

Re: Is there an Open Source Vulnerability Analysis Framework?

# Re: Is there an Open Source Vulnerability Analysis Framework?

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2006-07/msg00206.html>

---

- *From:* <[frank.boldewin@xxxxxx](mailto:frank.boldewin@xxxxxx)>
  - *Date:* Mon, 17 Jul 2006 17:49:31 +0200
- 

i like the peach fuzzer.

<http://peachfuzz.sourceforge.net/>

----- Original Message ----- From: "Christian Martorella" <[laramies2k@xxxxxxxxxxxxxx](mailto:laramies2k@xxxxxxxxxxxxxx)>  
To: <[pen-test@xxxxxxxxxxxxxxxxxxxxxx](mailto:pen-test@xxxxxxxxxxxxxxxxxxxxxx)>  
Sent: Monday, July 17, 2006 9:02 AM  
Subject: Re: Is there an Open Source Vulnerability Analysis Framework?

Hi Steve, i think that ISSAF (Information System Security Assessment Framework) could suit your needs.

"The ISSAF is OISSG's flagship project. It is an effort to develop an end-to-end framework for security assessment. The ISSAF aims to provide a single point of reference for professionals involved in security assessment; it reflects and addresses the practical issues of security assessment. The ISSAF is an evolving framework and it will be further amended and updated."

You can get it here:

<http://www.oissg.org>

Hope it helps ;)

Regards,

Christian Martorella

On Saturday 15 July 2006 02:23, Steve Armstrong wrote:

Please excuse this request, if it sounds noddy. . . .

Re: Is there an Open Source Vulnerability Analysis Framework?

Having worked in the areas of penetration testing, vulnerability analysis, operational security, risk analysis and accreditation (the UK Government's process of getting authority to operate for 'classified' systems), I have yet to come across an open source vulnerability analysis framework.

We have loads of in-house procedures for actually doing the testing and documents for pre, during and post testing, but nothing that would allow another tester to repeat the same contract and produce the same results or report. More importantly there appears to be nothing in the public domain for the customer to read and understand what we were trying to achieve and what his role in the process was prior to our engagement.

It sort of comes down to the fact that there is no way of getting two testers to give you the same results for testing the same network, and while this is good for business in the short term, it does not seem useful for the client in the long term.

Thus my question to the lists is:

Bar the OSSTMM and the Hacking Exposed methodologies, what other open source or otherwise testing and test definition frameworks are out there?

I am looking really at all aspects of data access via network enabled connectivity at the moment, other types of access and risks will come later.

The main reason for asking is this that recently, I devised what appears to be a comprehensive process that should allow two different testing bodies to produce the same test plan and more importantly the same results; and while some generally ignore variations in the testers skills, this will allow the client to confirm before the testing occurs that the tester has the necessary skills.

So before I go through the stages of developing this framework (will be open source) further, I thought it best to check it has not already been done. I would be grateful for any pointers and urls.

Thx

Steve A  
(nebs)

---

--- This List Sponsored by: Cenzic

Concerned about Web Application Security?  
Why not go with the #1 solution – Cenzic, the only one to win the Analyst's Choice Award from eWeek. As attacks through web applications continue to rise, you need to proactively protect your applications from hackers.

Re: Is there an Open Source Vulnerability Analysis Framework?

Cenzic has the most comprehensive solutions to meet your application security penetration testing and vulnerability management needs. You have an option to go with a managed service (Cenzic ClickToSecure) or an enterprise software (Cenzic Hailstorm). Download FREE whitepaper on how a managed service can help you: [http://www.cenzic.com/news\\_events/wpappsec.php](http://www.cenzic.com/news_events/wpappsec.php)  
And, now for a limited time we can do a FREE audit for you to confirm your results from other product. Contact us at request@xxxxxxxxxx for details.

---

---

Horóscopos, Salud y belleza, Chistes, Consejos de amor:  
el contenido más divertido para tu celular está en Yahoo! Móvil.  
Obtenelo en <http://movil.yahoo.com.ar>

---

This List Sponsored by: Cenzic

Concerned about Web Application Security?  
Why not go with the #1 solution – Cenzic, the only one to win the Analyst's Choice Award from eWeek. As attacks through web applications continue to rise, you need to proactively protect your applications from hackers. Cenzic has the most comprehensive solutions to meet your application security penetration testing and vulnerability management needs. You have an option to go with a managed service (Cenzic ClickToSecure) or an enterprise software (Cenzic Hailstorm). Download FREE whitepaper on how a managed service can help you: [http://www.cenzic.com/news\\_events/wpappsec.php](http://www.cenzic.com/news_events/wpappsec.php)  
And, now for a limited time we can do a FREE audit for you to confirm your results from other product. Contact us at request@xxxxxxxxxx for details.

---

--  
No virus found in this incoming message.  
Checked by AVG Free Edition.  
Version: 7.1.394 / Virus Database: 268.10.1/389 – Release Date: 14.07.2006

---

This List Sponsored by: Cenzic

Concerned about Web Application Security? Why not go with the #1 solution – Cenzic, the only one to win

Re: Is there an Open Source Vulnerability Analysis Framework?

Re: Is there an Open Source Vulnerability Analysis Framework?

the Analyst's Choice Award from eWeek. As attacks through web applications continue to rise, you need to proactively protect your applications from hackers. Cenzic has the most comprehensive solutions to meet your application security penetration testing and vulnerability management needs. You have an option to go with a managed service (Cenzic ClickToSecure) or an enterprise software (Cenzic Hailstorm). Download FREE whitepaper on how a managed service can help you: [http://www.cenzic.com/news\\_events/wpappsec.php](http://www.cenzic.com/news_events/wpappsec.php) And, now for a limited time we can do a FREE audit for you to confirm your results from other product. Contact us at [request@xxxxxxxxxx](mailto:request@xxxxxxxxxx) for details.

---