



# 軟體源碼檢查系統之使用

國立中央大學 電算中心  
劉劍青 (center5@cc.ncu.edu.tw)



# 源碼掃描使用之系統

---

- ❑ Fortify SCA 360
- ❑ <https://www.fortify.com/products/fortify360/source-code-analyzer.html>



# 使用方式概要

- ☐ 帳號申請 (請提供要使用的 IP Address 以及 Email)
- ☐ 上傳軟體源碼  
目前支援 php 和 java 的軟體專案, 關於 asp, 或 .Net 的部份暫未開放
- ☐ 稍侯待系統批次處理 (系統在完成時, 會以 Email 通知)
- ☐ 下載掃描結果的報告檔 (rtf, xml 格式)
- ☐ 清除系統上這些資料 (請在下載完報告檔之後, 自行將這些資料一併清除)



# 源碼上傳(I)

- ❑ 源碼以壓縮檔的方式上傳, PHP 的專案要做成 zip, tar, 或 tgz 的格式; Java 專案則做成 jar 或 war. 副檔名需與 archive 的方式一致. (.tar.gz 的檔, 請把副檔名改為 .tgz).
- ❑ 在上傳的根目錄下有建了 java3, java4, java5, java6 及 php 等目錄, 請將待掃描的軟體專案, 依類別放入適當目錄. 其中 java3, java4 ... 代表所使用的 JDK 版本.

```
ftp> dir
```

```
227 Entering Passive Mode (x.x.x.x,54,243)
```

```
150 Here comes the directory listing.
```

```
drwxr-xr-x  2 504    504      4096 Aug 14 23:45 java3
drwxr-xr-x  2 504    504      4096 Aug 14 23:45 java4
drwxr-xr-x  2 504    504      4096 Aug 16 02:37 java5
drwxr-xr-x  2 504    504      4096 Aug 14 23:45 java6
drwxr-xr-x  2 504    504      4096 Aug 16 01:36 php
drwx----- 7 504    504      4096 Aug 16 02:37 report
```

```
226 Directory send OK.
```



# 源碼上傳(II)

- ❑ 為了避免上傳未完全完成，而系統就偵測到檔案就開始掃描。上傳時建議先上傳在根目錄，再用 **rename** 的方式移到適當目錄

```
ftp> bi
```

```
200 Switching to Binary mode.
```

```
ftp> put sample.tgz
```

```
local: sample.tgz remote: sample.tgz
```

```
227 Entering Passive Mode (x.x.x.x,145,237)
```

```
150 Ok to send data.
```

```
226 File receive OK.
```

```
1457 bytes sent in 6.5e-05 secs (2.2e+04 Kbytes/sec)
```

```
ftp> dir
```

```
227 Entering Passive Mode (x.x.x.x,238,177)
```

```
150 Here comes the directory listing.
```

drwxr-xr-x	2	504	504	4096	Aug 14 23:45	java3
drwxr-xr-x	2	504	504	4096	Aug 14 23:45	java4
drwxr-xr-x	2	504	504	4096	Aug 16 07:11	java5
drwxr-xr-x	2	504	504	4096	Aug 14 23:45	java6
drwxr-xr-x	2	504	504	4096	Aug 16 07:06	php
-rw-----	1	504	504	1457	Aug 16 07:23	sample.tgz

```
226 Directory send OK.
```

```
ftp> rename sample.tgz php/sample.tgz
```

```
350 Ready for RNT0.
```

```
250 Rename successful.
```



# 取得報表 (I)

- ❑ 在 report 目錄下，又可以看到一些子目錄。每個子目錄會以時間命名；那是代表掃描的時間。
- ❑ 上傳的軟體專案會被移到那些時間目錄，包含報表也在那兒

```
ftp> cd report
```

```
250 Directory successfully changed.
```

```
ftp> dir
```

```
227 Entering Passive Mode (x.x.x.x,97,172)
```

```
150 Here comes the directory listing.
```

```
drwx-----  2 504    504      4096 Aug 16 03:42 20110816-114143
```

```
226 Directory send OK.
```



## 取得報表 (II)

❑ cd 到時間目錄, 可以下載 .rtf 檔和 .xml 檔

```
ftp> cd 20110816-114143
```

```
250 Directory successfully changed.
```

```
ftp> dir
```

```
227 Entering Passive Mode (x.x.x.x,249,179)
```

```
150 Here comes the directory listing.
```

-rw-----	1	504	504	32636	Aug 16 03:42	sample-report.fpr
-rw-----	1	504	504	57888	Aug 16 03:42	sample-report.log
-rw-----	1	504	504	373385	Aug 16 03:42	sample-report.rtf
-rw-----	1	504	504	31935	Aug 16 03:42	sample-report.xml
-rw-r--r--	1	0	0	1457	Aug 16 03:41	sample.tgz

```
226 Directory send OK.
```



# 取得報表 (III)

## ☐ 下載 .rtf 檔和 .xml 檔

```
ftp> mget *.rtf *.xml
```

```
mget sample-report.rtf? y
```

```
227 Entering Passive Mode (x.x.x.x,106,136)
```

```
150 Opening BINARY mode data connection for sample-report.rtf (373385 bytes).
```

```
226 File send OK.
```

```
373385 bytes received in 0.00679 secs (5.4e+04 Kbytes/sec)
```

```
mget sample-report.xml? y
```

```
227 Entering Passive Mode (x.x.x.x,198,31)
```

```
150 Opening BINARY mode data connection for sample-report.xml (31935 bytes).
```

```
226 File send OK.
```

```
31935 bytes received in 0.000997 secs (3.1e+04 Kbytes/sec)
```





# 清掉資料

```
ftp> mdel *  
mdel sample-report.fpr? y  
250 Delete operation successful.  
mdel sample-report.log? y  
250 Delete operation successful.  
mdel sample-report.rtf? y  
250 Delete operation successful.  
mdel sample-report.xml? y  
250 Delete operation successful.  
mdel sample.tgz? y  
250 Delete operation successful.  
ftp> dir  
227 Entering Passive Mode (x.x.x.x,214,12)  
150 Here comes the directory listing.  
226 Directory send OK.
```



# 掃描完成通知

- ☐ 系統將軟體掃描完成之後，會有簡單的電子郵件通知信，告知使用者掃描已完成。



# 掃描結果(I)

## □ RTF 格式的檔案，是供人閱讀的型式，參考如下

### Abstract:

這將會覆寫全域變數，但也等於是為攻擊者製造機會。

### Explanation:

函數若可覆寫已初始化的全域變數，則也會讓攻擊者得以影響依賴已覆寫變數的程式碼執行。

可覆寫全域變數。

範例1：若攻擊者在以下PHP程式碼區段提供str一個惡意值，則呼叫mb\_parse\_str()時可能會覆寫包括first在內的任意變數。在此案例中，若包含JavaScript的惡意值覆寫first，此程式會容易受到Cross-Site Scripting攻擊。

```
<?php
$first="User";

...
$str = $_SERVER['QUERY_STRING'];
mb_parse_str($str);
echo $first;
?>
```

### Recommendations:

利用以下方式，防止可覆寫全域變數的函數執行上述操作：

- 使用第二個引數呼叫mb\_parse\_str(string \$encoded\_string [, array &\$result ])以取得作業的結果，並防止函數覆寫全域變數。

- 將第二個引數設成EXTR\_SKIP，呼叫extract(array \$var\_array [, int \$extract\_type [, string \$prefix]])以防止函數覆寫已定義的全域變數。

範例2：以下程式碼使用mb\_parse\_str()的第二個引數以降低範例1的風險。



## 掃描結果(II)

□ 除了RTF 格式的檔案, 另有 XML 格式的掃描報告, 方面程式自動化處理

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ReportDefinition type="standard">
  <TemplateName>OWASP Top Ten 2004</TemplateName>
  <TemplatePath></TemplatePath>
  <LogoPath>/fortify.jpg</LogoPath>
  <Footnote>Copyright 2010 Fortify Software Inc.</Footnote>
  <UserName></UserName>
  <ReportSection optionalSubsections="false" enabled="true">
    <Title>Report Overview</Title>
    <SubSection enabled="true">
      <Title>Report Summary</Title>
      <Description>This provides a high level summary of the findings that the analysis produced. Also includes basic information on the scope of the scan.</Description>
      <Text>On Aug 16, 2011, a source code review was performed over the 20110816-152831 code base. 2 files, 9 LOC (Executable) were scanned. A total of 3 issues were uncovered during the analysis. This report provides a comprehensive description of all the types of OWASP Top Ten 2004 issues found in this project. Specific examples and source code are provided for each issue type.</Text>
```



# Computer Center, National Central University.

---



***Thank You!***