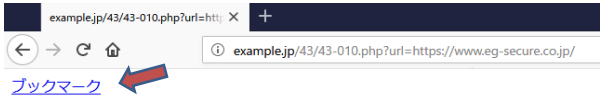
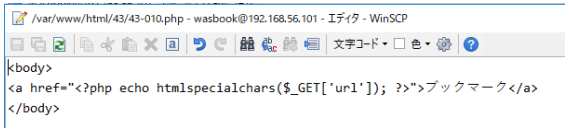
4.3 表示処理に伴う問題　クロスサイト・スクリプティング（発展編）

XSS（発展編） 43-010:href属性の動的生成(正常系)

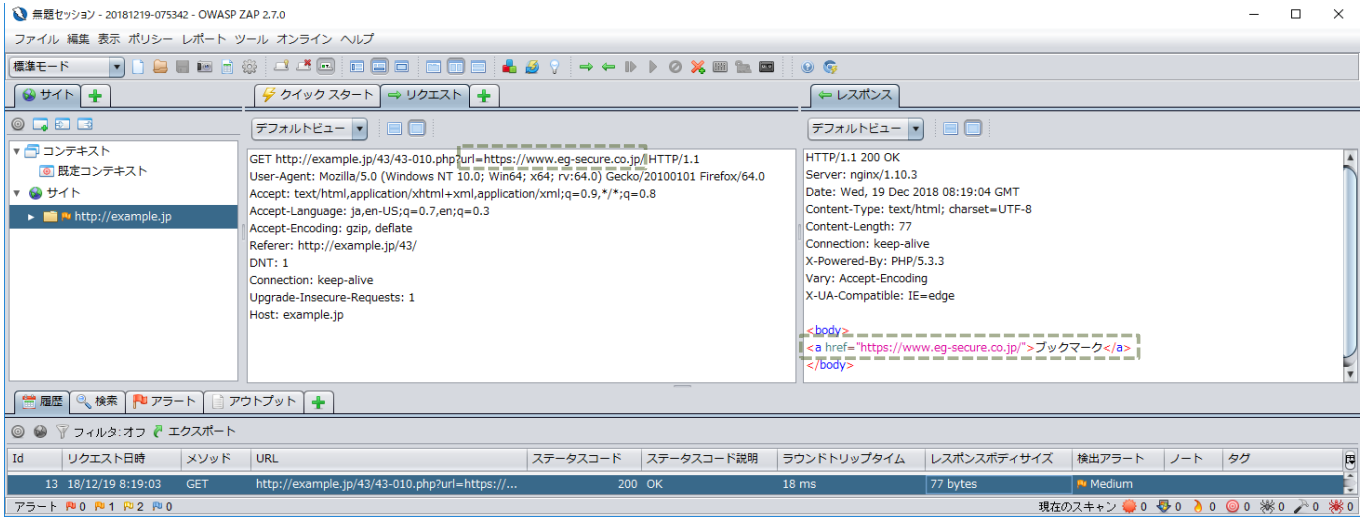
【ブラウザ】



【サーバ： 43/43-010.php 】



【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)



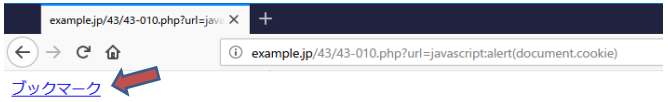
【ブラウザ】

XSS（発展編） 43-010:href属性の動的生成(XSS)

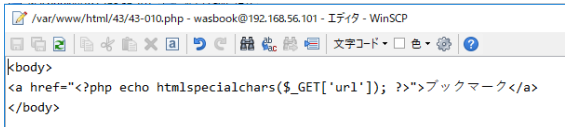
【ブラウザ】

- クロスサイト・スクリプティング（発展編）
  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)

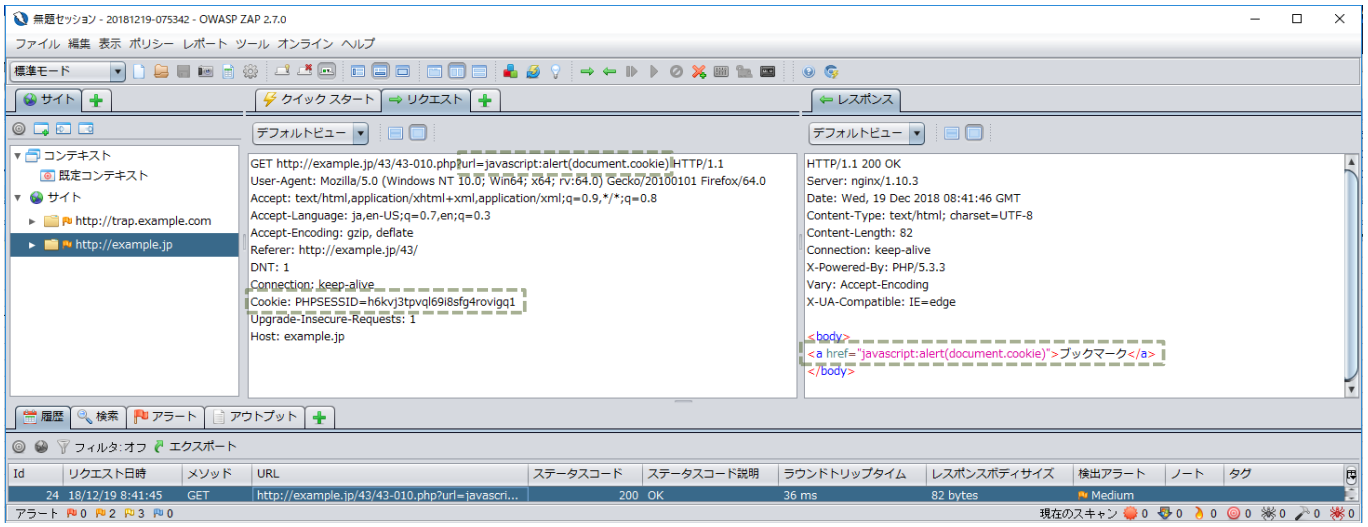
```
18 <li>クロスサイト・スクリプティング（発展編）</li>
19 <ol start="9">
20 <li><a href="43-010.php?url=https://www.eg-secure.co.jp/">43-030:href属性の動的生成(正常系)</a></li>
21 <li><a href="43-010.php?url=javascript:alert(document.cookie)">43-010:href属性の動的生成(XSS)</a></li>
22 <li><a href="43-010a.php?url=javascript:alert(document.cookie)">43-010a:href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>
```



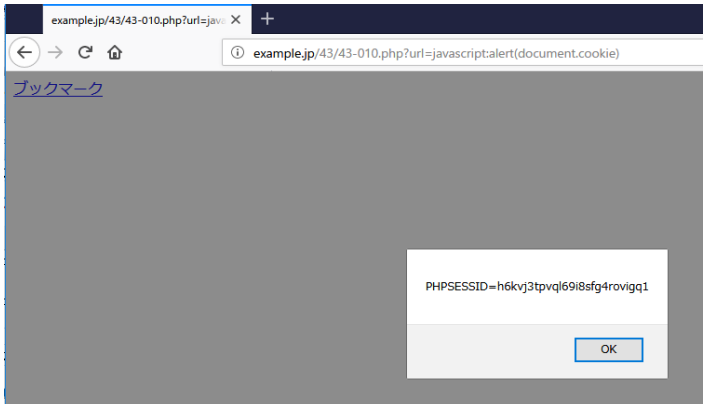
【サーバ： 43/43-010.php 】



【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)



【ブラウザ】


example.jp/43/43-010.php?url=jav
example.jp/43/43-010.php?url=javascript:alert(document.cookie)
ブックマーク
PHPSESSID=h6kvj3tpvql69i8sfg4rovigq1
OK

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)

```
<li>クロスサイト・スクリプティング（発展編）</li>
<ol start="9">
<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>
<li><a href="43-010.php?url=javascript:alert(document.cookie)">43-010:href属性の動的生成(XSS)</a></li>
<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>
<!--
<li><a href="43-011.html?name=Yamada">43-011:DOM Based XSS(正常系)</a></li>
<li><a href="43-011.html?name=&lt;script>alert(document.cookie)&lt;/script>">43-011:DOM Based XSS(XSS)</a></li>
<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>
-->
<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>
<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>
<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>
<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>
<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>
<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>
</ol>
```

【サーバ： 43/43-010a.php 】

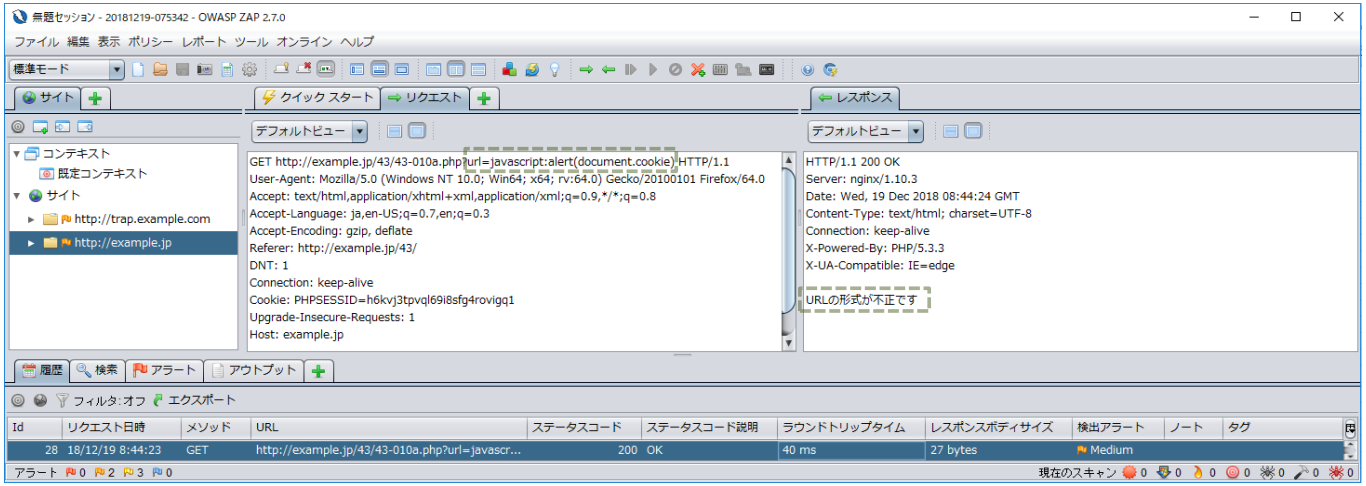
/var/www/html/43/43-010a.php - wasbook@192.168.56.101 - エディタ - WinSCP

```
<?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>
```

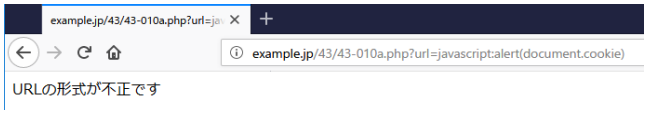
URLをプログラムで生成する場合には、以下のみ許す

- **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)



【ブラウザ】



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)

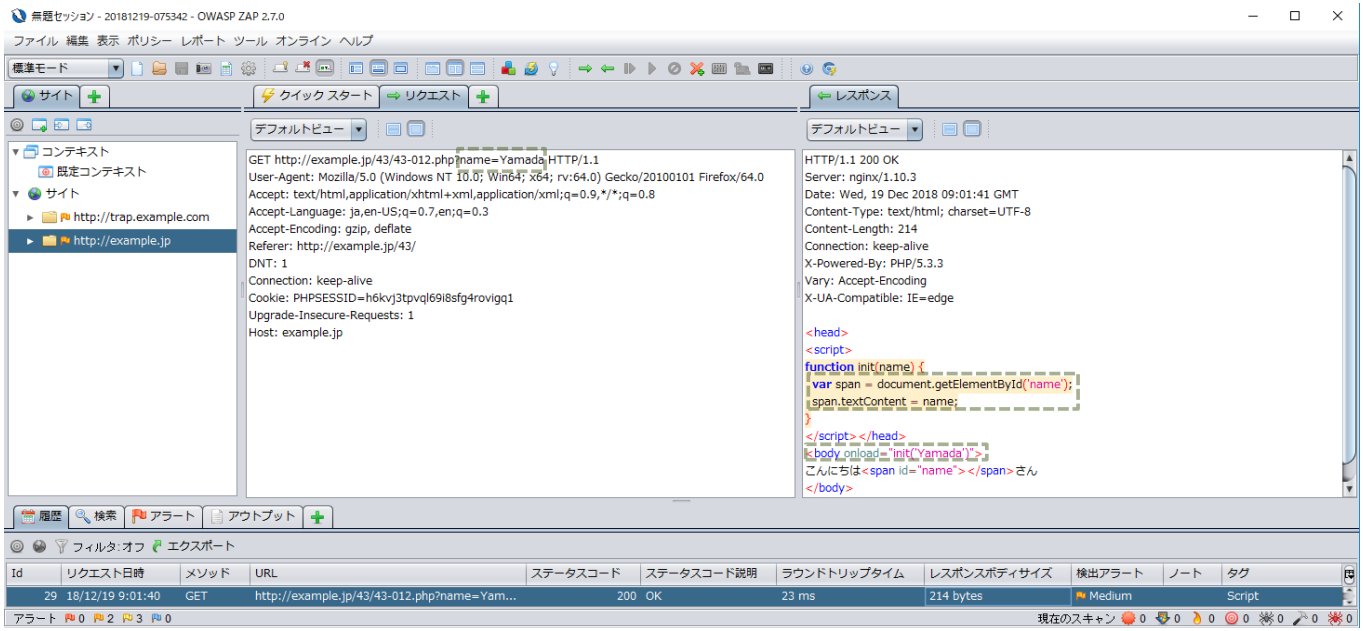
```
<li>クロスサイト・スクリプティング（発展編）</li>
<ol start="9">
<li><a href="43-010.php?url=https://www.eg-secure.co.jp/">43-030:href属性の動的生成(正常系)</a></li>
<li><a href="43-010.php?url=javascript:alert(document.cookie)">43-010:href属性の動的生成(XSS)</a></li>
<li><a href="43-010a.php?url=javascript:alert(document.cookie)">43-010a:href属性の動的生成(対策済み)</a></li>
<!--
<li><a href="43-011.html?name=Yamada">43-011:DOM Based XSS(正常系)</a></li>
<li><a href="43-011.html?name=&lt;script>alert(document.cookie)&lt;/script>">43-011:DOM Based XSS(XSS)</a></li>
<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>
-->
<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>
<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>
<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>
<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>
<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>
<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>
</ol>
```

【サーバ: 43/43-012.php 】

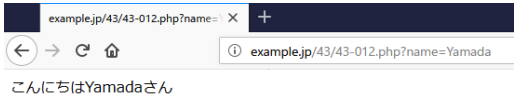
/var/www/html/43/43-012.php - wasbook@192.168.56.101 - エディタ - WinSCP

```
<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)



【ブラウザ】



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)

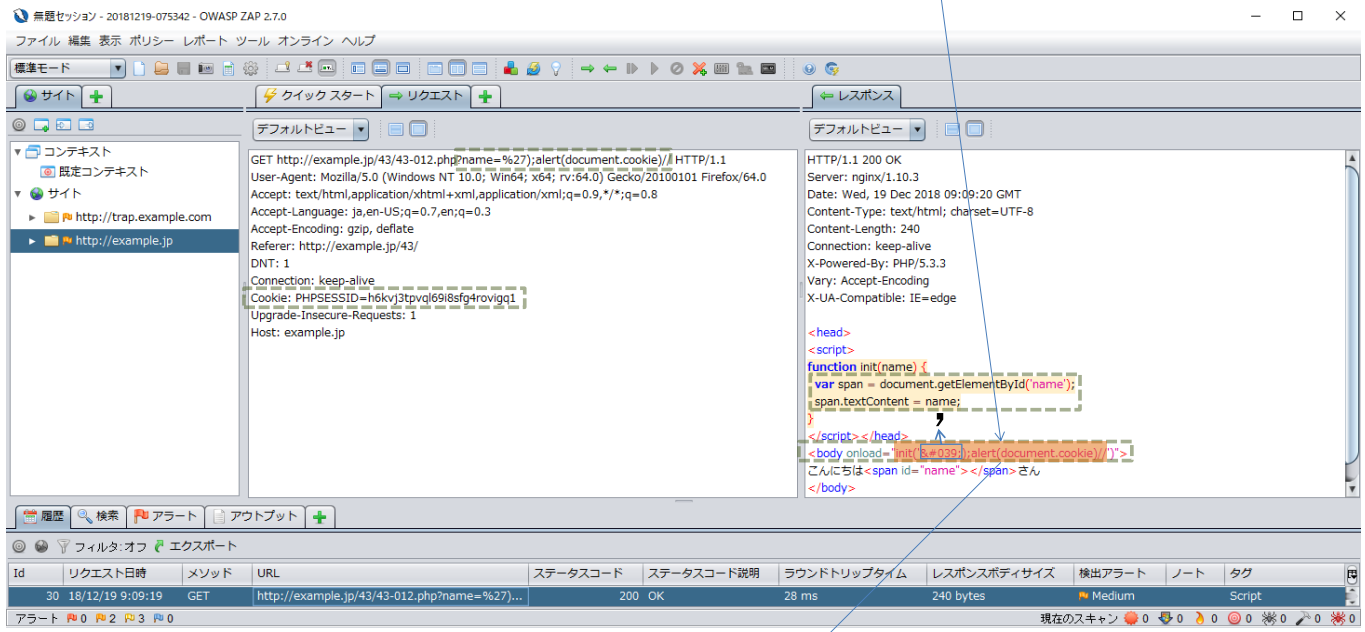
```
<li>クロスサイト・スクリプティング（発展編）</li>
<ol start="9">
<li><a href="43-010.php?url=https://www.eg-secure.co.jp/">43-030:href属性の動的生成(正常系)</a></li>
<li><a href="43-010.php?url=javascript:alert(document.cookie)">43-010:href属性の動的生成(XSS)</a></li>
<li><a href="43-010a.php?url=javascript:alert(document.cookie)">43-010a:href属性の動的生成(対策済み)</a></li>
<!--
<li><a href="43-011.html?name=Yamada">43-011:DOM Based XSS(正常系)</a></li>
<li><a href="43-011.html?name=&lt;script>alert(document.cookie)&lt;/script>">43-011:DOM Based XSS(XSS)</a></li>
<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>
-->
<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>
<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>
<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>
<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>
<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>
<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>
</ol>
```

【サーバ： 43/43-012.php 】

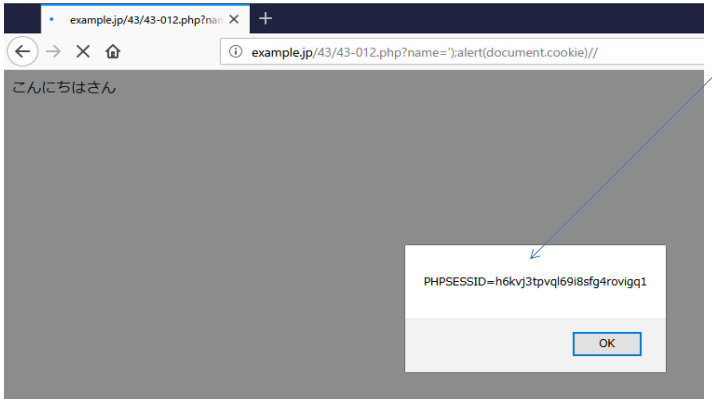
/var/www/html/43/43-012.php - wasbook@192.168.56.101 - エディタ - WinSCP

```
<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(XSS)



【ブラウザ】



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）
  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)

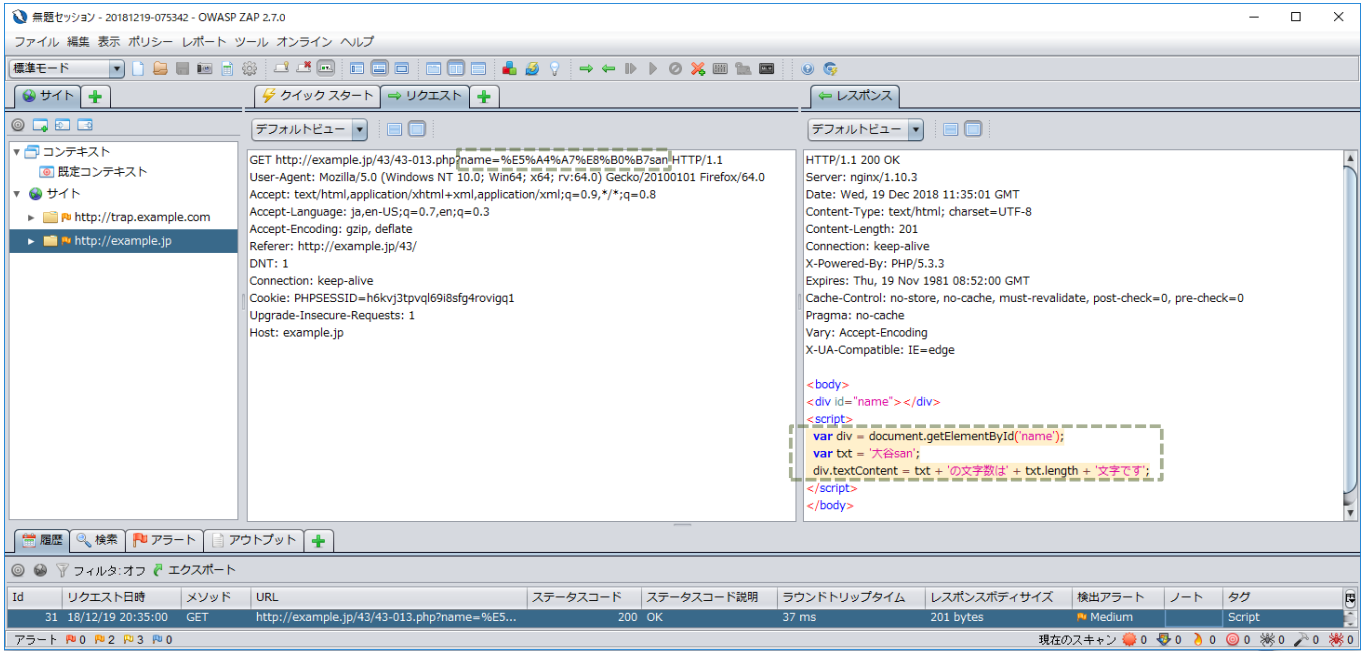
```
<li>クロスサイト・スクリプティング（発展編）</li>
<ol start="9">
<li><a href="43-010.php?url=https://www.eg-secure.co.jp/">43-030:href属性の動的生成(正常系)</a></li>
<li><a href="43-010.php?url=javascript:alert(document.cookie)">43-010:href属性の動的生成(XSS)</a></li>
<li><a href="43-010a.php?url=javascript:alert(document.cookie)">43-010a:href属性の動的生成(対策済み)</a></li>
<!--
<li><a href="43-011.html?name=Yamada">43-011:DOM Based XSS(正常系)</a></li>
<li><a href="43-011.html?name=&lt;script>alert(document.cookie)&lt;/script>">43-011:DOM Based XSS(XSS)</a></li>
<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>
-->
<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>
<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>
<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>
<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>
<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>
<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>
</ol>
```

【サーバ： 43/43-013.php 】

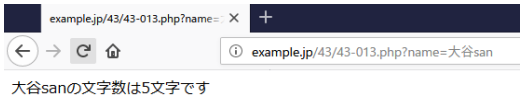
/var/www/html/43/43-013.php - wasbook@192.168.56.101 - エディタ - WinSCP

```
<?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)



【ブラウザ】



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）
  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)

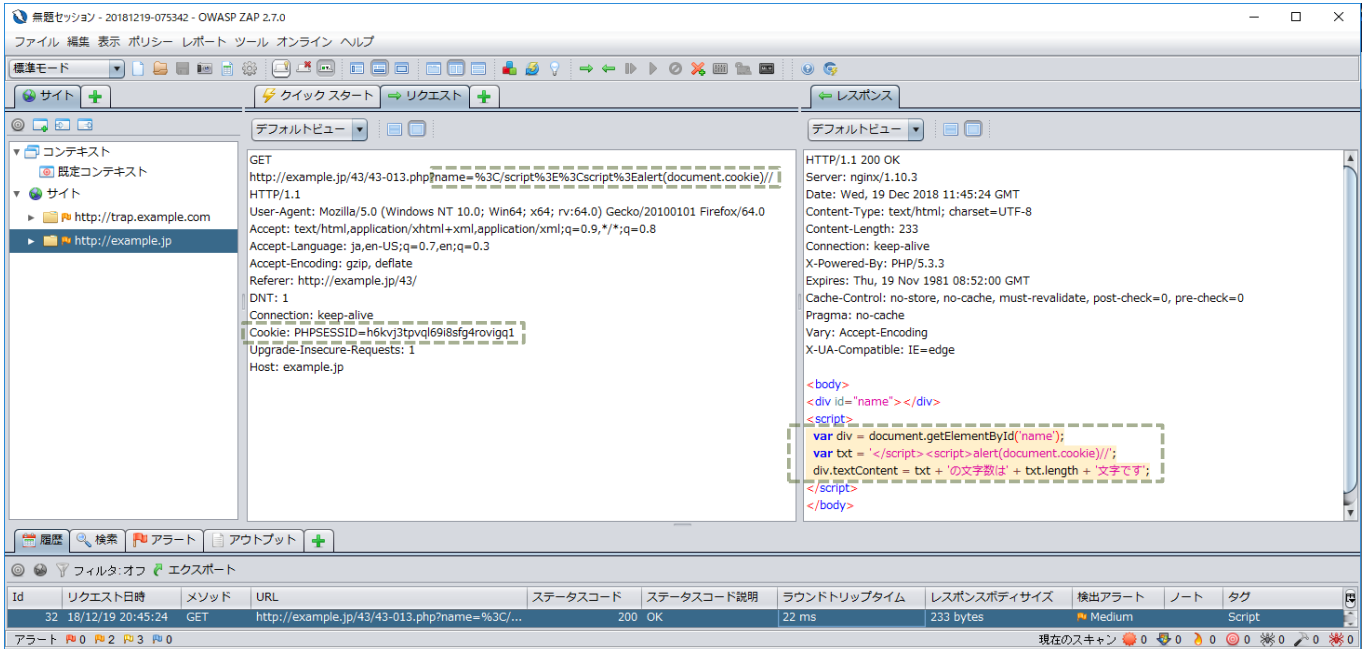
```
<li>クロスサイト・スクリプティング（発展編）</li>
<ol start="9">
<li><a href="43-030.php?url=https://www.eg-secure.co.jp/">43-030:href属性の動的生成(正常系)</a></li>
<li><a href="43-010.php?url=javascript:alert(document.cookie)">43-010:href属性の動的生成(XSS)</a></li>
<li><a href="43-010a.php?url=javascript:alert(document.cookie)">43-010a:href属性の動的生成(対策済み)</a></li>
<!--
<li><a href="43-011.html?name=Yamada">43-011:DOM Based XSS(正常系)</a></li>
<li><a href="43-011.html?name=&lt;script>alert(document.cookie)&lt;/script>">43-011:DOM Based XSS(XSS)</a></li>
<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>
-->
<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>
<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>
<li><a href="43-013.php?name=太合sap">43-013:script要素内の動的生成(正常系)</a></li>
<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>
<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>
<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>
</ol>
```

【サーバ： 43/43-013.php 】

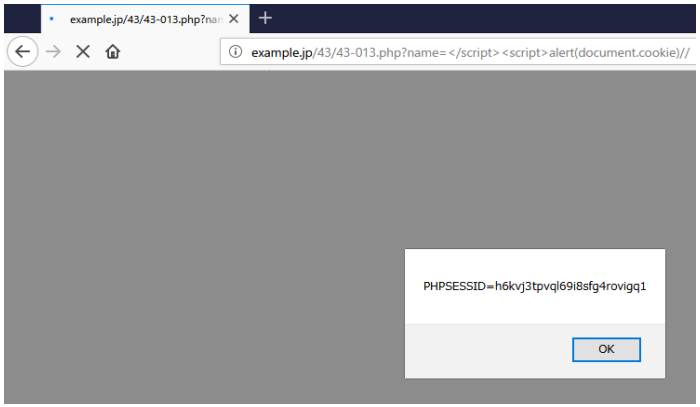
/var/www/html/43/43-013.php - wasbook@192.168.56.101 - エディタ - WinSCP

```
<?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)



【ブラウザ】



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）
  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)

```
<li>クロスサイト・スクリプティング（発展編）</li>
<ol start="9">
<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>
<li><a href="43-010.php?url=javascript:alert(document.cookie)">43-010:href属性の動的生成(XSS)</a></li>
<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>
<!--
<li><a href="43-011.html?name=Yamada">43-011:DOM Based XSS(正常系)</a></li>
<li><a href="43-011.html?name=&lt;script>alert(document.cookie)&lt;/script>">43-011:DOM Based XSS(XSS)</a></li>
<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>
-->
<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>
<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>
<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>
<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>
<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>
<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>
</ol>
```

【サーバ： 43/43-013a.php 】

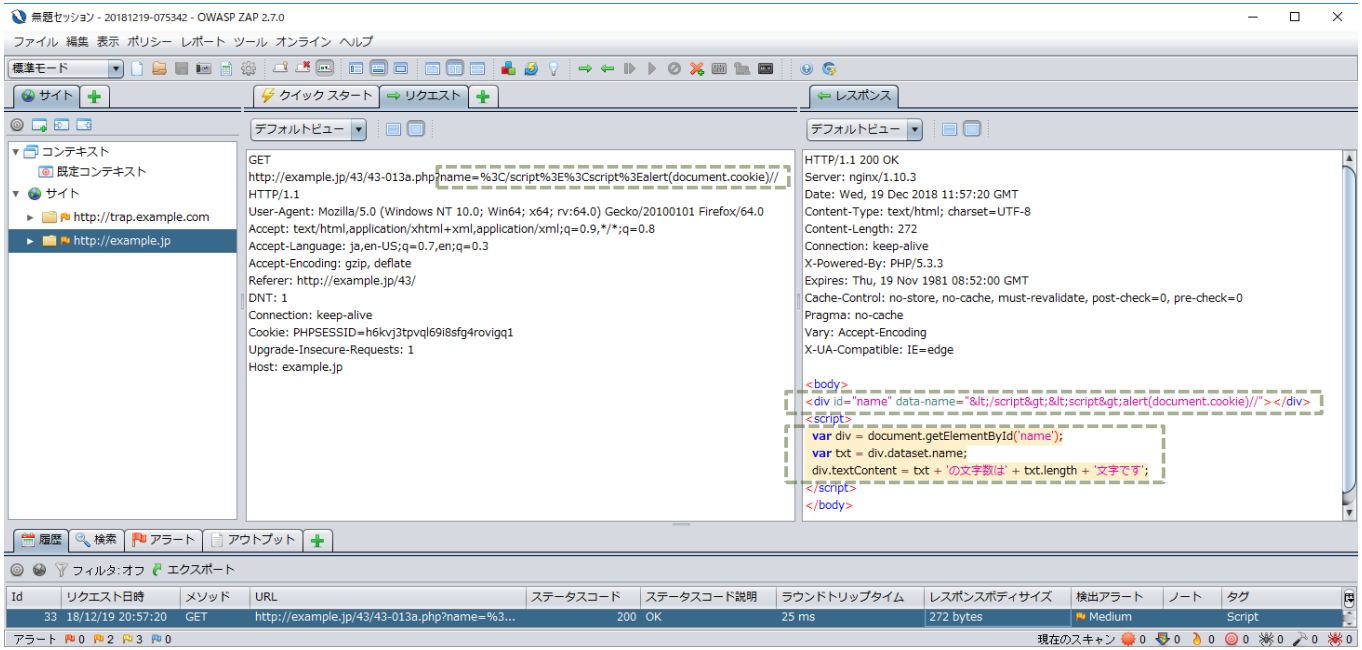
/var/www/html/43/43-013a.php - wasbook@192.168.56.101 - エディタ - WinSCP

```
<?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>
```

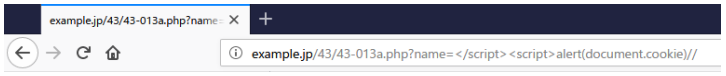
script要素の外部でパラメータを定義して、JavaScriptから参照します

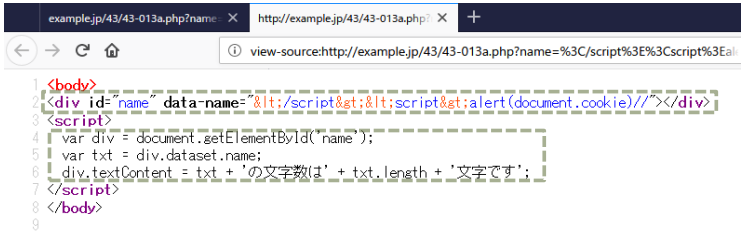
カスタムデータ属性(data-name="XXX")を使います

【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)



【ブラウザ】





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)

```
<li>クロスサイト・スクリプティング（発展編）</li>
<ol start="9">
<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>
<li><a href="43-010.php?url=javascript:alert(document.cookie)">43-010:href属性の動的生成(XSS)</a></li>
<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>
<!--
<li><a href="43-011.html?name=Yamada">43-011:DOM Based XSS(正常系)</a></li>
<li><a href="43-011.html?name=&lt;script>alert(document.cookie)&lt;/script>">43-011:DOM Based XSS(XSS)</a></li>
<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>
-->
<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>
<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>
<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>
<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>
<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>
<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>
</ol>
```

【サーバ： 43/43-013b.php 】

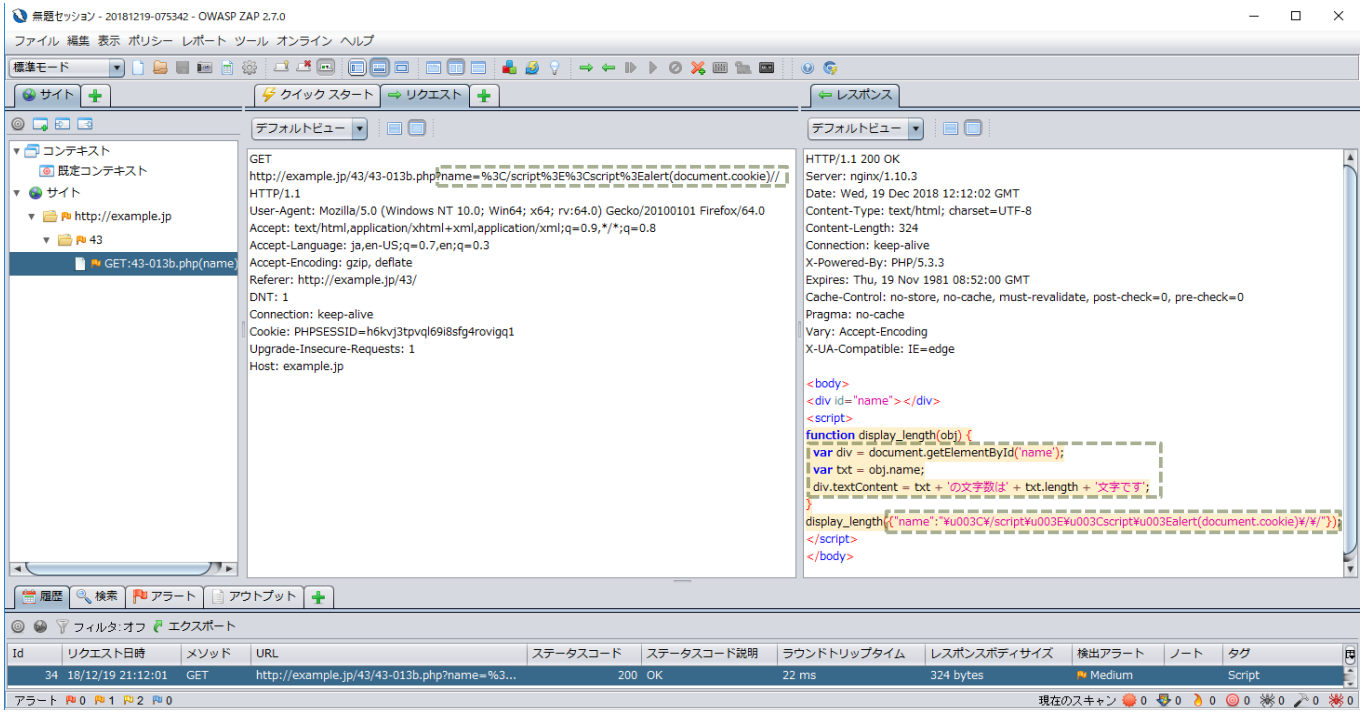
/var/www/html/43/43-013b.php - wasbook@192.168.56.101 - エディタ - WinSCP

```
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)



【ブラウザ】