expires'] = time() + $timeout;
?>
<body>
login successful<a href="51-003.php">next</a>
</body>
```

セッションの有効期間を1週間に
クッキーのExpires属性

本番ソースではログイン中ユーザIDセット
タイムアウト時間
タイムアウト期間

【サーバ: 51/51-003.php 】

```
/var/www/html/51/51-003.php - wasbook@example.jp - エディタ - WinSCP
k?php
session_start();
function islogin() {
    if (!isset($_SESSION['id'])) {
        return false;
    }
    if ($_SESSION['expires'] < time()) {
        session_destroy();
        return false;
    }
    $_SESSION['expires'] = time() + $_SESSION['timeout'];
    return true;
}
if (islogin()) {
    $id = $_SESSION['id'];
} else {
    $id = '???';
}
?>
<body>
<?php echo htmlspecialchars($id, ENT_NOQUOTES, 'UTF-8'); ?>
<?php
var_dump($_SESSION['id']);
var_dump($_SESSION['timeout']);
var_dump($_SESSION['expires']);
?>
</body>
```

IDがセットされていない場合

タイムアウトしている場合
セッション破棄

タイムアウト時刻を更新

【ブラウザ→サーバ: リクエスト 51/51-002.php → レスポンス】

無題セッション - 20190109-100359 - 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
 - http://example.jp
 - http://api.example.jp

```
GET http://example.jp/51/51-002.php?autologin=on 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/51/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 09 Jan 2019 13:49:58 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Set-Cookie: PHPSESSID=su089mctb0bsifs5thc40t3391; expires=Wed, 16-Jan-2019 13:49:58 GMT; Max-Age=604800; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=3u2keijb53che8uiblr11bju80; expires=Wed, 16-Jan-2019 13:49:58 GMT; Max-Age=604800; path=/
X-UA-Compatible: IE=edge
```

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...	URL	ステータス...	ステータスコード...	ラウンドトリップタ...	レスポンスボディサ...	検出アラ...	ノ...	タグ
18	19/01/09 22:4...	GET	http://example.jp/51/51-002.php?autol...	200	OK	7 ms	61 bytes	Medium		SetCookie
19	19/01/09 22:5...	GET	http://example.jp/51/51-003.php	200	OK	12 ms	68 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 51/51-003.php → レスポンス】

無題セッション - 20190109-100359 - 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
 - http://example.jp
 - http://api.example.jp

```
GET http://example.jp/51/51-003.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/51/51-002.php?autologin=on
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=3u2keijb53che8uiblr11bju80
Upgrade-Insecure-Requests: 1
Host: example.jp
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 09 Jan 2019 13:50:56 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

<body>
yamadastring(6) "yamada"
int(604800)
int(1547646656)
</body>
```

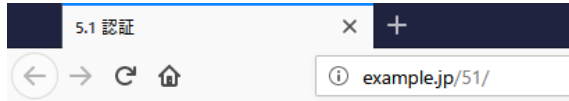
履歴 検索 アラート アウトプット +

フィルタ: オフ エクスポート

Id	リクエスト日時	メソ...	URL	ステータス...	ステータスコード...	ラウンドトリップタ...	レスポンスボディサ...	検出アラ...	ノ...	タグ
18	19/01/09 22:4...	GET	http://example.jp/51/51-002.php?autol...	200	OK	7 ms	61 bytes	Medium		SetCookie
19	19/01/09 22:5...	GET	http://example.jp/51/51-003.php	200	OK	12 ms	68 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

51-010:ログアウト確認のためのログイン画面

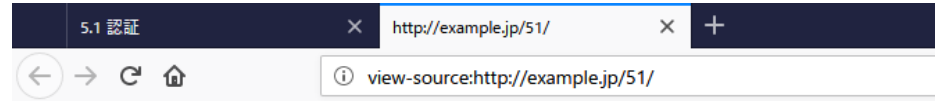


5.1 認証

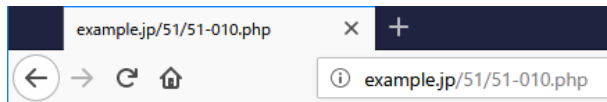
1. [51-001:パスワードのメッセージダイジェスト](#)
2. [51-002:自動ログイン](#)
3. [51-010:ログアウト確認のためのログイン画面](#)

[phpinfo](#)

[ホームに戻る](#)

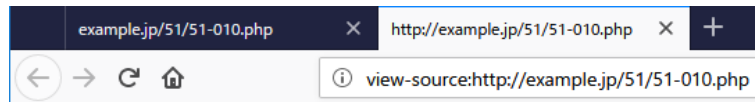


```
1 <html>
2 <head><title>5.1 認証</title></head>
3 <body>
4 5.1 認証
5 <ol>
6 <li><a href="51-001.php">51-001:パスワードのメッセージダイジェスト</a></li>
7 <li><a href="51-002.php?autologin=on">51-002:自動ログイン</a></li>
8 <li><a href="51-010.php">51-010:ログアウト確認のためのログイン画面</a></li>
9 </ol>
10 <a href="phpinfo.php">phpinfo</a><br>
11 <a href="/">ホームに戻る</a>
12 </body>
13 </html>
..
```

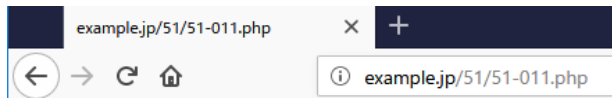


ログインしました(id=yamada)

[next](#)

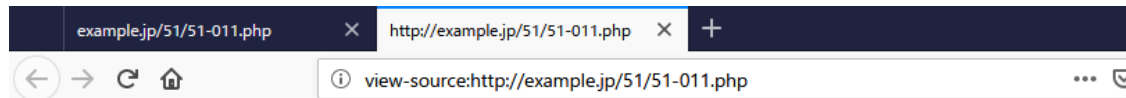


```
1 <body>
2 ログインしました(id=yamada)<br>
3 <a href="51-011.php">next</a>
4 </body>
..
```

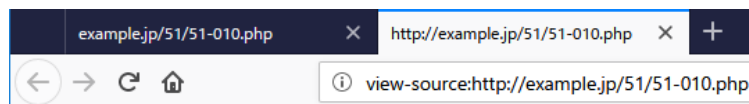
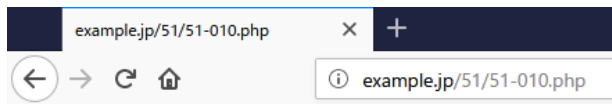
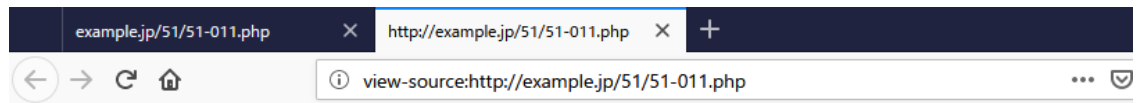
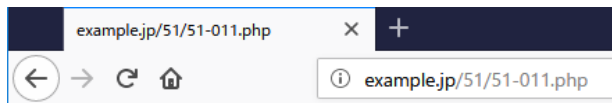
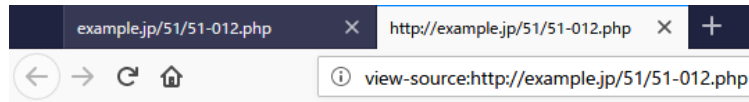
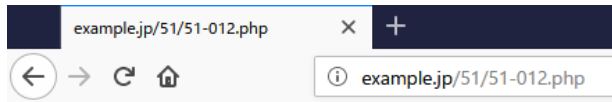


id = yamada

[login](#)



```
1 <body>
2 id = yamada<br>
3 <form action="51-012.php" method="POST">
4 <!-- 以下はCSRF防止用トークン -->
5 <input type="hidden" name="token" value="c7b70127c251d4f46b7846b159e9a55fb9322b7581c0a7a1">
6 <input type="submit" value="ログアウト">
7 </form>
8 <a href="51-010.php">login</a>
9 </body>
..
```



【サーバ: 51/51-010.php 】

```
/var/www/html/51/51-010.php - wasbook@
k?php
  session_start();
  $_SESSION['id'] = 'yamada';
?>
<body>
ログインしました(id=yamada)<br>
<a href="51-011.php">next</a>
</body>
```

【サーバ: 51/51-011.php 】

```
/var/www/html/51/51-011.php - wasbook@example.jp - エディタ - WinSCP
k?php
  session_start();
  $id = $_SESSION['id'];
  if (empty($_SESSION['token'])) {
    $token = bin2hex(openssl_random_pseudo_bytes(24));
    $_SESSION['token'] = $token;
  } else {
    $token = $_SESSION['token'];
  }
?>
<body>
id = <?php echo htmlspecialchars($id); ?><br>
<form action="51-012.php" method="POST">
<!-- 以下はCSRF防止用トークン -->
<input type="hidden" name="token" value="<?php echo
  htmlspecialchars($token); ?>">
<input type="submit" value="ログアウト">
</form>
<a href="51-010.php">login</a>
</body>
```

【サーバ: 51/51-012.php 】

```
/var/www/html/51/51-012.php - wasbook@example.jp - エディタ - WinSCP
k?php
  session_start();
  $p_token = filter_input(INPUT_POST, 'token');
  $s_token = @$_SESSION['token'];
  if (empty($p_token) || $p_token !== $s_token) {
    die('ログアウトボタンからログアウトしてください');
  }
  $_SESSION = array();
  session_destroy();
?><body>
ログアウトしました<br>
<a href="51-011.php">back</a>
</body>
```

【ブラウザ→サーバ: リクエスト 51/51-010.php → レスポンス】

無題セッション - 20190109-100359 - 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...
- サイト
 - http://ex...
 - http://api.e...

```

GET http://example.jp/51/51-010.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/51/
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=3u2keijb53che8uiblr11bju80
Upgrade-Insecure-Requests: 1
Host: example.jp
          
```

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 09 Jan 2019 14:00:13 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 85
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>
ログインしました(id=yamada)<br>
<a href="51-011.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...	URL	ステータス...	ステータスコ...	ラウンドトリップ...	レスポンスボディ...	検出ア...	ノ...	タグ
22	19/01/09 23:...	GET	http://example.jp/51/51-010.php	200	OK	10 ms	85 bytes	Medi...		
23	19/01/09 23:...	GET	http://example.jp/51/51-011.php	200	OK	7 ms	293 bytes	Medi...		Form, Hidde...
24	19/01/09 23:...	POST	http://example.jp/51/51-012.php	200	OK	8 ms	77 bytes	Medi...		
25	19/01/09 23:...	GET	http://example.jp/51/51-011.php	200	OK	6 ms	287 bytes	Medi...		Form, Hidde...
26	19/01/09 23:...	GET	http://example.jp/51/51-010.php	200	OK	6 ms	85 bytes	Medi...		

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 51/51-011.php → レスポンス】

無題セッション - 20190109-100359 - 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
 - http://exam
 - http://api.exan

```

GET http://example.jp/51/51-011.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/51/51-010.php
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=3u2keijb53che8uiblr11bju80
Upgrade-Insecure-Requests: 1
Host: example.jp
            
```

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 09 Jan 2019 14:01:04 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 293
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>
id = yamada<br>
<form action="51-012.php" method="POST">
<!-- 以下はCSRF防止用トークン -->
<input type="hidden" name="token" value=
"c7b70127c251d4f46b7846b159e9a55fb9322b7581c0a7a1">
<input type="submit" value="ログアウト">
</form>
<a href="51-010.php">login</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...	URL	ステータスコ...	ステータスコ...	ラウンドトリップタ...	レスポンスボディサ...	検出アラ...	ノ...	タグ
22	19/01/09 23:0...	GET	http://example.jp/51/51-010.php	200	OK	10 ms	85 bytes	Medium		
23	19/01/09 23:0...	GET	http://example.jp/51/51-011.php	200	OK	7 ms	293 bytes	Medium		Form, Hidden,...
24	19/01/09 23:0...	POST	http://example.jp/51/51-012.php	200	OK	8 ms	77 bytes	Medium		
25	19/01/09 23:0...	GET	http://example.jp/51/51-011.php	200	OK	6 ms	287 bytes	Medium		Form, Hidden,...
26	19/01/09 23:0...	GET	http://example.jp/51/51-010.php	200	OK	6 ms	85 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→サーバ: リクエスト 51/51-012.php → レスポンス】

無題セッション - 20190109-100359 - 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
 - http://exam
 - http://api.exan

```

POST http://example.jp/51/51-012.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/51/51-011.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 54
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=3u2keijb53che8uiblr11bju80
Upgrade-Insecure-Requests: 1
Host: example.jp

token=c7b70127c251d4f46b7846b159e9a55fb9322b7581c0a7a1
            
```

デフォルトビュー

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 09 Jan 2019 14:03:47 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 77
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>
ログアウトしました<br>
<a href="51-011.php">back</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...	URL	ステータスコ...	ステータスコード...	ラウンドトリップタ...	レスポンスボディサ...	検出アラ...	ノ...	タグ
22	19/01/09 23:0...	GET	http://example.jp/51/51-010.php	200	OK	10 ms	85 bytes	Medium		
23	19/01/09 23:0...	GET	http://example.jp/51/51-011.php	200	OK	7 ms	293 bytes	Medium		Form, Hidden,...
24	19/01/09 23:0...	POST	http://example.jp/51/51-012.php	200	OK	8 ms	77 bytes	Medium		
25	19/01/09 23:0...	GET	http://example.jp/51/51-011.php	200	OK	6 ms	287 bytes	Medium		Form, Hidden,...
26	19/01/09 23:0...	GET	http://example.jp/51/51-010.php	200	OK	6 ms	85 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 51/51-011.php → レスポンス】

無題セッション - 20190109-100359 - 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
 - http://exam
 - http://api.exan

```
GET http://example.jp/51/51-011.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/51/51-012.php
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=3u2kej53che8uiblr11bju80
Upgrade-Insecure-Requests: 1
Host: example.jp
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 09 Jan 2019 14:04:30 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 287
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>
id = <br>
<form action="51-012.php" method="POST">
<!-- 以下はCSR防止用トークン -->
<input type="hidden" name="token" value=
"f5992d2e71974de3d3b03721635dd491815fb6bf76773b25">
<input type="submit" value="ログアウト">
</form>
<a href="51-010.php">login</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...	URL	ステータスコ...	ステータスコード...	ラウンドトリップタ...	レスポンスボディサ...	検出アラ...	ノ...	タグ
22	19/01/09 23:0...	GET	http://example.jp/51/51-010.php	200	OK	10 ms	85 bytes	Medium		
23	19/01/09 23:0...	GET	http://example.jp/51/51-011.php	200	OK	7 ms	293 bytes	Medium		Form, Hidden,...
24	19/01/09 23:0...	POST	http://example.jp/51/51-012.php	200	OK	8 ms	77 bytes	Medium		
25	19/01/09 23:0...	GET	http://example.jp/51/51-011.php	200	OK	6 ms	287 bytes	Medium		Form, Hidden,...
26	19/01/09 23:0...	GET	http://example.jp/51/51-010.php	200	OK	6 ms	85 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 51/51-010.php → レスポンス】

無題セッション - 20190109-100359 - 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
 - http://exam
 - http://api.exan

```

GET http://example.jp/51/51-010.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/51/51-011.php
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=3u2keijb53che8uiblr11bju80
Upgrade-Insecure-Requests: 1
Host: example.jp
            
```

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 09 Jan 2019 14:05:34 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 85
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>
ログインしました(id=yamada)<br>
<a href="51-011.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...	URL	ステータスコ...	ステータスコード...	ラウンドトリップタ...	レスポンスボディサ...	検出アラ...	ノ...	タグ
22	19/01/09 23:0...	GET	http://example.jp/51/51-010.php	200	OK	10 ms	85 bytes	Medium		
23	19/01/09 23:0...	GET	http://example.jp/51/51-011.php	200	OK	7 ms	293 bytes	Medium		Form, Hidden,...
24	19/01/09 23:0...	POST	http://example.jp/51/51-012.php	200	OK	8 ms	77 bytes	Medium		
25	19/01/09 23:0...	GET	http://example.jp/51/51-011.php	200	OK	6 ms	287 bytes	Medium		Form, Hidden,...
26	19/01/09 23:0...	GET	http://example.jp/51/51-010.php	200	OK	6 ms	85 bytes	Medium		

アラート 0 1 2 0

現在のスキャン 0 0 0 0 0 0