



# IITAC Certification Labs

## CESD

Certified Exploit & Shellcode Developer

## Certification Workbook





## DISCLAIMER

*This disclaimer is not meant to sidestep the responsibility for the material we will share with you, but rather is designed to emphasize the purpose of this "IITAC - International Institute for Training, Assessment, and Certification" feature, which is to provide information for your own purposes. The subjects presented have been chosen for their educational value. The information contained herein consists of Software Engineering, Software Development, Secure Software Engineering, Software Security Engineering, Security in general, Software Management, Security Analysis, Algorithms, Virus-Research, Software-Protection and Reverse Code Engineering, Cryptanalysis, White Hat and Black Hat Content, and is derived from authors of academically institutions, commercials, organizations, as well as private persons. The information should not be considered to be completely error-free or to include all relevant information; nor should it be used as an exclusive basis for decision-making. The user understands and accepts that if "IITAC - International Institute for Training, Assessment, and Certification" were to accept the risk of harm to the user from use of this information, it would not be able to make the information available because the cost to cover the risk of harms to all users would be too great. Thus, use of the information is strictly voluntary and at the user's sole risk.*

*The information contained herein is not a license, either expressly or impliedly, to any intellectual property owned or controlled by any of the authors or developers of "IITAC - International Institute for Training, Assessment, and Certification". The information contained herein is provided on an "AS IS" basis and to the maximum extent permitted by applicable law, this information is provided AS IS AND WITH ALL FAULTS, and the authors and developers of "IITAC - International Institute for Training, Assessment, and Certification" hereby disclaim all other warranties and conditions, either express, implied or statutory, including, but not limited to, any (if any) implied warranties, duties or conditions of merchantability, of fitness for a particular purpose, of accuracy or completeness of responses, of results, of workmanlike effort, of lack of viruses, and of lack of negligence, all with regard to the contribution. Certification material might use material from the Wikipedia.*

*ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION OR NON-INFRINGEMENT WITH REGARD TO "IITAC - International Institute for Training, Assessment, and Certification".*

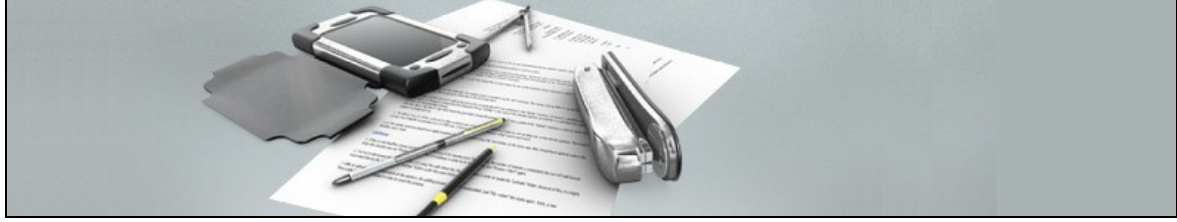
*IN NO EVENT WILL ANY MEMBER, AUTHOR OR DEVELOPER OF "IITAC - International Institute for Training, Assessment, and Certification" BE LIABLE TO ANY OTHER PARTY FOR THE COST OF PROCURING SUBSTITUTE GOODS OR SERVICES, LOST PROFITS, LOSS OF USE, LOSS OF DATA, OR ANY INCIDENTAL, CONSEQUENTIAL, DIRECT, INDIRECT, OR PUNITIVE OR SPECIAL DAMAGES WHETHER UNDER CONTRACT, TORT, WARRANTY, OR OTHERWISE, ARISING IN ANY WAY OUT OF THIS OR ANY OTHER AGREEMENT RELATING TO "IITAC - International Institute for Training, Assessment, and Certification", WHETHER OR NOT SUCH PARTY HAD ADVANCE NOTICE OF THE POSSIBILITY OF SUCH DAMAGE.*

*"IITAC - International Institute for Training, Assessment, and Certification" is a management consulting, technology services, and research organization with high academically background. Committed to delivering innovation, "IITAC - International Institute for Training, Assessment, and Certification" collaborates with its clients to help them become high-performance business and governments. With industry, and business process expertise, and broad knowledge resources, "IITAC - International Institute for Training, Assessment, and Certification" can mobilize the right people, skills, and technologies to help clients improve their performance. "IITAC - International Institute for Training, Assessment, and Certification" facilitates knowledge transfer to people, companies, and organizations, and helps to increase qualification significant. The "IITAC - International Institute for Training, Assessment, and Certification" trainings, assessments, and certifications are building upon experts' knowledge. For this "IITAC - International Institute for Training, Assessment, and Certification" certifications are in compliance with the ISO 17024. The ISO/IEC 17024 ("General Requirements for bodies operating certification of persons") is intended as a framework for certification bodies operating a certification program for persons and as the standard against which an accreditation body can accredit the certification body.*

*The certifications are designed to do for professionals what other licenses do for information systems professionals - namely, to warrant that they understand the general principles that dictate professional behaviour, and that they know how to apply a specific body of knowledge to a well-understood area of technical activity. In theory "IITAC - International Institute for Training, Assessment, and Certification" certified know how to handle matters ranging from project management to marketing, from IT-security to IT-anti-security, from quality assurance to quality management. In practice IITAC certified must master a sufficiently large body of knowledge to pass iterative-incremental exams, assessments, and evaluations that covers the most important and specific areas. The "IITAC - International Institute for Training, Assessment, and Certification" certification has the reputation of being very difficult. Obtaining a "IITAC - International Institute for Training, Assessment, and Certification" certificate is a long-time but not a lifetime achievement. This rule set by the ISO/IEC 17024 is to keep up one's skills and knowledge base and to continue learning new topics and technologies. Organizations staffed with "IITAC - International Institute for Training, Assessment, and Certification" certified gain a complete edge. Because "IITAC - International Institute for Training, Assessment, and Certification" certified are the best in their business, organizations demonstrate to customers, suppliers, and employees alike, the importance they place on professionalism. Additionally, the "IITAC - International Institute for Training, Assessment, and Certification" certified designation reflects a properly and consistently trained professional staff.*

*Any reproduction or storage of this document in public systems is strictly forbidden.*

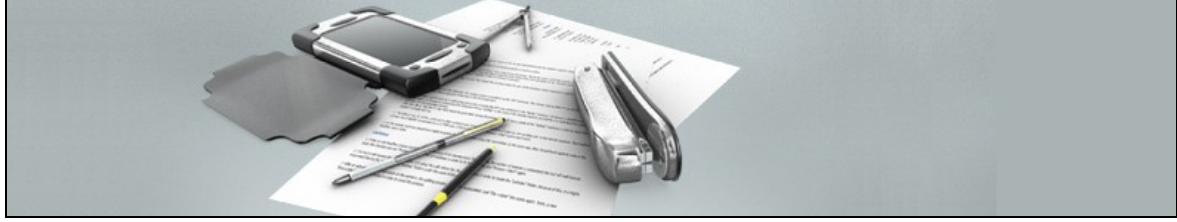
© IITAC - International Institute for Training, Assessment, and Certification, Lange Strasse 31, 32051 Herford, Germany, <http://www.iitac.org>





## Table of Contents

<b>1 Semester 01.....</b>	<b>8</b>
<i>1.1 Practical Assessment 01.....</i>	<i>8</i>
<i>1.2 Practical Assessment 02.....</i>	<i>9</i>
<i>1.3 Practical Assessment 03.....</i>	<i>10</i>
<i>1.4 Practical Assessment 04.....</i>	<i>11</i>
<i>1.5 Practical Assessment 05.....</i>	<i>12</i>





**General Instructions:** Solve each of these assessments as specified. Some of these assessments expect the user to enter data. The values some of these assessments use are "hard wired" into the application with declaration statements or assignment statements. Usually this is a poor way to write a program but with respect of the certification goals one can accept this temporary.

**Note:** Each of these assessments asks you to run the application several times with different values. This is important to do! Playing with the assessment applications is vital to understand them and getting "feel" of programming under you skin.

**Note:** If marked with a note you are allowed to use HLA (High Level Assembly) for this exercise! HLA is pre-installed at the Damn Vulnerable Linux distribution. For further information about HLA visit <http://webster.cs.ucr.edu>. This website contains information material about HLA as well the free e-book „Art of Assembly“ which is highly recommened for this certification! If you like it please support the work by Randall Hyde.

**Certification Flow:** Solve the given assessments. Provide the requested solution by packaging it into a .zip or .tar.gz package. Please use a package structure with folders and subfolders. Provide all – tutorial, source and binary files. You might add additional information within .txt files. For solving the assessments use the training environment Damn Vulnerable Linux (<http://DamnVulnerableLinux.org>) only! Submit the solution package using your account at the IITAC Certification-Labs located at <http://certification.iitac.org>. The certification process requires human activity so it might take some time to check your solutions. After proving your solution there can be two possible results: (1) you might have to do some corrections. For this the assessor will contact you by mail. (2) The solution was accepted and the next certification semester will be activated. By finishing all certification semesters you will receive the final certification examination. After the final assessment exercises you will receive your certification.



## 1 Semester 01

### 1.1 Practical Assessment 01

<b>Filename:</b>	01_exploitme01
<b>Assessment Goal:</b>	Show the candidate's understanding on how to exploit and analyse a simple buffer overflow.
<b>Task:</b>	<ul style="list-style-type: none"><li>• Analyse the target binary</li><li>• Exploit the target binary</li><li>• Write a detailed tutorial about your analysis results</li><li>• Shellcode not necessary, but is recommended</li></ul>
<b>Constraints:</b>	The analysis has to be done under Damn Vulnerable Linux
<b>Tools Allowed:</b>	GDB
<b>Solution Format:</b>	Simple text file

**|** *You are allowed to use HLA if you want to write a Shellcode!*





## 1.2 Practical Assessment 02

<b>Filename:</b>	01_exploitme02
<b>Assessment Goal:</b>	Show the candidate's understanding on how to exploit and analyse a simple buffer overflow.
<b>Task:</b>	<ul style="list-style-type: none"><li>• Analyse the target binary</li><li>• Exploit the target binary</li><li>• Write a detailed tutorial about your analysis results</li><li>• Shellcode not necessary, but is recommended</li></ul>
<b>Constraints:</b>	The analysis has to be done under Damn Vulnerable Linux
<b>Tools Allowed:</b>	GDB
<b>Solution Format:</b>	Simple text file

**|** *You are allowed to use HLA if you want to write a Shellcode!*



### 1.3 Practical Assessment 03

<b>Filename:</b>	01_exploitme03
<b>Assessment Goal:</b>	Show the candidate's understanding on how to exploit and analyse a simple buffer overflow.
<b>Task:</b>	<ul style="list-style-type: none"><li>• Analyse the target binary</li><li>• Exploit the target binary</li><li>• Write a detailed tutorial about your analysis results</li><li>• Shellcode not necessary, but is recommended</li><li>• Answer the following question: „If the buffer size would have a length of 8, would you be able to solve this assessment as well?“</li></ul>
<b>Constraints:</b>	The analysis has to be done under Damn Vulnerable Linux
<b>Tools Allowed:</b>	GDB
<b>Solution Format:</b>	Simple text file

**|** *You are allowed to use HLA if you want to write a Shellcode!*



## 1.4 Practical Assessment 04

<b>Filename:</b>	01_exploitme04
<b>Assessment Goal:</b>	Show the candidate's understanding on how to exploit and analyse a simple buffer overflow.
<b>Task:</b>	<ul style="list-style-type: none"><li>• Analyse the target binary</li><li>• Exploit the target binary</li><li>• Write a detailed tutorial about your analysis results</li><li>• Shellcode not necessary, but is recommended</li></ul>
<b>Constraints:</b>	The analysis has to be done under Damn Vulnerable Linux
<b>Tools Allowed:</b>	GDB
<b>Solution Format:</b>	Simple text file

**|** *You are allowed to use HLA if you want to write a Shellcode!*



## 1.5 Practical Assessment 05

<b>Filename:</b>	01_exploitme05
<b>Assessment Goal:</b>	Show the candidate's understanding on how to exploit and analyse a simple buffer overflow.
<b>Task:</b>	<ul style="list-style-type: none"><li>• Analyse the target binary</li><li>• Exploit the target binary</li><li>• Write a detailed tutorial about your analysis results</li><li>• Shellcode not necessary, but is recommended</li></ul>
<b>Constraints:</b>	The analysis has to be done under Damn Vulnerable Linux
<b>Tools Allowed:</b>	GDB
<b>Solution Format:</b>	Simple text file

**|** *You are allowed to use HLA if you want to write a Shellcode!*

