

## 4-15 共有資源やキャッシュに関する問題

### 4.15.1 競合状態の脆弱性

#### 競合状態(レース・コンデション)の脆弱性

共有資源として、複数のプロセスやスレッドから同時に利用している変数、共有メモリ、ファイル、データベースなどの排他制御が不十分な場合、競合状態(レース・コンデション)の脆弱性が発生します

※ Java のサーブレットクラスのインスタンス変数は共有資源

#### 競合状態の脆弱性の影響

他人の個人情報などが画面に表示される(別人問題)  
データベースの不整合、ファイル内容破壊

#### 競合状態の脆弱性の対策

共有資源の利用を避ける  
共有資源の排他制御を行う

Javaの場合、変数名は、ローカル変数 String name に変える ※JSPも似た表記

Javaのマルチスレッド環境で排他制御を行うには、synchronized文やsynchronizedメソッドを使う

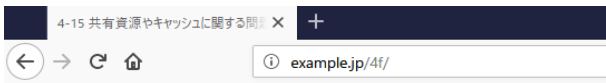
※ 待ち合わせが発生するので、サービス妨害攻撃の要因になります

※ JavaのSingleThreadModelインターフェイスはシングルスレッドで動くため、インスタンス変数をロックせずに済みますが、Servlet2.4以降では非推奨になっているので、今後は使用しないほうが無難

### C4e-001:3秒待ってユーザ名を表示(tanaka)

### C4e-001:3秒待ってユーザ名を表示(yamada)

#### 【ブラウザ】



#### 4-15 共有資源やキャッシュに関する問題

##### 4.15.1 競合状態の脆弱性

1. [C4e-001:3秒待ってユーザ名を表示\(tanaka\)](#)
2. [C4e-001:3秒待ってユーザ名を表示\(yamada\)](#)

左ブラウ

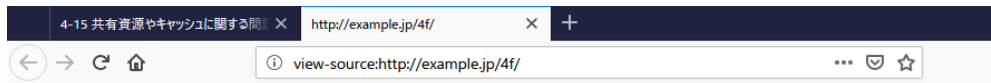
右ブラウ

##### 4.15.2 キャッシュからの情報漏洩

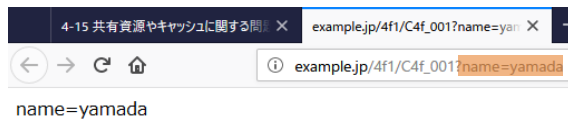
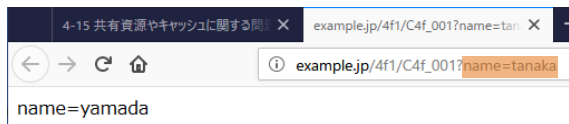
1. [4f-010 :ログインしてユーザ名を表示](#)
2. [4f-010 :ログインしてユーザ名を表示 \(過剰なキャッシュ\)](#)
3. [4e-011 :好みの色を表示\(正常系\)](#)
4. [4e-900:攻撃用クッキーの生成 \(攻撃\)](#)
5. [4e-010a:好みの色を示すクッキーの設定\(JSON版\)](#)
6. [4e-011a:好みの色を表示\(JSON版\)](#)

[phpinfo](#)

[ホームに戻る](#)



```
1 <html>
2 <head><title>4-15 共有資源やキャッシュに関する問題</title></head>
3 <body>
4 4-15 共有資源やキャッシュに関する問題
5 <ul>
6 <li>4.15.1 競合状態の脆弱性</li>
7 <ol>
8 <li><a href="/4f1/C4f_001?name=tanaka" target="_blank">C4e-001:3秒待ってユーザ名を表示(tanaka)</a></li>
9 <li><a href="/4f1/C4f_001?name=yamada" target="_blank">C4e-001:3秒待ってユーザ名を表示(yamada)</a></li>
10 </ol>
11 <li>4.15.2 キャッシュからの情報漏洩</li>
12 <ol>
13 <li><a href="/4f-010.html">4f-010 :ログインしてユーザ名を表示</a></li>
14 <li><a href="/4f3/4f-010.html">4f-010 :ログインしてユーザ名を表示 (過剰なキャッシュ) </a></li>
15 <li><a href="/4e-011.php">4e-011 :好みの色を表示(正常系)</a></li>
16 <li><a href="http://trap.example.com/4e/4e-900.php">4e-900:攻撃用クッキーの生成 (攻撃) </a></li>
17 <li><a href="/4e-010a.php">4e-010a:好みの色を示すクッキーの設定(JSON版)</a></li>
18 <li><a href="/4e-011a.php">4e-011a:好みの色を表示(JSON版)</a></li>
19 </ol>
20 </ul>
21 <a href="/phpinfo.php">phpinfo</a><br>
22 <a href="/">ホームに戻る</a>
23 </body>
24 </html>
```



### 【サーバ: 4f/C4f\_001.java】

`/var/www/html/4f/C4f_001.java - wasbook@example.jp - エディタ - WinSCP`

```
import java.io.*;
import javax.servlet.http.*;
import org.apache.commons.lang3.StringEscapeUtils;

public class C4f_001 extends HttpServlet {
    String name; // インスタンス変数として宣言
    protected void doGet(HttpServletRequest req,
        HttpServletResponse res)
        throws IOException {
        PrintWriter out = res.getWriter();
        out.print("<body>name=");
        try {
            name = req.getParameter("name"); // クエリストリングname
            Thread.sleep(3000); // 3秒待つ (時間のかかる処理のつもり)
            out.print(StringEscapeUtils.escapeHtml4(name)); // ユーザ名の表示
            // out.print(name); // ユーザ名の表示
        } catch (InterruptedException e) {
            out.println(e);
        }
        out.println("</body>");
        out.close();
    }
}
```

【ブラウザ→サーバ: リクエスト 4f/C4f\_001.java(左ブラウザ) → レスポンス】

The screenshot shows the OWASP ZAP 2.7.0 interface. The 'Request' pane on the left displays the following details:

```

GET http://example.jp/4f1/C4f_001?name=tanaka 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/4f/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp
    
```

The 'Response' pane on the right displays the following details:

```

HTTP/1.1 200
Server: nginx/1.10.3
Date: Sat, 05 Jan 2019 13:21:36 GMT
Content-Length: 25
Connection: keep-alive

<body>name=yamada</body>
    
```

The table below the interface shows the request and response details:

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...	検出アラ...	ノート	タグ
8	19/01/05 22:2...	GET	http://example.jp/4f1/C4f_001?name=tanaka	200		3.01 s	25 bytes	Low		
11	19/01/05 22:2...	GET	http://example.jp/4f1/C4f_001?name=yamada	200		3.02 s	25 bytes	Low		

【ブラウザ→サーバ: リクエスト 4f/C4f\_001.java(右ブラウザ) → レスポンス】

The screenshot shows the OWASP ZAP 2.7.0 interface. The 'Request' pane on the left displays the following details:

```

GET http://example.jp/4f1/C4f_001?name=yamada 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/4f/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp
    
```

The 'Response' pane on the right displays the following details:

```

HTTP/1.1 200
Server: nginx/1.10.3
Date: Sat, 05 Jan 2019 13:21:37 GMT
Content-Length: 25
Connection: keep-alive

<body>name=yamada</body>
    
```

The table below the interface shows the request and response details:

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...	検出アラ...	ノート	タグ
8	19/01/05 22:2...	GET	http://example.jp/4f1/C4f_001?name=tanaka	200		3.01 s	25 bytes	Low		
11	19/01/05 22:2...	GET	http://example.jp/4f1/C4f_001?name=yamada	200		3.02 s	25 bytes	Low		

## 4.15.2 キャッシュからの情報漏洩

### キャッシュからの情報漏洩の脆弱性

Webアプリケーションは処理高速化や負荷軽減のために、多くの箇所でキャッシュを使いますが、キャッシュが過剰に働くと個人情報漏洩などの原因になる場合があります

#### キャッシュからの情報漏洩の影響

他人の個人情報などが画面に表示される(別人問題)

#### キャッシュからの情報漏洩の原因

##### アプリケーション側のキャッシュ機能不備

Cache-Controlヘッダのキャッシュ方法の種類(ディレクティブ)

ディレクティブ	説明
no-store	全くキャッシュしない
no-cache	キャッシュの有効性を毎回、サーバに確認する
private	1人のユーザのためのキャッシュを許可する。典型的にはブラウザのキャッシュは許可するが、キャッシュサーバのキャッシュは許可しない。
public	全てのキャッシュを保存する。
must-revalidate	リソースを使う場合にキャッシュが無効化していないことを確認する
max-age	キャッシュの有効期限を設定する(秒数)

PHPの session cache limiter関数は「public」指定で、以下ヘッダを返す

```
Expires: session.cache_expireだけ未来の日時  
Cache-Control: public,max-age=session.cache_expireを分⇒秒の数値
```

##### キャッシュサーバ側のキャッシュ機能不備

```
proxy ignore headers Cache-Control Expires Set-Cookie;
```

(Cache-Control Expires Set-Cookie)を無視する。アプリ側の設定を無視して、キャッシュサーバ側の設定を返す。(/etc/nginx/conf.d/defaultなどの設定)

#### キャッシュからの情報漏洩の対策

リバースプロキシの他に、CDNやロードバランサもキャッシュ機能があるので、インフラ担当者との調整が必要

##### アプリケーション側の対策

ブラウザやキャッシュサーバの挙動を検討し、適切と思われる設定は以下である。Pragma:no-cache は古いソフト用伝統的記法だが、絶対安全ではない。

```
Cache-Control: private,no-store,no-cache,must-revalidate  
Pragma: no-cache
```

PHP対策(ただし、デフォルト設定)

```
session_cache_limiter('nocache');
```

レスポンス

→

```
Cache-Control: no-store,no-cache,must-revalidate,post-check=0,  
pre-check=0  
Pragma: no-cache
```

※ private 設定されないが、通常はこれで問題ない。  
キャッシュサーバやCDN側が必要な場合は別途、header関数で設定するとよい。

##### キャッシュサーバ側のキャッシュ対策

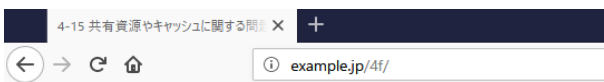
```
proxy ignore headers Cache-Control Expires Set-Cookie; #この行を削除
```

#### URLに乱数を付与する対策(キャッシュバスタ)

キャッシュはURL毎に別リソースとして扱われるので、URLを強制的に変えることで、キャッシュ経由の情報漏洩を防止できます  
ただし、キャッシュ用ストレージの無駄使いであり、URLが知られると情報漏洩につながります

## 4f-010 :ログインしてユーザ名を表示

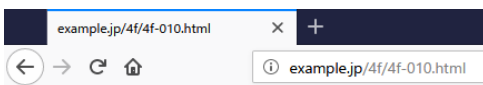
### 【ブラウザ】



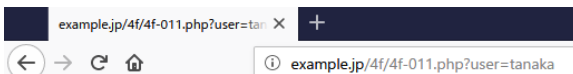
#### 4-15 共有資源やキャッシュに関する問題

- 4.15.1 競合状態の脆弱性
  - C4e-001:3秒待ってユーザ名を表示(tanaka)
  - C4e-001:3秒待ってユーザ名を表示(yamada)
- 4.15.2 キャッシュからの情報漏洩
  - 4f-010 :ログインしてユーザ名を表示
  - 4f-010 :ログインしてユーザ名を表示 (過剰なキャッシュ)
  - 4e-011 :好みの色を表示(正常系)
  - 4e-900:攻撃用クッキーの生成 (攻撃)
  - 4e-010a:好みの色を示すクッキーの設定(JSON版)
  - 4e-011a:好みの色を表示(JSON版)

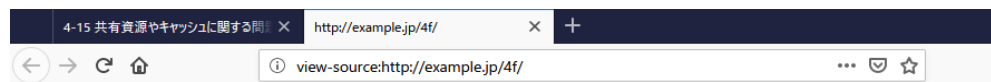
[phpinfo](#)  
[ホームに戻る](#)



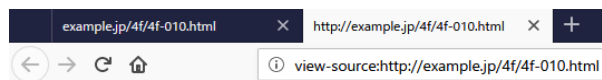
[田中でログイン](#)  
[山田でログイン](#)



ログインしました(tanaka)  
[マイページ \(キャッシュなし\)](#)  
[マイページ \(キャッシュあり\)](#)



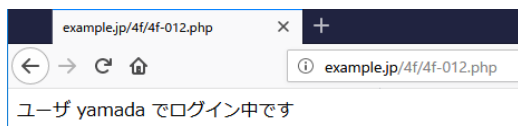
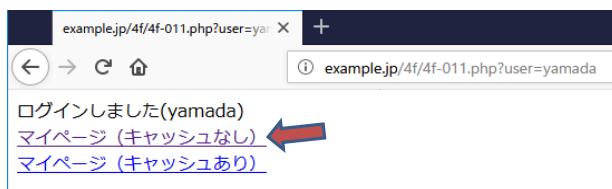
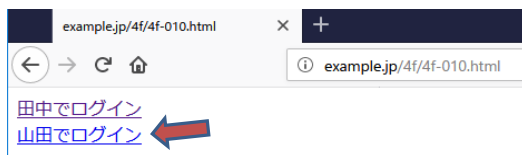
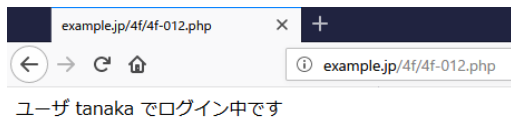
```
1 <html>
2 <head><title>4-15 共有資源やキャッシュに関する問題</title></head>
3 <body>
4 4-15 共有資源やキャッシュに関する問題
5 <ul>
6 <li>4.15.1 競合状態の脆弱性</li>
7 <ol>
8 <li><a href="/4f1/C4f_001?name=tanaka" target="_blank">C4e-001:3秒待ってユーザ名を表示(tanaka)</a></li>
9 <li><a href="/4f1/C4f_001?name=yamada" target="_blank">C4e-001:3秒待ってユーザ名を表示(yamada)</a></li>
10 </ol>
11 <li>4.15.2 キャッシュからの情報漏洩</li>
12 <ol>
13 <li><a href="4f-010.html">4f-010 :ログインしてユーザ名を表示</a></li>
14 <li><a href="4f3/4f-010.html">4f-010 :ログインしてユーザ名を表示 (過剰なキャッシュ) </a></li>
15 <li><a href="4e-011.php">4e-011 :好みの色を表示(正常系)</a></li>
16 <li><a href="http://trap.example.com/4e/4e-900.php">4e-900:攻撃用クッキーの生成 (攻撃) </a></li>
17 <li><a href="4e-010a.php">4e-010a:好みの色を示すクッキーの設定(JSON版)</a></li>
18 <li><a href="4e-011a.php">4e-011a:好みの色を表示(JSON版)</a></li>
19 </ol>
20 </ul>
21 <a href="phpinfo.php">phpinfo</a><br>
22 <a href="/">ホームに戻る</a>
23 </body>
24 </html>
```



```
1 <body>
2 <a href="4f-011.php?user=tanaka">田中でログイン</a><br>
3 <a href="4f-011.php?user=yamada">山田でログイン</a>
4 </body>
```



```
1 <body>ログインしました(tanaka)<br><a href="4f-012.php">マイページ (キャッシュなし) </a><br><a href="4f-012a.php">マイページ (キャッシュあり) </a></body>
```



#### 【サーバ: 4f/4f\_010.html 】

```
/var/www/html/4f/4f-010.html - wasbook@example.jp - エディタ - WinSCP  
<body>  
<a href="4f-011.php?user=tanaka">田中でログイン</a><br>  
<a href="4f-011.php?user=yamada">山田でログイン</a>  
</body>
```

#### 【サーバ: 4f/4f\_011.php 】

```
/var/www/html/4f/4f-011.php - wasbook@example.jp - エディタ - WinSCP  
<body><?php  
$user = $_GET['user'];  
if ($user === 'tanaka' || $user === 'yamada') {  
    session_start();  
    session_regenerate_id(true);  
    $_SESSION['user'] = $user;  
    echo 'ログインしました(' . htmlspecialchars($user) . ')<br>';  
    echo '<a href="4f-012.php">マイページ (キャッシュなし) </a><br>';  
    echo '<a href="4f-012a.php">マイページ (キャッシュあり) </a>';  
} else {  
    echo 'ユーザ名が違います';  
}  
>>  
</body>
```

## 【サーバ: 4f/4f\_012.php 】

```
/var/www/html/4f/4f-012.php - wasbook@example.jp - エディタ - WinSCP
kbody><?php
session_start();
if (empty($_SESSION['user'])) {
    die("ログインしていません");
}
echo "ユーザ ".$_SESSION['user'] でログイン中です";
?></body>
```

## 【サーバ: 4f/4f\_012a.php 】

```
/var/www/html/4f/4f-012a.php - wasbook@example.jp - エディタ - WinSCP
kbody><?php
session_cache_limiter('public');
session_cache_expire(1);
session_start();
if (empty($_SESSION['user'])) {
    die("ログインしていません");
}
echo "ユーザ ".$_SESSION['user'] でログイン中です";
?></body>
```

PHPの session\_cache\_limiter関数は「public」指定で、以下ヘッダを返す  
Expires: session\_cache\_expireだけ未来の日時  
Cache-Control: public,max-age=session\_cache\_expireを分⇒秒の数値

## 【ブラウザ→サーバ: リクエスト 4f/4f-010.html → レスポンス 】

無題セッション - 20190105-221150 - 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

GET http://example.jp/4f/4f-010.html HTTP/1.1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Language: ja,en-US;q=0.7,en;q=0.3  
Accept-Encoding: gzip, deflate  
Referer: http://example.jp/4f/  
DNT: 1  
Connection: keep-alive  
Upgrade-Insecure-Requests: 1  
Host: example.jp

HTTP/1.1 200 OK  
Server: nginx/1.10.3  
Date: Sat, 05 Jan 2019 13:52:41 GMT  
Content-Type: text/html; charset=UTF-8  
Content-Length: 137  
Connection: keep-alive  
Last-Modified: Mon, 14 May 2018 13:08:18 GMT  
ETag: "89-56c2a2de8b816-gzip"  
Vary: Accept-Encoding  
X-UA-Compatible: IE=edge  
Accept-Ranges: bytes

```
<body>
<a href="4f-011.php?user=tanaka">田中でログイン</a><br>
<a href="4f-011.php?user=yamada">山田でログイン</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	ステータススコ...	ステータスコ...	ラウンドトリップ...	レスポンスボディサ...	検出アラ...	ノート	タグ
32	19/01/05 22:5...	GET	http://example.jp/4f/4f-010.html	200	OK	13 ms	137 bytes	Medium		
35	19/01/05 22:5...	GET	http://example.jp/4f/4f-011.php?user=tanaka	200	OK	23 ms	189 bytes	Medium	SetC...	
36	19/01/05 22:5...	GET	http://example.jp/4f/4f-012.php	200	OK	26 ms	55 bytes	Medium		
37	19/01/05 22:5...	GET	http://example.jp/4f/4f-011.php?user=yamada	200	OK	23 ms	189 bytes	Medium	SetC...	
38	19/01/05 22:5...	GET	http://example.jp/4f/4f-012.php	200	OK	29 ms	55 bytes	Medium		

アラート 0 1 3 0 0 現在のスキャン 0 0 0 0 0 0 0 0 0 0 0

【ブラウザ→サーバ: リクエスト 4f/4f-011.php → レスポンス】

無題セッション - 20190105-221150 - 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

```
GET http://example.jp/4f/4f-011.php?user=tanaka 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/4f/4f-010.html
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Sat, 05 Jan 2019 13:54:06 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 189
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: PHPSESSID=femotcnq27ffgu4emq067gd62; path=/
Set-Cookie: PHPSESSID=879s2odnkuqc49qu01s9v0oui2; path=/
Vary: Accept-Encoding
X-UA-Compatible: IE=edge
```

```
<body>ログインしました(tanaka)<br><a href="4f-012.php">
マイページ (キャッシュなし) </a><br><a href="4f-012a.php">
マイページ (キャッシュあり) </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...	レスポンスボディサ...	検出アラ...	ノート	タグ
32	19/01/05 22:5...	GET	http://example.jp/4f/4f-010.html	200	OK	13 ms	137 bytes	Medium		
35	19/01/05 22:5...	GET	http://example.jp/4f/4f-011.php?user=tanaka	200	OK	23 ms	189 bytes	Medium	SetC...	
36	19/01/05 22:5...	GET	http://example.jp/4f/4f-012.php	200	OK	26 ms	55 bytes	Medium		
37	19/01/05 22:5...	GET	http://example.jp/4f/4f-011.php?user=yamada	200	OK	23 ms	189 bytes	Medium	SetC...	
38	19/01/05 22:5...	GET	http://example.jp/4f/4f-012.php	200	OK	29 ms	55 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 4f/4f-012.php → レスポンス】

無題セッション - 20190105-221150 - 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

```
GET http://example.jp/4f/4f-012.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/4f/4f-011.php?user=tanaka
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=879s2odnkuqc49qu01s9v0oui2
Upgrade-Insecure-Requests: 1
Host: example.jp
```

レスポンス

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Sat, 05 Jan 2019 13:55:59 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
X-UA-Compatible: IE=edge

<body>ユーザ tanaka でログイン中です</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...	レスポンスボディサ...	検出アラ...	ノート	タグ
32	19/01/05 22:5...	GET	http://example.jp/4f/4f-010.html	200	OK	13 ms	137 bytes	Medium		
35	19/01/05 22:5...	GET	http://example.jp/4f/4f-011.php?user=tanaka	200	OK	23 ms	189 bytes	Medium	SetC...	
36	19/01/05 22:5...	GET	http://example.jp/4f/4f-012.php	200	OK	26 ms	55 bytes	Medium		
37	19/01/05 22:5...	GET	http://example.jp/4f/4f-011.php?user=yamada	200	OK	23 ms	189 bytes	Medium	SetC...	
38	19/01/05 22:5...	GET	http://example.jp/4f/4f-012.php	200	OK	29 ms	55 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 4f/4f-011.php → レスポンス】

無題セッション - 20190105-221150 - 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

GET http://example.jp/4f/4f-011.php?user=yamada 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/4f/4f-010.html  
 DNT: 1  
 Connection: keep-alive  
 Cookie: PHPSESSID=879s2odnkuqc49qu01s9v0oui2  
 Upgrade-Insecure-Requests: 1  
 Host: example.jp

HTTP/1.1 200 OK  
 Server: nginx/1.10.3  
 Date: Sat, 05 Jan 2019 13:57:10 GMT  
 Content-Type: text/html; charset=UTF-8  
 Content-Length: 189  
 Connection: keep-alive  
 X-Powered-By: PHP/5.3.3  
 Expires: Thu, 19 Nov 1981 08:52:00 GMT  
 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0  
 Pragma: no-cache  
 Set-Cookie: PHPSESSID=gvmrob1glf6oc8qvg12i0fttu2; path=/  
 Vary: Accept-Encoding  
 X-UA-Compatible: IE=edge

<body>ログインしました(yamada)<br><a href="4f-012.php">マイページ (キャッシュなし) </a><br><a href="4f-012a.php">マイページ (キャッシュあり) </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...	レスポンスボディサ...	検出アラ...	ノート	タグ
32	19/01/05 22:5...	GET	http://example.jp/4f/4f-010.html	200	OK	13 ms	137 bytes	Medium		
35	19/01/05 22:5...	GET	http://example.jp/4f/4f-011.php?user=tanaka	200	OK	23 ms	189 bytes	Medium	SetC...	
36	19/01/05 22:5...	GET	http://example.jp/4f/4f-012.php	200	OK	26 ms	55 bytes	Medium		
37	19/01/05 22:5...	GET	http://example.jp/4f/4f-011.php?user=yamada	200	OK	23 ms	189 bytes	Medium	SetC...	
38	19/01/05 22:5...	GET	http://example.jp/4f/4f-012.php	200	OK	29 ms	55 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 4f/4f-012.php → レスポンス】

無題セッション - 20190105-221150 - 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

```
GET http://example.jp/4f/4f-012.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/4f/4f-011.php?user=yamada
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=gymrob1glf6oc8qvg2i0ftu2
Upgrade-Insecure-Requests: 1
Host: example.jp
```

レスポンス

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Sat, 05 Jan 2019 13:57:40 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
X-UA-Compatible: IE=edge

<body>ユーザ yamada でログイン中です</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

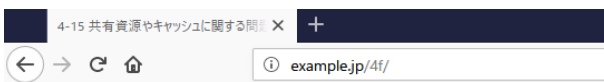
Id	リクエスト日時	メソ...	URL	ステータスコ...	ステータスコード...	ラウンドトリップ...	レスポンスボディサ...	検出アラ...	ノート	タグ
32	19/01/05 22:5...	GET	http://example.jp/4f/4f-010.html	200	OK	13 ms	137 bytes	Medium		
35	19/01/05 22:5...	GET	http://example.jp/4f/4f-011.php?user=tanaka	200	OK	23 ms	189 bytes	Medium	SetC...	
36	19/01/05 22:5...	GET	http://example.jp/4f/4f-012.php	200	OK	26 ms	55 bytes	Medium		
37	19/01/05 22:5...	GET	http://example.jp/4f/4f-011.php?user=yamada	200	OK	23 ms	189 bytes	Medium	SetC...	
38	19/01/05 22:5...	GET	http://example.jp/4f/4f-012.php	200	OK	29 ms	55 bytes	Medium		

アラート 0 0 1 3 0

現在のスキャン 0 0 0 0 0 0 0 0

## 4f-010 :ログインしてユーザ名を表示(過剰なキャッシュ)

### 【ブラウザ】

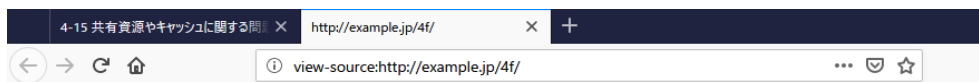


#### 4-15 共有資源やキャッシュに関する問題

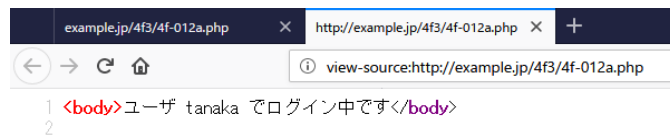
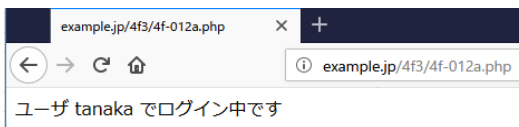
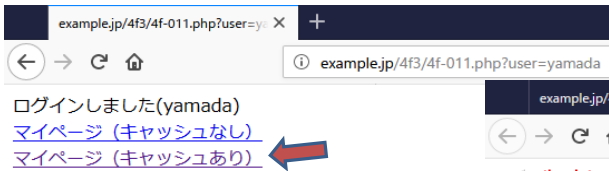
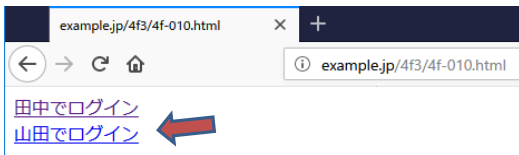
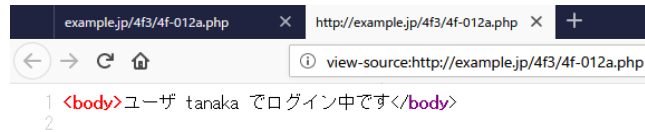
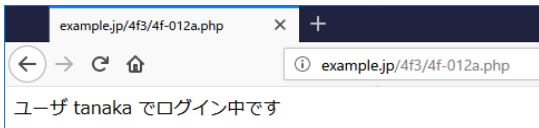
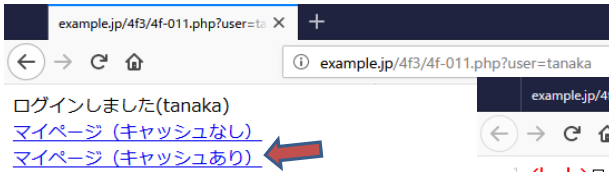
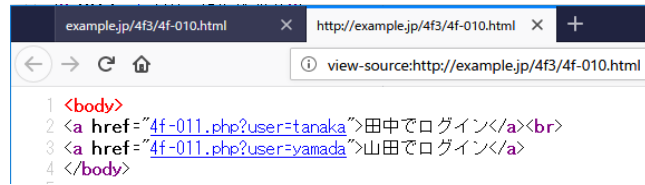
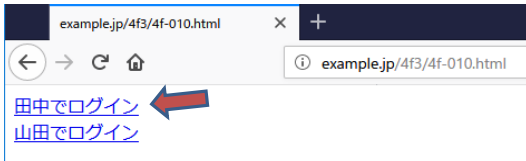
- 4.15.1 競合状態の脆弱性
  1. [C4e-001:3秒待ってユーザ名を表示\(tanaka\)](#)
  2. [C4e-001:3秒待ってユーザ名を表示\(yamada\)](#)
- 4.15.2 キャッシュからの情報漏洩
  1. [4f-010 :ログインしてユーザ名を表示](#)
  2. [4f-010 :ログインしてユーザ名を表示\(過剰なキャッシュ\)](#)
  3. [4e-011 :好みの色を表示\(正常系\)](#)
  4. [4e-900:攻撃用クッキーの生成\(攻撃\)](#)
  5. [4e-010a:好みの色を示すクッキーの設定\(JSON版\)](#)
  6. [4e-011a:好みの色を表示\(JSON版\)](#)

[phpinfo](#)

[ホームに戻る](#)



```
1 <html>
2 <head><title>4-15 共有資源やキャッシュに関する問題</title></head>
3 <body>
4 4-15 共有資源やキャッシュに関する問題
5 <ul>
6 <li>4.15.1 競合状態の脆弱性</li>
7 <ol>
8 <li><a href="/4f1/C4f_001?name=tanaka" target="_blank">C4e-001:3秒待ってユーザ名を表示(tanaka)</a></li>
9 <li><a href="/4f1/C4f_001?name=yamada" target="_blank">C4e-001:3秒待ってユーザ名を表示(yamada)</a></li>
10 </ol>
11 <li>4.15.2 キャッシュからの情報漏洩</li>
12 <ol>
13 <li><a href="/4f-010.html">4f-010 :ログインしてユーザ名を表示</a></li>
14 <li><a href="/4f3/4f-010.html">4f-010 :ログインしてユーザ名を表示(過剰なキャッシュ)</a></li>
15 <li><a href="4e-011.php">4e-011 :好みの色を表示(正常系)</a></li>
16 <li><a href="http://trap.example.com/4e/4e-900.php">4e-900:攻撃用クッキーの生成(攻撃)</a></li>
17 <li><a href="4e-010a.php">4e-010a:好みの色を示すクッキーの設定(JSON版)</a></li>
18 <li><a href="4e-011a.php">4e-011a:好みの色を表示(JSON版)</a></li>
19 </ol>
20 </ul>
21 <a href="phpinfo.php">phpinfo</a><br>
22 <a href="/">ホームに戻る</a>
23 </body>
24 </html>
~>
```



### 【サーバ: 4f/4f\_010.html 】

```
/var/www/html/4f/4f-010.html - wasbook@example.jp - エディタ - WinSCP
kbody>
<a href="4f-011.php?user=tanaka">田中でログイン</a><br>
<a href="4f-011.php?user=yamada">山田でログイン</a>
</body>
```

### 【サーバ: 4f/4f\_012.php 】

```
/var/www/html/4f/4f-012.php - wasbook@example.jp - エディタ - WinSCP
kbody><?php
session_start();
if (empty($_SESSION['user'])) {
    die("ログインしていません");
}
echo "ユーザ {$_SESSION['user']} でログイン中です";
?></body>
```

### 【サーバ: 4f/4f\_011.php 】

```
/var/www/html/4f/4f-011.php - wasbook@example.jp - エディタ - WinSCP
kbody><?php
$user = $_GET['user'];
if ($user === 'tanaka' || $user === 'yamada') {
    session_start();
    session_regenerate_id(true);
    $_SESSION['user'] = $user;
    echo 'ログインしました(' . htmlspecialchars($user) . ')<br>';
    echo '<a href="4f-012.php">マイページ (キャッシュなし) </a><br>';
    echo '<a href="4f-012a.php">マイページ (キャッシュあり) </a>';
} else {
    echo 'ユーザ名が違います';
}
?>
</body>
```

### 【サーバ: 4f/4f\_012a.php 】

```
/var/www/html/4f/4f-012a.php - wasbook@example.jp - エディタ - WinSCP
kbody><?php
session_cache_limiter('public');
session_cache_expire(1);
session_start();
if (empty($_SESSION['user'])) {
    die("ログインしていません");
}
echo "ユーザ {$_SESSION['user']} でログイン中です";
?></body>
```

PHPの `session_cache_limiter` 関数は「public」指定で、以下ヘッダを返す  
Expires: session.cache\_expireだけ未来の日時  
Cache-Control: public,max-age=session.cache\_expireを分⇒秒の数値

【ブラウザ→サーバ: リクエスト 4f/4f-010.html → レスポンス】

無題セッション - 20190105-221150 - 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

```

GET http://example.jp/4f3/4f-010.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://example.jp/4f/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp
    
```

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Sat, 05 Jan 2019 14:35:40 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 137
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: "89-56c2a2de8b816-gzip"
Vary: Accept-Encoding
X-UA-Compatible: IE=edge
Accept-Ranges: bytes

<body>
<a href="4f-011.php?user=tanaka">田中でログイン</a><br>
<a href="4f-011.php?user=yamada">山田でログイン</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...	レスポンスボディサ...	検出アラ...	ノート	タグ
57	19/01/05 23:3...	GET	http://example.jp/4f3/4f-010.html	200	OK	3 ms	137 bytes	Medium		
58	19/01/05 23:3...	GET	http://example.jp/4f3/4f-011.php?user=tanaka	200	OK	4 ms	189 bytes	Medium	SetC...	
59	19/01/05 23:3...	GET	http://example.jp/4f3/4f-012a.php	200	OK	23 ms	55 bytes	Medium		
60	19/01/05 23:3...	GET	http://example.jp/4f3/4f-011.php?user=yamada	200	OK	31 ms	189 bytes	Medium	SetC...	

アラート 0 0 0 0 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 4f/4f-011.php → レスポンス】

無題セッション - 20190105-221150 - 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

GET http://example.jp/4f3/4f-011.php?user=tanaka 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/4f3/4f-010.html  
DNT: 1  
Connection: keep-alive  
Upgrade-Insecure-Requests: 1  
Host: example.jp

HTTP/1.1 200 OK  
Server: nginx/1.10.3  
Date: Sat, 05 Jan 2019 14:35:57 GMT  
Content-Type: text/html; charset=UTF-8  
Content-Length: 189  
Connection: keep-alive  
X-Powered-By: PHP/5.3.3  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0  
Pragma: no-cache  
Set-Cookie: PHPSESSID=9d5aj7fignrtnum7hokv3d443; path=/  
Set-Cookie: PHPSESSID=7131u827cd39qc4t8m756qkgu0; path=/  
Vary: Accept-Encoding  
X-UA-Compatible: IE=edge

<body>ログインしました(tanaka)<br><a href="4f-012.php">  
マイページ (キャッシュなし) </a><br><a href="4f-012a.php">  
マイページ (キャッシュあり) </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...	ラウンドトリップ...	レスポンスボディサ...	検出アラ...	ノート	タグ
57	19/01/05 23:3...	GET	http://example.jp/4f3/4f-010.html	200	OK	3 ms	137 bytes	Medium		
58	19/01/05 23:3...	GET	http://example.jp/4f3/4f-011.php?user=tanaka	200	OK	4 ms	189 bytes	Medium	SetC...	
59	19/01/05 23:3...	GET	http://example.jp/4f3/4f-012a.php	200	OK	23 ms	55 bytes	Medium		
60	19/01/05 23:3...	GET	http://example.jp/4f3/4f-011.php?user=yamada	200	OK	31 ms	189 bytes	Medium	SetC...	

アラート 0 0 0 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 4f/4f-012a.php → レスポンス】

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

- Request:** GET http://example.jp/4f3/4f-012a.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/4f3/4f-011.php?user=tanaka  
DNT: 1  
Connection: keep-alive  
Cookie: PHPSESSID=7131u827cd39qc4t8m756qkgu0  
Upgrade-Insecure-Requests: 1  
Host: example.jp
- Response:** HTTP/1.1 200 OK  
Server: nginx/1.10.3  
Date: Sat, 05 Jan 2019 14:36:05 GMT  
Content-Type: text/html; charset=UTF-8  
Connection: keep-alive  
X-Powered-By: PHP/5.3.3  
Expires: Sat, 05 Jan 2019 14:37:05 GMT  
Cache-Control: public, max-age=60  
Last-Modified: Mon, 14 May 2018 13:08:18 GMT  
X-UA-Compatible: IE=edge  
Body: <body>ユーザ tanaka でログイン中です</body>

The interface also shows a history table at the bottom:

Id	リクエスト日時	メソ...	URL	ステータススコ...	ステータスコード...	ラウンドトリップ...	レスポンスボディサ...	検出アラ...	ノート	タグ
57	19/01/05 23:3...	GET	http://example.jp/4f3/4f-010.html	200	OK	3 ms	137 bytes	Medium		
58	19/01/05 23:3...	GET	http://example.jp/4f3/4f-011.php?user=tanaka	200	OK	4 ms	189 bytes	Medium	SetC...	
59	19/01/05 23:3...	GET	http://example.jp/4f3/4f-012a.php	200	OK	23 ms	55 bytes	Medium		
60	19/01/05 23:3...	GET	http://example.jp/4f3/4f-011.php?user=yamada	200	OK	31 ms	189 bytes	Medium	SetC...	

キャッシュは常に有効(最長60秒)

【ブラウザ→サーバ: リクエスト 4f3/4f-011.php → レスponse】

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

**Request:**  
 GET http://example.jp/4f3/4f-011.php?user=yamada 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/4f3/4f-010.html  
 DNT: 1  
 Connection: keep-alive  
 Cookie: PHPSESSID=7131u827cd39qc4t8m756qkgu0  
 Upgrade-Insecure-Requests: 1  
 Host: example.jp

**Response:**  
 HTTP/1.1 200 OK  
 Server: nginx/1.10.3  
 Date: Sat, 05 Jan 2019 14:36:34 GMT  
 Content-Type: text/html; charset=UTF-8  
 Content-Length: 189  
 Connection: keep-alive  
 X-Powered-By: PHP/5.3.3  
 Expires: Thu, 19 Nov 1981 08:52:00 GMT  
 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0  
 Pragma: no-cache  
 Set-Cookie: PHPSESSID=f3lm7o2vpj161nm4mavkd3hs91; path=/  
 Vary: Accept-Encoding  
 X-UA-Compatible: IE=edge

**Body:**  
 <body>ログインしました(yamada)<br><a href="4f-012.php">  
 マイページ (キャッシュなし) </a><br><a href="4f-012a.php">  
 マイページ (キャッシュあり) </a></body>

**Request List:**

ID	Request Time	Method	URL	Status	Status Code	Round Trip	Response Size	Output	Note	Tag
57	19/01/05 23:3...	GET	http://example.jp/4f3/4f-010.html	200	OK	3 ms	137 bytes	Medium		
58	19/01/05 23:3...	GET	http://example.jp/4f3/4f-011.php?user=tanaka	200	OK	4 ms	189 bytes	Medium		SetC...
59	19/01/05 23:3...	GET	http://example.jp/4f3/4f-012a.php	200	OK	23 ms	55 bytes	Medium		
60	19/01/05 23:3...	GET	http://example.jp/4f3/4f-011.php?user=yamada	200	OK	31 ms	189 bytes	Medium		SetC...