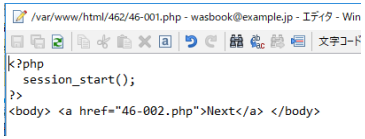
4.6 セッション管理の不備

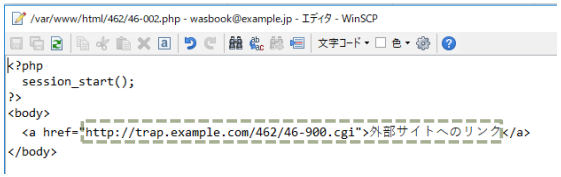
46-001:Refererからのセッション ID漏洩

【ブラウザ】

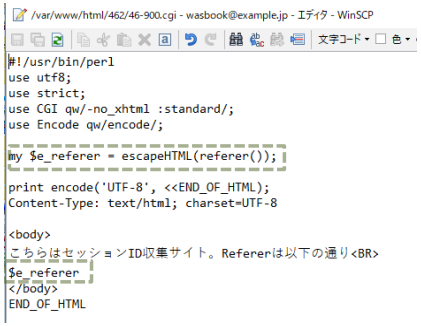
【サーバ: 462/46-001.php 】



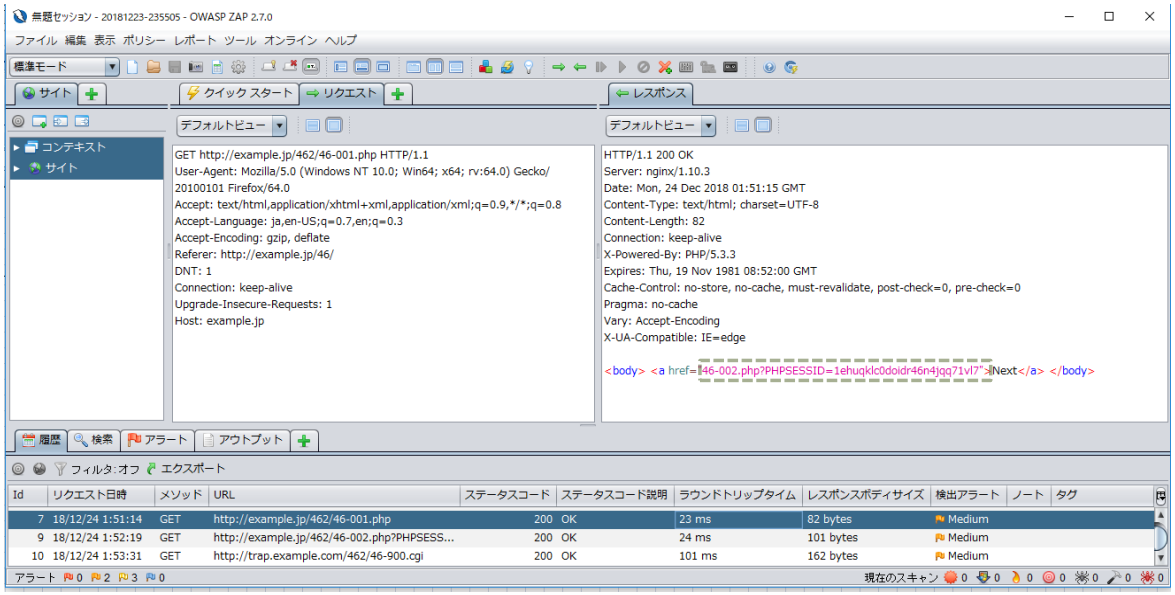
【サーバ: 462/46-002.php 】



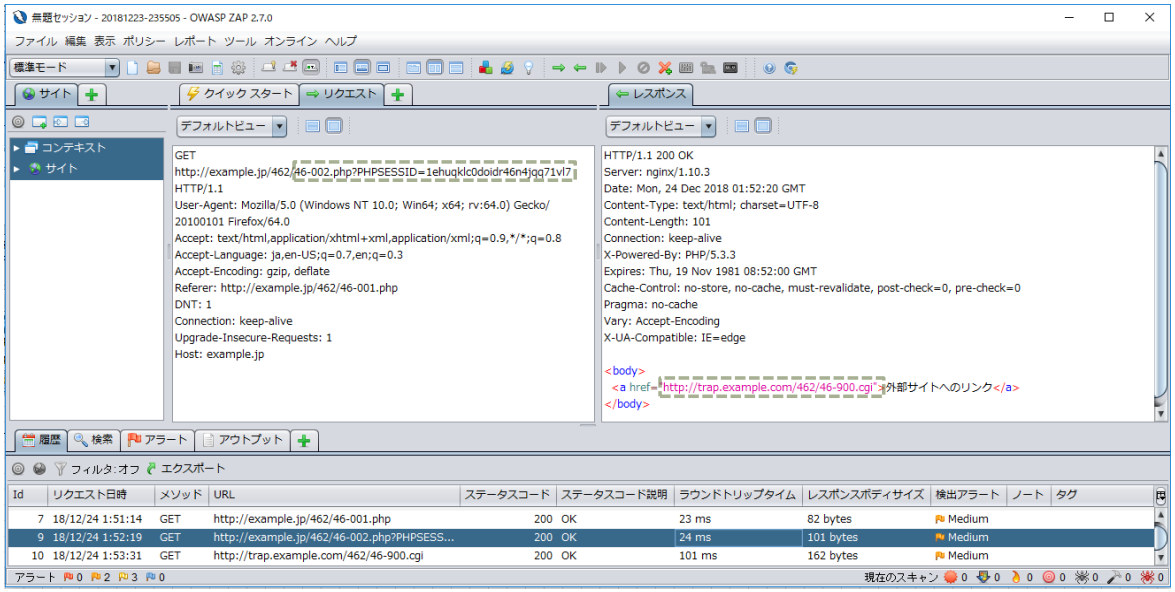
【サーバ: 462/46-900.cgi 】



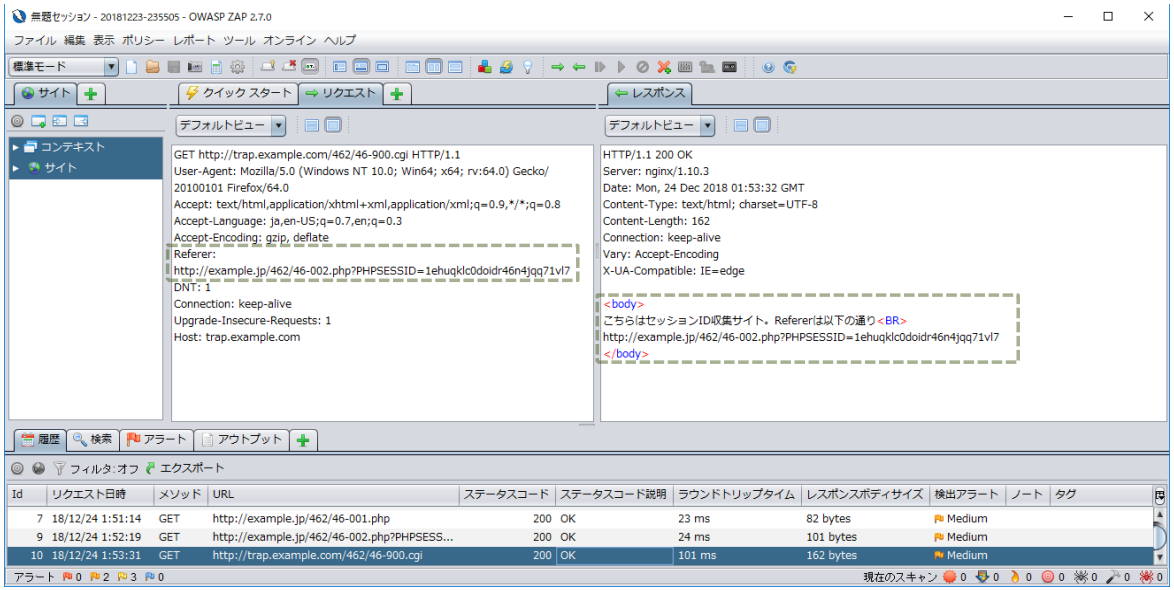
【ブラウザ→サーバ： リクエスト 462/46-001.php → レスポンス 】 RefererからのセッションID漏洩



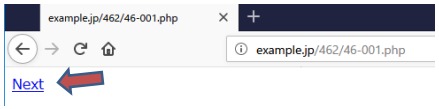
【ブラウザ→サーバ： リクエスト 462/46-002.php → レスポンス 】 RefererからのセッションID漏洩

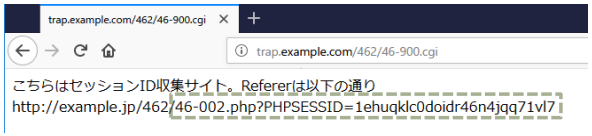


【ブラウザ→偽サーバ：リクエスト http://trap.example.com/462/46-900.cgi → レスポンス 】 Refererからのセッション ID漏洩



【ブラウザ】





46-010:セッションIDの固定化(正常系)

【ブラウザ】

【サーバ： 463/45-010.php 】

/var/www/html/463/46-010.php - wasbook@example.jp - エディタ

```
<?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

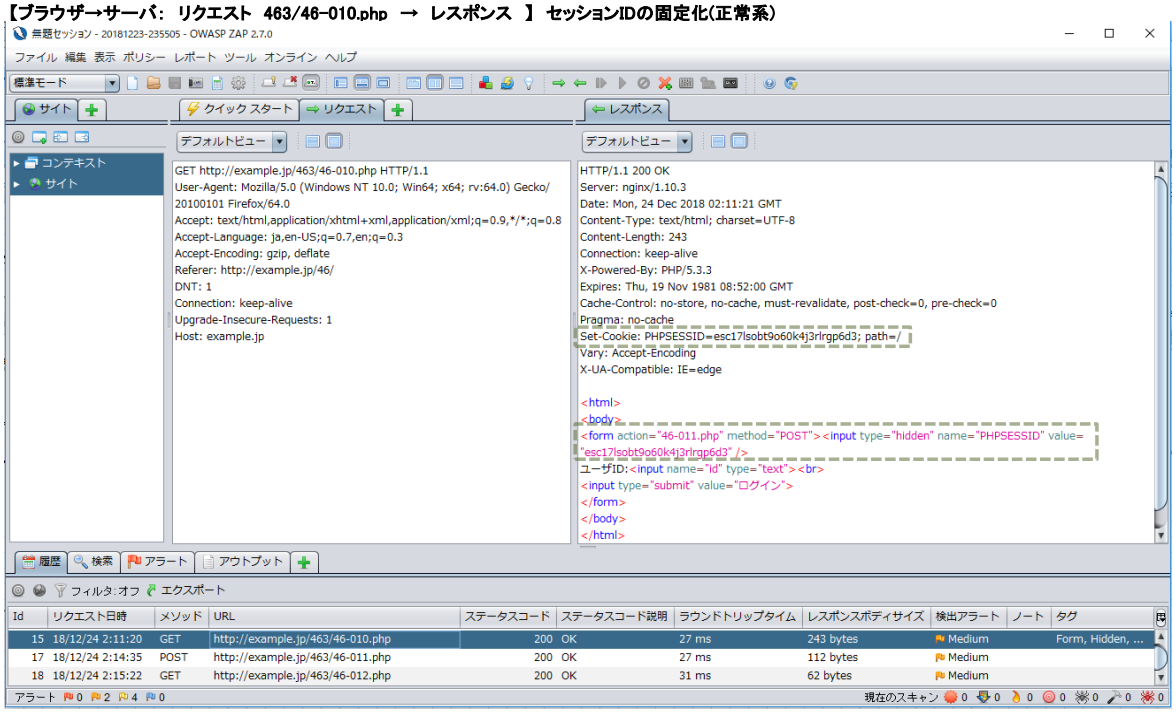
```
<?php
  session_start();
  $id = filter_input(INPUT_POST, 'id'); // 必ずログインに成功する（仕様）
  $_SESSION['id'] = $id; // ユーザIDをセッションに保存
?>
<html>
<body>
<?php echo htmlspecialchars($id, ENT_COMPAT, 'UTF-8'); ?>
さん、ログイン成功です<BR>
<a href="46-012.php">個人情報</a>
</body>
</html>
```

【サーバ： 463/45-012.php 】

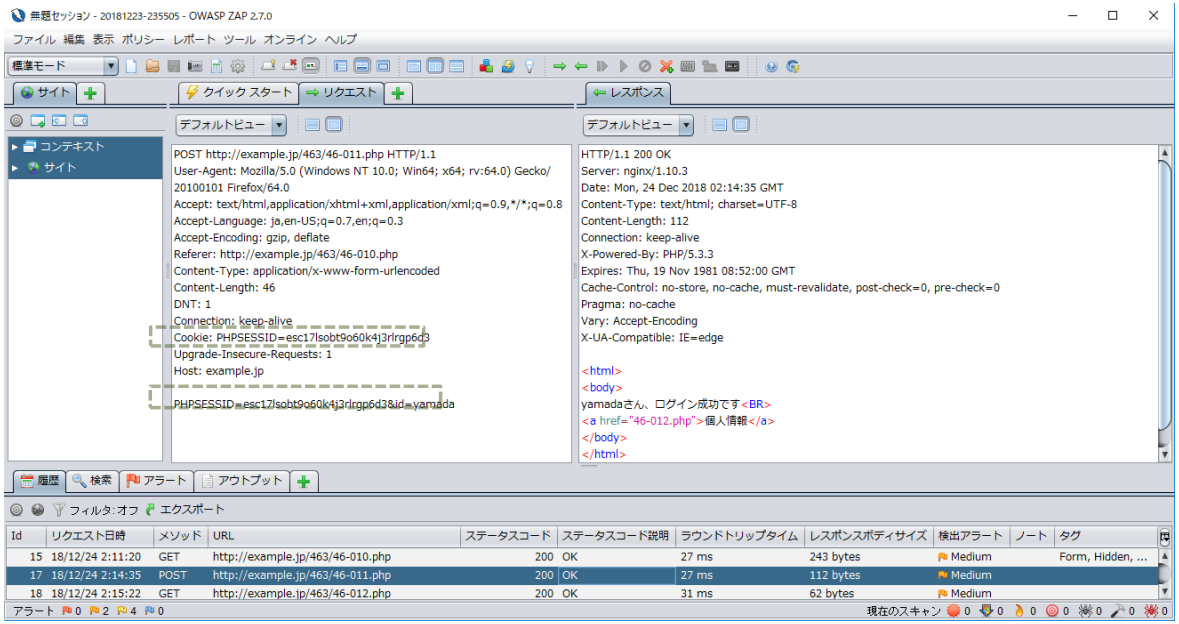
/var/www/html/463/46-012.php - wasbook@example.jp - エディタ - WinSCP

```
<?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)

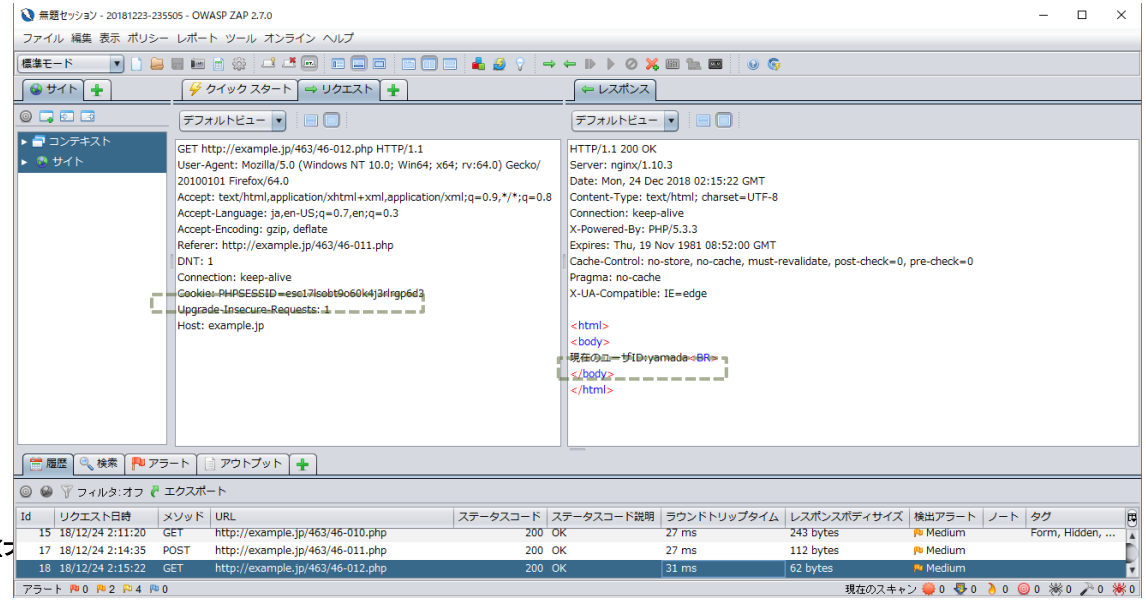


【ブラウザ→サーバ： リクエスト 463/46-010.php → レスポンス 】 セッションIDの固定化(正常系)

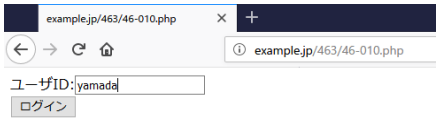


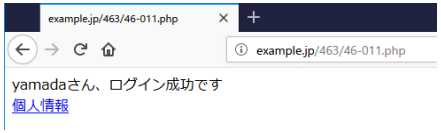
【ブラウザ→偽サーバ：リクエスト trap.example.com/45/45-901.html → レスポンス 】CSRFの罠(iframe版)

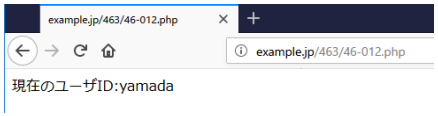
【ブラウザ→サーバ：リクエスト 463/46-012.php → レスポンス 】セッションIDの固定化(正常系)



【ブラウザ】



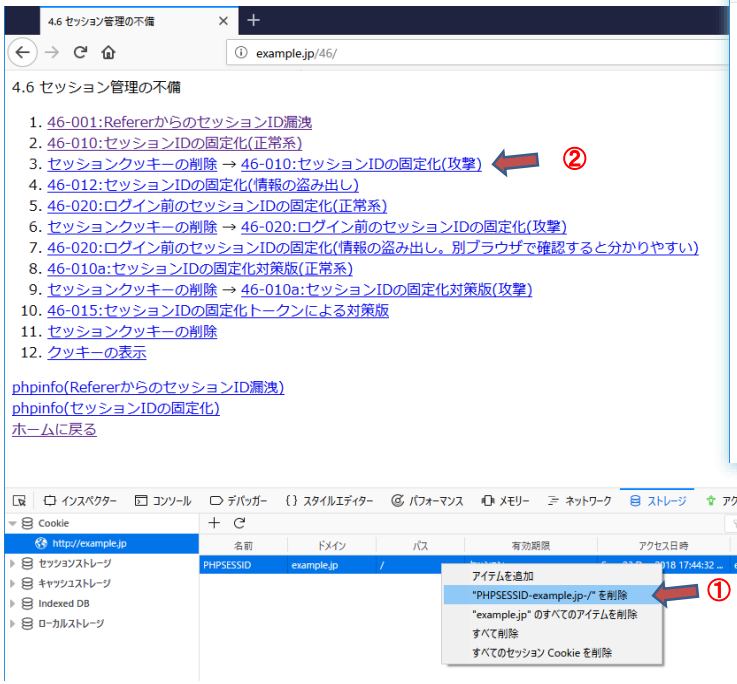




セッションクッキーの削除 → 46-010:セッションIDの固定化(攻撃)

【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



【サーバ: 463/45-010.php 】

/var/www/html/463/46-010.php - wasbook@example.jp - エディタ

```
<?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

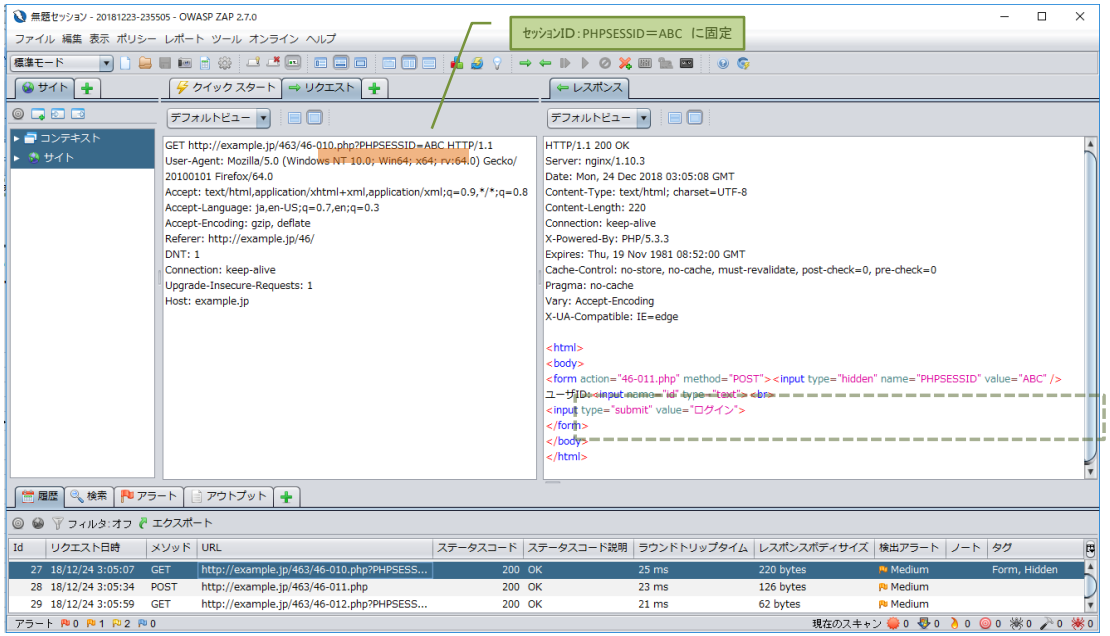
```
<?php
  session_start();
  $id = filter_input(INPUT_POST, 'id'); // 必ずログインに成功する（仕様）
  $_SESSION['id'] = $id; // ユーザIDをセッションに保存
?>
<html>
<body>
<?php echo htmlspecialchars($id, ENT_COMPAT, 'UTF-8'); ?>
さん、ログイン成功です<BR>
<a href="46-012.php">個人情報</a>
</body>
</html>
```

【サーバ: 463/45-012.php 】

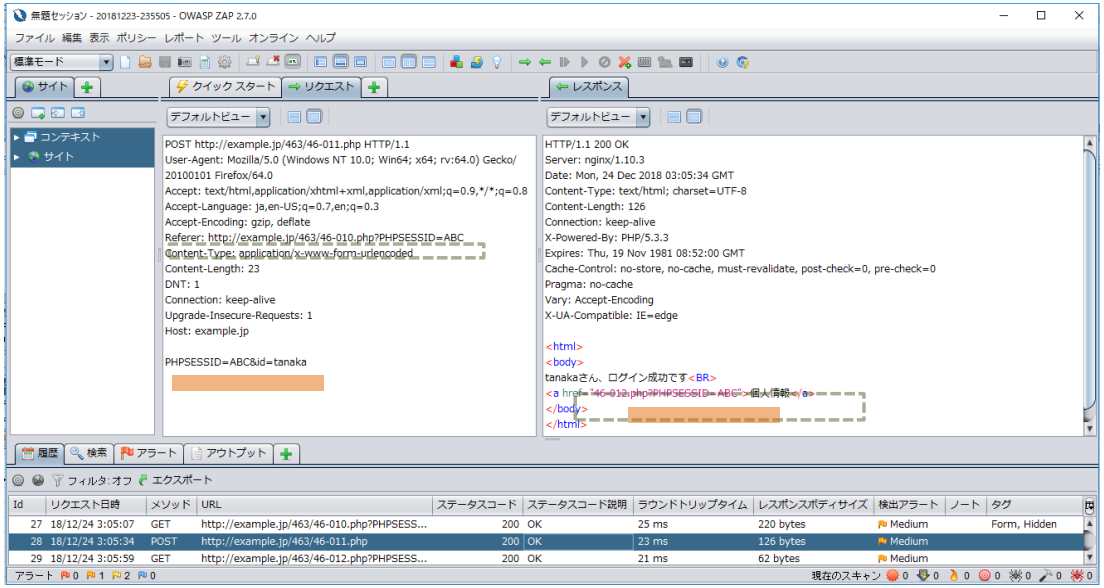
/var/www/html/463/46-012.php - wasbook@example.jp - エディタ - WinSCP

```
<?php
  session_start();
?>
<html>
<body>
現在のユーザID:<?php echo  htmlspecialchars(@$_SESSION['id'], ENT_COMPAT, 'UTF-8'); ?><BR>
</body>
</html>
```

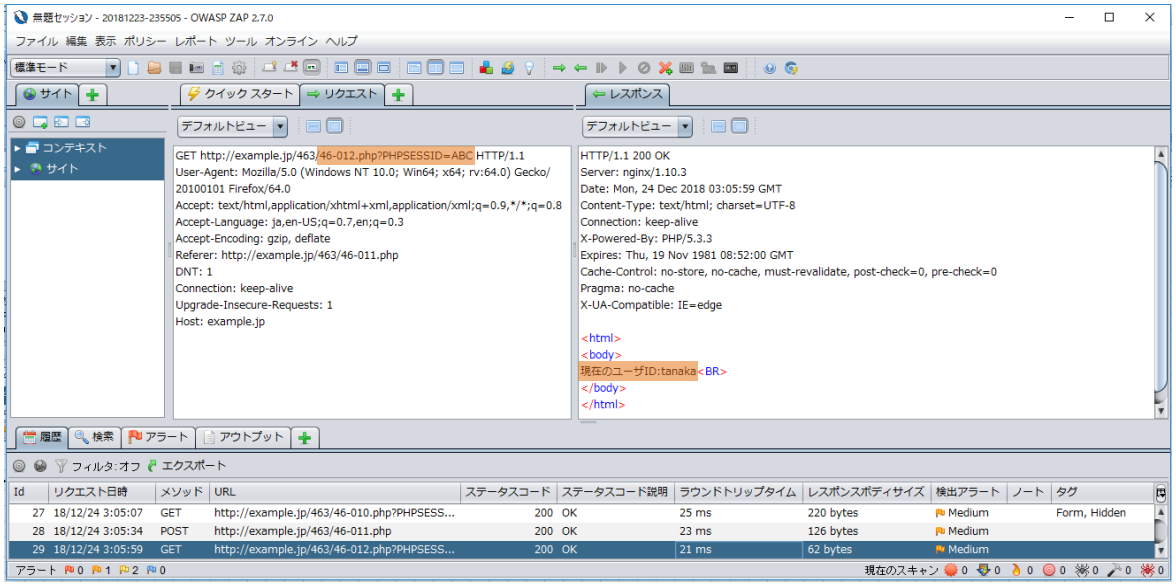
【ブラウザ→サーバ： リクエスト 463/46-010.php → レスポンス 】 セッションクッキーの削除 → 46-010:セッションIDの固定化(攻撃)



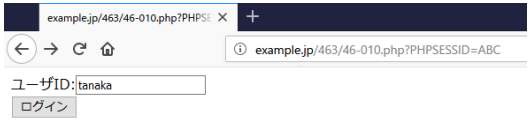
【ブラウザ→サーバ： リクエスト 463/46-011.php → レスポンス 】 セッションクッキーの削除 → 46-010:セッションIDの固定化(攻撃)

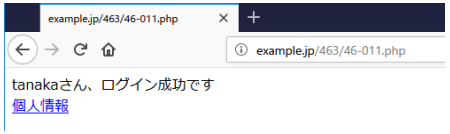


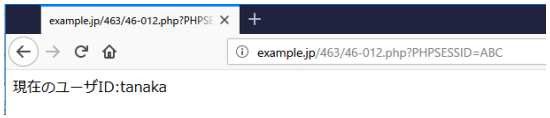
【ブラウザ→サーバ： リクエスト 463/46-012.php → レスポンス 】 セッションクッキーの削除 → 46-010:セッションIDの固定化(攻撃)



【ブラウザ】



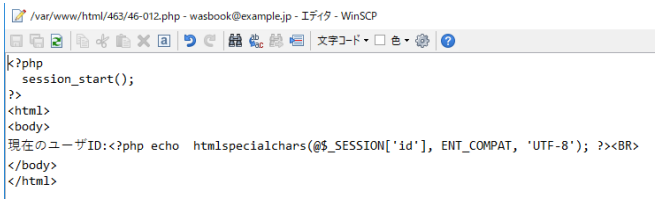




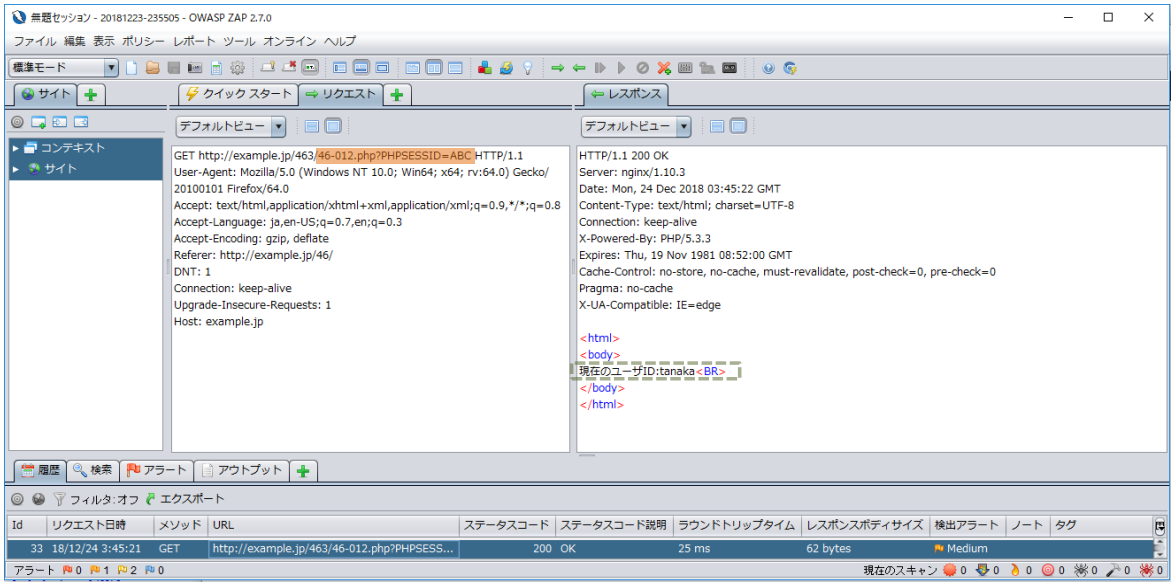
46-012:セッションIDの固定化(情報の盗み出し)

【ブラウザ】

【サーバ: 463/46-012.php 】

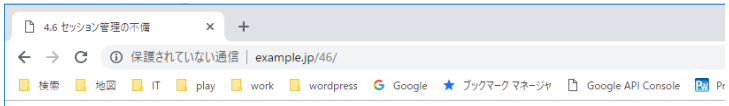


【ブラウザ→サーバ： リクエスト 463/46-012.php → レスポンス 】 46-012:セッションIDの固定化(情報の盗み出し)



OWASP ZAPからPHPSESSID=ABC
をスニファー

【ブラウザ】

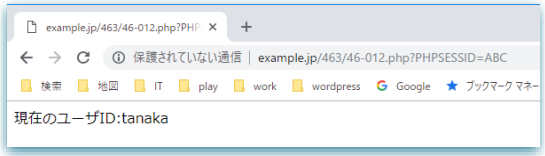


他の端末から攻撃者がPHPSESSID=ABCを確認する
というストーリで、ChromeからWebブラウズ

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

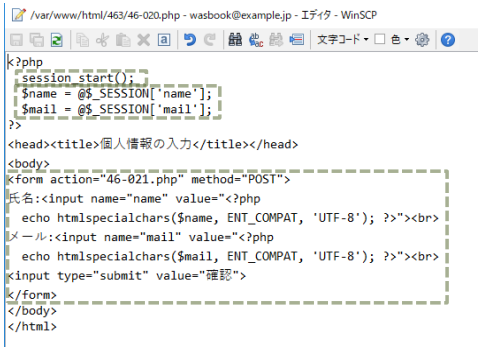


ユーザID：tanaka　を盗み見できる

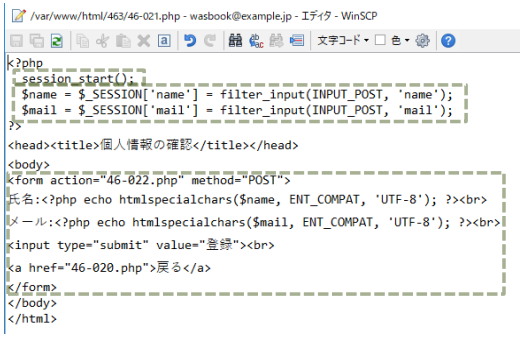
46-020:ログイン前のセッションIDの固定化(正常系)

【ブラウザ】

【サーバ: 463/46-020.php 】

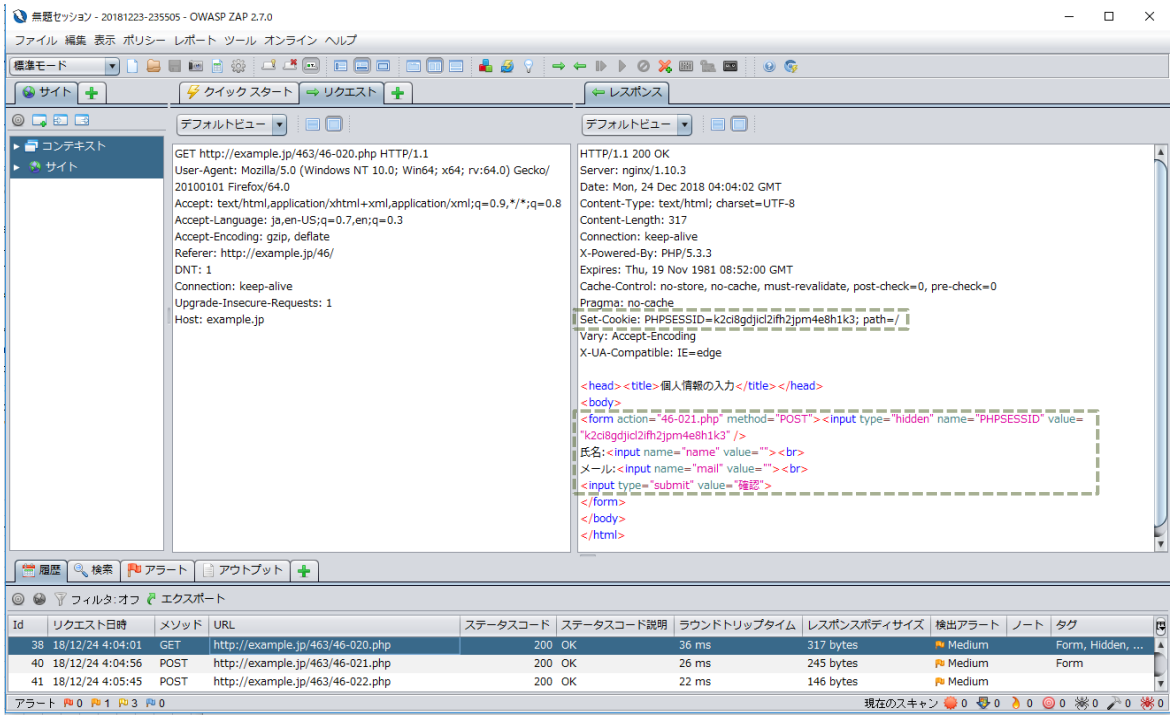


【サーバ: 463/46-021.php 】

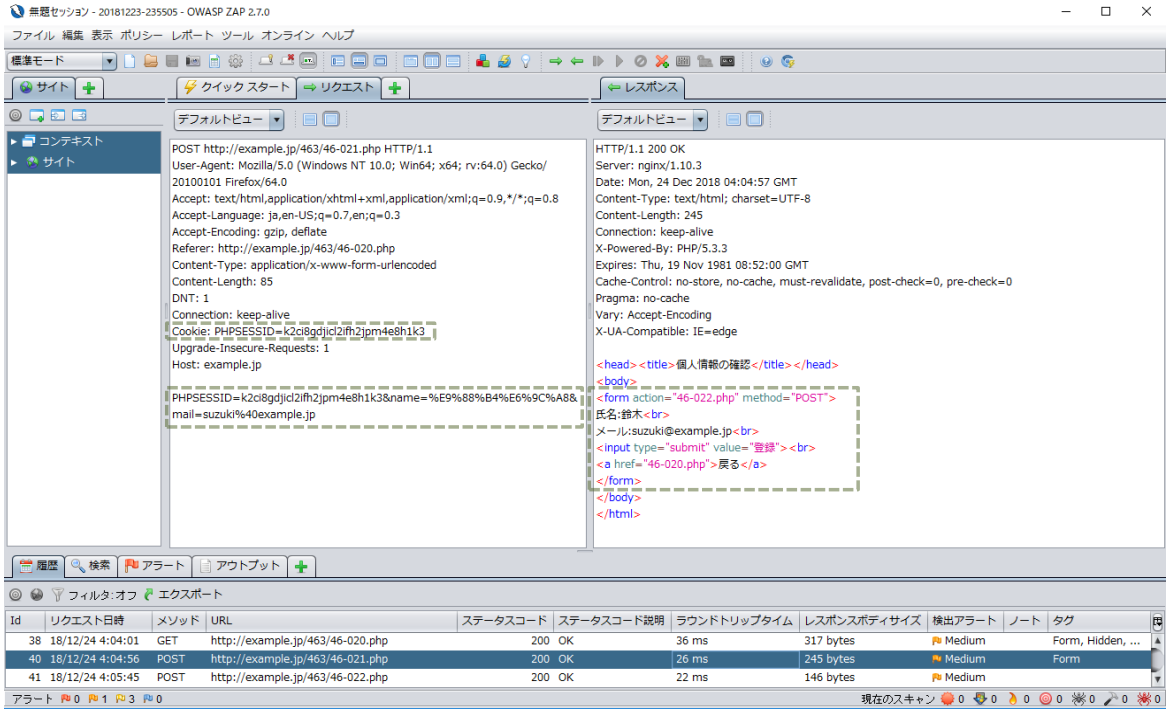


【サーバ: 463/46-022.php 】

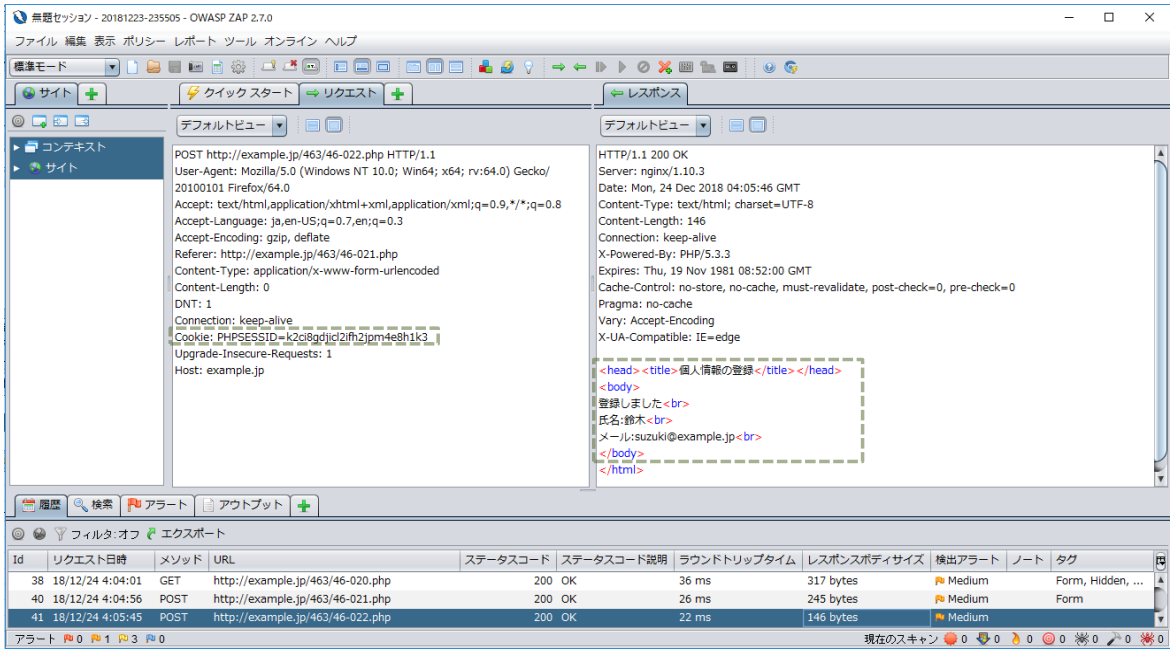
【ブラウザ→サーバ： リクエスト 463/46-020.php → レスポンス 】ログイン前のセッションIDの固定化(正常系)



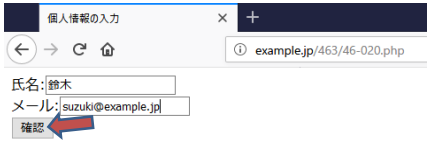
【ブラウザ→サーバ： リクエスト 463/46-021.php → レスポンス 】ログイン前のセッションIDの固定化(正常系)

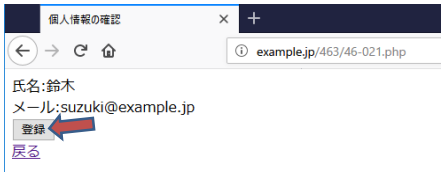


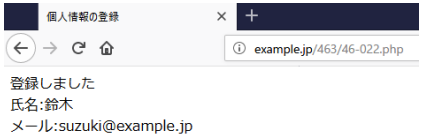
【ブラウザ→サーバ： リクエスト 463/46-022.php → レスポンス 】ログイン前のセッションIDの固定化(正常系)



【ブラウザ】



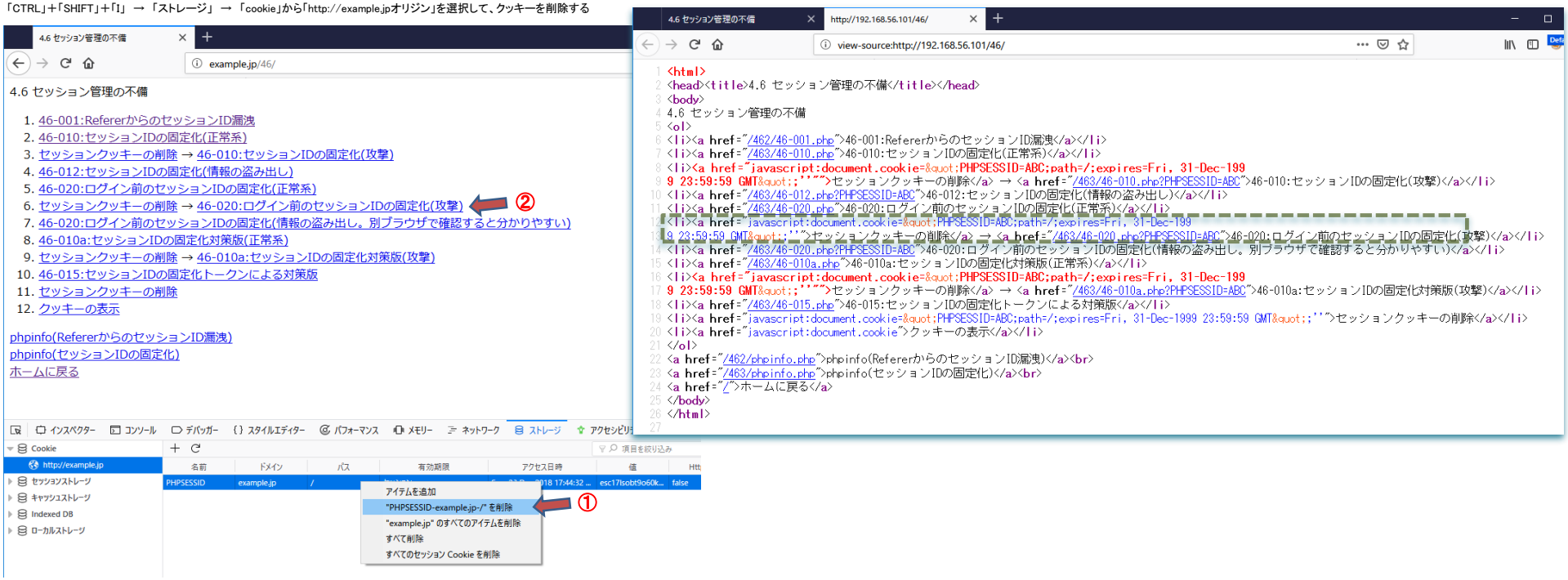




セッションクッキーの削除 → 46-020:ログイン前のセッションIDの固定化(攻撃)

【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



【サーバ: 463/46-020.php 】

/var/www/html/463/46-020.php - wasbook@example.jp - エディタ - WinSCP

```
<?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

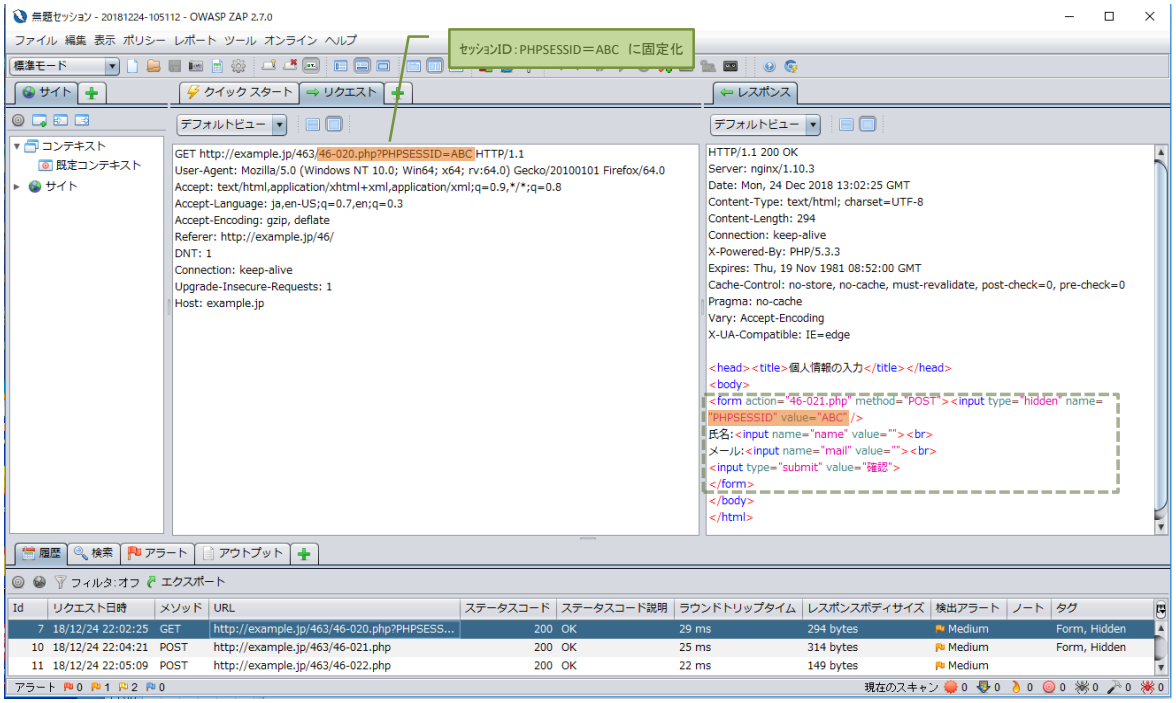
```
<?php
  session_start();
  $name = $_SESSION['name'] = filter_input(INPUT_POST, 'name');
  $mail = $_SESSION['mail'] = filter_input(INPUT_POST, 'mail');
?>
<head><title>個人情報の確認</title></head>
<body>
<form action="46-022.php" method="POST">
氏名:<?php echo htmlspecialchars($name, ENT_COMPAT, 'UTF-8'); ?><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 】

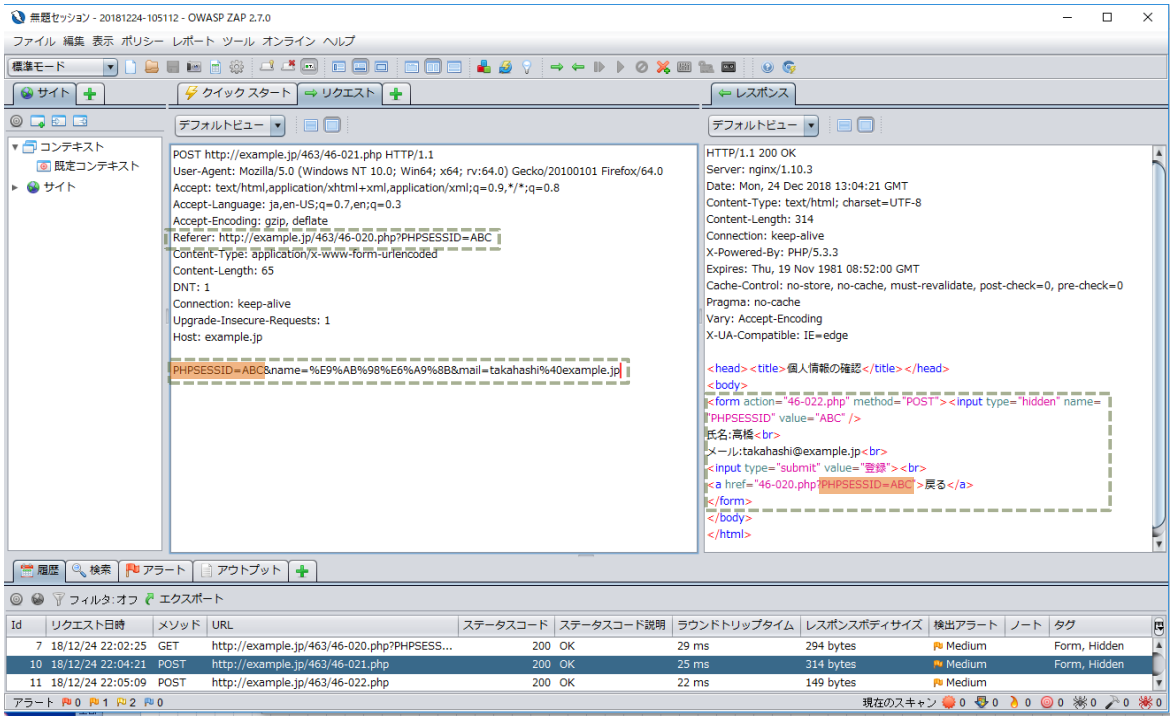
/var/www/html/463/46-022.php - wasbook@example.jp - エディタ - WinSCP

```
<?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>
```

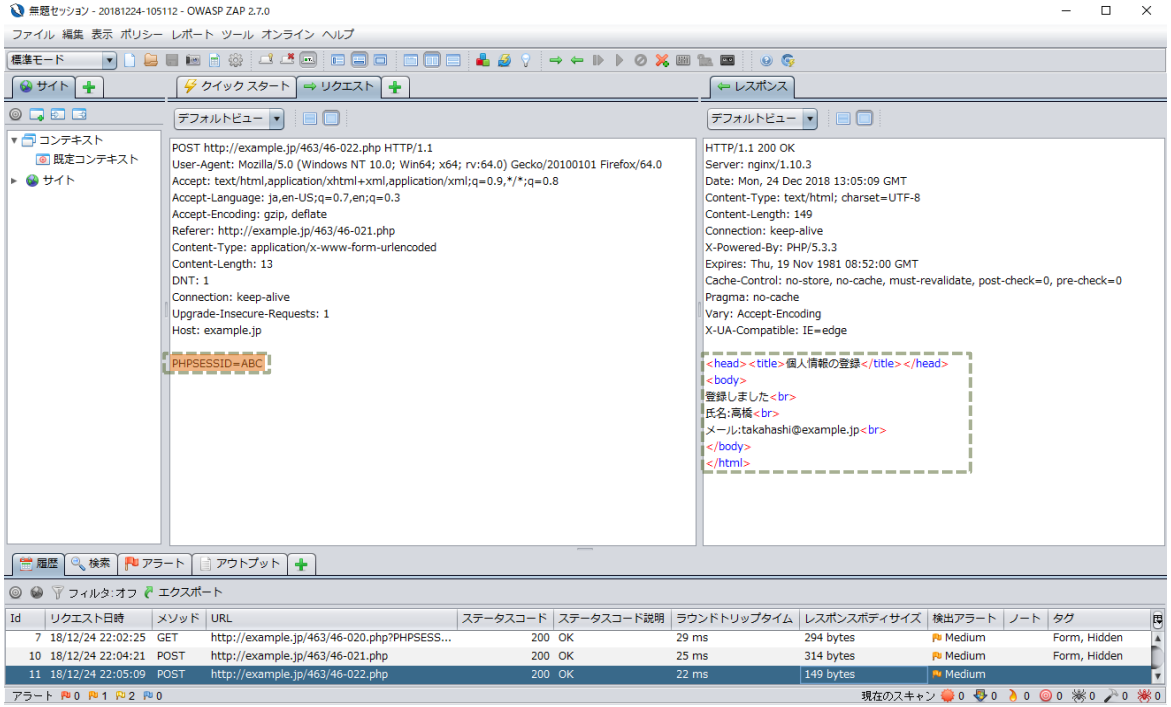
【ブラウザ→サーバ： リクエスト 463/46-020.php → レスポンス 】ログイン前のセッションIDの固定化(攻撃)



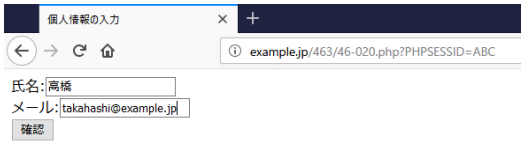
【ブラウザ→サーバ： リクエスト 463/46-021.php → レスポンス 】ログイン前のセッションIDの固定化(攻撃)



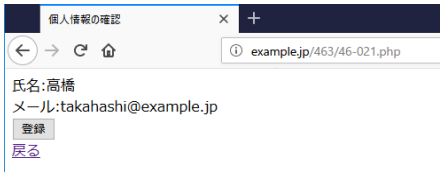
【ブラウザ→サーバ： リクエスト 463/46-022.php → レスポンス 】ログイン前のセッションIDの固定化(攻撃)



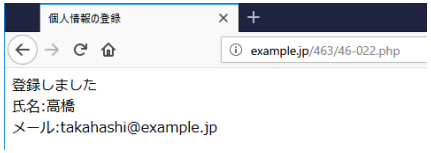
【ブラウザ】

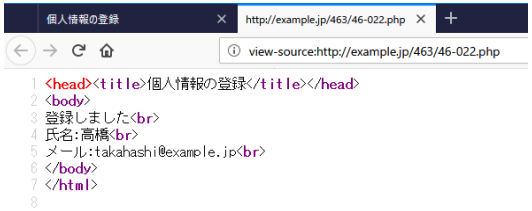

個人情報の入力
example.jp/463/46-020.php?PHPSESSID=ABC
氏名:高橋
メール:takahashi@example.jp
確認


個人情報の入力
http://example.jp/463/46-020.php?
view-source:http://example.jp/463/46-020.php?PHPSESSID=ABC
<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="">
メール:<input name="mail" value="">
<input type="submit" value="確認">
</form>
</body>
</html>


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
<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
メール:takahashi@example.jp
<input type="submit" value="登録">
戻る
</form>
</body>
</html>

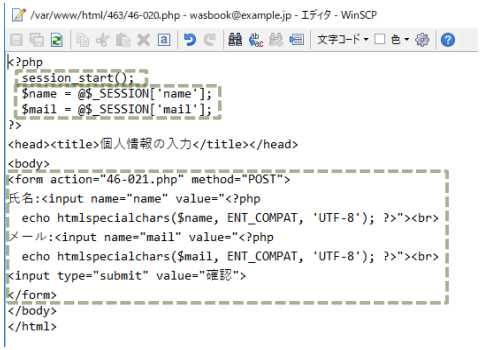

個人情報の登録
example.jp/463/46-022.php
登録しました
氏名:高橋
メール:takahashi@example.jp


個人情報の登録
http://example.jp/463/46-022.php
view-source:http://example.jp/463/46-022.php
<head><title>個人情報の登録</title></head>
<body>
登録しました
氏名:高橋
メール:takahashi@example.jp
</body>
</html>

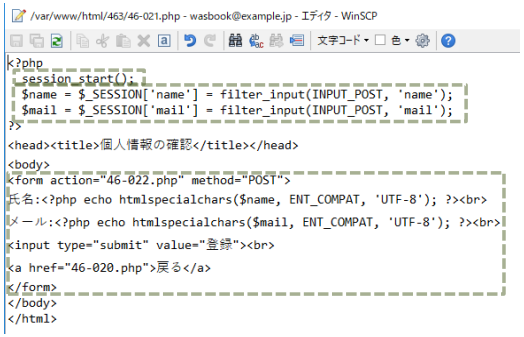
46-020:ログイン前のセッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)

【ブラウザ】

【サーバ: 463/46-020.php 】

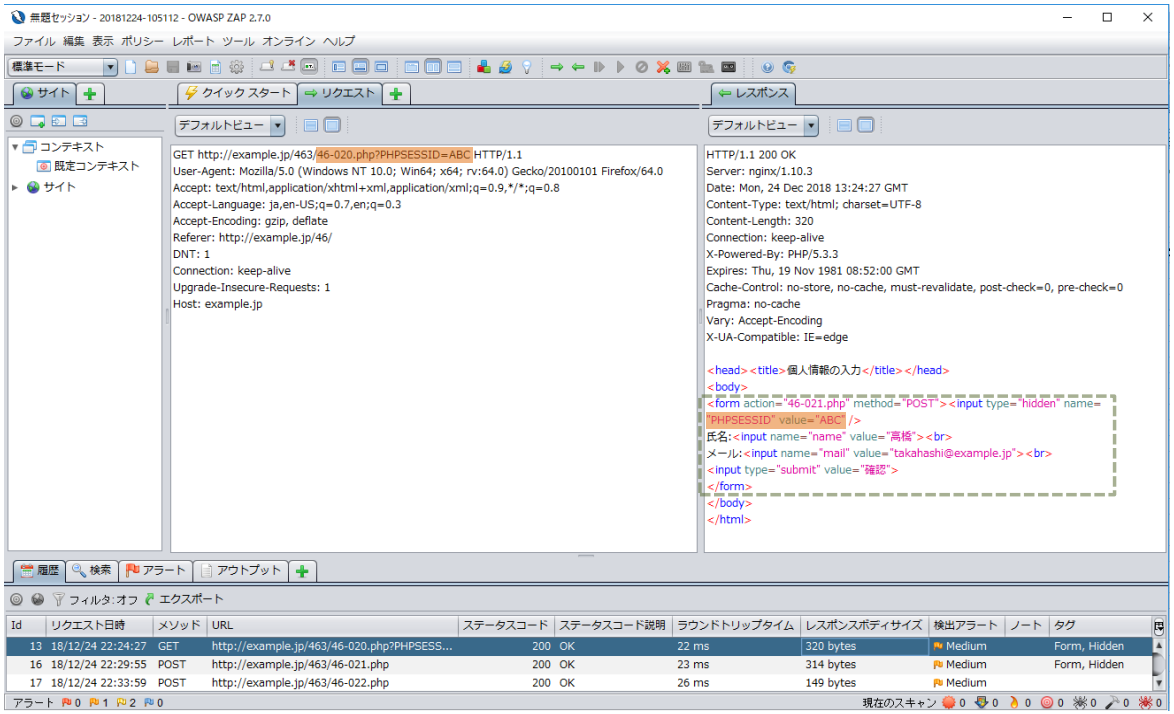


【サーバ: 463/46-021.php 】

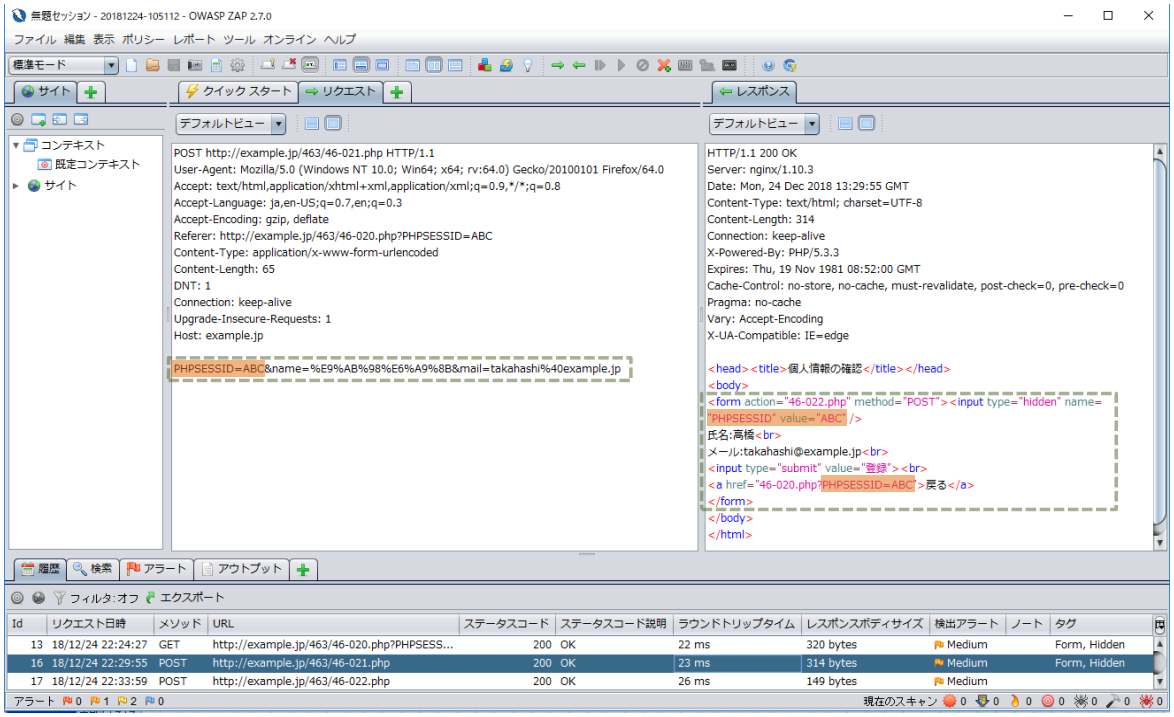


【サーバ: 463/46-022.php 】

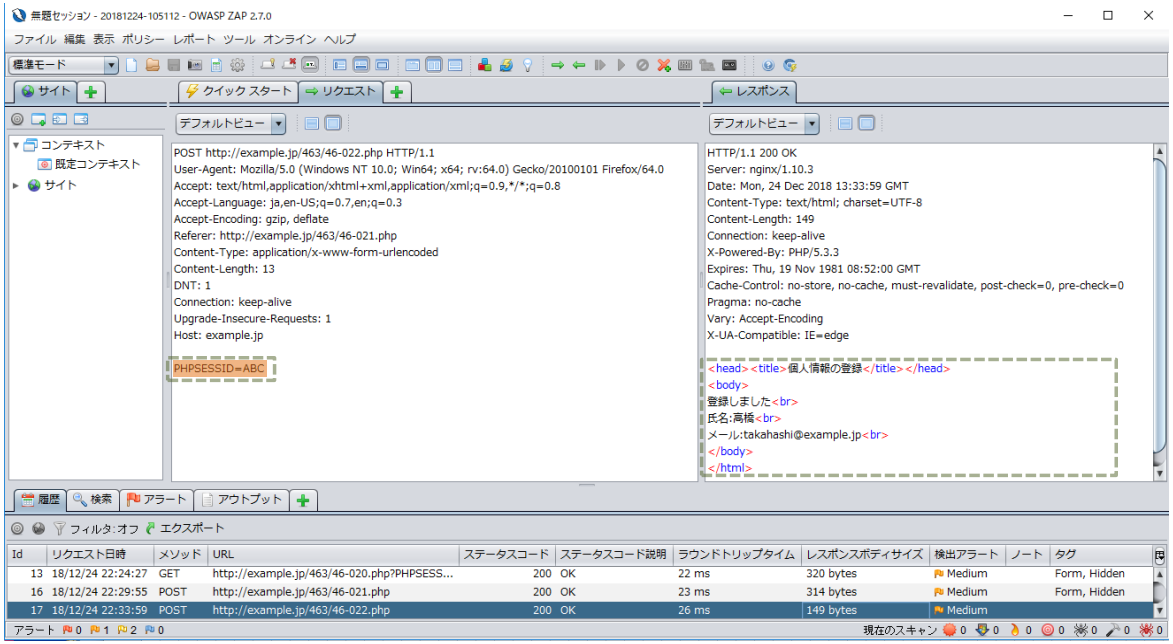
【ブラウザ→サーバ： リクエスト 463/46-020.php → レスポンス 】ログイン前のセッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)



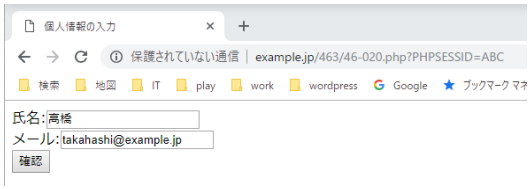
【ブラウザ→サーバ： リクエスト 463/46-021.php → レスポンス 】ログイン前のセッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)

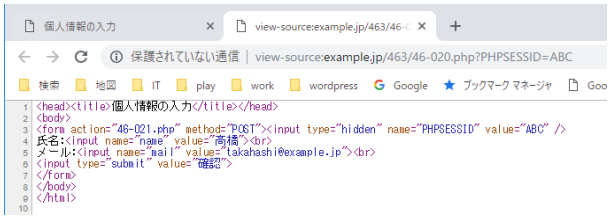


【ブラウザ→サーバ： リクエスト 463/46-022.php → レスポンス 】ログイン前のセッションIDの固定化(情報の盗み出し。別ブラウザで確認すると分かりやすい)

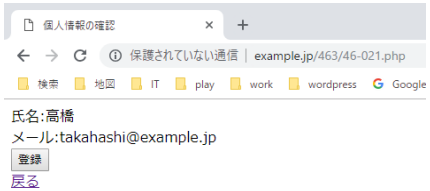


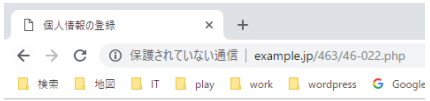
【ブラウザ】

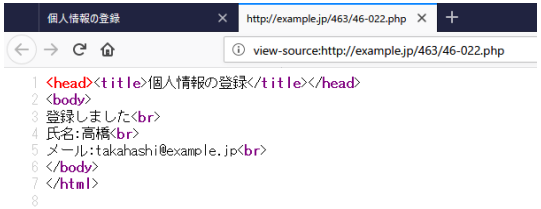




他の端末から攻撃者がPHPSESSID=ABCを確認する
というストーリで、ChromeからWebブラウズ

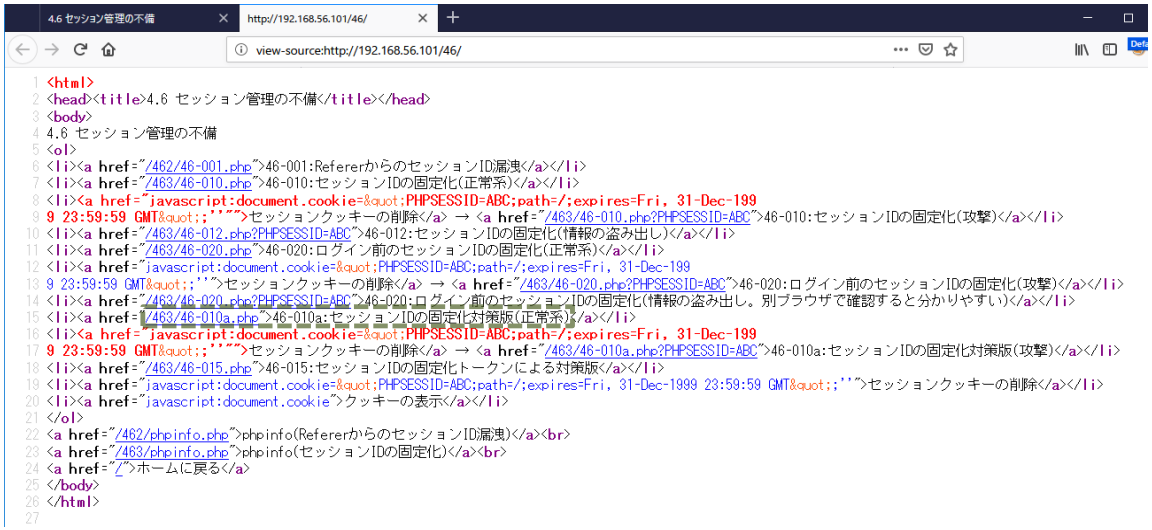






46-010a:セッションIDの固定化対策版(正常系)

【ブラウザ】



【サーバ： 463/46-010a.php 】

/var/www/html/463/46-010a.php - wasbook@example.jp - エディタ

```
<?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

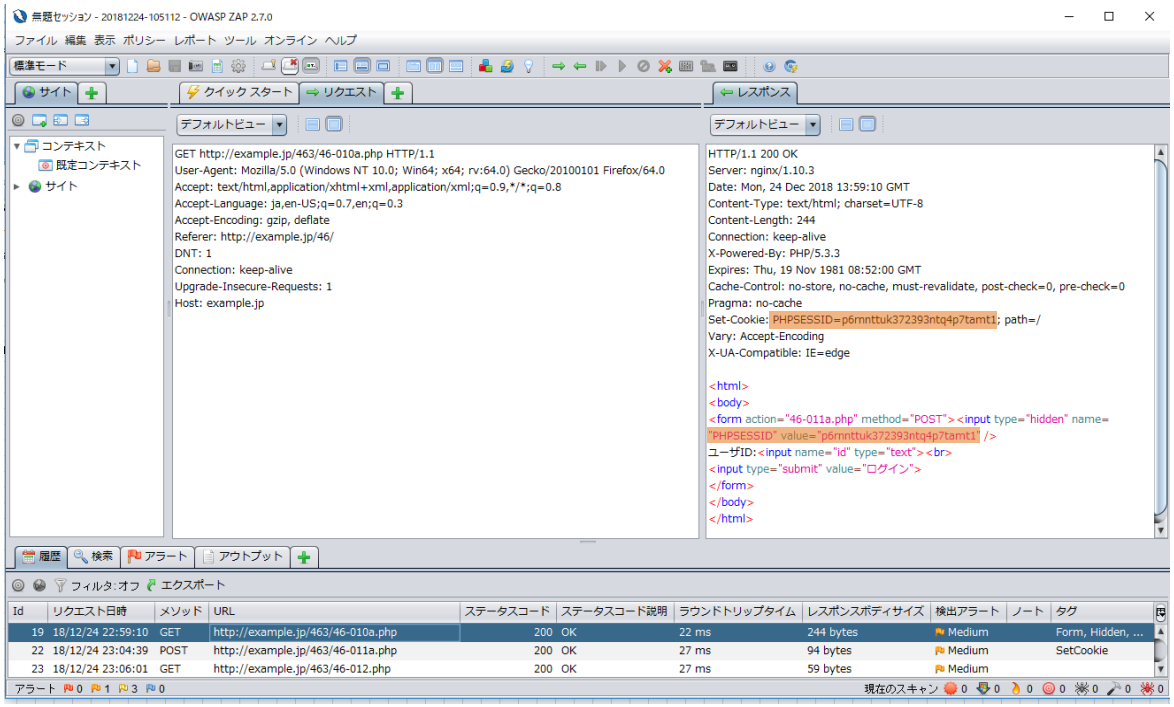
```
<?php
 session_start();
 $id = filter_input(INPUT_POST, 'id'); // 必ずログインに成功する（仕様）
 session_regenerate_id(true); // セッションIDの変更
 $_SESSION['id'] = $id; // ユーザIDをセッションに保存
?>
<body>
<?php echo htmlspecialchars($id, ENT_COMPAT, 'UTF-8'); ?>さん、ログイン成功です<BR>
<a href="46-012.php">個人情報</a>
</body>
```

【サーバ： 463/46-012.php 】

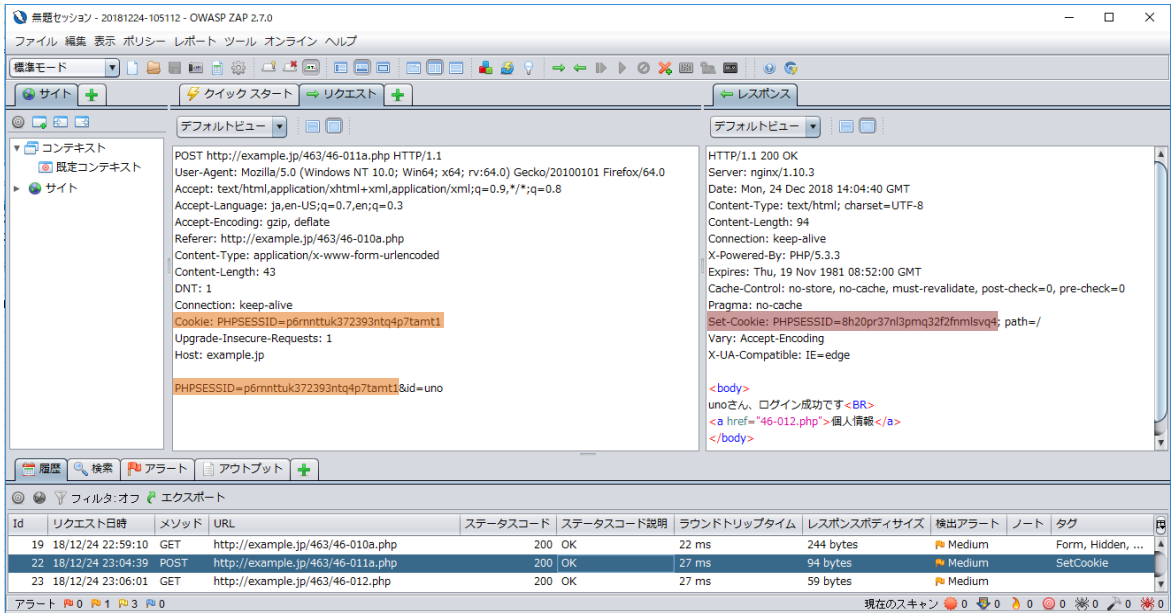
/var/www/html/463/46-012.php - wasbook@example.jp - エディタ - WinSCP

```
<?php
 session_start();
?>
<html>
<body>
現在のユーザID:<?php echo  htmlspecialchars(@$_SESSION['id'], ENT_COMPAT, 'UTF-8'); ?><BR>
</body>
</html>
```

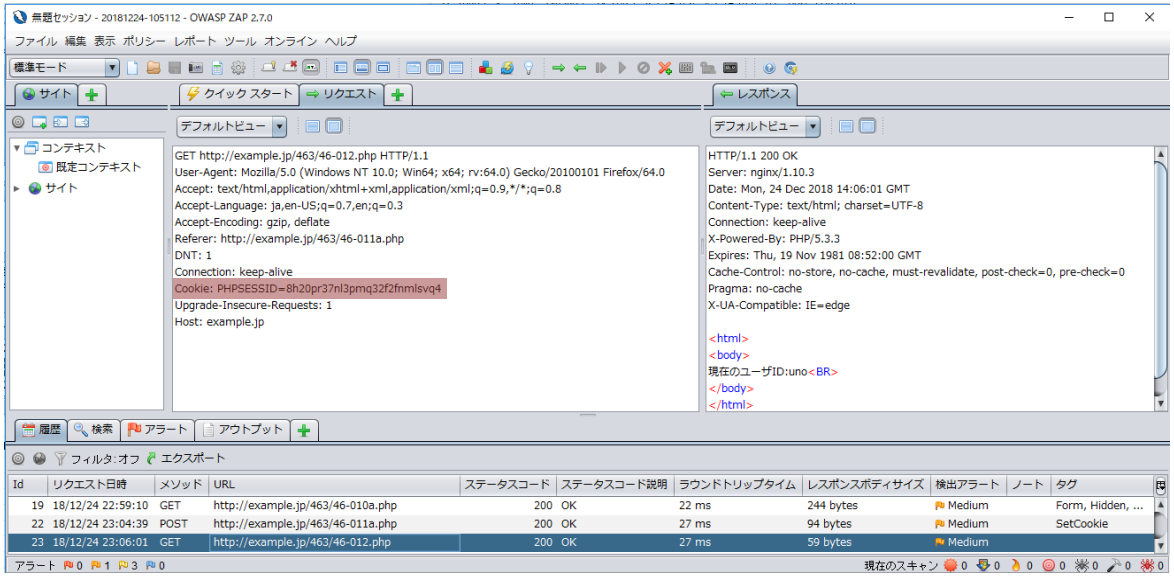
【ブラウザ→サーバ： リクエスト 463/46-010a.php → レスポンス 】セッションIDの固定化対策版(正常系)



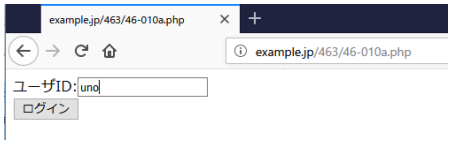
【ブラウザ→サーバ： リクエスト 463/46-011a.php → レスポンス 】セッションIDの固定化対策版(正常系)

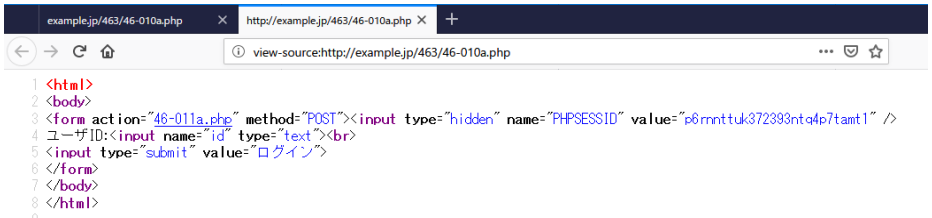


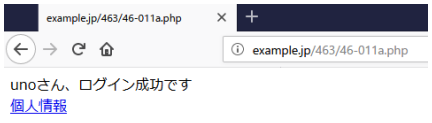
【ブラウザ→サーバ： リクエスト 463/46-012.php → レスポンス 】セッションIDの固定化対策版(正常系)

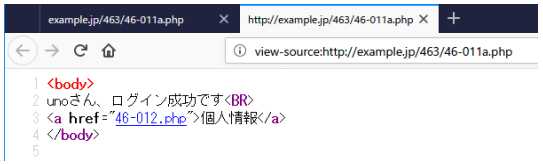


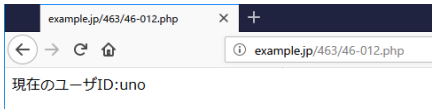
【ブラウザ】

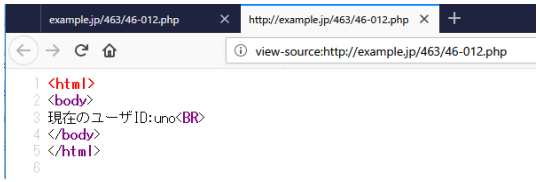

example.jp/463/46-010a.php
example.jp/463/46-010a.php
ユーザID:uno
ログイン


example.jp/463/46-010a.php
http://example.jp/463/46-010a.php
view-source:http://example.jp/463/46-010a.php
<html>
<body>
<form action="46-011a.php" method="POST"><input type="hidden" name="PHPSESSID" value="p6rnnttuk372393ntq4p7tamt1" />
ユーザID:<input name="id" type="text">
<input type="submit" value="ログイン">
</form>
</body>
</html>


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

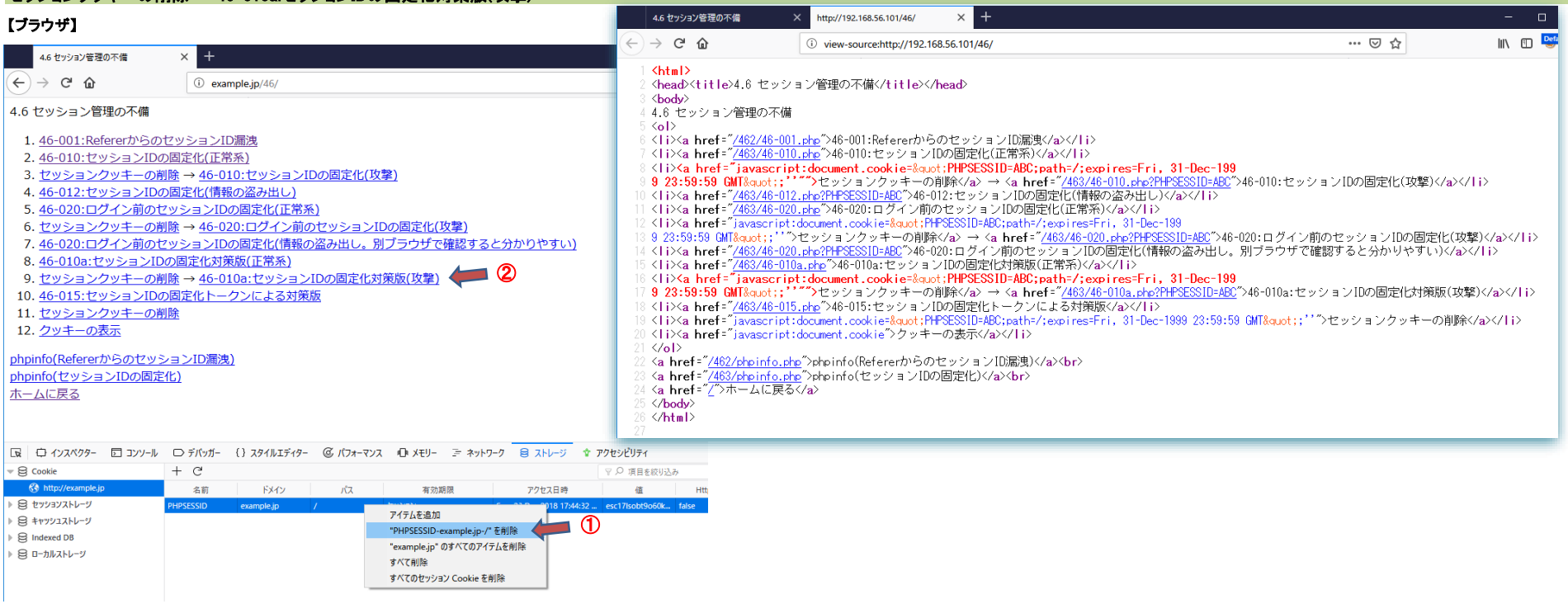

example.jp/463/46-011a.php
http://example.jp/463/46-011a.php
view-source:http://example.jp/463/46-011a.php
<body>
unoさん、ログイン成功です
個人情報
</body>


example.jp/463/46-012.php
example.jp/463/46-012.php
現在のユーザID:uno


example.jp/463/46-012.php
http://example.jp/463/46-012.php
view-source:http://example.jp/463/46-012.php
<html>
<body>
現在のユーザID:uno
</body>
</html>

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】



【サーバ： 463/46-010a.php 】

/var/www/html/463/46-010a.php - wasbook@example.jp - エディタ

```
<?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

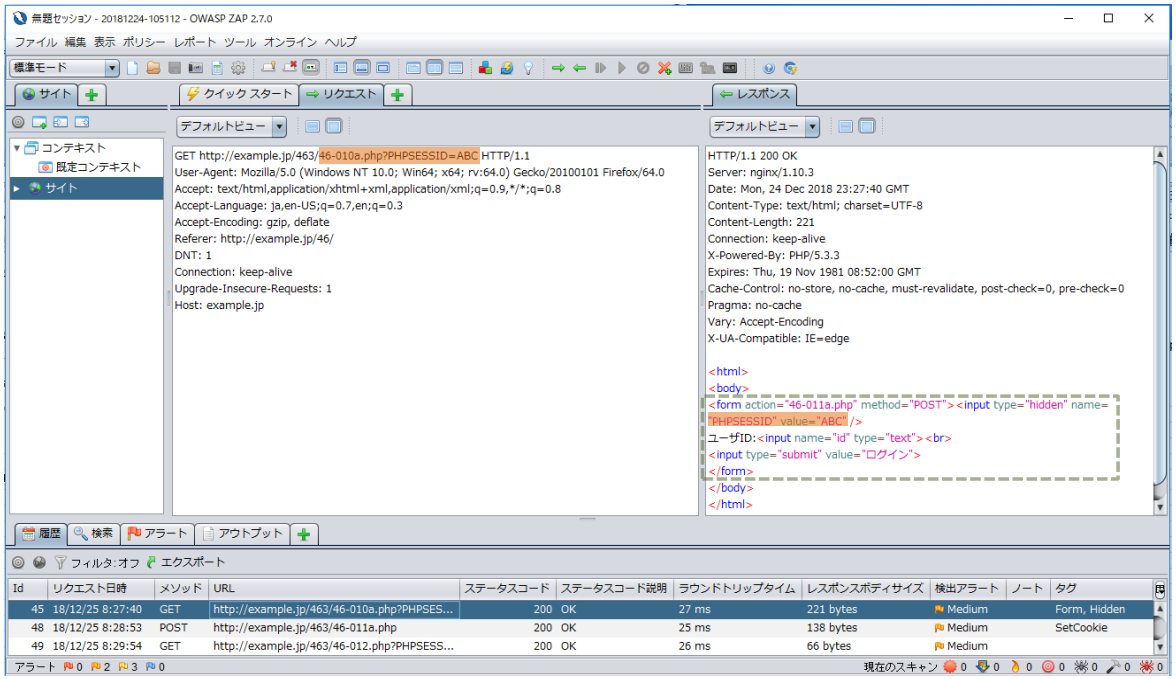
```
<?php
 session_start();
 $id = filter_input(INPUT_POST, 'id'); // 必ずログインに成功する（仕様）
 session_regenerate_id(true); // セッションIDの変更
 $_SESSION['id'] = $id; // ユーザIDをセッションに保存
?>
<body>
<?php echo htmlspecialchars($id, ENT_COMPAT, 'UTF-8'); ?>さん、ログイン成功です<BR>
<a href="46-012.php">個人情報</a>
</body>
```

【サーバ： 463/46-012.php 】

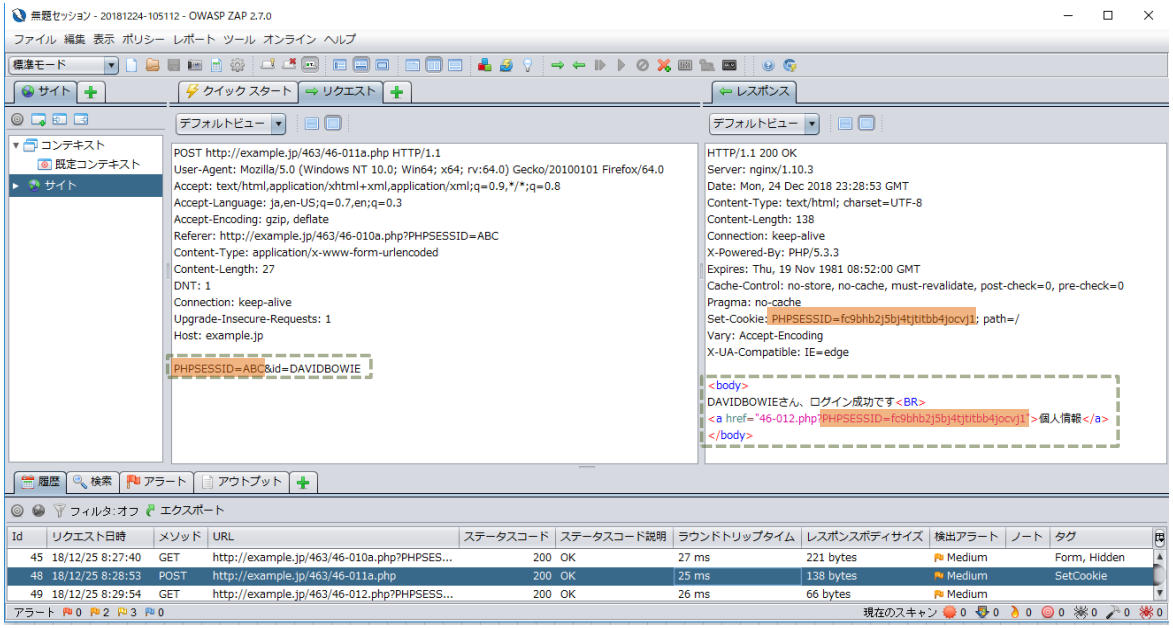
/var/www/html/463/46-012.php - wasbook@example.jp - エディタ - WinSCP

```
<?php
 session_start();
?>
<html>
<body>
現在のユーザID:<?php echo  htmlspecialchars(@$_SESSION['id'], ENT_COMPAT, 'UTF-8'); ?><BR>
</body>
</html>
```

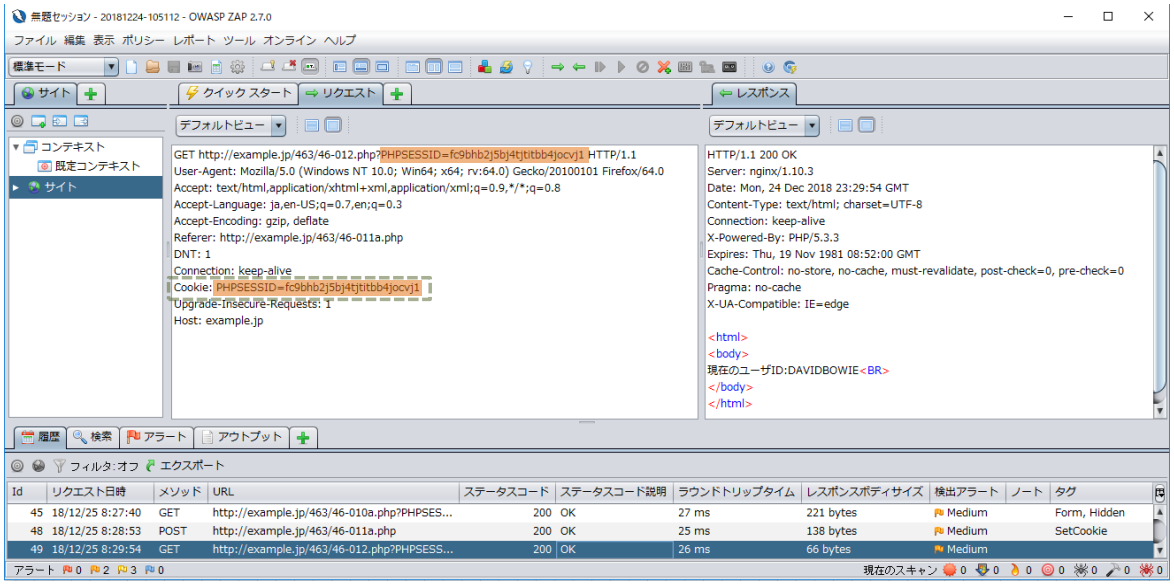
【ブラウザ→サーバ： リクエスト 463/46-010a.php → レスポンス 】セッションクッキーの削除 → 46-010a:セッションIDの固定化対策版(攻撃)



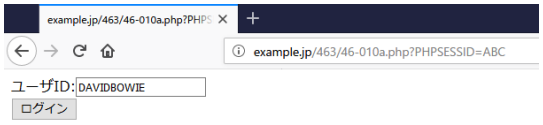
【ブラウザ→サーバ： リクエスト 463/46-011a.php → レスポンス 】セッションクッキーの削除 → 46-010a:セッションIDの固定化対策版(攻撃)

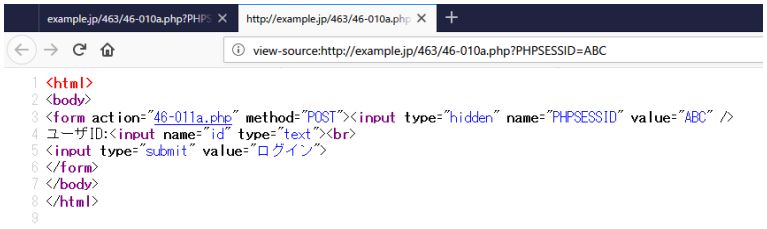


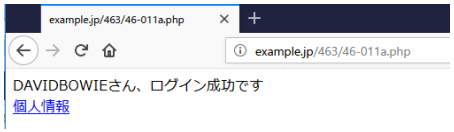
【ブラウザ→サーバ： リクエスト 463/46-012.php → レスポンス 】セッションクッキーの削除 → 46-010a:セッションIDの固定化対策版(攻撃)



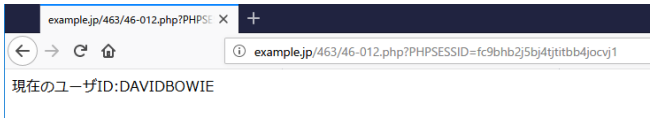
【ブラウザ】

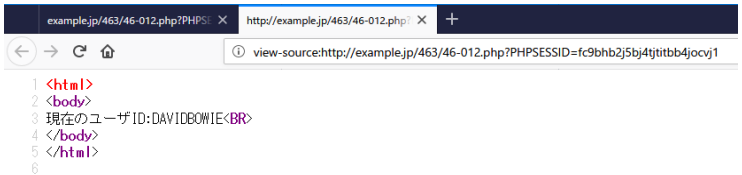

example.jp/463/46-010a.php?PHPS
example.jp/463/46-010a.php?PHPSESSID=ABC
ユーザID:DAVIDBOWIE
ログイン


example.jp/463/46-010a.php?PHPS
http://example.jp/463/46-010a.php
view-source:http://example.jp/463/46-010a.php?PHPSESSID=ABC
<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">
<input type="submit" value="ログイン">
</form>
</body>
</html>


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/463/46-011a.php
http://example.jp/463/46-011a.php
view-source:http://example.jp/463/46-011a.php
<body>
DAVIDBOWIEさん、ログイン成功です
個人情報
</body>


example.jp/463/46-012.php?PHPSE
example.jp/463/46-012.php?PHPSESSID=fc9bhb2j5bj4tjtitbb4jocvj1
現在のユーザID:DAVIDBOWIE


example.jp/463/46-012.php?PHPSE
http://example.jp/463/46-012.php
view-source:http://example.jp/463/46-012.php?PHPSESSID=fc9bhb2j5bj4tjtitbb4jocvj1
<html>
<body>
現在のユーザID:DAVIDBOWIE
</body>
</html>

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】

【サーバ: 462/46-015.php 】

/var/www/html/463/46-015.php - wasbook@example.jp - エディタ - WinSCP

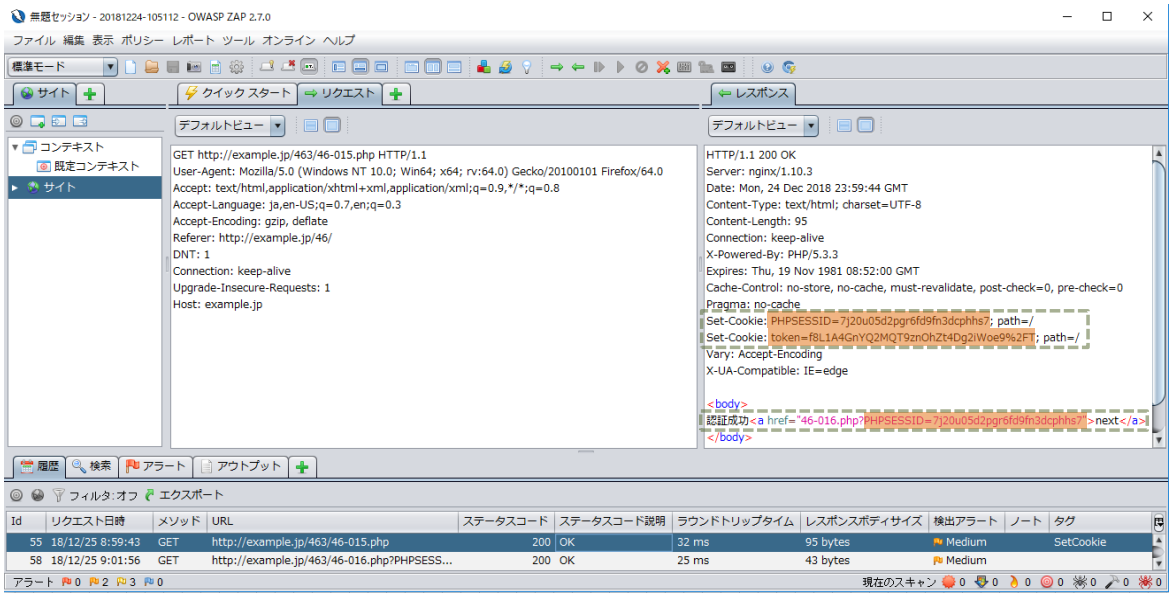
```php
k?php
// /dev/urandomによる疑似乱数生成器
function getToken() {
  // /dev/urandomから24バイト読み込み
  $s = file_get_contents('/dev/urandom', false, NULL, 0, 24);
  return base64_encode($s); // base64エンコードして返す
}

  // 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 】

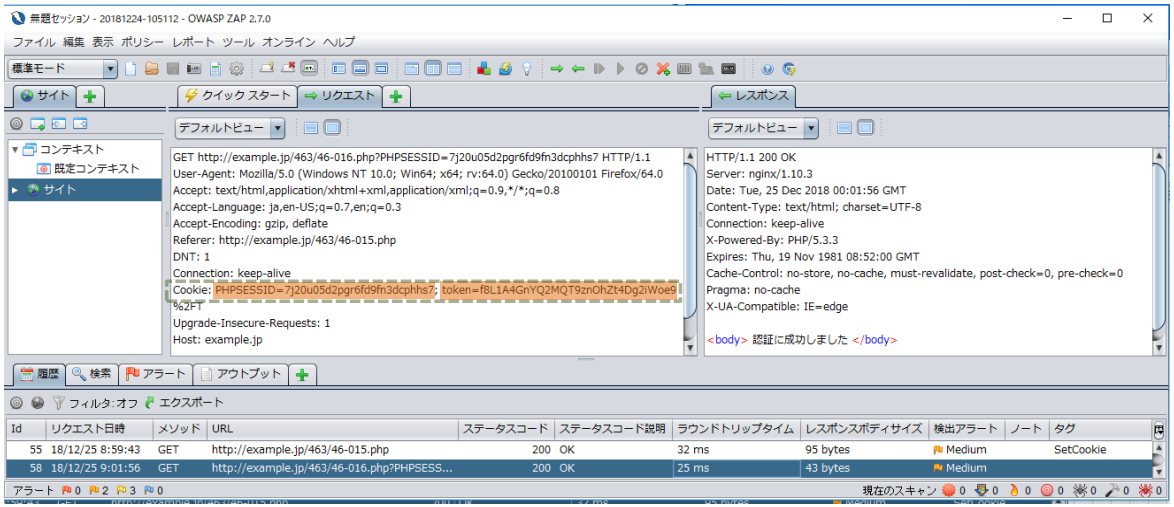
/var/www/html/463/46-016.php - wasbook@example.jp - エディタ - WinSCP

```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>
```

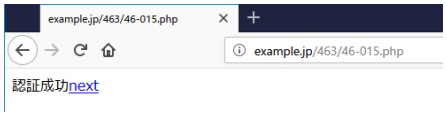
【ブラウザ→サーバ： リクエスト 463/46-015.php → レスポンス 】セッションIDの固定化トークンによる対策版



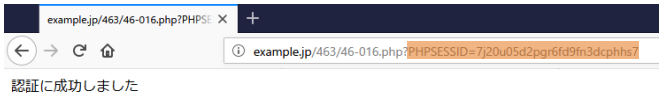
【ブラウザ→サーバ： リクエスト 463/46-016.php → レスポンス 】セッションIDの固定化トークンによる対策版

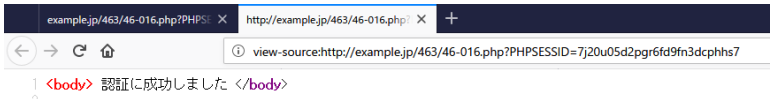


【ブラウザ】


example.jp/463/46-015.php
example.jp/463/46-015.php
認証成功next

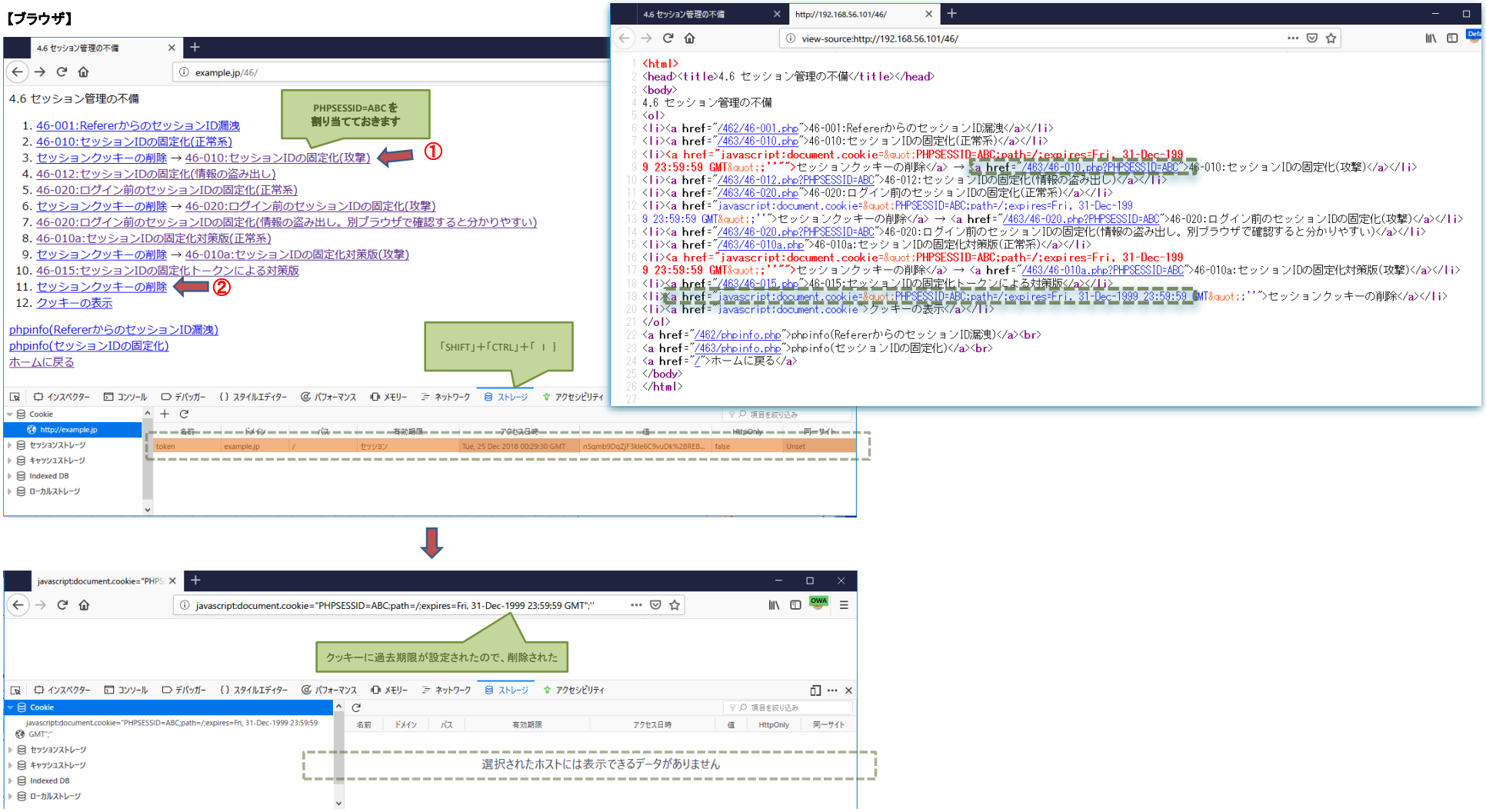

example.jp/463/46-015.php
http://example.jp/463/46-015.php
view-source:http://example.jp/463/46-015.php
<body>
認証成功next
</body>


example.jp/463/46-016.php?PHPSE
example.jp/463/46-016.php?PHPSESSID=7j20u05d2pgr6fd9fn3dcphhs7
認証に成功しました


example.jp/463/46-016.php?PHPSE
http://example.jp/463/46-016.php?
view-source:http://example.jp/463/46-016.php?PHPSESSID=7j20u05d2pgr6fd9fn3dcphhs7
<body> 認証に成功しました </body>

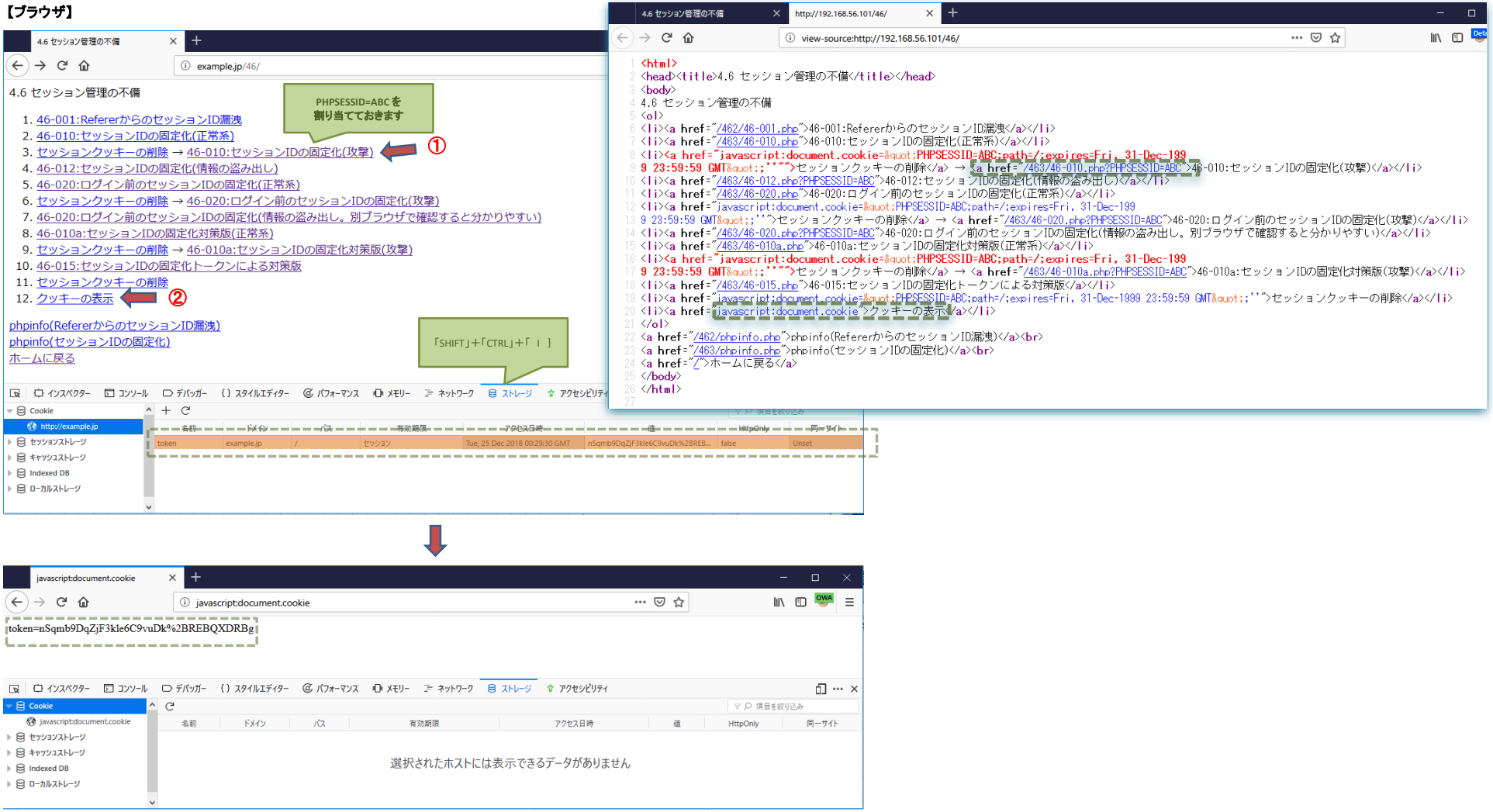
セッションクッキーの削除

【ブラウザ】



クッキーの表示

【ブラウザ】

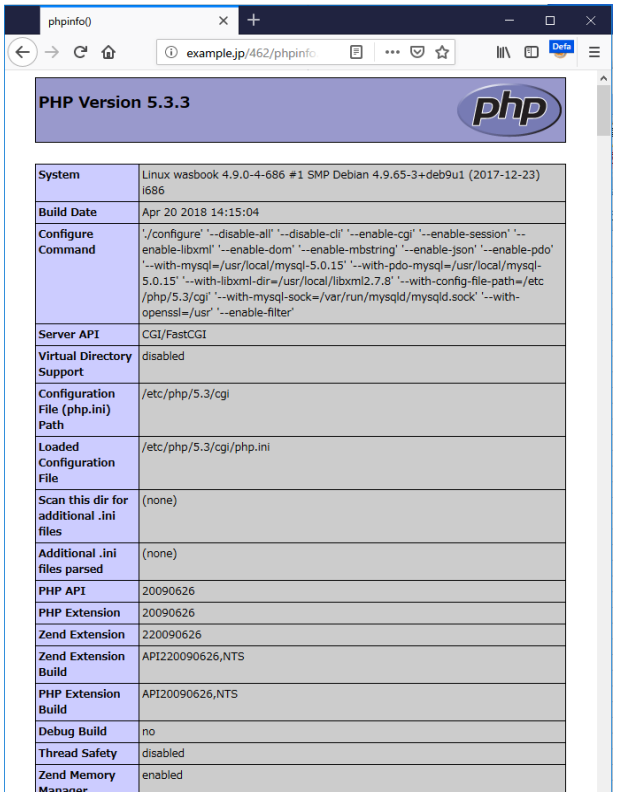


phpinfo

4.6 セッション管理の不備

1. 46-001:Refererからのセッション漏洩
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からのセッション漏洩)
phpinfo(セッションIDの固定化)
ホームに戻る



PHP Version 5.3.3

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

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

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	*no value*	*no value*
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	*no value*	*no value*

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 -lmysqlclient

Directive	Local Value	Master Value
mysql.allow_local_infile	On	On
mysql.allow_persistent	On	On
mysql.connect_timeout	60	60
mysql.default_host	*no value*	*no value*
mysql.default_password	*no value*	*no value*
mysql.default_port	*no value*	*no value*
mysql.default_socket	/var/run/mysqld/mysqld.sock	/var/run/mysqld/mysqld.sock
mysql.default_user	*no value*	*no value*
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	8.02 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

SPL support	enabled
Interfaces	Countable, OuterIterator, RecursiveIterator, SeekableIterator, SplObserver, SplSubject
Classes	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

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

Directive	Local Value	
assert.active	1	1
assert.bail	0	0
assert.callback	*no value*	*no value*
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	*no value*	*no value*

Additional Modules

Module Name

Environment

Variable	Value
GATEWAY_INTERFACE	CGI/1.1
HTTP_DNT	1
REMOTE_ADDR	127.0.0.1
QUERY_STRING	*no value*
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"]	*no value*
_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