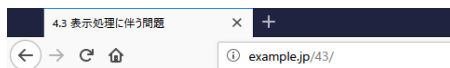


4.3 表示処理に伴う問題 クロスサイト・スクリプティング(発展編)

XSS(発展編) 43-010:href属性の動的生成(正常系)

【ブラウザ】



4.3 表示処理に伴う問題

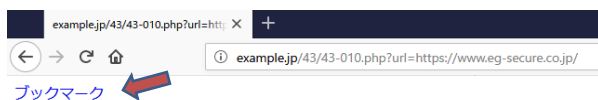
- クロスサイト・スクリプティング (基本編)
 - 43-001:正常系
 - 43-001:XSS攻撃
 - 43-900:罠サイト
 - 43-002:粗大ゴミ申し込み(正常系)
 - 43-902:粗大ゴミ悪用
 - 43-003:引用符で囲まない属性値(正常系)
 - 43-003:引用符で囲まない属性値(XSS)
 - 43-004:引用符で囲った属性値(正常系)
 - 43-004:引用符で囲った属性値(XSS)
- クロスサイト・スクリプティング (発展編)
 - 43-030:href属性の動的生成(正常系)
 - 43-010:href属性の動的生成(XSS)
 - 43-010a:href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&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?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:%d%aalert(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?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=1+onmouseover:%d%aalert(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.eg-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>
25 <li><a href="43-011.html?name=Yamada">43-011:DOM Based XSS(正常系)</a></li>
26 <li><a href="43-011.html?name=&lt;script>alert(document.cookie)&lt;/script>">43-011:DOM Based XSS(XSS)</a></li>
27 <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>
28 </ol>
29 <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>
30 <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>
31 <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>
32 <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>
33 <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>
34 <li><a href="43-013b.php?name=&lt;script>&lt;script>alert(document.cookie)//">43-013b:script要素内の動的生成(対策済みB)</a></li>
35 </ol>
36 <br>
37 <a href="phpinfo.php">phpinfo</a><br>
38 <a href="/">ホームに戻る</a>
39 </body>
40 </html>
```



【サーバ: 43/43-010.php】

```
/var/www/html/43/43-010.php - wasbook@192.168.56.101 - エディタ - WinSCP
kbody>
<a href=""?php echo htmlspecialchars($_GET['url']); ?>">ブックマーク</a>
</body>
```

【ブラウザ→サーバ: リクエスト 43/43-010.php → レスポンス】 href属性の動的生成(正常系)

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

- Request:** GET http://example.jp/43/43-010.php?url=https://www.eg-secure.co.jp/ 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
- Response:** HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 19 Dec 2018 08:19:04 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 77
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Vary: Accept-Encoding
X-UA-Compatible: IE=edge
- Body:** ブックマーク
- 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
13	18/12/19 8:19:03	GET	http://example.jp/43/43-010.php?url=https://...	200	OK	18 ms	77 bytes	Medium		

Alerts: 0 1 2 0 (Current scan: 0 0 0 0 0 0)

【ブラウザ】

The screenshot shows a web browser displaying the homepage of EG Secure Solutions. The page includes the following elements:

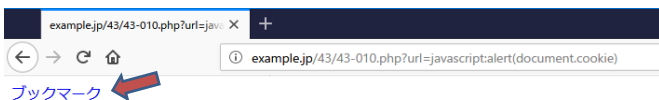
- Header:** EG Secure Solutions logo and navigation menu (HOME, サービス案内, 導入事例, 会社概要, 採用情報, お知らせ・イベント情報).
- Main Content:** Text stating "HASHコンサルティング株式会社は EGセキュアソリューションズ株式会社に社名変更しました" (HASH Consulting Co., Ltd. has changed its name to EG Secure Solutions Co., Ltd.).
- Footer:** "安全なウェブアプリケーションのプロフェッショナル集団 EGセキュアソリューションズ株式会社" (Professional group of secure web applications EG Secure Solutions Co., Ltd.).

XSS(発展編) 43-010:href属性の動的生成(XSS)

【ブラウザ】

- 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)

```
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/">43-030: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 </ol>
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>
```



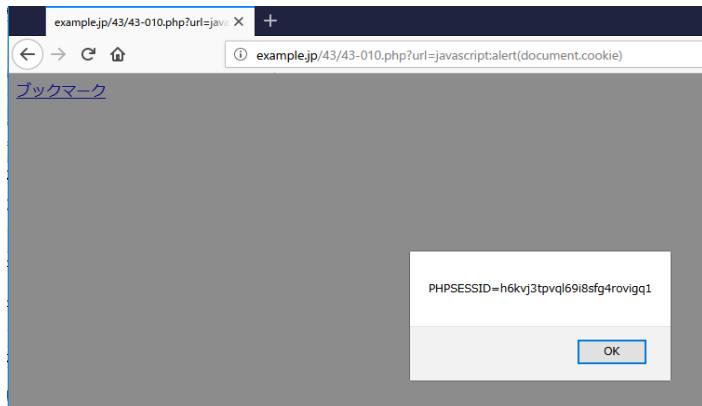
【サーバ: 43/43-010.php】

```
/var/www/html/43/43-010.php - wasbook@192.168.56.101 - エディタ - WinSCP
kbody>
<a href="<?php echo htmlspecialchars($_GET['url']); ?>">ブックマーク</a>
</body>
```

【ブラウザ→サーバ: リクエスト 43/43-010.php → レスポンス】 href属性の動的生成(XSS)


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
24	18/12/19 8:41:45	GET	http://example.jp/43/43-010.php?url=javascri...	200	OK	36 ms	82 bytes	Medium		

【ブラウザ】



XSS(発展編) 43-010:href属性の動的生成(対策済み)

【ブラウザ】

- クロスサイト・スクリプティング (発展編)
 - 9. [43-030:href属性の動的生成\(正常系\)](#)
 - 10. [43-010:href属性の動的生成\(XSS\)](#)
 - 11. [43-010a:href属性の動的生成\(対策済み\)](#) 
 - 12. [43-012:イベントハンドラの動的生成\(正常系\)](#)
 - 13. [43-012:イベントハンドラの動的生成\(XSS\)](#)
 - 14. [43-013:script要素内の動的生成\(正常系\)](#)
 - 15. [43-013:script要素内の動的生成\(XSS\)](#)
 - 16. [43-013a:script要素内の動的生成\(対策済みA\)](#)
 - 17. [43-013b:script要素内の動的生成\(対策済みB\)](#)

```
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.eg-secure.co.jp/">43-030: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 </ol>
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>
```

【サーバ: 43/43-010a.php】

```
/var/www/html/43/43-010a.php - wasbook@192.168.56.101 - エディタ - WinSCP
k?php
function check_url($url) {
    if (preg_match('/\Ahttp:/', $url)
        || preg_match('/\Ahttps:/', $url)
        || preg_match('/\A#/', $url)) {
        return true;
    } else {
        return false;
    }
}
$url = $_GET['url'];
if (!check_url($url)) {
    die('URLの形式が不正です');
}
?>
<body>
<a href="<?php echo htmlspecialchars($url); ?>">ブックマーク</a>
</body>
```

URLをプログラムで生成する場合には、以下のみ許す

- http: https: で始まる絶対URL
- スラッシュ「/」で始まる相対URL

【ブラウザ→サーバ: リクエスト 43/43-010.php → レスポンス】 href属性の動的生成(XSS)

The screenshot shows the OWASP ZAP interface. The left pane shows the context tree with 'http://example.jp' selected. The main pane displays the request and response details. The request is a GET request to 'http://example.jp/43/43-010a.php?url=javascript:alert(document.cookie)'. The response is an HTTP/1.1 200 OK from 'Server: nginx/1.10.3'. A red box highlights the error message 'URLの形式が不正です' (Invalid URL format) in the response 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
28	18/12/19 8:44:23	GET	http://example.jp/43/43-010a.php?url=javascr...	200	OK	40 ms	27 bytes	Medium		

【ブラウザ】

The screenshot shows a browser address bar with the URL 'example.jp/43/43-010a.php?url=ja...'. Below the address bar, an error message reads 'URLの形式が不正です' (Invalid URL format).

XSS(発展編) 43-012:イベントハンドラの動的生成(正常系)

【ブラウザ】

- クロスサイト・スクリプティング (発展編)
 9. [43-030:href属性の動的生成\(正常系\)](#)
 10. [43-010:href属性の動的生成\(XSS\)](#)
 11. [43-010a:href属性の動的生成\(対策済み\)](#)
 12. [43-012:イベントハンドラの動的生成\(正常系\)](#) 
 13. [43-012:イベントハンドラの動的生成\(XSS\)](#)
 14. [43-013:script要素内の動的生成\(正常系\)](#)
 15. [43-013:script要素内の動的生成\(XSS\)](#)
 16. [43-013a:script要素内の動的生成\(対策済みA\)](#)
 17. [43-013b:script要素内の動的生成\(対策済みB\)](#)

```
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.eg-secure.co.jp/">43-030: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 <li>←
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 →
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=&lt;script>&lt;script>alert(document.cookie)//">43-013b:script要素内の動的生成(対策済みB)</a></li>
34 </ol>
```

【サーバ: 43/43-012.php】

```
/var/www/html/43/43-012.php - wasbook@192.168.56.101 - エディタ - WinSCP
<head>
<script>
function init(name) {
    var span = document.getElementById('name');
    span.textContent = name;
}
</script></head>
<body onload="init('<?php echo htmlspecialchars($_GET['name'], ENT_QUOTES) ?>')">
こんにちは<span id="name"></span>さん
</body>
```

【ブラウザ→サーバ: リクエスト 43/43-012.php → レスポンス】 イベントハンドラの動的生成(正常系)

無題セッション - 20181219-075342 - 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.example.com
http://example.jp

```
GET http://example.jp/43/43-012.php?name=Yamada 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=h6kvj3tpvql69i8sfg4rovigq1
Upgrade-Insecure-Requests: 1
Host: example.jp
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 19 Dec 2018 09:01:41 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 214
Connection: keep-alive
X-Powered-By: PHP/5.3.3
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<head>
<script>
function init(name) {
var span = document.getElementById(name);
span.textContent = name;
}
</script></head>
<body onload="init('Yamada')">
こんにちは<span id="name"></span>さん
</body>
```

履歴 検索 アラート アウトプット +

フィルタ: オフ エクスポート

ID	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	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
29	18/12/19 9:01:40	GET	http://example.jp/43/43-012.php?name=Yam...	200	OK	23 ms	214 bytes	Medium		Script

アラート 0 2 3 0 現在のスキャン 0 0 0 0 0 0

【ブラウザ】

example.jp/43/43-012.php?name= Yamada

example.jp/43/43-012.php?name=Yamada

こんにちはYamadaさん

XSS(発展編) 43-012:イベントハンドラの動的生成(XSS)

【ブラウザ】

- クロスサイト・スクリプティング (発展編)
 9. [43-030:href属性の動的生成\(正常系\)](#)
 10. [43-010:href属性の動的生成\(XSS\)](#)
 11. [43-010a:href属性の動的生成\(対策済み\)](#)
 12. [43-012:イベントハンドラの動的生成\(正常系\)](#)
 13. [43-012:イベントハンドラの動的生成\(XSS\)](#)
 14. [43-013:script要素内の動的生成\(正常系\)](#)
 15. [43-013:script要素内の動的生成\(XSS\)](#)
 16. [43-013a:script要素内の動的生成\(対策済みA\)](#)
 17. [43-013b:script要素内の動的生成\(対策済みB\)](#)

```
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.eg-secure.co.jp/">43-030: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 <!--
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 -->
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>
```

【サーバ: 43/43-012.php】

/var/www/html/43/43-012.php - wasbook@192.168.56.101 - エディタ - WinSCP

```
<thead>
<script>
function init(name) {
    var span = document.getElementById('name');
    span.textContent = name;
}
</script></head>
<body onload="init('<?php echo htmlspecialchars($_GET['name'], ENT_QUOTES) ?>')">
こんにちは<span id="name"></span>さん
</body>
```

【ブラウザ→サーバ: リクエスト 43/43-012.php → レスポンス】 イベントハンドラの動的生成(XSS)

The screenshot shows the OWASP ZAP interface. The left pane shows the site tree with 'http://example.jp' selected. The middle pane displays the request details for 'GET http://example.jp/43/43-012.php?name=%27);alert(document.cookie)//'. The right pane shows the response details, including headers and a body containing a JavaScript function and an onload event. The function 'init(name)' is defined to set the text content of a span element with the given name. The onload event is triggered by the URL parameter '%27);alert(document.cookie)//'. The bottom pane shows a table of request logs.

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
30	18/12/19 9:09:19	GET	http://example.jp/43/43-012.php?name=%27);...	200	OK	28 ms	240 bytes	Medium	Script	


【ブラウザ】

The screenshot shows a browser window with the URL 'example.jp/43/43-012.php?name=');alert(document.cookie)//'. An alert box is displayed with the text 'PHPSESSID=h6kvj3tpvq69i8sfg4rovigq1' and an 'OK' button.

JavaScriptの文字列リテラルのエスケープ処理が抜けていたのでシングルクォート「'」がデータの「'」ではなく、JavaScriptの終端文字として使われたのが、脆弱性が混入した原因です

XSS(発展編) 43-013:script要素内の動的生成(正常系)

【ブラウザ】

- 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)

```
18 </li></crosssite scripting (発展編) </li>
19 <ol start="9">
20 <li><a href="43-010.php?url=https://www.eg-secure.co.jp/">43-030: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 </ol>
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>
```

【サーバ: 43/43-013.php】

```
/var/www/html/43/43-013.php - wasbook@192.168.56.101 - エディタ - WinSCP
k?php
session_start();
function escape_js($s) {
    return mb_ereg_replace('([\\"\'\`])', '\\\1', $s);
}
?>
<body>
<div id="name"></div>
<script>
    var div = document.getElementById('name');
    var txt = '<?php echo escape_js($_GET['name']); ?>';
    div.textContent = txt + 'の文字数は' + txt.length + '文字です';
</script>
</body>
```

【ブラウザ→サーバ: リクエスト 43/43-013.php → レスポンス】 script要素内の動的生成(正常系)

The screenshot shows the OWASP ZAP interface. The left pane shows the site tree with 'http://example.jp' selected. The main pane displays the request and response details for a GET request to 'http://example.jp/43/43-013.php?name=%E5%A4%A7%E8%B0%B7san'. The response body contains HTML with a JavaScript script that dynamically generates content based on the 'name' parameter.

```
GET http://example.jp/43/43-013.php?name=%E5%A4%A7%E8%B0%B7san 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=h6kvj3tpvql6918sfg4rovigq1
Upgrade-Insecure-Requests: 1
Host: example.jp

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Wed, 19 Dec 2018 11:35:01 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 201
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>
<div id="name"></div>
<script>
var div = document.getElementById("name");
var txt = "大谷san";
div.textContent = txt + 'の文字数は' + txt.length + '文字です';
</script>
</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
31	18/12/19 20:35:00	GET	http://example.jp/43/43-013.php?name=%E5...	200	OK	37 ms	201 bytes	Medium		Script

【ブラウザ】

The browser window shows the URL 'example.jp/43/43-013.php?name=大谷san' and the rendered content: '大谷sanの文字数は5文字です'.

XSS(発展編) 43-013:script要素内の動的生成(XSS)

【ブラウザ】

- 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)

```
18 </li></crosssite scripting (発展編) </li>
19 <ol start="9">
20 <li><a href="43-010.php?url=https://www.eg-secure.co.jp/">43-030: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 </ol>
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=大谷さか">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=&lt;script>&lt;script>alert(document.cookie)//">43-013b:script要素内の動的生成(対策済みB)</a></li>
34 </ol>
```

【サーバ: 43/43-013.php】

```
/var/www/html/43/43-013.php - wasbook@192.168.56.101 - エディタ - WinSCP
k?php
session_start();
function escape_js($s) {
    return mb_ereg_replace('([\\"\\\']|";', '\\\\1', $s);
}
?>
<body>
<div id="name"></div>
<script>
    var div = document.getElementById('name');
    var txt = '<?php echo escape_js($_GET['name']); ?>';
    div.textContent = txt + 'の文字数は' + txt.length + '文字です';
</script>
</body>
```

【ブラウザ→サーバ: リクエスト 43/43-013.php → レスポンス】 script要素内の動的生成(XSS)

The screenshot shows the OWASP ZAP interface. The 'Request' pane displays a GET request to `http://example.jp/43/43-013.php?name=%3C/script%3E%3Cscript%3Ealert(document.cookie)//`. The 'Response' pane shows an HTTP 200 OK response with headers including `Server: nginx/1.10.3` and `Date: Wed, 19 Dec 2018 11:45:24 GMT`. The response body contains HTML with a script tag: `<script>var div = document.getElementById('name'); var txt = '</script><script>alert(document.cookie)//'; div.textContent = txt + 'の文字数は' + txt.length + '文字です';</script>`. A table at the bottom summarizes 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
32	18/12/19 20:45:24	GET	http://example.jp/43/43-013.php?name=%3C/...	200	OK	22 ms	233 bytes	Medium		Script


【ブラウザ】

The browser screenshot shows the address bar with the URL `example.jp/43/43-013.php?name=</script><script>alert(document.cookie)//`. An alert dialog box is displayed with the text `PHPSESSID=h6kvj3tpvql69isfg4rovigq1` and an 'OK' button.

script要素内はタグや文字参照を解釈しないので、HTMLエスケープは必要ないが、JavaScriptの文字列リテラルとしてのエスケープ処理は必要です。さらに、`</script>` はJavaScriptの終端として認識するので、脆弱性原因になります。

XSS(発展編) 43-013a:script要素内の動的生成(対策済みA)

【ブラウザ】

- 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)

```
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.eg-secure.co.jp/">43-030: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 <!--
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 -->
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=&lt;script>&lt;script>alert(document.cookie)//">43-013b:script要素内の動的生成(対策済みB)</a></li>
34 </ol>
```

【サーバ: 43/43-013a.php】

```
/var/www/html/43/43-013a.php - wasbook@192.168.56.101 - エディタ - WinSCP
k?php
session_start();
?>
<body>
<div id="name" data-name="">?php echo htmlspecialchars($_GET['name'], ENT_COMPAT, 'utf-8'); ?></div>
<script>
|| var div = document.getElementById('name');
|| var txt = div.dataset.name;
|| div.textContent = txt + 'の文字数は' + txt.length + '文字です';
</script>
</body>
```

script要素の外でパラメータを定義して、JavaScriptから参照します
カスタムデータ属性(data-name="XXX")を使います

【ブラウザ→サーバ: リクエスト 43/43-013a.php → レスポンス】 script要素内の動的生成(対策済みA)

The screenshot shows the OWASP ZAP interface. The left pane shows the site tree with 'http://example.jp' selected. The main pane is split into 'Request' and 'Response' views. The request is a GET to 'http://example.jp/43/43-013a.php?name=%3C/script%3E%3Cscript%3Ealert(document.cookie)//'. The response is an HTTP 200 OK with headers from nginx/1.10.3 and a body containing HTML with a script element. The script element is highlighted with a dashed box and contains the following code:

```
<div id="name" data-name="&lt;/script&gt;&lt;/script&gt;alert(document.cookie)//"></div>
<script>
var div = document.getElementById("name");
var txt = div.dataset.name;
div.textContent = txt + 'の文字数は' + txt.length + '文字です';
</script>
</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
33	18/12/19 20:57:20	GET	http://example.jp/43/43-013a.php?name=%3C...	200	OK	25 ms	272 bytes	Medium		Script

【ブラウザ】


The browser shows the URL 'example.jp/43/43-013a.php?name=</script><script>alert(document.cookie)//'. The page content displays the alert message: '</script><script>alert(document.cookie)//の文字数は41文字です'.

The browser shows the source code of the page. The script element is highlighted with a dashed box and contains the following code:

```
<div id="name" data-name="&lt;/script&gt;&lt;/script&gt;alert(document.cookie)//"></div>
<script>
var div = document.getElementById("name");
var txt = div.dataset.name;
div.textContent = txt + 'の文字数は' + txt.length + '文字です';
</script>
</body>
```


XSS(発展編) 43-013b:script要素内の動的生成(対策済みB)

【ブラウザ】

- クロスサイト・スクリプティング (発展編)
 9. 43-030:href属性の動的生成(正常系)
 10. 43-010:href属性の動的生成(XSS)
 11. 43-010a:href属性の動的生成(対策済み)
 12. 43-012:イベントハンドラの動的生成(正常系)
 13. 43-012:イベントハンドラの動的生成(XSS)
 14. 43-013:script要素内の動的生成(正常系)
 15. 43-013:script要素内の動的生成(XSS)
 16. 43-013a:script要素内の動的生成(対策済みA)
 17. 43-013b:script要素内の動的生成(対策済みB) 

```
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.eg-secure.co.jp/">43-030: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 </ol>
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=&lt;script>&lt;script>alert(document.cookie)//">43-013b:script要素内の動的生成(対策済みB)</a></li>
34 </ol>
```

【サーバ: 43/43-013b.php】

/var/www/html/43/43-013b.php - wasbook@192.168.56.101 - エディタ - WinSCP

```

k?php
session_start();
$array = array('name' => $_GET['name']);
?><body>
<div id="name"></div>
<script>
function display_length(obj) {
    | var div = document.getElementById('name');
    | var txt = obj.name;
    | div.textContent = txt + 'の文字数は' + txt.length + '文字です';
}
display_length(<?php echo json_encode($array, JSON_HEX_TAG | JSON_HEX_AMP); ?>);
</script>
</body>
```

JSON形式のパラメータを伴う関数をscript要素で呼び出します

JSONを安全に呼び出す関数json_encodeにJSON生成処理をまかせます

【ブラウザ→サーバ: リクエスト 43/43-013b.php → レスポンス】 script要素内の動的生成(対策済みB)

The screenshot shows the Burp Suite interface with a request and response view. The request is a GET request to `http://example.jp/43/43-013b.php?name=%3C/script%3E%3Cscript%3Ealert(document.cookie)//`. The response is an HTML page with a JavaScript function `display_length(obj)` that calculates the length of the `name` attribute. The response body contains the following code:

```
<body>
<div id="name"></div>
<script>
function display_length(obj) {
  var div = document.getElementById("name");
  var txt = obj.name;
  div.textContent = txt + 'の文字数は' + txt.length + '文字です';
}
display_length({"name": "%u003C/script%u003E%u003Cscript%u003Ealert(document.cookie)%u003C/script%3E"});
</script>
</body>
```

The bottom table 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
34	18/12/19 21:12:01	GET	http://example.jp/43/43-013b.php?name=%3...	200	OK	22 ms	324 bytes	Medium		Script

【ブラウザ】

The screenshot shows a browser window with the address bar containing `example.jp/43/43-013b.php?name=</script><script>alert(document.cookie)//`. The page content displays the following text:

```
</script><script>alert(document.cookie)//の文字数は41文字です
```

The screenshot shows a browser window with the address bar containing `view-source:http://example.jp/43/43-013b.php?name=%3C/script%3E%3Cscript%3Eal`. The page content displays the following code:

```
1 <body>
2 <div id="name"></div>
3 <script>
4 function display_length(obj) {
5   var div = document.getElementById("name");
6   var txt = obj.name;
7   div.textContent = txt + 'の文字数は' + txt.length + '文字です';
8 }
9 display_length({"name": "%u003C/script%u003E%u003Cscript%u003Ealert(document.cookie)%u003C/script%3E"});
10 </script>
11 </body>
12
```