



The OWASP Foundation
<http://www.owasp.org>

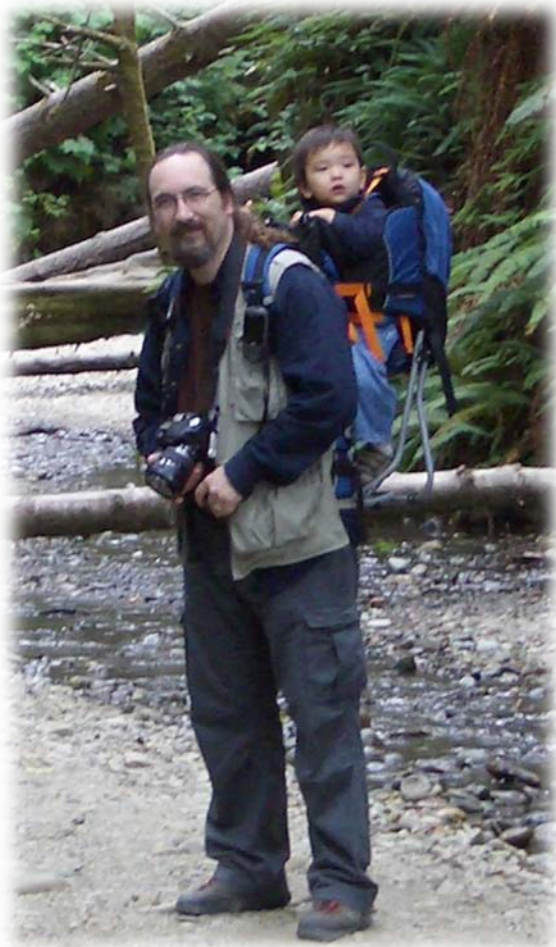
OWASP

Broken Web Application VMWare Image

Rik A. Jones, CISSP

rikjones@computer.org

Rik A. Jones



- Web developer since 1995 (16+ years)
- Involved with information security since 2006 (5+ years)



- Senior Information Security Analysts for Dallas County Community College District

- CISSP and GIAC certified



- Member of the Dallas OWASP Leadership Team



- Member of the Dallas Chapter of InfraGard





Broken Web Applications Project (BWA)

The Broken Web Applications Project (BWA) is an effort to provide a wealth of applications with known vulnerabilities for those interested in:

- learning about web application security
- testing manual assessment techniques
- testing automated tools
- testing source code analysis tools
- observing web attacks
- testing WAFs and similar code technologies

all the while saving people interested in doing either learning or testing the pain of having to compile, configure, and catalog all of the things normally involved in doing this process from scratch.

Broken Web Applications Project (BWA)

BWA includes some common testing and training Web applications as well as old versions of real “broken” software

- WebGoat 5.3.x
- Damn Vulnerable Web App 1.07x
- WordPress 2.0.0
- AWStats 6.4 (build 1.814)
- and more

Broken Web Applications Project (BWA)

It is distributed on a Virtual Machine in [VMware](#) format compatible with their no-cost [VMware Player](#) and [VMware Server](#) products (along with their commercial products).

Broken Web Applications Project (BWA)

At launch in the VM is just a command line.

You access the interface via a Web Browser

```
Welcome to the OWASP Broken Web Apps VM

!!! This VM has many serious security issues. We strongly recommend that you run
     it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://192.168.206.134/

You can administer / configure this machine through the console here, by SSHing
to 192.168.206.134, via Samba at \\192.168.206.134\, or via phpmyadmin at
http://192.168.206.134/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

OWASP Broken Web Applications VM Version 0.94
Log in with username = root and password = owaspbwa

owaspbwa login:
```

Broken Web Applications Project (BWA)

You have to login to the VM for the Web applications to work properly

```
You can access the web apps at http://192.168.206.134/

You can administer / configure this machine through the console here, by SSHing
to 192.168.206.134, via Samba at \\192.168.206.134\, or via phpmyadmin at
http://192.168.206.134/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

OWASP Broken Web Applications VM Version 0.94
Log in with username = root and password = owaspbwa

owaspbwa login: root
Password:
Last login: Mon Jan 30 17:28:37 EST 2012 on tty1
You have mail.

Welcome to the OWASP Broken Web Apps VM

!!! This VM has many serious security issues. We strongly recommend that you run
it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://192.168.206.134/

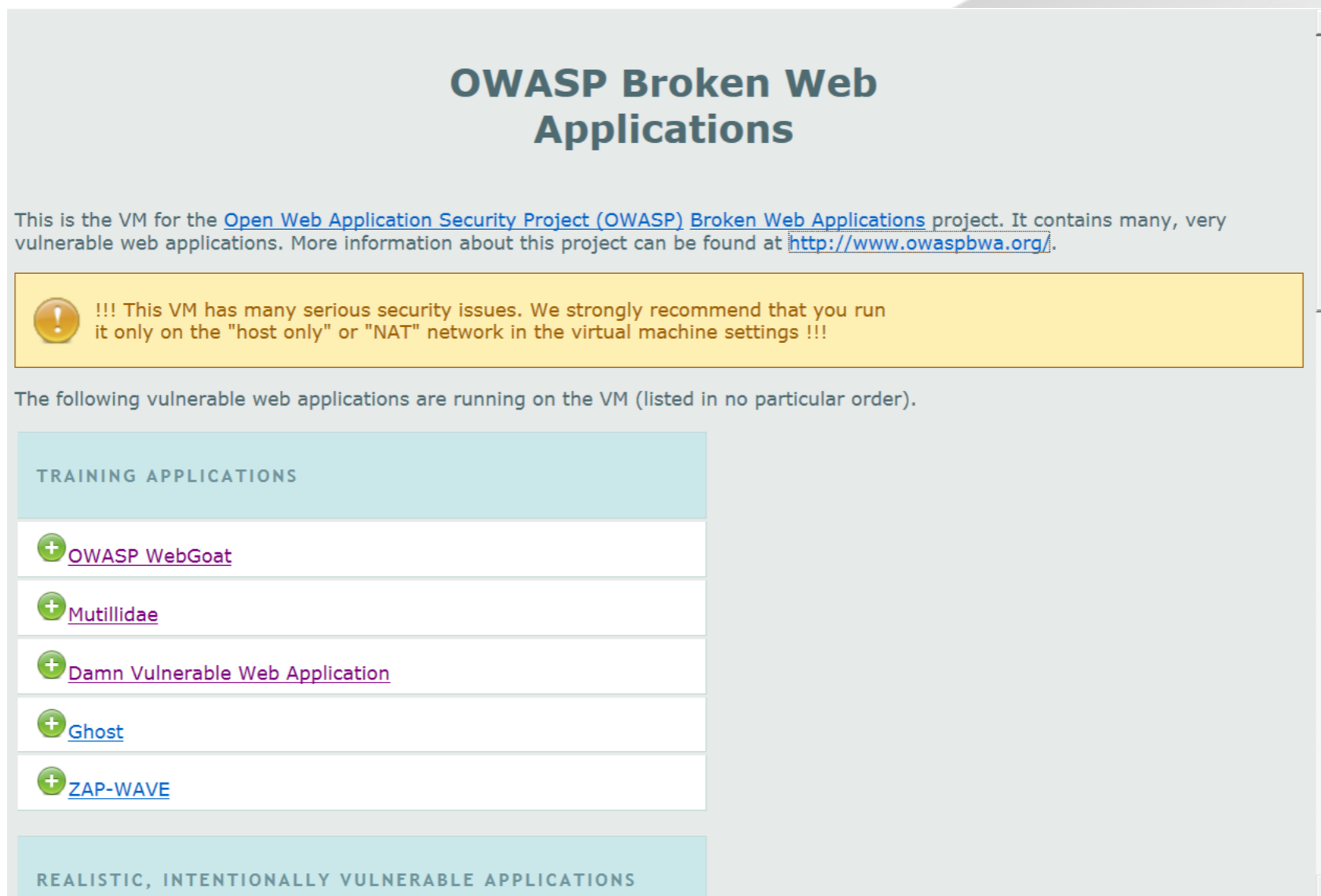
You can administer / configure this machine through the console here, by SSHing
to 192.168.206.134, via Samba at \\192.168.206.134\, or via phpmyadmin at
http://192.168.206.134/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

root@owaspbwa:~# _
```

Broken Web Applications Project (BWA)

Web Page interface



OWASP Broken Web Applications

This is the VM for the [Open Web Application Security Project \(OWASP\) Broken Web Applications](http://www.owaspbwa.org/) project. It contains many, very vulnerable web applications. More information about this project can be found at <http://www.owaspbwa.org/>.

!!! This VM has many serious security issues. We strongly recommend that you run it only on the "host only" or "NAT" network in the virtual machine settings !!!

The following vulnerable web applications are running on the VM (listed in no particular order).

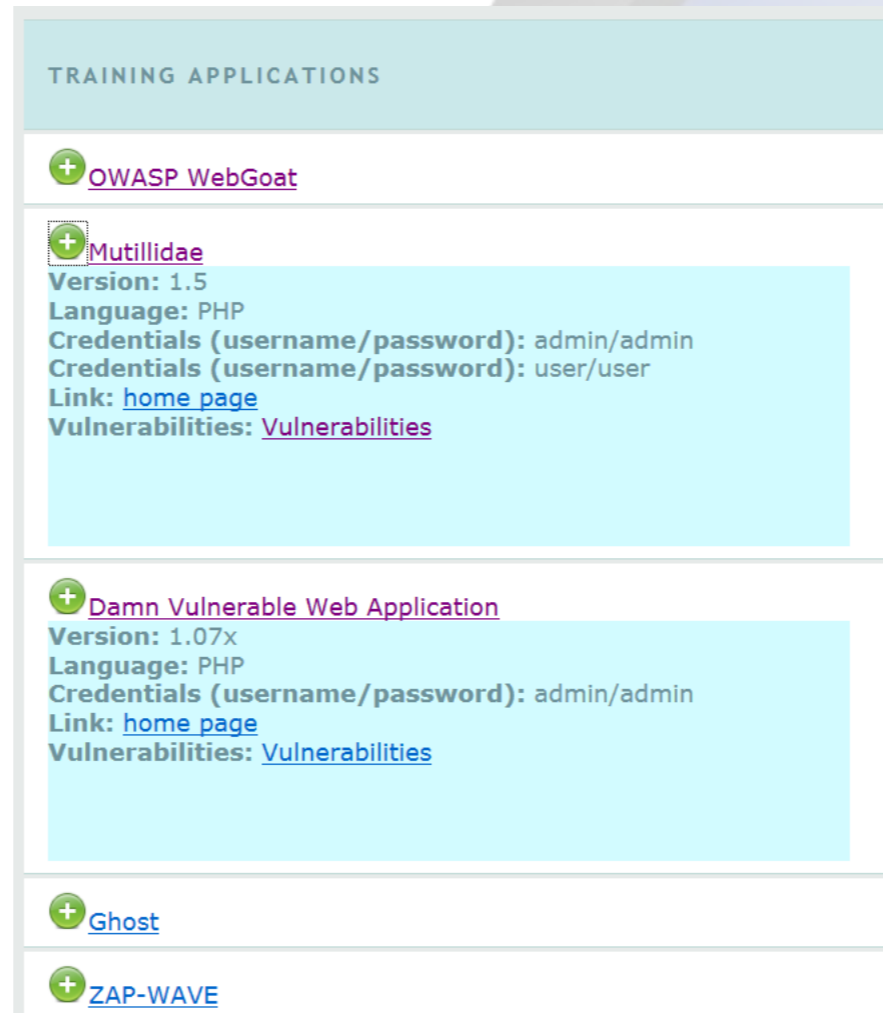
TRAINING APPLICATIONS

- + [OWASP WebGoat](#)
- + [Mutillidae](#)
- + [Damn Vulnerable Web Application](#)
- + [Ghost](#)
- + [ZAP-WAVE](#)

REALISTIC, INTENTIONALLY VULNERABLE APPLICATIONS

Broken Web Applications Project (BWA)

The plus sign “+” by each Web application gives more details about the applications including accounts and passwords



TRAINING APPLICATIONS

- + [OWASP WebGoat](#)
- + [Mutillidae](#)
Version: 1.5
Language: PHP
Credentials (username/password): admin/admin
Credentials (username/password): user/user
Link: [home page](#)
Vulnerabilities: [Vulnerabilities](#)
- + [Damn Vulnerable Web Application](#)
Version: 1.07x
Language: PHP
Credentials (username/password): admin/admin
Link: [home page](#)
Vulnerabilities: [Vulnerabilities](#)
- + [Ghost](#)
- + [ZAP-WAVE](#)

Broken Web Applications Project (BWA)

For some of the Web applications a list of vulnerabilities is provided

OWASP VICNUM		
SEVERITY	TYPE	LINK TO VULNERABILITY OR PAGE
High		When playing the game, the "correct" answer is stored in Base64 encoded form in a hidden form field named VIEWSTATE. An attacker can decode this value in order to determine the correct answer to the game or manipulate it.
Medium	Reflected XSS	http://owaspbwa/vicnum/cgi-bin/vicnum1.pl?player=Foo%3Cscript%3Ealert%281%29%3C%2Fscript%3E
Medium	Reflected XSS	To illustrate this issue, send a POST request POST http://owaspbwa/vicnum/vicnum5.php player=<script>alert(1)</script>

Resources

OWASP Broken Web Applications Project

<http://www.owaspbwa.org/>

<http://code.google.com/p/owaspbwa/>