Skipfish

Devin Ford
Latana Banks

Midterm Report
Table of Contents

Introduction to Skipfish pg.3

What we plan to do with Skipfish pg.3

Security Issues Skipfish focuses on pg.3-4

What we have completed pg.4-6
   (a) Installation process pg.4-5
   (b) Challenges we faced pg.5-6
   (c) Lessons learned pg.6

The hands on pg.7
   (a) The purpose of our lab pg.7
   (b) Description of Devin’s lab pg.7
   (c) Description of Latana’s lab pg.7

The part of project that we are planning to do pg.7

Future directions and/or conclusions pg.8

References/work cited pg.9
Introduction

What is Skipfish? Skipfish is a new open source web application scanner, written in C programming, developed by Google. The goal of Skipfish is similar to the goals of previous web security hole scanners like Nmap and Nessus, it allows web developers to scan their application or site for possible security issues that may be lurking around. Skipfish can be used to determine if code is vulnerable to common attacks such as cross-site scripting (XSS), SQL, and XML injection attacks because it performs high risk flaw, medium risk flaw, and low issue scans.

After Skipfish completes its scan it prepares an interactive site-map for the targeted site by carrying out a recursive crawl and dictionary based probes. Skipfish is said to easily process over two thousand HTTP requests per second if the server being tested can handle the load.

What we plan on doing

The first task we must complete is that we must create a test application to run the web application scanner. To complete this task we used Google App Engine. Google App Engine is a form of cloud computing that allows you to run web application on Google’s infrastructure. We used the eclipse development environment to develop our java application so we downloaded the Google plug-in for eclipse, which allows test and create App Engine application within eclipse. Once the web application is developed we then will the show how to run Skipfish on our application and document finding from the crawl results.

Security Issues Skipfish focuses on
The security issues Skipfish focuses on is those of website and web application on the internet and their insecure interfaces. As stated earlier Skipfish allows developer to scan their application for vulnerabilities. A vulnerability being any situation or condition that increases threat which in turn increases risk, the probability that something can happen. The significance of this tool is that developers do not have to wait and see if their application is vulnerable to an attack they can check for themselves. “Once we know our weaknesses, they cease to do us any harm” a quote by George Christoph Lichtenberg which we believe relates to Skipfish because it allows you to find the weakness in your application and perform the necessary safeguards to reduce it.

_What we have completed_

**(a) The Installation process**

Skipfish requires that you use a Linux operating system so we downloaded Ubuntu and next had to download Skipfish. Other requirements were: GNU C Compiler, GNU Make, GNU C Library (including development header), Zlib (including development header), OpenSSL (including development header), and Libidn (including development header).

1. Once in the terminal type `wget http://skipfish.googlecode.com/files/skipfish-`
1.69b.tgz

2. Type `zxvf Skipfish-1.69b` to extract

3. Type `cd Skipfish-1.69b` to change to the Skipfish directory and then type `nice make` to compile

---

**What we have completed**

**(b) Challenges we faced**

Throughout this project we faced several problems because one this was our first time using Ubuntu Linux and two first time using a web application scanner. The first problem we encountered was during the installation phase. While trying to compile Skipfish we kept...
receiving the error, http_client.c:37:25: error: openssl/ssl.h: No such file or directory. After
reading multiple forms it turned out that it was a fairly common problem even if your machine
has a fairly good set of dependencies downloaded. There was a fix to our problem all we had to
do was type sudo apt-get install libssl-dev build-essential zlibc zlib-bin libidn11-dev libidn11
and it acted as a catchall and we were able to compile Skipfish.

The next problem we encountered was when we were trying to scan our test website. The
original plan was to create a basic web page in HTML, transfer in to the internet using FileZilla,
and scan it with Skipfish. The problem was once we transferred our web page to the internet
using FAMU as a host it gave us the default address www.cis.famu.edu/~dford/website name.
The problem with this is when trying to scan the website we received the error one of specified
scan targets is not a valid absolute URL. The website was not a valid URL so as stated early in
the report we then went to Google App Engine and created a test App and it was able to scan it
just fine.

What we have completed

(c)Lessons Learned

One lessoned we learned from this experience is that if you are experiencing an error
with a certain program you are probably the not the only person who has experienced that
problem. There are forums available, via the internet for most programs and software and can
greatly help you when it comes to trouble shooting. Another lesson was that in order to scan a
web site with Skipfish you must use the absolute URL.
The Hands on

(a) The purpose of our lab

We will demonstrate how the scan works by creating a test web application and performing a scan. Demonstrate the use of the scan to our web application for possible security issues which might be lurking around.

The Hands on

(b) Devin’s lab

In This lab I will use the Google App Engine to create a web application that will be stored on Google’s Infrastructure. The App will be called devinguestbook, and the URL will be devinguestbook.appspot.com/guestbook. The application will simply say hello and whatever your user name is you used to login. After the application is built I will demonstrate how to use Skipfish in order to check the application for vulnerabilities.

The Hands on

(c) Latana’s lab

In This Lab I will use the Google Skipfish web application scanner to scan websites, document the finding and explain the crawl results.

The part of our lab that we plan to do

We plan to demonstrate both labs that we mentioned in the text above of the 21 of November.
**Future direction and/or conclusions**

When using Skipfish remember that it is open source Google web application and site scanner and it is not a hundred percent accurate and it should not be the only security measure you deploy in protecting your web application or site, it should be coupled with other technologies.
Works Cited


