

4.11 OSコマンド呼び出しの際に発生する脆弱性

OSコマンドインジェクションの脆弱性

Webアプリケーションが、シェル経由でOSコマンドを実行できる脆弱性

OSコマンドインジェクション脆弱性の典型的な攻撃シナリオ

- ① 攻撃ツールを外部からダウンロードする
- ② ダウンロードしたツールに実行権限を与える
- ③ OS脆弱性を内部から攻撃して、管理者権限を得る(権限昇格)
- ④ 攻撃者はサーバを自由に悪用する

OSコマンドインジェクション脆弱性の対策

- ① OSコマンド呼び出し機能のある関数の利用を避ける
- ② OSコマンド呼び出し機能のある関数には外部からのパラメータを渡さない
- ③ OSコマンドに渡すパラメータを安全な関数によりエスケープする

Unixのfindコマンドでは、-execオプションにより、検索したファイル名に対して、コマンドを実行することができます。この機能を利用して、想定外のコマンドを実行されてしまう危険性があります

シュルの持つ以下の機能が攻撃に役立ちます

```
$ echo aaa ; echo bbb          # コマンドを続けて実行
$ echo aaa & echo bbb          # バックグラウンドとフォアグラウンドで実行
$ echo aaa && echo bbb          # 最初のコマンドが成功したら、第2のコマンドを実行
$ echo aaa || echo bbb        # 最初のコマンドが失敗したら、第2のコマンドを実行
$ wc `ls`                      # バッククォートで囲った文字列をコマンドとして実行
$ echo aaa | wc                # 第1のコマンドの出力を第2のコマンドの入力とする
```

OSコマンドインジェクション脆弱性への保険的対策

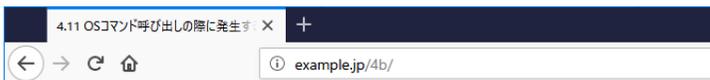
- ① パラメータの検証(数値の最小値、最大値、英数字のみなど)
- ② アプリケーションのユーザー権限を必要最低限にする
- ③ WebサーバなどのOSやミドルウェアのパッチ適用(最新の状態にする)

参考: 内部でシェルを呼び出す関数

PHP	system()	exec()	passthru()	proc_open()	popen()	shell_exec()
Perl	exec()	system()	...	qx/.../	open()	
Ruby	exec()	system()	...			

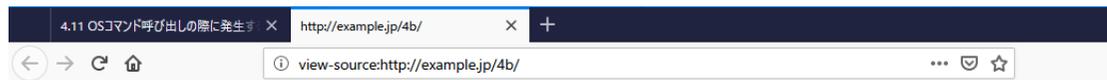
4b-001:お問い合わせフォーム(OSコマンドインジェクション)

【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

1. [4b-001:お問い合わせフォーム\(OSコマンドインジェクション\)](#)
2. [4b-001:お問い合わせフォーム\(OSコマンドインジェクション\)\(攻撃\)](#)
3. [4b-001a:お問い合わせフォーム\(OSコマンドを呼ばない\)](#)
4. [4b-001a:お問い合わせフォーム\(OSコマンドを呼ばない\)\(攻撃\)](#)
5. [4b-001b:お問い合わせフォーム\(シェルを経由しない\)](#)
6. [4b-001b:お問い合わせフォーム\(シェルを経由しない\)\(攻撃\)](#)
7. [4b-001c:お問い合わせフォーム\(コマンドラインにパラメータを渡さない\)](#)
8. [4b-001c:お問い合わせフォーム\(コマンドラインにパラメータを渡さない\)\(攻撃\)](#)
9. [4b-001d:お問い合わせフォーム\(パラメータをエスケープ\)](#)
10. [4b-001d:お問い合わせフォーム\(パラメータをエスケープ\)\(攻撃\)](#)



```
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>
```

11. [4b-001d:お問い合わせフォーム\(環境変数経由のパラメータ渡し\)](#)
12. [4b-001d:お問い合わせフォーム\(環境変数経由のパラメータ渡し\)\(攻撃\)](#)
13. [4b-003:Perlのopen文によるpwdコマンド呼び出し](#)
14. [4b-004:Perlのopen文によるOSコマンドインジェクション \(正常系\)](#)
15. [4b-004:Perlのopen文によるOSコマンドインジェクション \(ls /sbin\)](#)
16. [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 \(正常系\)](#)
17. [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-001.html】

```

/var/www/html/4b/4b-001.html - wasbook@example.jp - エディタ
<body>
<form action="4b-002.php" method="POST">
お問い合わせどうぞ<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-002.php】

```

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

```

OSコマンド・インジェクション脆弱性があります

```

19 </li><a href="/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">/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>
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-001.html → レスポンス】

The screenshot displays the OWASP ZAP 2.7.0 interface. The main window shows the request and response for the URL `http://example.jp/4b/4b-001.html`. The request is a GET method with various headers including `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0`. The response is an HTTP/1.1 200 OK with headers such as `Server: nginx/1.10.3` and `Date: Mon, 31 Dec 2018 07:40:06 GMT`. The response body contains HTML code for a form with a submit button labeled "送信".

```
GET http://example.jp/4b/4b-001.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 07:40:06 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 259
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: "103-56c2a2dec32ba-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
<form action="4b-002.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>
```

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
1	18/12/31 16:40:06	GET	http://example.jp/4b/4b-001.html	200	OK	6 ms	259 bytes	Medium		Form

現在のスキャン: 0 0 0 0 0 0 0 0 0 0

【ブラウザ→サーバ: リクエスト 4b/4b-002.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-002.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-001.html
 Content-Type: application/x-www-form-urlencoded
 Content-Length: 117
 DNT: 1
 Connection: keep-alive
 Upgrade-Insecure-Requests: 1
 Host: example.jp

mail=bob%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 07:44:24 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
4	18/12/31 16:44:23	POST	http://example.jp/4b/4b-002.php	200	OK	70 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

【ブラウザ】

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

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

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

```

1 <body>
2 <form action="4b-002.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-001.html

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

お問い合わせをどうぞ

メールアドレス bob@example.jp

お問い合わせ よろしくお願ひします

お問い合わせ

送信

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

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

お問い合わせを受け付けました

example.jp/4b/4b-002.php http://example.jp/4b/4b-002.php

view-source:http://example.jp/4b/4b-002.php

```

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

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)

【ブラウザ】



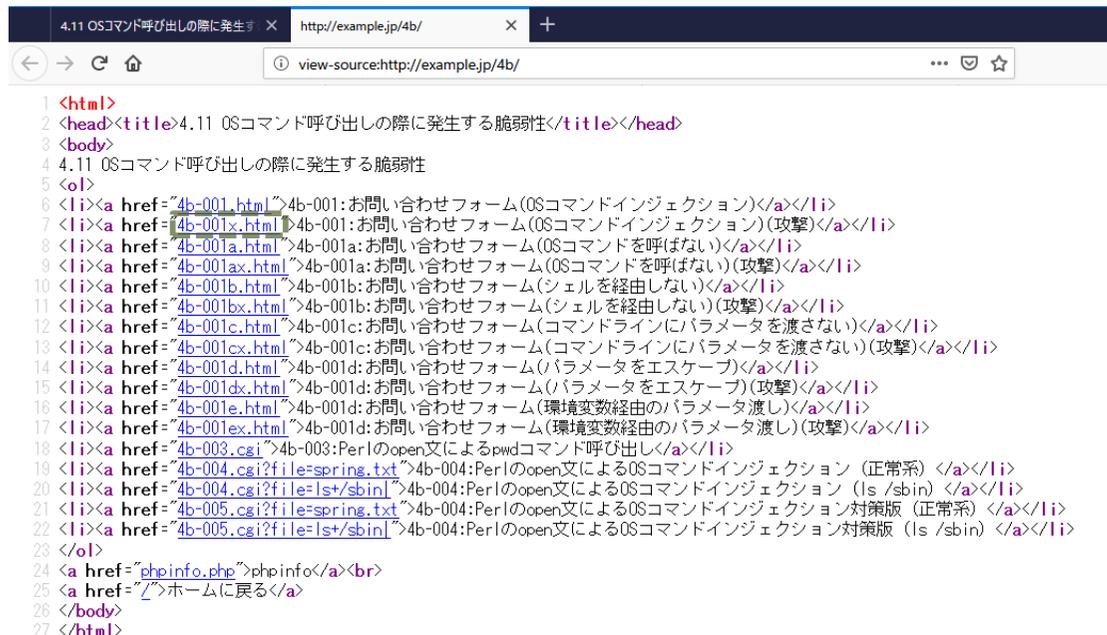
4.11 OSコマンド呼び出しの際に発生する脆弱性

- 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-001x.html】

```
/var/www/html/4b/4b-001x.html - wasbook@example.jp - エディタ - WinSCP
kbody>
<form action="4b-002.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-002.php】

```
/var/www/html/4b/4b-002.php - wasbook@example.jp - エディタ - WinSCP
k?php
$mail = filter_INPUT(INPUT_POST, 'mail');
system("/usr/sbin/sendmail -i <template.txt $mail");
?>
<body>
お問い合わせを受け付けました
</body>
OSコマンド・インジェクション脆弱性があります
```

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

The screenshot displays the OWASP ZAP 2.7.0 interface. The main window 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 for 'http://example.jp/4b-001x.html'. The response pane shows an HTML document with a form for contacting the site.

Request:

```
GET http://example.jp/4b-001x.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
```

Response:

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 31 Dec 2018 08:17:31 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 298
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: "12a-56c2a2debf43a-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
<form action="/4b-002.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>
```

At the bottom, a table lists the captured requests and responses:

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
103	18/12/31 17:17:30	GET	http://example.jp/4b-001x.html	200	OK	4 ms	298 bytes	Medium		Form
105	18/12/31 17:17:44	POST	http://example.jp/4b-002.php	200	OK	45 ms	1,907 bytes	Medium		

The status bar at the bottom shows '現在のスキャン' (Current Scan) with various icons and counts.

【ブラウザ】

example.jp/4b/4b-001x.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-001x.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-002.php

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false _apt:x:104:65534:/:/nonexistent:/bin/false messagebus:x:105:109:/:/var/run/dbus:/bin/false sshd:x:106:65534:/:/run/sshd:/usr/sbin/nologin wasbook:x:1000:1000:wasbook,,,:/home/wasbook:/bin/bash mysql:x:107:112:MySQL Server,,,:/nonexistent:/bin/false postfix:x:108:113:/:/var/spool/postfix:/bin/false dovecot:x:109:115:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false dovenull:x:110:116:Dovecot login user,,,:/nonexistent:/bin/false tomcat8:x:111:117:/:/var/lib/tomcat8:/bin/false ftp:x:112:118:ftp daemon,,,:/srv/ftp:/bin/false alice:x:1001:1001:,:/home/alice:/bin/bash bob:x:1002:1002:,:/home/bob:/bin/bash carol:x:1003:1003:,:/home/carol:/bin/bash お問い合わせを受け付けました
```

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

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

```
1 <body>
2 <form action="4b-002.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
```

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

view-source:http://example.jp/4b/4b-002.php

```
1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin:x:2:2:bin:/bin:/usr/sbin/nologin
4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
7 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
8 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
9 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
10 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
11 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
12 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
13 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
14 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
15 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
16 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
17 gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
18 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19 systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
20 systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
21 systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
22 systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
23 _apt:x:104:65534:/:/nonexistent:/bin/false
24 messagebus:x:105:109:/:/var/run/dbus:/bin/false
25 sshd:x:106:65534:/:/run/sshd:/usr/sbin/nologin
26 wasbook:x:1000:1000:wasbook,,,:/home/wasbook:/bin/bash
27 mysql:x:107:112:MySQL Server,,,:/nonexistent:/bin/false
28 postfix:x:108:113:/:/var/spool/postfix:/bin/false
29 dovecot:x:109:115:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false
30 dovenull:x:110:116:Dovecot login user,,,:/nonexistent:/bin/false
31 tomcat8:x:111:117:/:/var/lib/tomcat8:/bin/false
32 ftp:x:112:118:ftp daemon,,,:/srv/ftp:/bin/false
33 alice:x:1001:1001:,:/home/alice:/bin/bash
34 bob:x:1002:1002:,:/home/bob:/bin/bash
35 carol:x:1003:1003:,:/home/carol:/bin/bash
36 <body>
37 お問い合わせを受け付けました
38 </body>
39
```

4b-001a:お問い合わせフォーム(OSコマンドを呼ばない)

【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

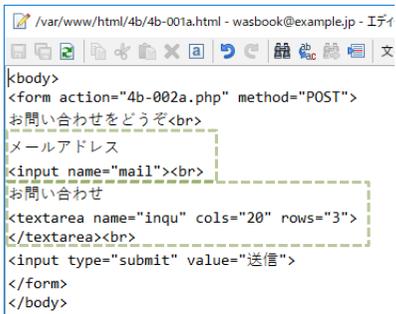
- 4b-001:お問い合わせフォーム(OSコマンドインジェクション)
- 4b-001:お問い合わせフォーム(OSコマンドインジェクション)(攻撃)
- 4b-001a:お問い合わせフォーム(OSコマンドを呼ばない) 
- 4b-001a:お問い合わせフォーム(OSコマンドを呼ばない)(攻撃)
- 4b-001b:お問い合わせフォーム(シェルを経由しない)
- 4b-001b:お問い合わせフォーム(シェルを経由しない)(攻撃)
- 4b-001c:お問い合わせフォーム(コマンドラインにパラメータを渡さない)
- 4b-001c:お問い合わせフォーム(コマンドラインにパラメータを渡さない)(攻撃)
- 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](#)



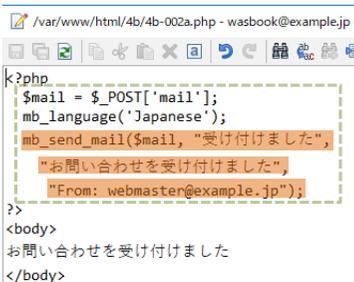
```
1 <html>
2 <head><title>4.11 OSコマンド呼び出しの際に発生する脆弱性</title></head>
3 <body>
4 4.11 OSコマンド呼び出しの際に発生する脆弱性
5 <ol>
6 <li><a href="4b-001.html">4b-001: お問い合わせフォーム(OSコマンドインジェクション)</a></li>
7 <li><a href="4b-001x.html">4b-001: お問い合わせフォーム(OSコマンドインジェクション)(攻撃)</a></li>
8 <li><a href="4b-001a.html">4b-001a: 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-001a.html】



```
<body>
<form action="4b-002a.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-002a.php】



```
<?php
$mail = $_POST['mail'];
mb_language('Japanese');
mb_send_mail($mail, "受け付けました",
"お問い合わせを受け付けました",
"From: webmaster@example.jp");
?>
<body>
お問い合わせを受け付けました
</body>
```

OSコマンド・インジェクション脆弱性は対策しましたが、
メールヘッダ・インジェクション脆弱性があります

【ブラウザ→サーバ: リクエスト 4b/4b-001a.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-001a.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 08:35:51 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: "104-56c2a2dec425a-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge
```

```
<body>
<form action="/4b-002a.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
162	18/12/31 17:35:29	GET	http://example.jp/4b/4b-001a.html	200	OK	21.03 s	260 bytes	Medium		Form
165	18/12/31 17:43:56	POST	http://example.jp/4b/4b-002a.php	200	OK	205 ms	58 bytes	Medium		

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→サーバ: リクエスト 4b/4b-002a.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

デフォルトビュー

```
POST http://example.jp/4b/4b-002a.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-001a.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 119
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp

mail=candy%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 08:43:57 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
162	18/12/31 17:35:29	GET	http://example.jp/4b/4b-001a.html	200	OK	21.03 s	260 bytes	Medium		Form
165	18/12/31 17:43:56	POST	http://example.jp/4b/4b-002a.php	200	OK	205 ms	58 bytes	Medium		

アラート 0 0 1 0 2 0 0

現在のスキャン 0 0 0 0 0 0 0 0 0 0 0 0

【ブラウザ】

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

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

example.jp/4b/4b-001a.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-002a.php

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

お問い合わせを受け付けました

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

http://example.jp/4b/4b-001a.html

```
1 <body>
2 <form action="4b-002a.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-002a.php

http://example.jp/4b/4b-002a.php

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

4b-001a:お問い合わせフォーム(OSコマンドを呼ばない)

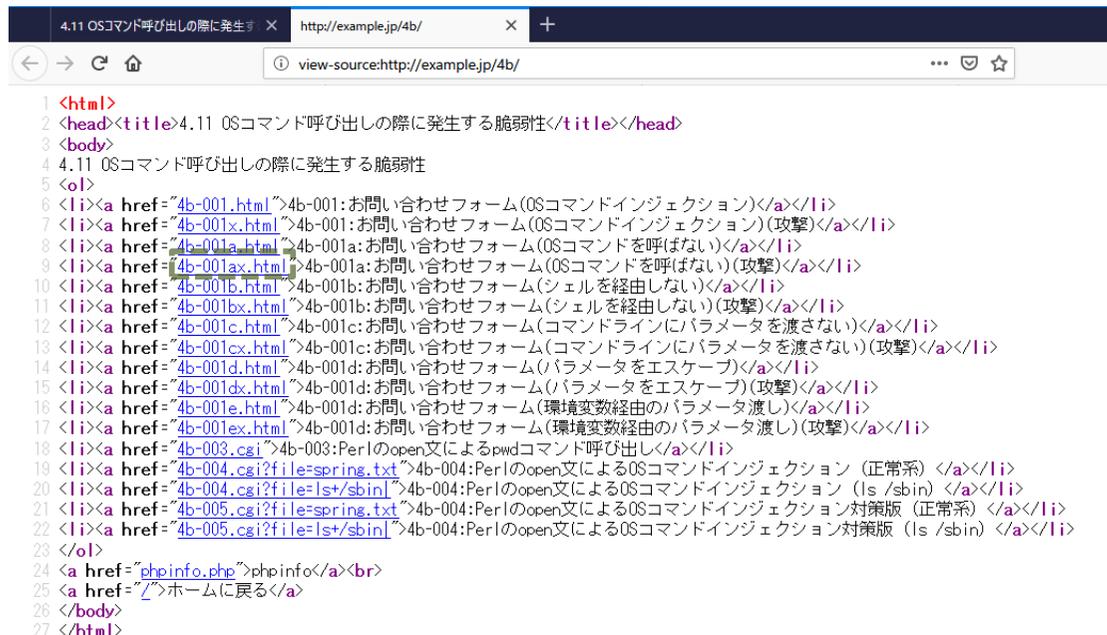
【ブラウザ】



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](#)



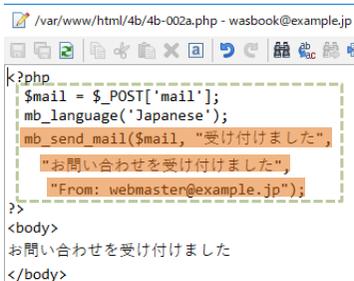
```
1 <html>
2 <head><title>4.11 OSコマンド呼び出しの際に発生する脆弱性</title></head>
3 <body>
4 4.11 OSコマンド呼び出しの際に発生する脆弱性
5 <ol>
6 <li><a href="4b-001.html">4b-001: お問い合わせフォーム(OSコマンドインジェクション)</a></li>
7 <li><a href="4b-001x.html">4b-001: お問い合わせフォーム(OSコマンドインジェクション)(攻撃)</a></li>
8 <li><a href="4b-001a.html">4b-001a: 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-001ax.html】



```
/var/www/html/4b/4b-001ax.html - wasbook@example.jp - エディタ - WinSCP
<body>
<form action="4b-002a.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-002a.php】



```
/var/www/html/4b/4b-002a.php - wasbook@example.jp
<?php
$mail = $_POST['mail'];
mb_language('Japanese');
mb_send_mail($mail, "受け付けました",
"お問い合わせを受け付けました",
"From: webmaster@example.jp");
?>
<body>
お問い合わせを受け付けました
</body>
```

OSコマンド・インジェクション脆弱性は対策しましたが、
メールヘッダ・インジェクション脆弱性があります

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

The screenshot displays 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 window is split into two panes: 'デフォルトビュー' (Default View) on the left and 'デフォルトビュー' (Default View) on the right. The left pane shows the request details for 'http://example.jp/4b/4b-001ax.html HTTP/1.1'. The right pane shows the response details for 'HTTP/1.1 200 OK'. Below the panes is a toolbar with '履歴' (History), '検索' (Search), 'アラート' (Alerts), and 'アウトプット' (Output). At the bottom, a table lists the request and response details.

Request Details:

```

GET http://example.jp/4b/4b-001ax.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
    
```

Response Details:

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 31 Dec 2018 08:58:56 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-56c2a2dec137a-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
<form action="4b-002a.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>
    
```

Request/Response Log Table:

Id	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
223	18/12/31 17:58:55	GET	http://example.jp/4b/4b-001ax.html	200	OK	5 ms	299 bytes	Medium		Form
225	18/12/31 18:01:12	POST	http://example.jp/4b/4b-002a.php	200	OK	51 ms	58 bytes	Medium		

アラート: 0 0 1 0 2 0 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-002a.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

クイック スタート リクエスト レスポンス

サイト

デフォルトビュー

コンテキスト

既定コンテ

サイト

```

POST http://example.jp/4b/4b-002a.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-001ax.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 139
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 09:01:13 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>

```

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

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
223	18/12/31 17:58:55	GET	http://example.jp/4b/4b-001ax.html	200	OK	5 ms	299 bytes	Medium		Form
225	18/12/31 18:01:12	POST	http://example.jp/4b/4b-002a.php	200	OK	51 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-001ax.html

お問い合わせをどうぞ

メールアドレス bob@example.jp;cat/etc

お問い合わせ

送信

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

お問い合わせをどうぞ

メールアドレス bob@example.jp;cat/etc

お問い合わせ

送信

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

お問い合わせを受け付けました

```
1 <body>
2 <form action="4b-002a.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-001b:お問い合わせフォーム(シェルを経由しない)

【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-001b.html 】

```
/var/www/html/4b/4b-001b.html - wasbook@example.jp - エディタ
<body>
<form action="4b-002b.cgi" 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-002b.cgi 】

```
/var/www/html/4b/4b-002b.cgi - wasbook@example.jp - エディタ - WinSCP
#!/usr/bin/perl
use strict;
use CGI;
use utf8;
use Encode;

my $q = new CGI;
my $mail = $q->param('mail');

# シェルを経由せずにsendmailコマンドをパイプとしてオープンする
open my $pipe, '|-', '/usr/sbin/sendmail', $mail or die $!;

# メール内容の流し込み
print $pipe encode('UTF-8', <<EndOfMail);
To: $mail
From: webmaster@example.jp
Subject: =?UTF-8?B?5Y+X44GR5LuY44GR44G+44GX44Gf?=
Content-Type: text/plain; charset="UTF-8"
Content-Transfer-Encoding: 8bit

お問い合わせを受け付けました
EndOfMail

close $pipe;

# 以下は画面表示
print encode('UTF-8', <<EndOfHTML);
Content-Type: text/html; charset=UTF-8

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

OSコマンド・インジェクション脆弱性は対策しましたが、
メールヘッダ・インジェクション脆弱性があります

※ '/usr/sbin/sendmail_ \$mail' のようにスペースで区切って
指定すると、シェル経由の呼び出しとなって、OSコマンド
脆弱性となります

【ブラウザ→サーバ: リクエスト 4b/4b-001b.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
サイト

```
GET http://example.jp/4b/4b-001b.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 09:28:05 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: "104-56c2a2debb5b9-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
<form action="4b-002b.cgi" 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
315	18/12/31 18:28:...	GET	http://example.jp/4b/4b-001b.html	200	OK	4 ms	260 bytes	Medium		Form

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-002b.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

コンテキスト

- 既定コンテキ
- サイト

```

POST http://example.jp/4b/4b-002b.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/4b-001b.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 118
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp

mail=dick%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 09:28:42 GMT
Content-Type: text/html;
charset=UTF-8
Connection: keep-alive
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
315	18/12/31 18:28:04	GET	http://example.jp/4b/4b-001b.html	200	OK	4 ms	260 bytes	Medium		Form
317	18/12/31 18:28:41	POST	http://example.jp/4b/4b-002b.cgi	200	OK	131 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

【ブラウザ】

example.jp/4b/4b-001b.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-001b.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-002b.cgi

お問い合わせを受け付けました

```
1 <body>
2 <form action="4b-002b.cgi" 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-001b:お問い合わせフォーム(シェルを経由しない)(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](#)

```
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-001bx.html】

```
/var/www/html/4b/4b-001bx.html - wasbook@example.jp - エディタ - WinSCP
<body>
<form action="4b-002b.cgi" 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-002b.cgi】

```
/var/www/html/4b/4b-002b.cgi - wasbook@example.jp - エディタ - WinSCP
#!/usr/bin/perl
use strict;
use CGI;
use utf8;
use Encode;

my $q = new CGI;
my $mail = $q->param('mail');

# シェルを経由せずにsendmailコマンドをパイプとしてオープンする
open my $pipe, '|-', '/usr/sbin/sendmail', $mail or die $!;

# メール内容の流し込み
print $pipe encode('UTF-8', <<EndOfMail);
To: $mail
From: webmaster@example.jp
Subject: =?UTF-8?B?5Y+X44GR5LuY44GR44G+44GX44Gf?=@
Content-Type: text/plain; charset="UTF-8"
Content-Transfer-Encoding: 8bit

お問い合わせを受け付けました
EndOfMail

<close $pipe;

# 以下は画面表示
print encode('UTF-8', <<EndOfHTML);
Content-Type: text/html; charset=UTF-8

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

OSコマンド・インジェクション脆弱性は対策しましたが、
メールヘッダ・インジェクション脆弱性があります

※ '/usr/sbin/sendmail_ \$mail' のようにスペースで区切って
指定すると、シェル経由の呼び出しとなって、OSコマンド
脆弱性となります

【ブラウザ→サーバ: リクエスト 4b/4b-001bx.html → 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: 'コンテキスト' (Context) on the left and 'デフォルトビュー' (Default View) on the right. The context pane shows a tree view with 'コンテキスト' and 'サイト'. The default view pane displays the request and response details.

Request Details:

```

GET http://example.jp/4b/4b-001bx.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
    
```

Response Details:

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Mon, 31 Dec 2018 09:40:13 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-56c2a2dec137a-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
<form action="4b-002b.cgi" 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>
    
```

At the bottom, there is a table showing the request and response 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
320	18/12/31 18:40:12	GET	http://example.jp/4b/4b-001bx.html	200	OK	4 ms	299 bytes	Medium		Form
322	18/12/31 18:41:56	POST	http://example.jp/4b/4b-002b.cgi	200	OK	113 ms	58 bytes	Medium		

The bottom status bar shows '現在のスキャン' (Current Scan) with various icons and counts.

【ブラウザ→サーバ: リクエスト 4b/4b-002b.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

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

POST http://example.jp/4b/4b-002b.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/4b-001bx.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 09:41:57 GMT

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

Connection: keep-alive

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...	URL	ステータスコ...	ステータスコード...	ラウンドトリップ...	レスポンスボディ...	検出アラ...	ノ...	タグ
320	18/12/31 18:...	GET	http://example.jp/4b/4b-001bx.html	200	OK	4 ms	299 bytes	Medium		Form
322	18/12/31 18:...	POST	http://example.jp/4b/4b-002b.cgi	200	OK	113 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-001bx.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-001bx.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-002b.cgi

お問い合わせを受け付けました

```
1 <body>
2 <form action="4b-002b.cgi" 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-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)

【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](#)

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>
```

【サーバ: 4b/4b-001c.html 】

```
/var/www/html/4b/4b-001c.html - wasbook@example.jp - イディ  
<body>  
<form action="4b-002c.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-002c.php 】

```
/var/www/html/4b/4b-002c.php - wasbook@example.jp - イディタ - WinSCP  
<?php  
$mail = $_POST['mail'];  
$h = popen('/usr/sbin/sendmail -t -i', 'w');  
if ($h === FALSE) {  
    die('ただいま混み合っております。しばらくたってから..');  
}  
fwrite($h, <<<EndOfMail  
To: $mail  
From: webmaster@example.jp  
Subject: =?UTF-8?B?5Y+X44GR5LuY44GR44G+44GX44Gf?=  
Content-Type: text/plain; charset="UTF-8"  
Content-Transfer-Encoding: 8bit  
  
お問い合わせを受け付けました  
EndOfMail  
>);  
  
pclose($h);  
?>  
<body>  
お問い合わせを受け付けました  
</body>
```

OSコマンド・インジェクション脆弱性是对策しましたが、
メールヘッダ・インジェクション脆弱性があります

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

The screenshot displays the OWASP ZAP 2.7.0 interface. The top menu includes 'ファイル', '編集', '表示', 'ポリシー', 'レポート', 'ツール', 'オンライン', and 'ヘルプ'. The main window is split into two panes: 'リクエスト' (Request) and 'レスポンス' (Response). The request pane shows a GET request for 'http://example.jp/4b/4b-001c.html' with various headers. The response pane shows an 'HTTP/1.1 200 OK' status with headers and an HTML body containing a form with a text input and a submit button.

```
GET http://example.jp/4b/4b-001c.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 11:30:11 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: "104-56c2a2deba619-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
<form action="/4b-002c.php" method="POST">
お問い合わせどうぞ<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>
```

Id	リクエスト日時	メソ...	URL	ステータスコ...	ステータスコード...	ラウンドトリップ...	レスポンスボディ...	検出アラ...	ノ...	タグ
326	18/12/31 20:...	GET	http://example.jp/4b/4b-001c.html	200	OK	5 ms	260 bytes	Medium		Form
328	18/12/31 20:...	POST	http://example.jp/4b/4b-002c.php	200	OK	59 ms	58 bytes	Medium		

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→サーバ: リクエスト 4b/4b-0012c.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-002c.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-001c.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 118
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp

mail=edyi%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 11:44:07 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>
```

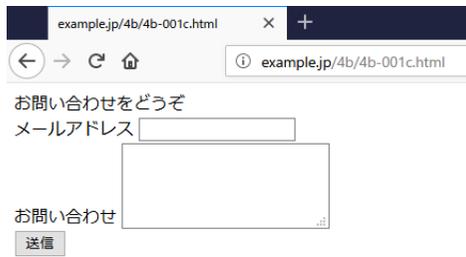
履歴 検索 アラート アウトプット +

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
326	18/12/31 20:30:10	GET	http://example.jp/4b/4b-001c.html	200	OK	5 ms	260 bytes	Medium		Form
328	18/12/31 20:44:06	POST	http://example.jp/4b/4b-002c.php	200	OK	59 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

【ブラウザ】



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

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

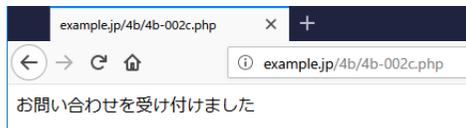
example.jp/4b/4b-001c.html

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-002c.php

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

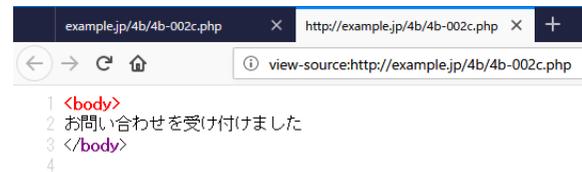
お問い合わせを受け付けました



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

http://example.jp/4b/4b-001c.html

```
1 <body>
2 <form action="4b-002c.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-002c.php

http://example.jp/4b/4b-002c.php

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

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)

【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-001cx.html 】

```
/var/www/html/4b/4b-001cx.html - wasbook@example.jp - エディタ - WinSCP
<body>
<form action="4b-002c.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-002c.php 】

```
/var/www/html/4b/4b-002c.php - wasbook@example.jp - エディタ - WinSCP
<?php
$mail = $_POST['mail'];
$h = popen('/usr/sbin/sendmail -t -i', 'w');
if ($h == FALSE) {
    die('ただいま混み合っております。しばらくたってから..');
}
fwrite($h, <<<EndOfMail
To: $mail
From: webmaster@example.jp
Subject: =?UTF-8?B?5Y+X44GR5LuY44GR44G+44GX44Gf?=@
Content-Type: text/plain; charset="UTF-8"
Content-Transfer-Encoding: 8bit

お問い合わせを受け付けました
EndOfMail
);

pclose($h);
?>
<body>
お問い合わせを受け付けました
</body>
```

OSコマンド・インジェクション脆弱性は対策しましたが、
メールヘッダ・インジェクション脆弱性があります

【ブラウザ→サーバ: リクエスト 4b/4b-001cx.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-001cx.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 11:57:31 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-56c2a2dec425a-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
<form action="/4b-002c.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
331	18/12/31 20:57...	GET	http://example.jp/4b/4b-001cx.html	200	OK	5 ms	299 bytes	Medium		Form
333	18/12/31 20:59...	POST	http://example.jp/4b/4b-002c.php	200	OK	59 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-002c.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-002c.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-001cx.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+%2Ffetc%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 11:59:31 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
331	18/12/31 20:57...	GET	http://example.jp/4b/4b-001cx.html	200	OK	5 ms	299 bytes	Medium	Form	
333	18/12/31 20:59...	POST	http://example.jp/4b/4b-002c.php	200	OK	59 ms	58 bytes	Medium		

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-001cx.html

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

example.jp/4b/4b-001cx.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-002c.php

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

お問い合わせを受け付けました

```
1 <body>
2 <form action="4b-002c.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
```