Lab Report

SECURITY INSIDER LAB II
PART 4: IMPLEMENTING SECURE WEB APPLICATIONS

Group 5

Abhijeet Patil
Mohammad Saiful Islam
Thejeswi Preetham Nagendra Kamatchi

Exercise 1: White-Box Web Application Vulnerability Testing

Exercise 2: Black-Box Web Application Vulnerability Testing

1. Download two (or more) web vulnerability scanners and describe how you setup all the appropriate environment settings needed.

For Black-box web application vulnerability testing, we have downloaded OWASP Zed Attack Proxy(also known as OWASP ZAP), nikto and uniscan.

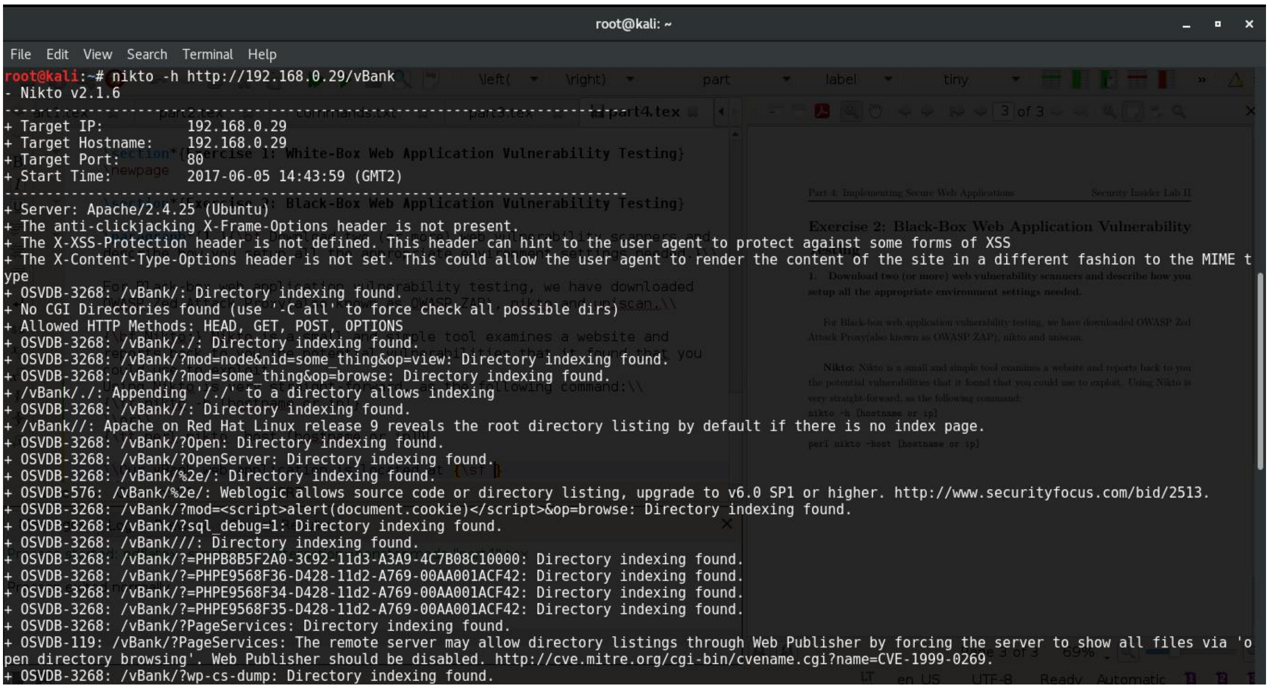
Nikto: Nikto is a small and simple tool examines a website and reports back to you the potential vulnerabilities that it found that you could use to exploit. Using Nikto is very straight-forward, as the following command:

```
nikto -h [hostname or ip]
```

or

```
perl nikto -host [hostname or ip]
```

Our vBank web application is located at http://192.168.0.29/vBank. Here is the screenshot of the nikto scan:



```
root@kali:~# nikto -h http://192.168.0.29/vBank
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.0.29
+ Target Hostname:    192.168.0.29
+ Target Port:        80
+ Start Time:         2017-06-05 14:43:59 (GMT2)
---------------------------------------------------------------------------
+ Server: Apache/2.4.25 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME t
ype
+ OSVDB-3268: /vBank/: Directory indexing found.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: HEAD, GET, POST, OPTIONS
+ OSVDB-3268: /vBank/./: Directory indexing found.
+ OSVDB-3268: /vBank/?mod=node&nid=some_thing&op=view: Directory indexing found.
+ OSVDB-3268: /vBank/?mod=some_thing&op=browse: Directory indexing found.
+ /vBank/./: Appending '/./' to a directory allows indexing
+ OSVDB-3268: /vBank//: Directory indexing found.
+ /vBank//: Apache on Red Hat Linux release 9 reveals the root directory listing by default if there is no index page.
+ OSVDB-3268: /vBank/?Open: Directory indexing found.
+ OSVDB-3268: /vBank/?OpenServer: Directory indexing found.
+ OSVDB-3268: /vBank/%2e/: Directory indexing found.
+ OSVDB-576: /vBank/%2e/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher. http://www.securityfocus.com/bid/2513.
+ OSVDB-3268: /vBank/?mod=<script>alert(document.cookie)</script>&op=browse: Directory indexing found.
+ OSVDB-3268: /vBank/?sql_debug=1: Directory indexing found.
+ OSVDB-3268: /vBank///: Directory indexing found.
+ OSVDB-3268: /vBank/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: Directory indexing found.
+ OSVDB-3268: /vBank/?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: Directory indexing found.
+ OSVDB-3268: /vBank/?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: Directory indexing found.
+ OSVDB-3268: /vBank/?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: Directory indexing found.
+ OSVDB-3268: /vBank/?PageServices: Directory indexing found.
+ OSVDB-119: /vBank/?PageServices: The remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'o
pen directory browsing'. Web Publisher should be disabled. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269.
+ OSVDB-3268: /vBank/?wp-cs-dump: Directory indexing found.
```

Figure 1: request a loan