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
③OS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

①OSコマンド呼び出し機能のある関数の利用を避ける
②OS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
③OS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`                             # バッククウ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

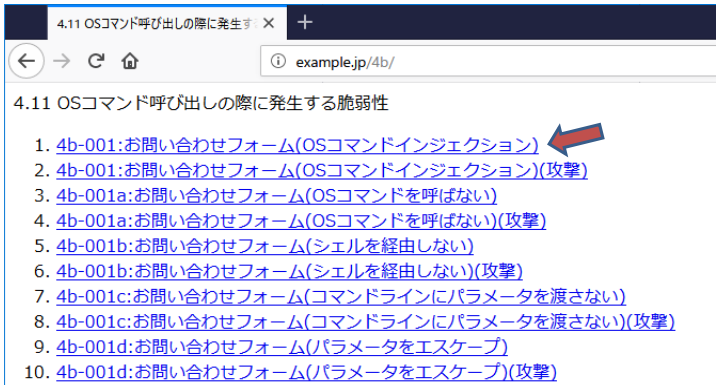
①パラメータの検証（数値の最小値、最大値、英数字のみなど）
②アプリケーションのユーザ権限を必要最低限にする
③WebサーバなどのOSやミドルウエアのパッチ適用（最新の状態にする）

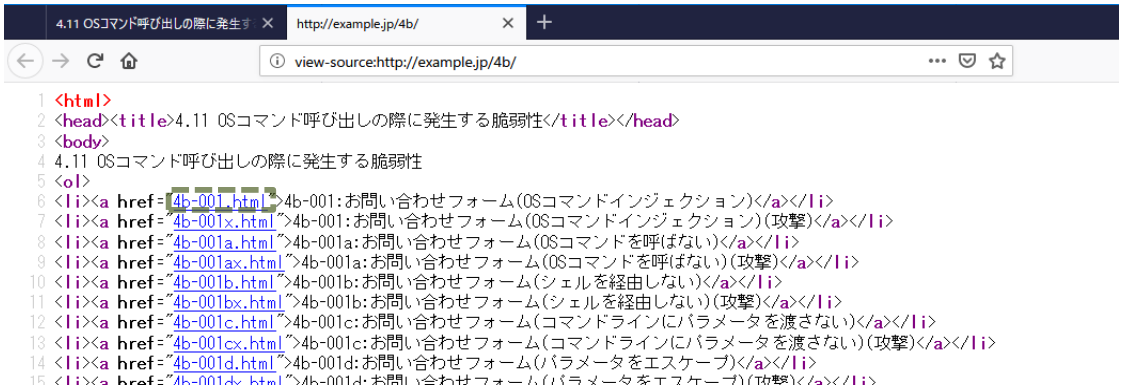
参考：内部でシェルを呼び出す関数

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】





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

```
<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>
<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>
<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>
<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>
<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>
<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>
<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>
</ol>
<a href="phpinfo.php">phpinfo</a><br>
<a href="/">ホームに戻る</a>
</body>
</html>
```

【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>
```

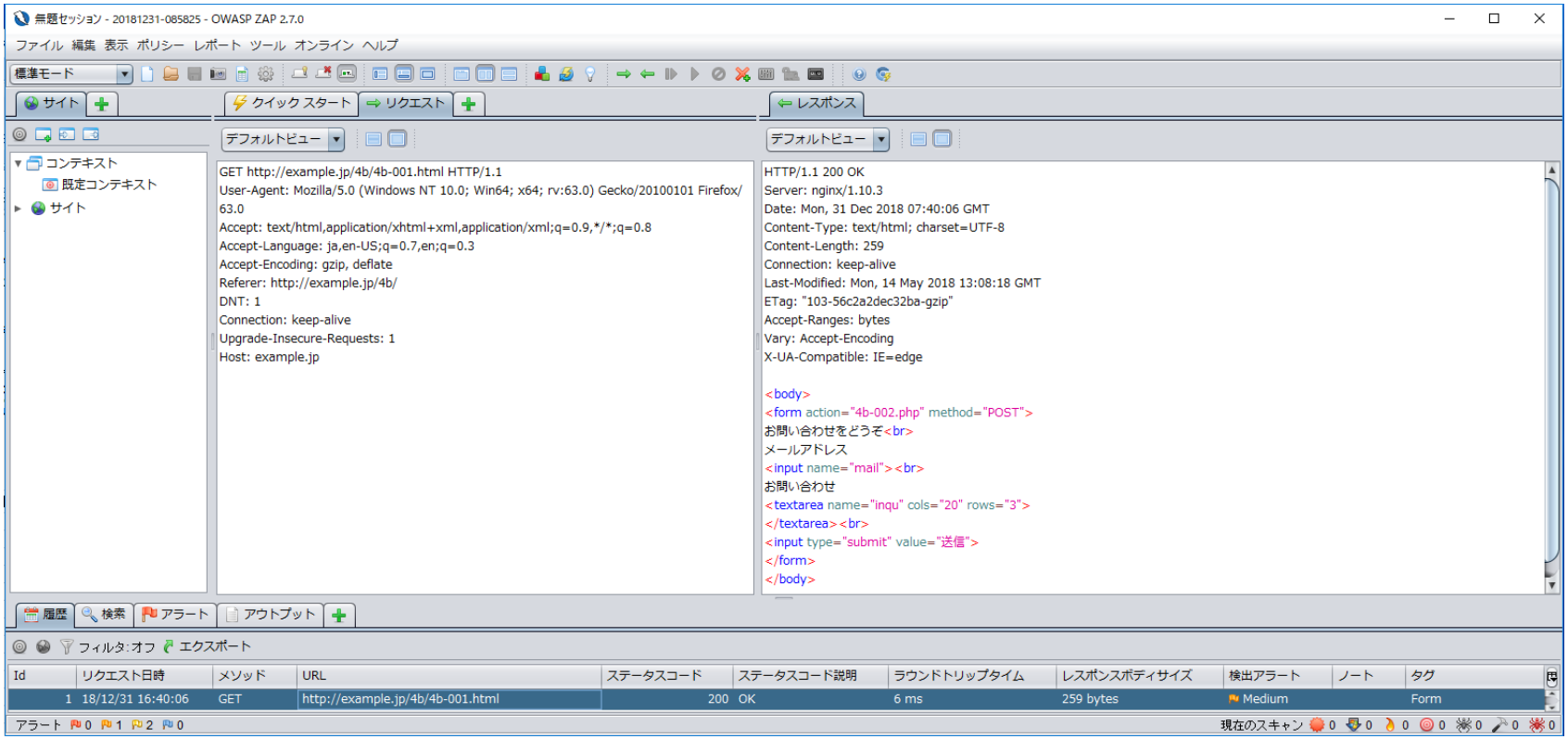
【サーバ： 4b/4b-002.php 】

/var/www/html/4b/4b-002.php - wasbook@example.jp - エディタ - WinSCP

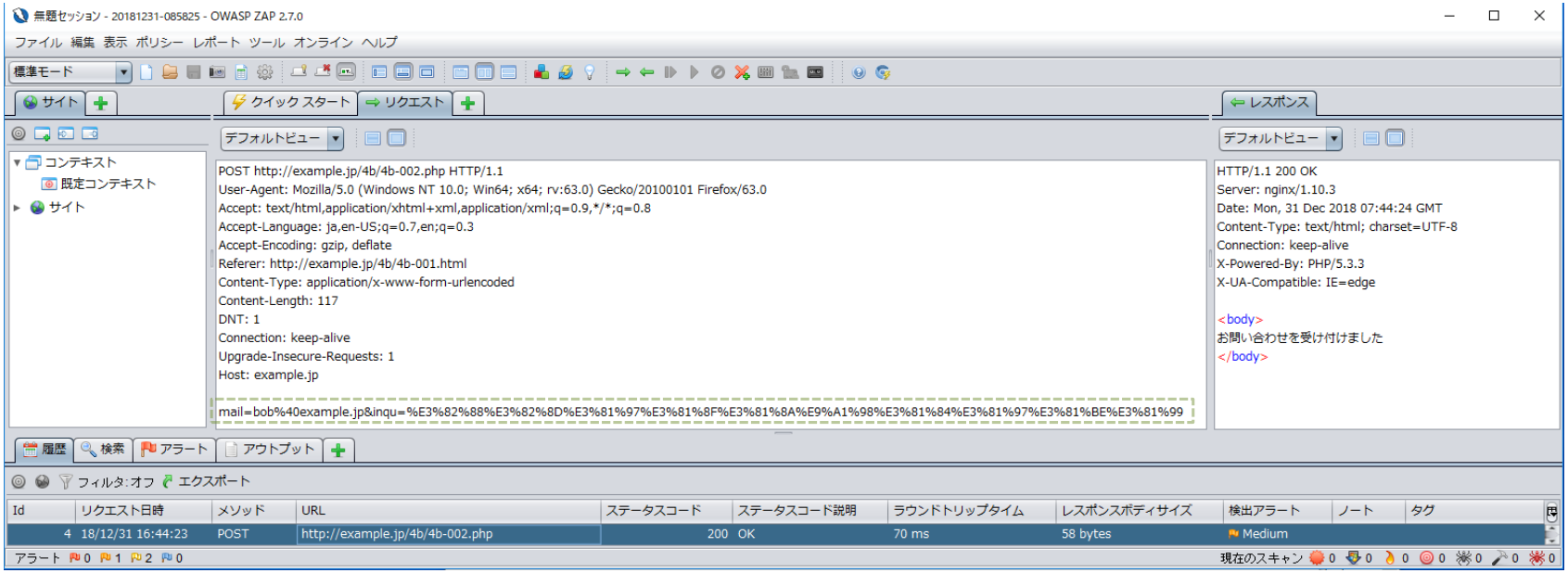
```
<?php
  $mail = filter_INPUT(INPUT_POST, 'mail');
  system("/usr/sbin/sendmail -i <template.txt $mail");
?>
<body>
お問い合わせを受け付けました
</body>
```

OSコマンド・インジェクション脆弱性があります

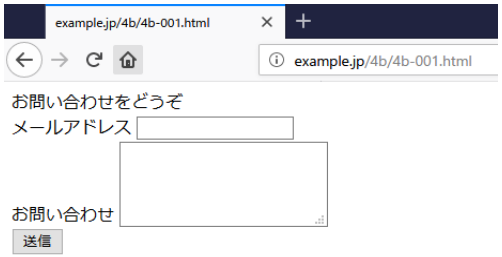
【ブラウザ→サーバ： リクエスト 4b/4b-001.html → レスポンス 】

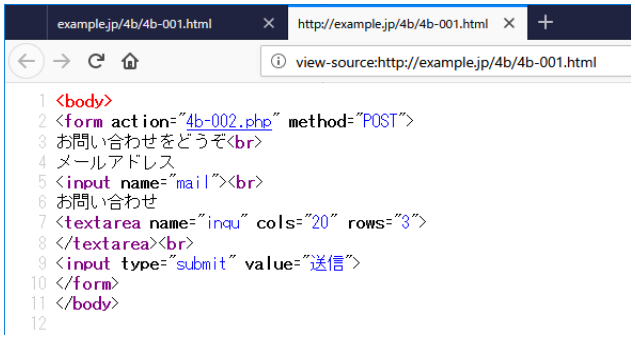


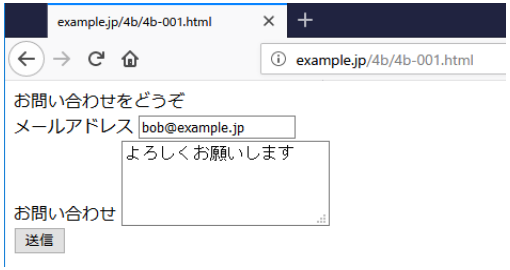
【ブラウザ→サーバ：リクエスト 4b/4b-002.php → レスポンス 】

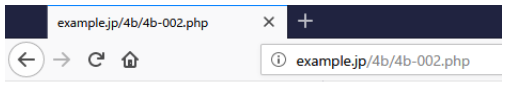


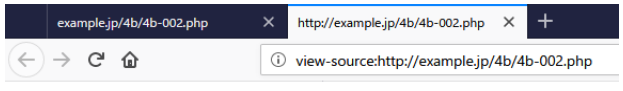
【ブラウザ】





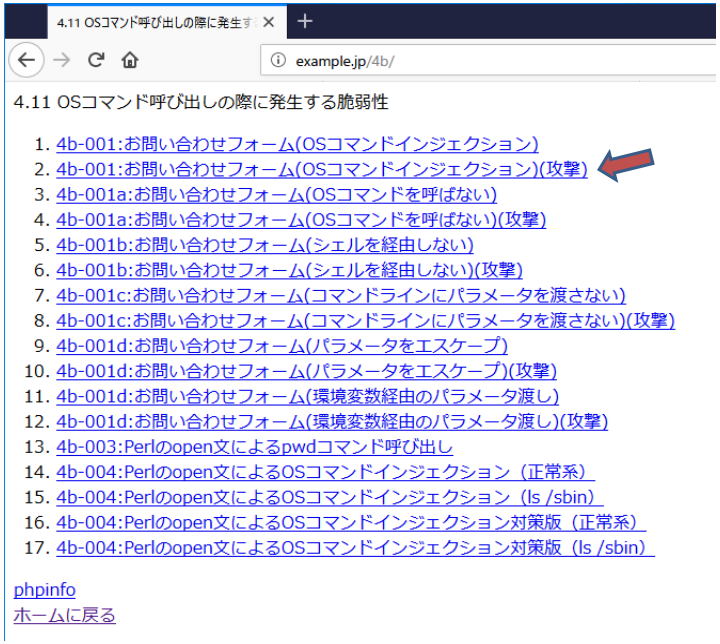




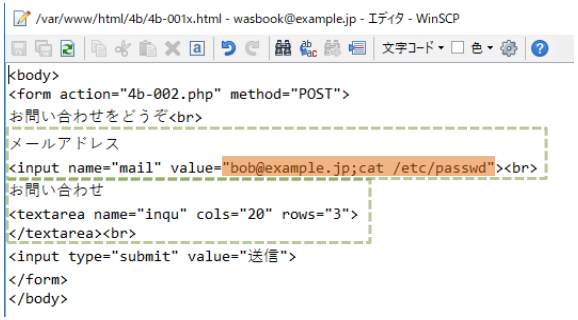


4b-001:お問い合わせフォーム(OSコマンドインジェクション)(攻撃)

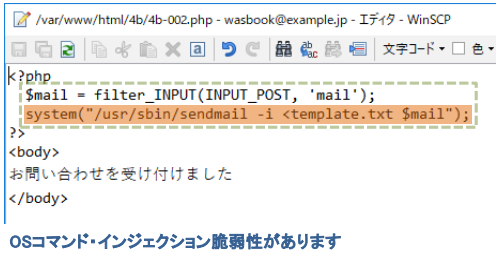
【ブラウザ】



【サーバ： 4b/4b-001x.html 】

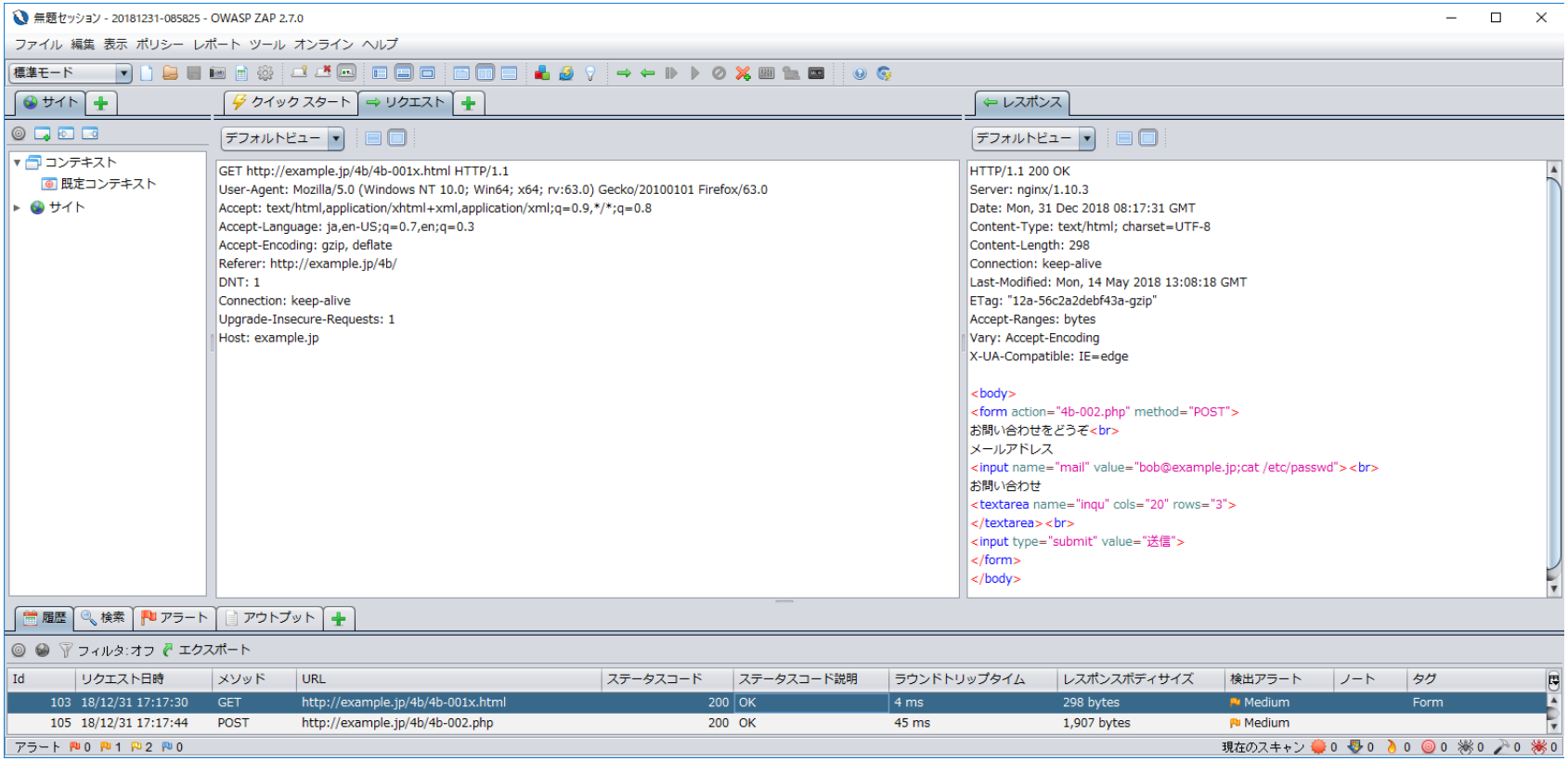


【サーバ： 4b/4b-002.php 】

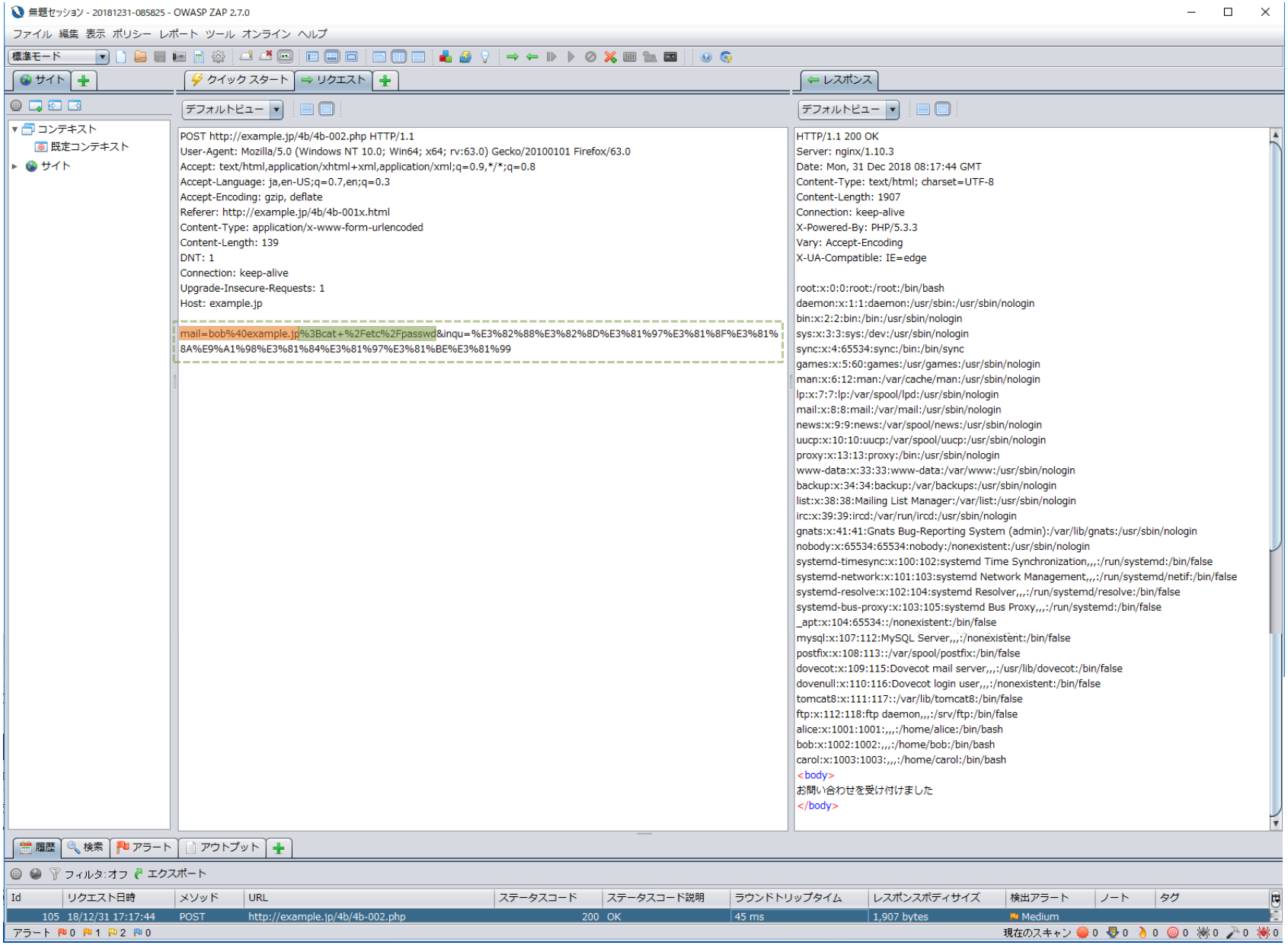


OSコマンド・インジェクション脆弱性があります

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

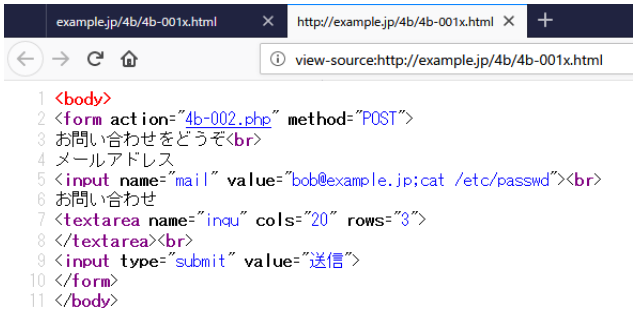


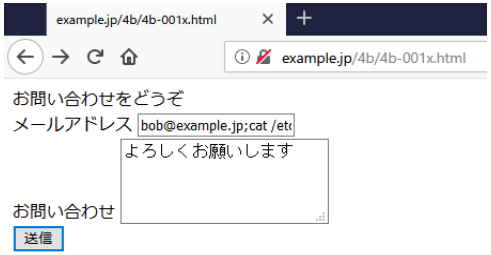
【ブラウザ→サーバ：リクエスト 4b/4b-002.php → レスポンス 】

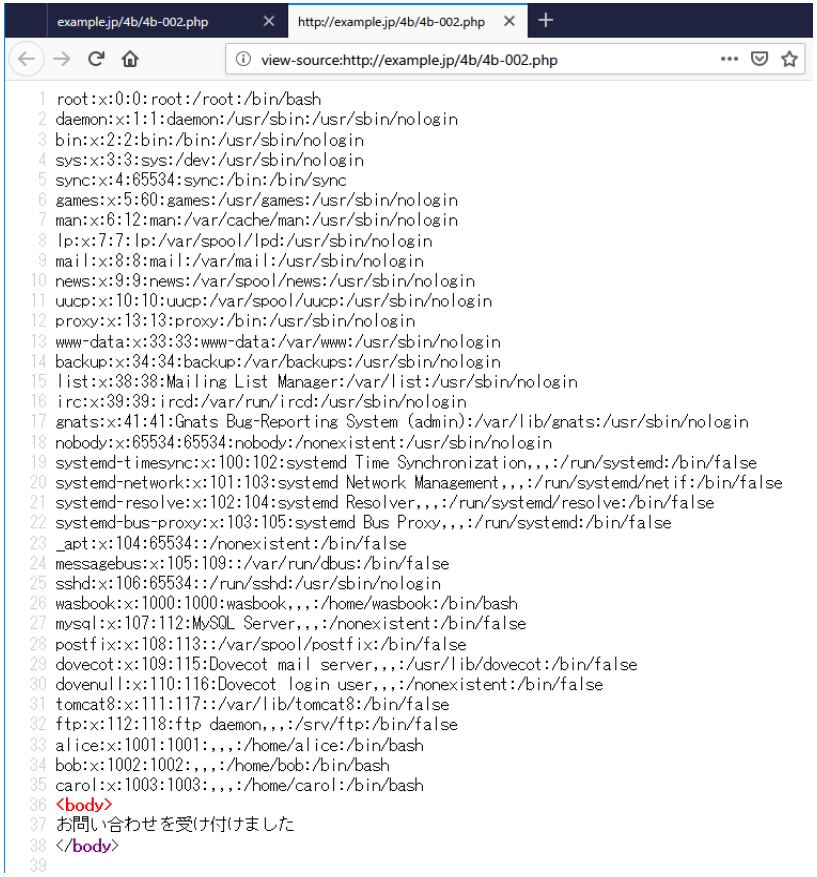


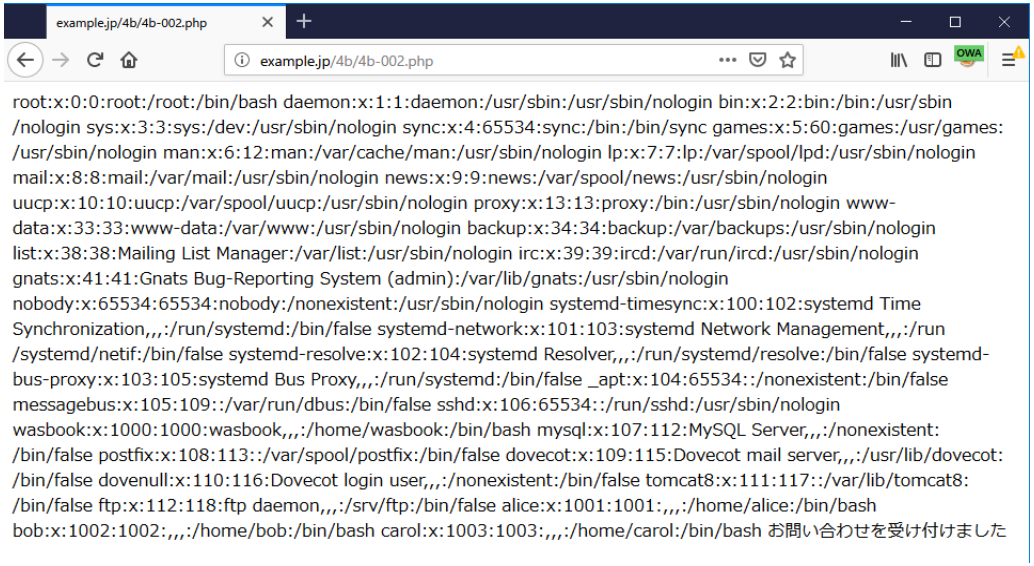
【ブラウザ】


example.jp/4b/4b-001x.html
example.jp/4b/4b-001x.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-001x.html
http://example.jp/4b/4b-001x.html
view-source:http://example.jp/4b/4b-001x.html
<body>
<form action="4b-002.php" method="POST">
お問い合わせをどうぞ
メールアドレス
<input name="mail" value="bob@example.jp;cat /etc/passwd">
お問い合わせ
<textarea name="inqu" cols="20" rows="3">
</textarea>
<input type="submit" value="送信">
</form>
</body>


example.jp/4b/4b-001x.html
example.jp/4b/4b-001x.html
お問い合わせをどうぞ
メールアドレス
bob@example.jp;cat /etc
よろしくお願いします
お問い合わせ
送信


example.jp/4b/4b-002.php
http://example.jp/4b/4b-002.php
view-source:http://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
<body>
お問い合わせを受け付けました
</body>


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

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】

【サーバ： 4b/4b-001a.html 】

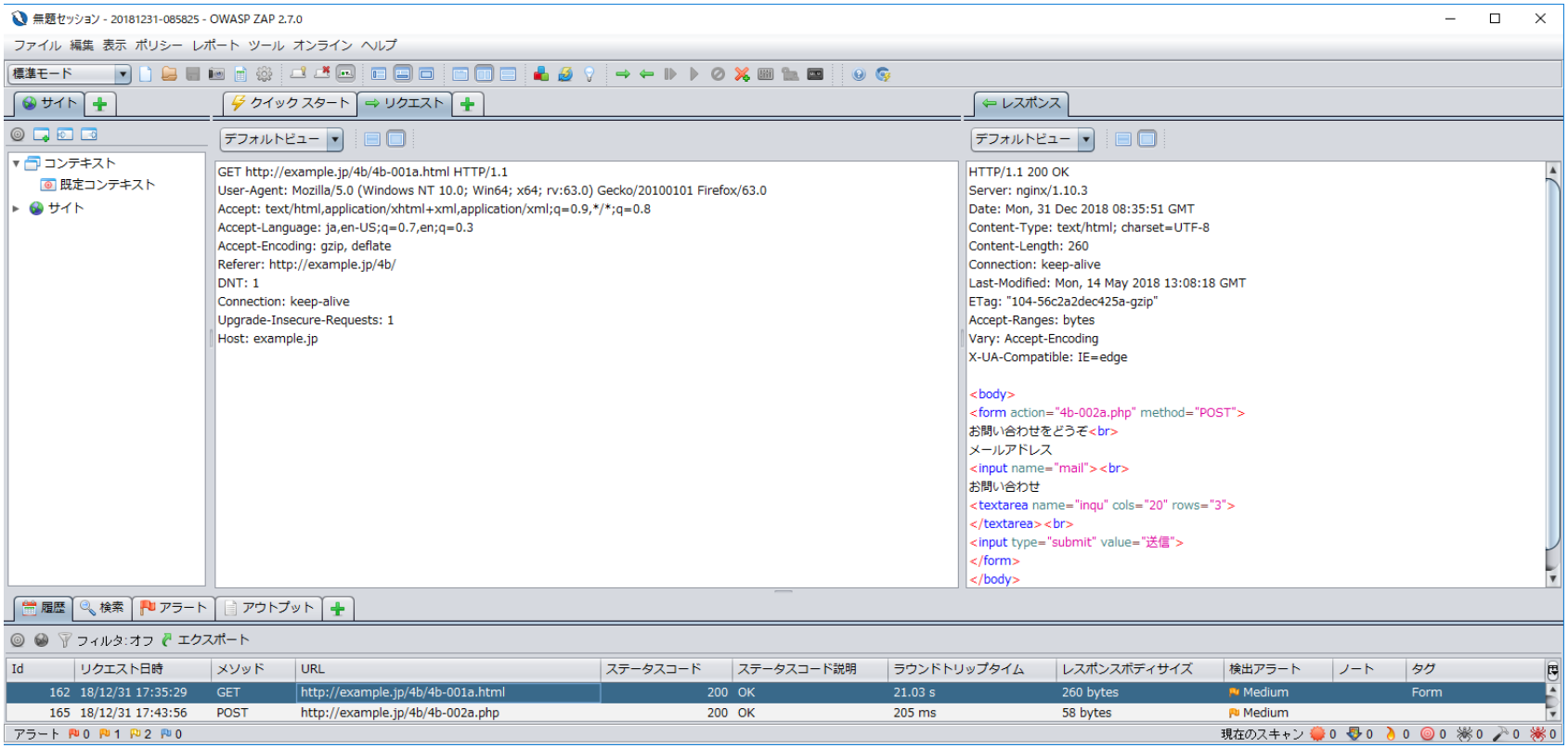
```
<body>
<form action="4b-002a.php" method="POST">
お問い合わせをどうぞ<br>
メールアドレス
<input name="mail"><br>
お問い合わせ
<textarea name="inqu" cols="20" rows="3">
</textarea><br>
<input type="submit" value="送信">
</form>
</body>
```

【サーバ： 4b/4b-002a.php 】

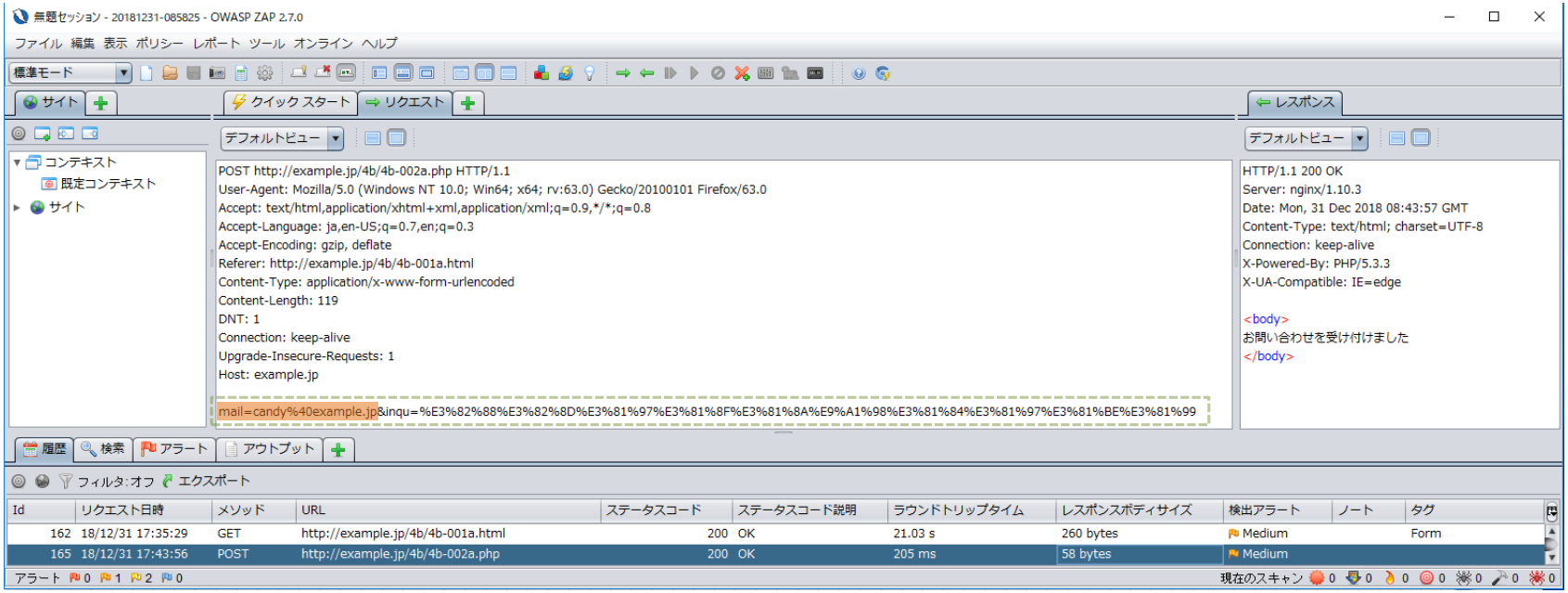
```
<?php
  $mail = $_POST['mail'];
  mb_language('Japanese');
  mb_send_mail($mail, "受け付けました",
    "お問い合わせを受け付けました",
    "From: webmaster@example.jp");
?>
<body>
お問い合わせを受け付けました
</body>
```

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

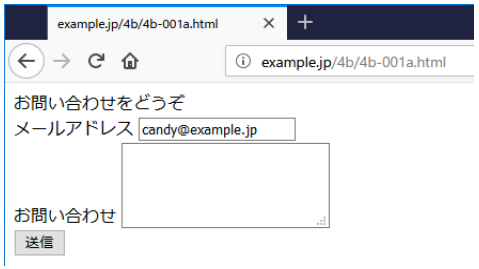
【ブラウザ→サーバ：リクエスト 4b/4b-001a.html → レスポンス 】

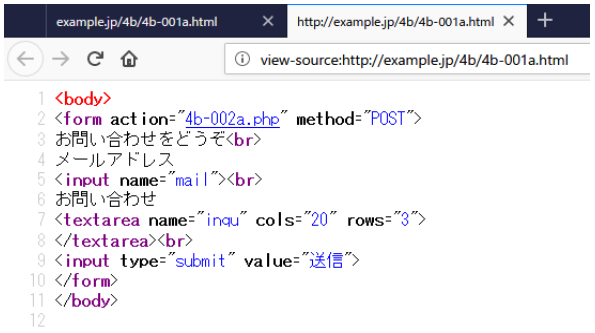


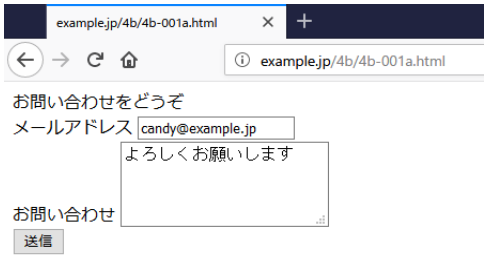
【ブラウザ→サーバ： リクエスト 4b/4b-002a.html → レスポンス 】

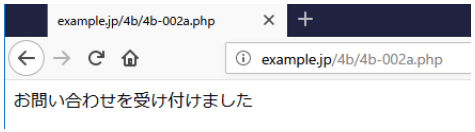


【ブラウザ】


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
candy@example.jp
お問い合わせ
送信


example.jp/4b/4b-001a.html
http://example.jp/4b/4b-001a.html
view-source:http://example.jp/4b/4b-001a.html
<body>
<form action="4b-002a.php" method="POST">
お問い合わせをどうぞ
メールアドレス
<input name="mail">
お問い合わせ
<textarea name="inqu" cols="20" rows="3">
</textarea>
<input type="submit" value="送信">
</form>
</body>


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
candy@example.jp
よろしくお願いします
お問い合わせ
送信

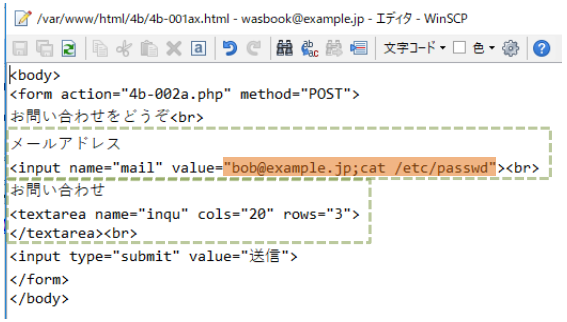

example.jp/4b/4b-002a.php
example.jp/4b/4b-002a.php
お問い合わせを受け付けました


example.jp/4b/4b-002a.php
http://example.jp/4b/4b-002a.php
view-source:http://example.jp/4b/4b-002a.php
<body>
お問い合わせを受け付けました
</body>

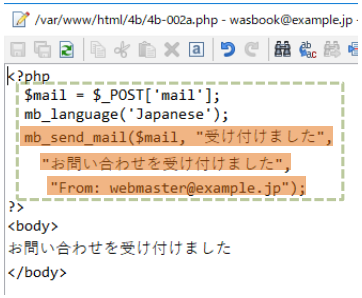
4b-001a:お問い合わせフォーム(OSコマンドを呼ばない)

【ブラウザ】

【サーバ： 4b/4b-001ax.html 】

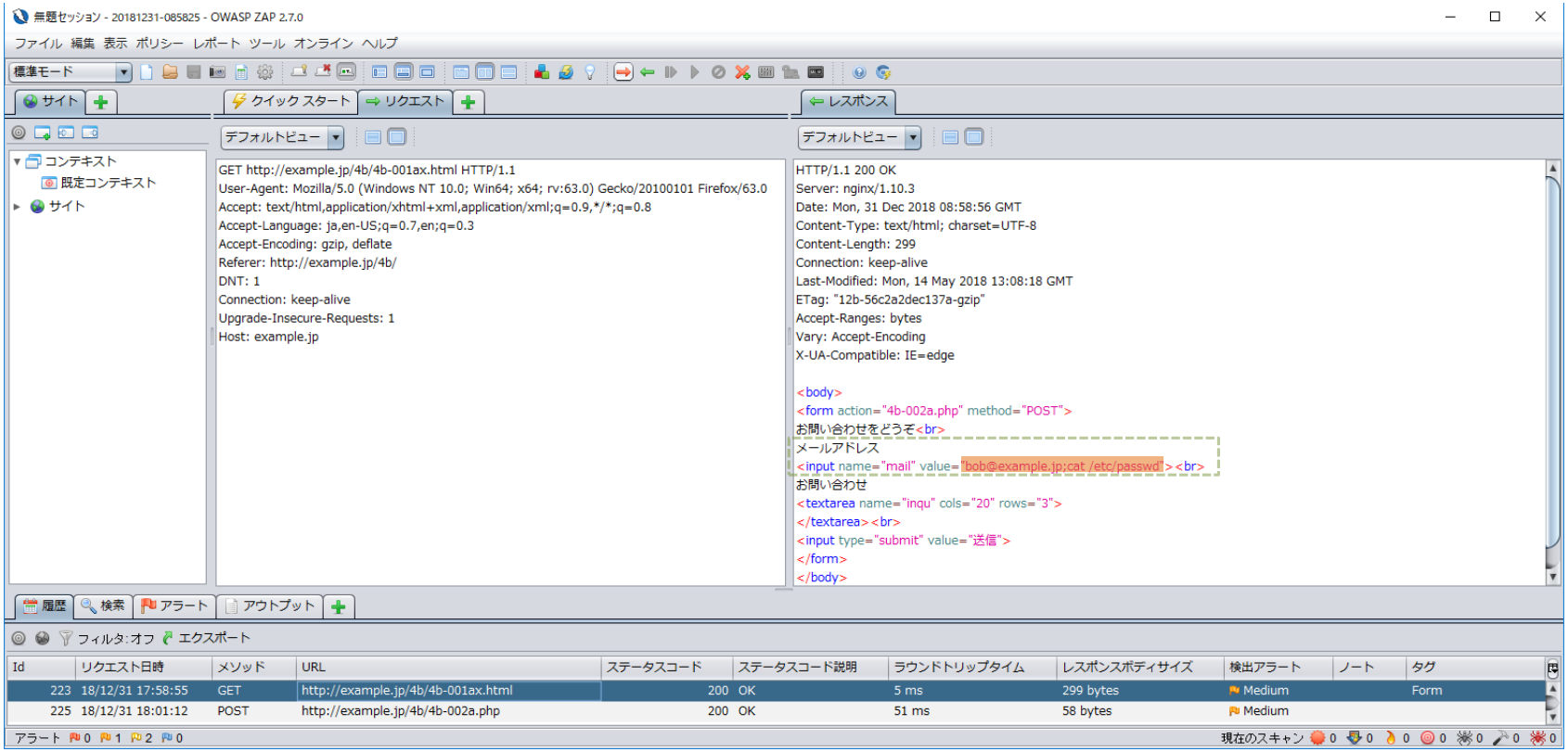


【サーバ： 4b/4b-002a.php 】

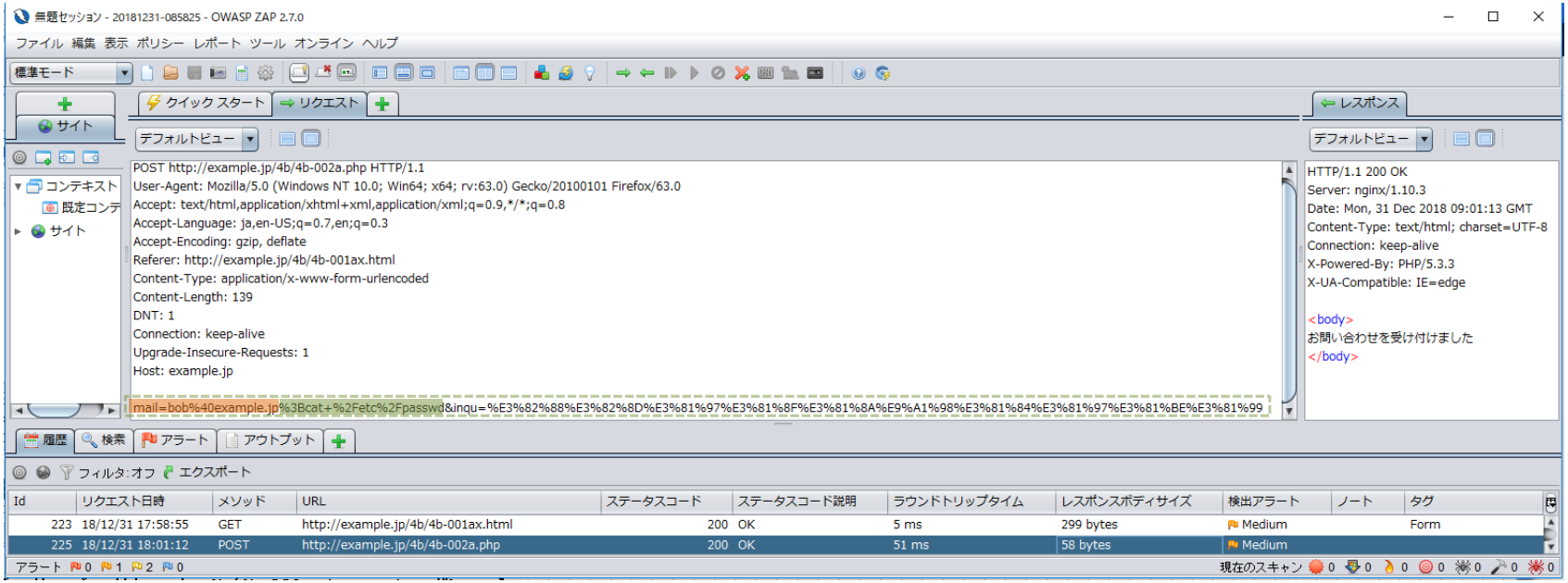


OSコマンド・インジェクション脆弱性は対策しましたが、
メールヘッダ・インジェクション脆弱性があります

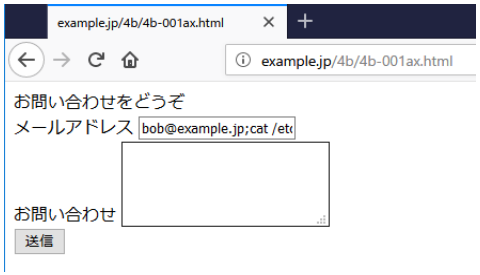
【ブラウザ→サーバ： リクエスト 4b/4b-001ax.html → レスポンス 】



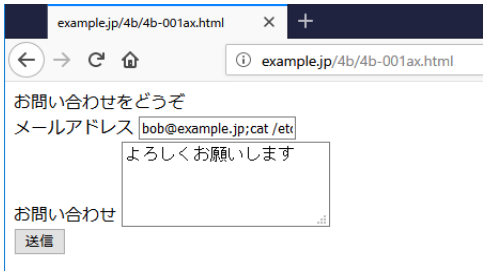
【ブラウザ→サーバ： リクエスト 4b/4b-002a.php → レスポンス 】

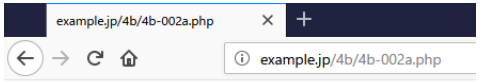


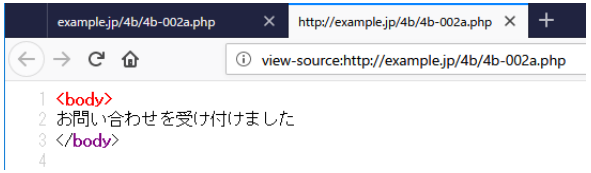
【ブラウザ】


example.jp/4b/4b-001ax.html
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 /et
お問い合わせ
送信


example.jp/4b/4b-001ax.html
http://example.jp/4b/4b-001ax.ht
view-source:http://example.jp/4b/4b-001ax.html
<body>
<form action="4b-002a.php" method="POST">
お問い合わせをどうぞ
メールアドレス
<input name="mail" value="bob@example.jp;cat /etc/passwd">
お問い合わせ
<textarea name="inqu" cols="20" rows="3">
</textarea>
<input type="submit" value="送信">
</form>
</body>


example.jp/4b/4b-001ax.html
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 /et
よろしくお願いします
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-002a.php
http://example.jp/4b/4b-002a.php
view-source:http://example.jp/4b/4b-002a.php
<body>
お問い合わせを受け付けました
</body>

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】

【サーバ： 4b/4b-001b.html 】

/var/www/html/4b/4b-001b.html - wasbook@example.jp - エデ

```
<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 】

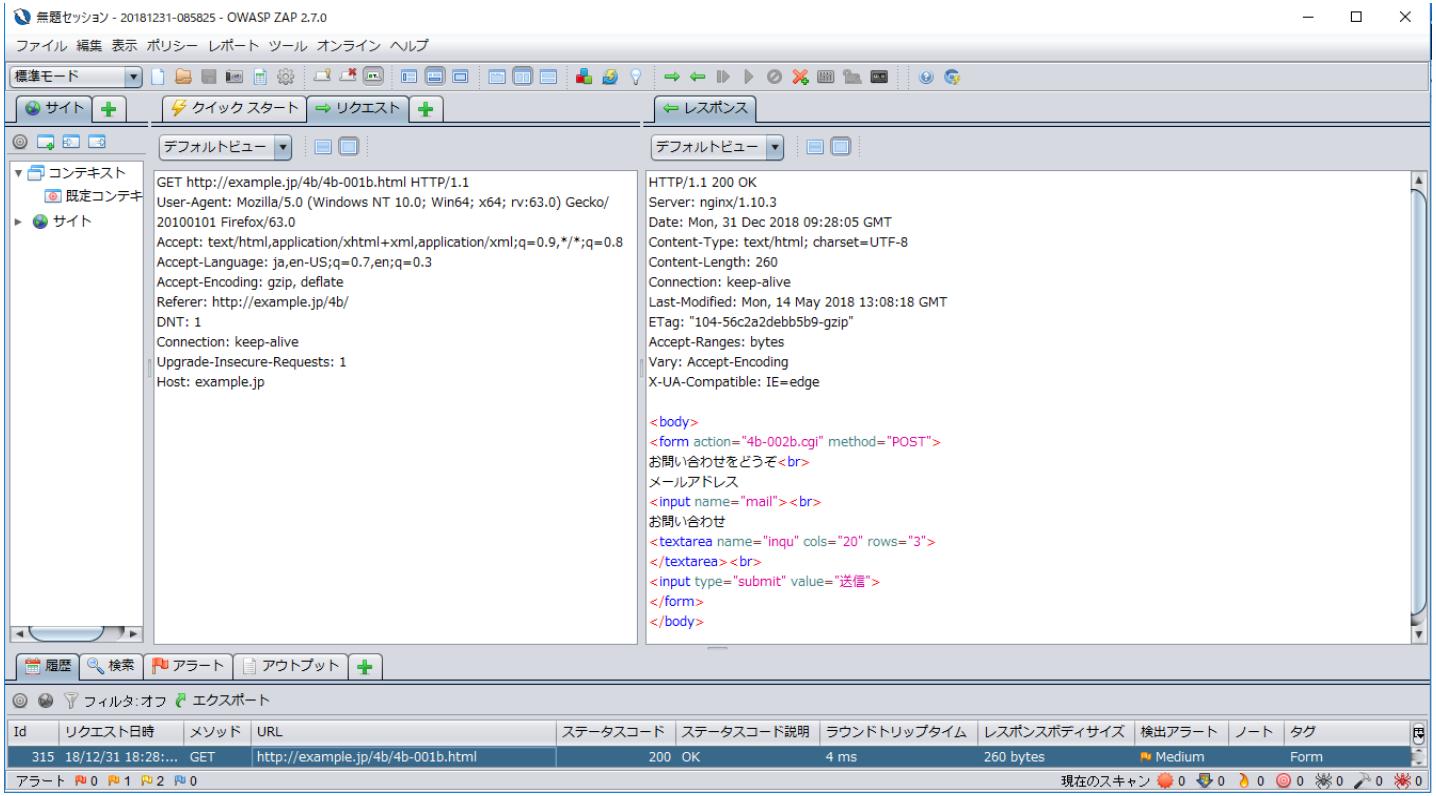
/var/www/html/4b/4b-002b.cgi - wasbook@example.jp - エディタ - WinSCP

```
#!/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
```

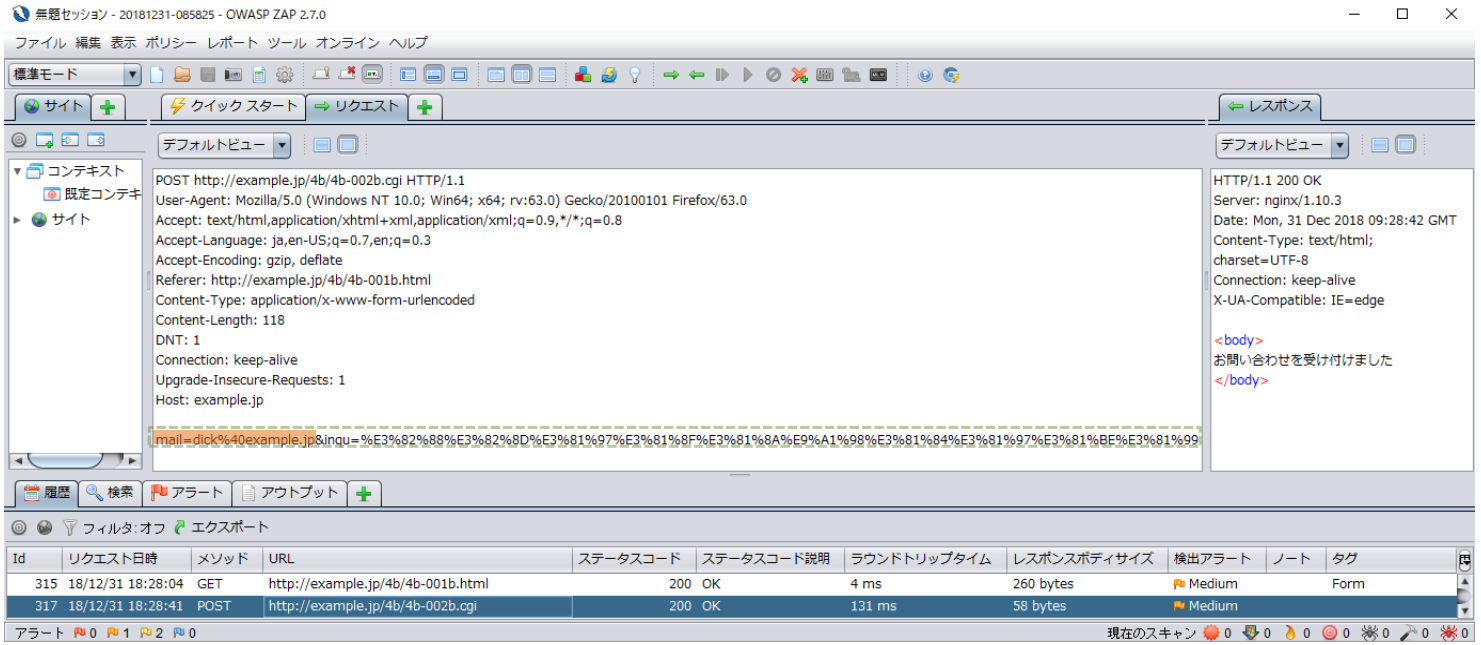
OSコマンド・インジェクション脆弱性は対策しましたが、メールヘッダ・インジェクション脆弱性があります

※ '/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 】

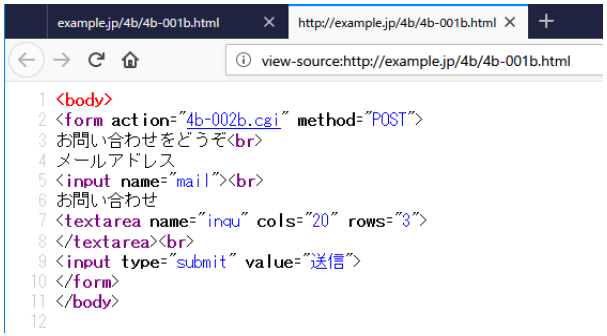


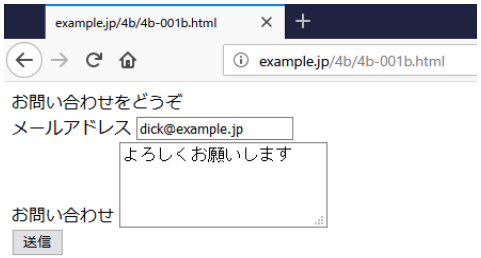
【ブラウザ→サーバ： リクエスト 4b/4b-002b.cgi → レスポンス 】

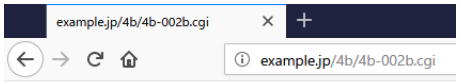


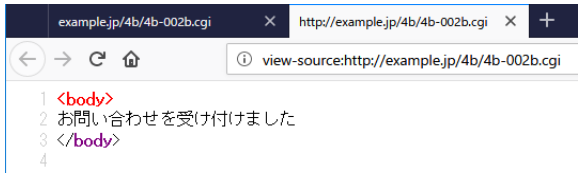
【ブラウザ】


example.jp/4b/4b-001b.html
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
送信


example.jp/4b/4b-001b.html
http://example.jp/4b/4b-001b.html
view-source:http://example.jp/4b/4b-001b.html
<body>
<form action="4b-002b.cgi" method="POST">
お問い合わせをどうぞ
メールアドレス
<input name="mail">
お問い合わせ
<textarea name="inqu" cols="20" rows="3">
</textarea>
<input type="submit" value="送信">
</form>
</body>


example.jp/4b/4b-001b.html
example.jp/4b/4b-001b.html
お問い合わせをどうぞ
メールアドレス
dick@example.jp
よろしくお願いします
お問い合わせ
送信


example.jp/4b/4b-002b.cgi
example.jp/4b/4b-002b.cgi
お問い合わせを受け付けました


example.jp/4b/4b-002b.cgi
http://example.jp/4b/4b-002b.cgi
view-source:http://example.jp/4b/4b-002b.cgi
<body>
お問い合わせを受け付けました
</body>

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】

【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 】

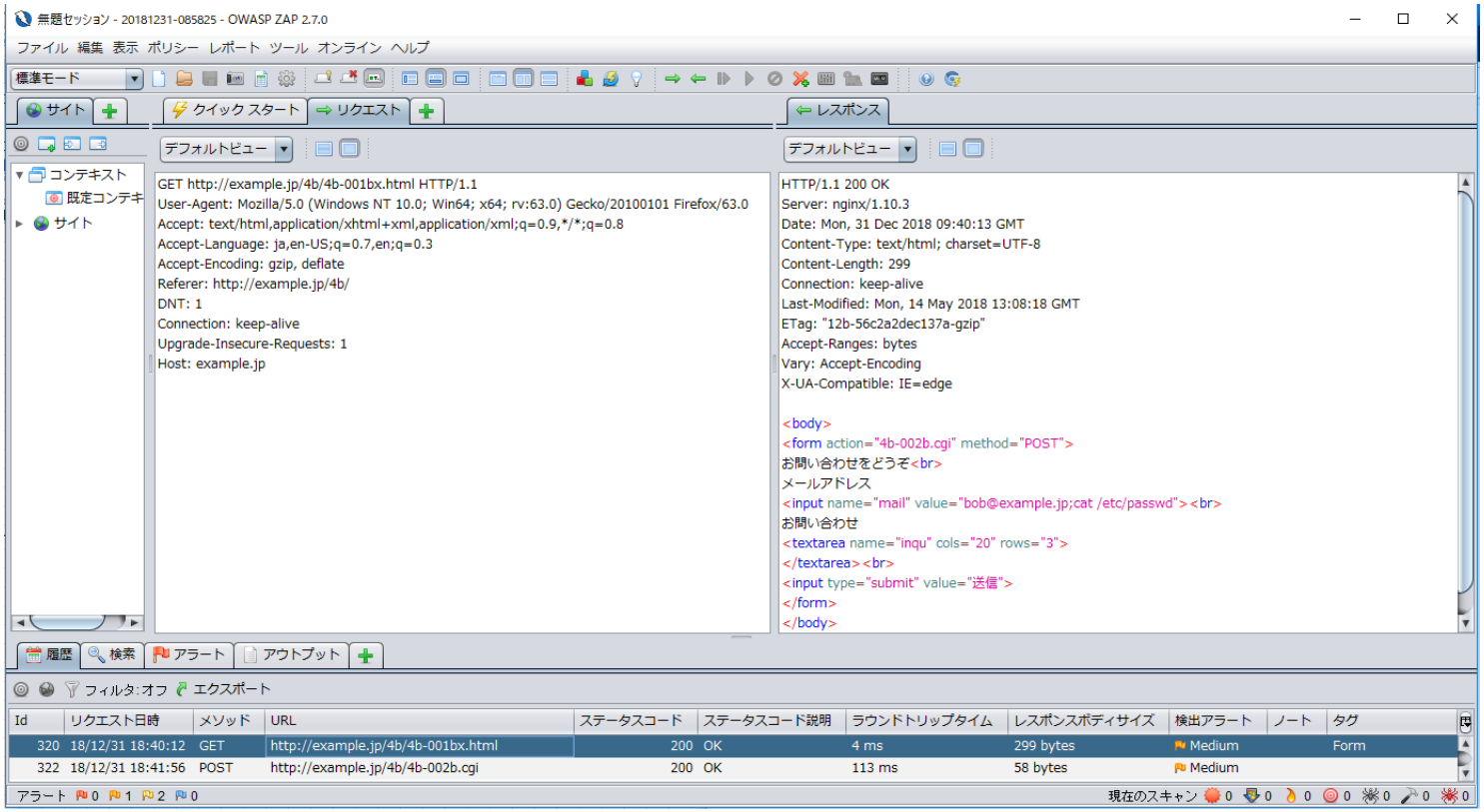
/var/www/html/4b/4b-002b.cgi - wasbook@example.jp - エディタ - WinSCP

```
#!/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
```

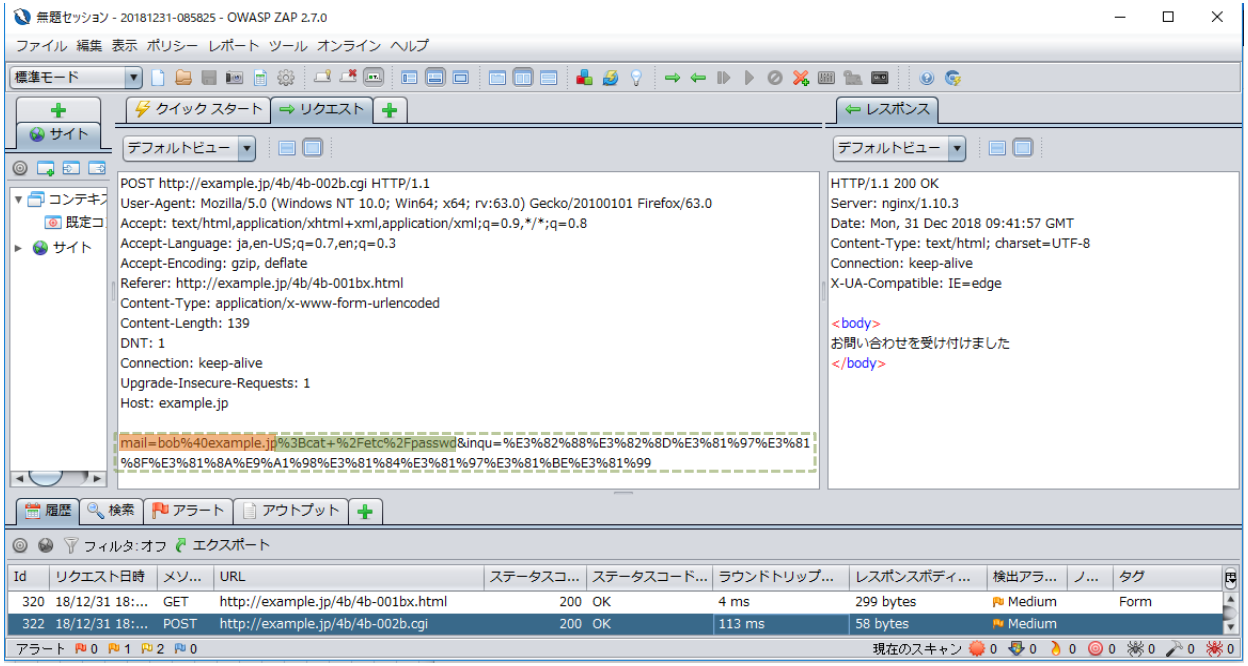
OSコマンド・インジェクション脆弱性は対策しましたが、メールヘッダ・インジェクション脆弱性があります

※ '/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 】



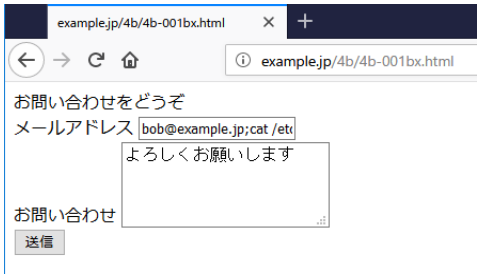
【ブラウザ→サーバ： リクエスト 4b/4b-002b.cgi → レスポンス 】

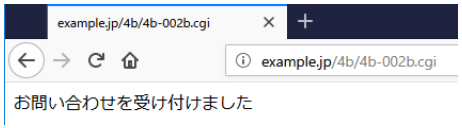


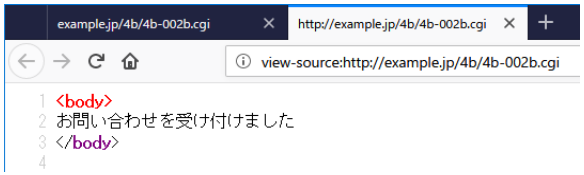
【ブラウザ】


example.jp/4b/4b-001bx.html
example.jp/4b/4b-001bx.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-001bx.html
http://example.jp/4b/4b-001bx.html
view-source:http://example.jp/4b/4b-001bx.html
<body>
<form action="4b-002b.cgi" method="POST">
お問い合わせをどうぞ
メールアドレス
<input name="mail" value="bob@example.jp;cat /etc/passwd">
お問い合わせ
<textarea name="inqu" cols="20" rows="3">
</textarea>
<input type="submit" value="送信">
</form>
</body>


example.jp/4b/4b-001bx.html
example.jp/4b/4b-001bx.html
お問い合わせをどうぞ
メールアドレス
bob@example.jp;cat /etc
よろしくお願いします
お問い合わせ
送信


example.jp/4b/4b-002b.cgi
example.jp/4b/4b-002b.cgi
お問い合わせを受け付けました


example.jp/4b/4b-002b.cgi
http://example.jp/4b/4b-002b.cgi
view-source:http://example.jp/4b/4b-002b.cgi
<body>
お問い合わせを受け付けました
</body>

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】

【サーバ： 4b/4b-001c.html 】

/var/www/html/4b/4b-001c.html - wasbook@example.jp - エディ

```
<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>
```

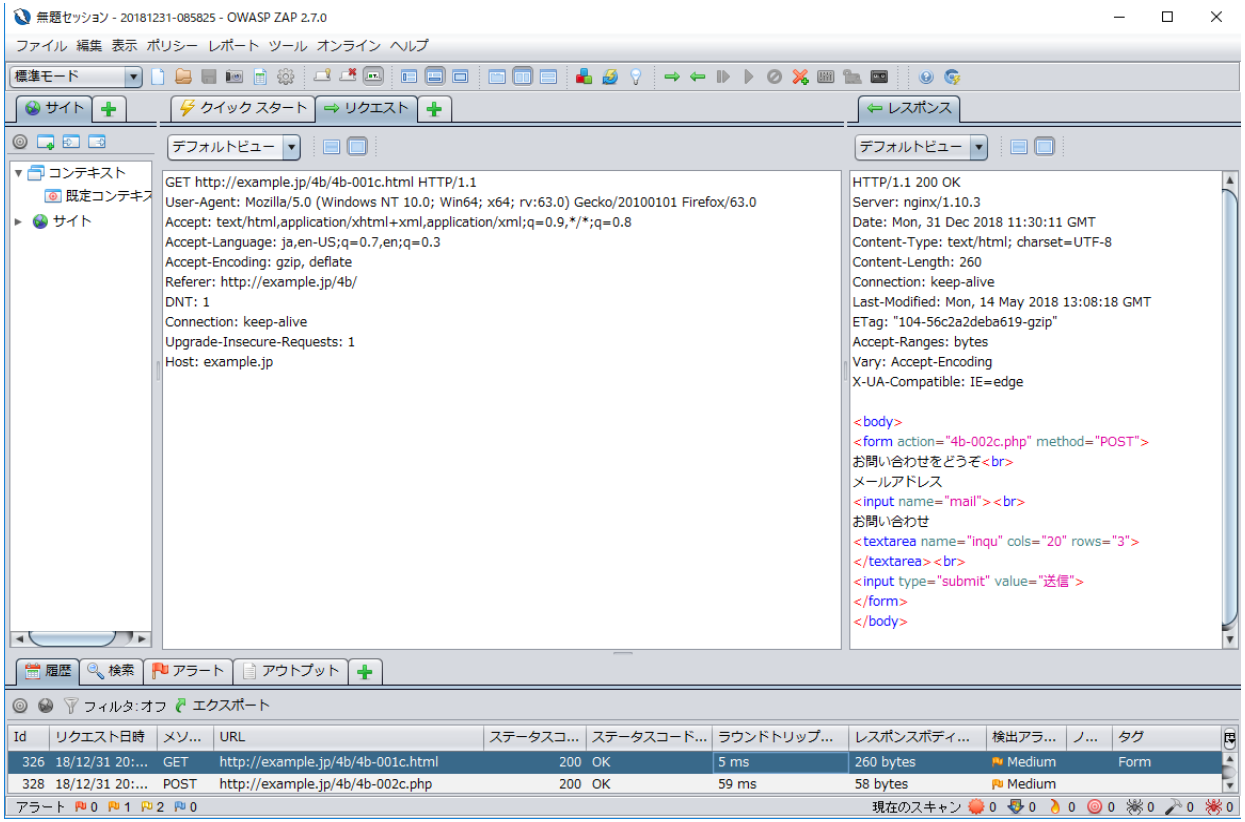
【サーバ： 4b/4b-002c.php 】

/var/www/html/4b/4b-002c.php - wasbook@example.jp - エディタ - WinSCP

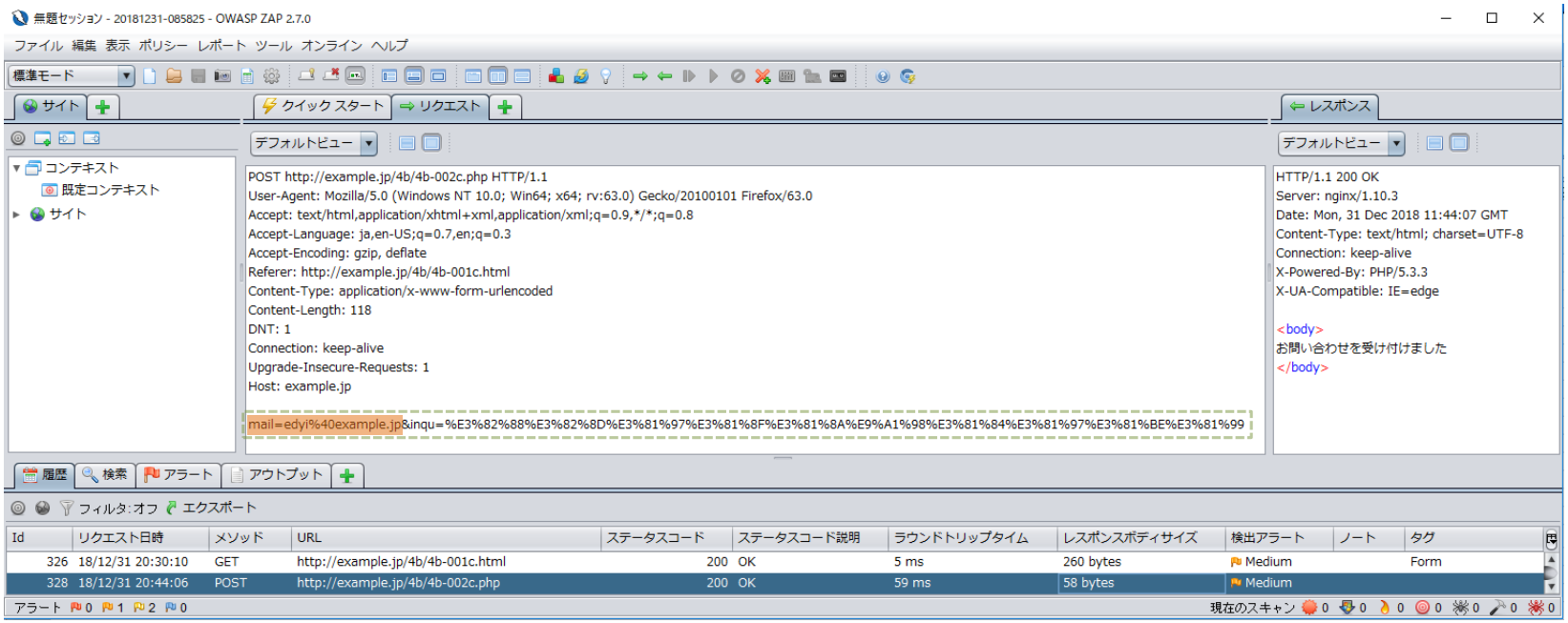
```
<?php
  $mail = $_POST['mail'];
  $h = popen('/usr/sbin/sendmail -t -i', 'w');
  if ($h === FALSE) {
    die('ただいま混み合っております。しばらくたってから..');
  }
  fwrite($h, <<<EndOfMail
To: $mail
From: webmaster@example.jp
Subject: =?UTF-8?B?5Y+X44GR5LuY44GR44G+44GX44Gf?=
Content-Type: text/plain; charset="UTF-8"
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-001c.html → レスポンス 】



【ブラウザ→サーバ： リクエスト 4b/4b-0012c.php → レスポンス 】

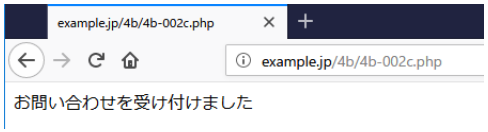


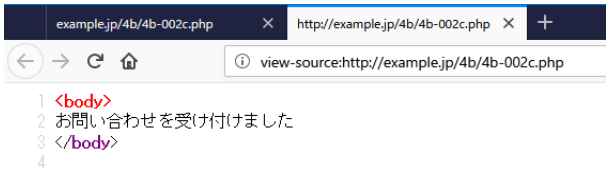
【ブラウザ】


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
http://example.jp/4b/4b-001c.html
view-source:http://example.jp/4b/4b-001c.html
<body>
<form action="4b-002c.php" method="POST">
お問い合わせをどうぞ
メールアドレス
<input name="mail">
お問い合わせ
<textarea name="inqu" cols="20" rows="3">
</textarea>
<input type="submit" value="送信">
</form>
</body>


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
edyi@example.jp
よろしくお願いします
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-002c.php
http://example.jp/4b/4b-002c.php
view-source:http://example.jp/4b/4b-002c.php
<body>
お問い合わせを受け付けました
</body>

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】

【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>
```

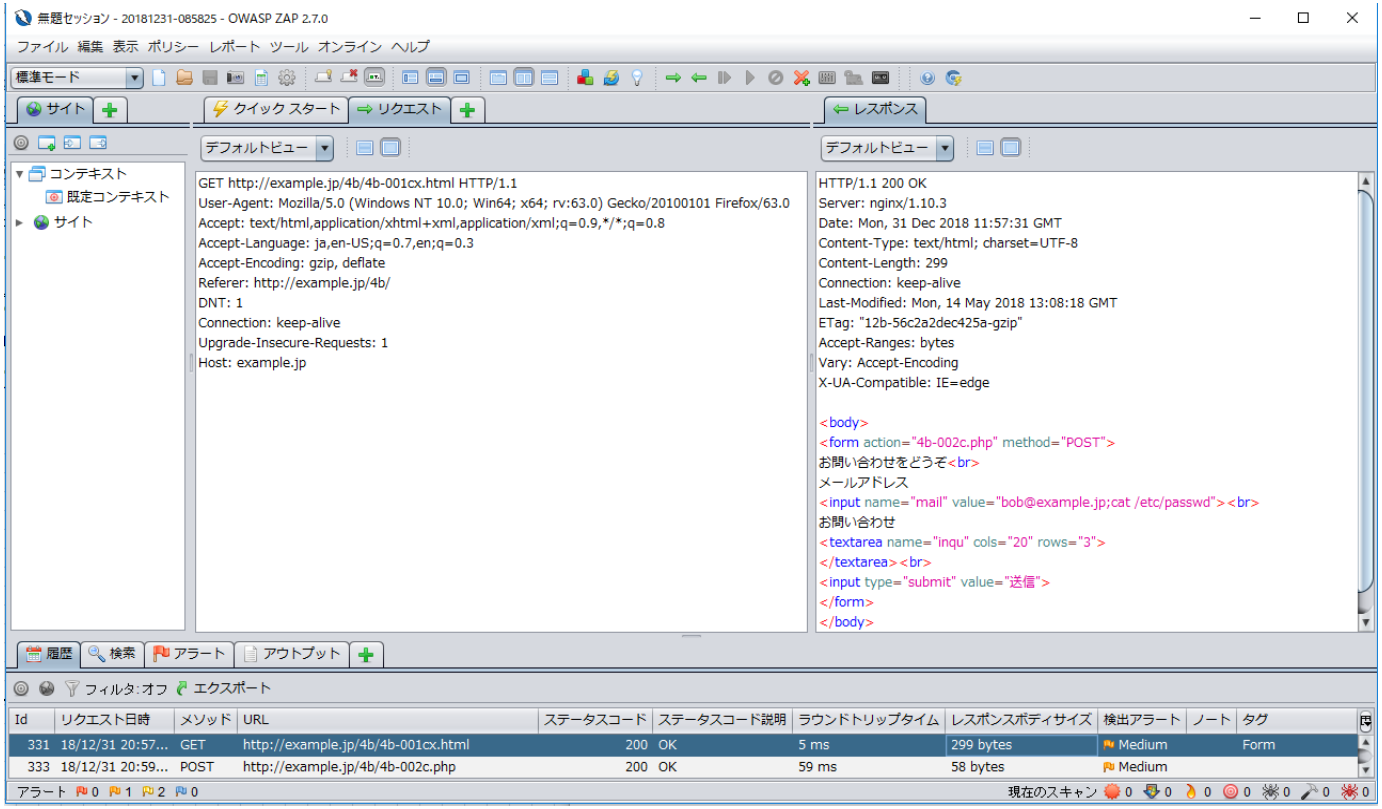
【サーバ： 4b/4b-002c.php 】

/var/www/html/4b/4b-002c.php - wasbook@example.jp - エディタ - WinSCP

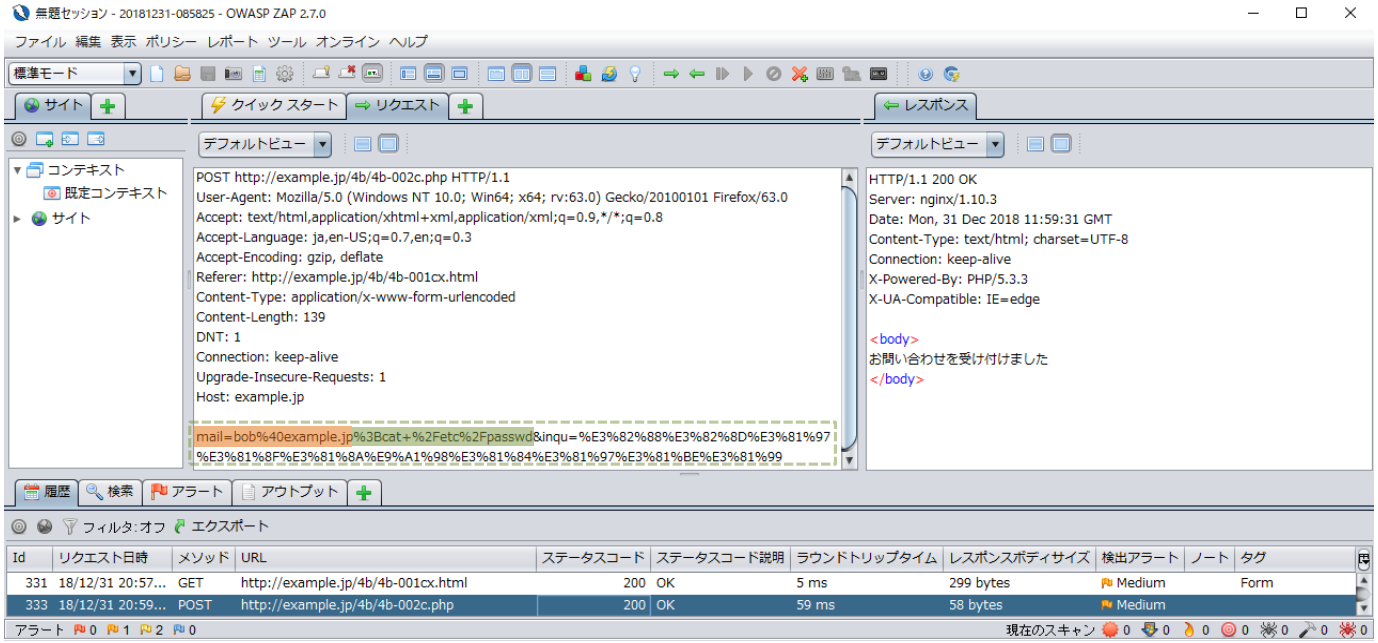
```
k?php
  $mail = $_POST['mail'];
  $h = popen('/usr/sbin/sendmail -t -i', 'w');
  if ($h === FALSE) {
    die('ただいま混み合っております。しばらくたってから..');
  }
  fwrite($h, <<<EndOfMail
To: $mail
From: webmaster@example.jp
Subject: =?UTF-8?B?5Y+X44GR5LuY44GR44G+44GX44Gf?=
Content-Type: text/plain; charset="UTF-8"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

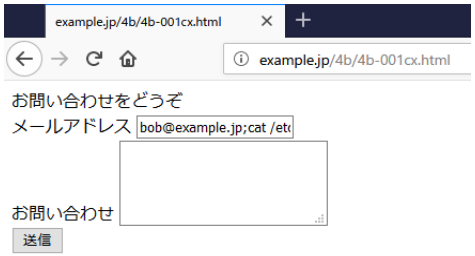
【ブラウザ→サーバ： リクエスト 4b/4b-001cx.html → レスポンス 】



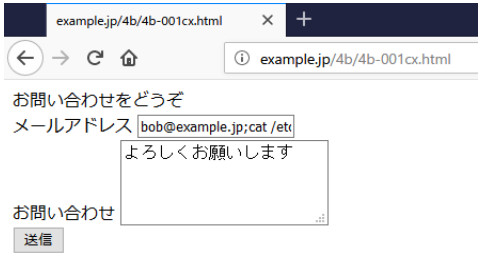
【ブラウザ→サーバ： リクエスト 4b/4b-002c.php → レスポンス 】

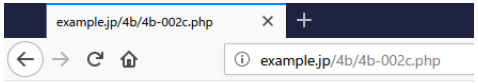


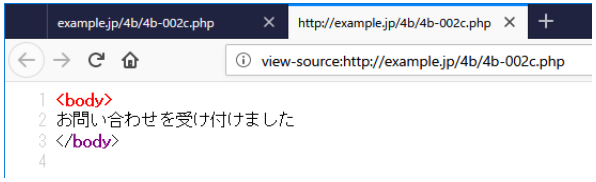
【ブラウザ】


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
bob@example.jp;cat /etc
お問い合わせ
送信


example.jp/4b/4b-001cx.html
http://example.jp/4b/4b-001cx.html
view-source:http://example.jp/4b/4b-001cx.html
<body>
<form action="4b-002c.php" method="POST">
お問い合わせをどうぞ
メールアドレス
<input name="mail" value="bob@example.jp;cat /etc/passwd">
お問い合わせ
<textarea name="inqu" cols="20" rows="3">
</textarea>
<input type="submit" value="送信">
</form>
</body>


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
bob@example.jp;cat /etc
よろしくお願いします
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-002c.php
http://example.jp/4b/4b-002c.php
view-source:http://example.jp/4b/4b-002c.php
<body>
お問い合わせを受け付けました
</body>