OWASP Certification Requirements

* [1What should an exam feel like?](https://www.owasp.org/index.php/Category:OWASP_Certification_Requirements#What_should_an_exam_feel_like.3F)
* [2Basic Information](https://www.owasp.org/index.php/Category:OWASP_Certification_Requirements#Basic_Information)
* [3Learning Outcomes](https://www.owasp.org/index.php/Category:OWASP_Certification_Requirements#Learning_Outcomes)
* [4Bloom's Taxonomy of Educational Objectives](https://www.owasp.org/index.php/Category:OWASP_Certification_Requirements#Bloom.27s_Taxonomy_of_Educational_Objectives)
* [5Content Area (Developer/Apprentice/Associate)](https://www.owasp.org/index.php/Category:OWASP_Certification_Requirements#Content_Area_.28Developer.2FApprentice.2FAssociate.29)
* [6Content Area (Architect/Journeyman/Professional)](https://www.owasp.org/index.php/Category:OWASP_Certification_Requirements#Content_Area_.28Architect.2FJourneyman.2FProfessional.29)
* [7Content Area (Master)](https://www.owasp.org/index.php/Category:OWASP_Certification_Requirements#Content_Area_.28Master.29)
* [8Exam Details](https://www.owasp.org/index.php/Category:OWASP_Certification_Requirements#Exam_Details)
* [9Branding](https://www.owasp.org/index.php/Category:OWASP_Certification_Requirements#Branding)
* [10Policies](https://www.owasp.org/index.php/Category:OWASP_Certification_Requirements#Policies)
* [11Conduct](https://www.owasp.org/index.php/Category:OWASP_Certification_Requirements#Conduct)
* [12Correspondence](https://www.owasp.org/index.php/Category:OWASP_Certification_Requirements#Correspondence)
* [13Other Disclaimers](https://www.owasp.org/index.php/Category:OWASP_Certification_Requirements#Other_Disclaimers)

What should an exam feel like?

* Exams are proctored, timed, and delivered in a secure environment. Most exams last approximately two hours.
* Candidates must acknowledge the OWASP Certification and Confidentiality Agreements online at the authorized testing center prior to taking any OWASP Certification exam. Candidates will not be able to proceed with the exam and a refund will not be provided. Signing this legal agreement is required to be officially certified.
* Exams can be very challenging, going beyond simple recall and requiring candidates to engage in on the job types of problem solving. Questions include multiple-choice single answer, multiple-choice multiple answers, drag and drop, fill in the blank and simulations.
* Exams other than final exams are delivered online, with questions in sequence, and do not allow a candidate to "mark" and return to an exam question.
* Candidates will be provided with an erasable note board and marker for notes and calculations to assist them as they answer the questions.
* Exams may contain non-scored items to collect performance data on new items. Non-scored items are not used in determining the passing score nor are reported in a subsection of the score report. All non-scored items are randomly placed in the exam with sufficient time calculated and given to complete the entire exam.
* At the completion of computer-based exams, candidates receive a score report along with a score breakout by exam section and the passing score for the given exam. For onsite proctored exams, candidates receive a score report along with a score breakout by exam section and the passing score for the given exam within ten business days.

Basic Information

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **OWASP Certification Project** | | | | | |
| **Project Name** | **OWASP Certification Requirements** | | | | | |
| **Summary** | This document outlines the basic requirements around the exam portion of certification. Separate pages will be created to discuss marketing, dispute resolution, study aids and other aspects. | | | | | |
| **Email Contacts** | Project Leader [**James McGovern**](mailto:owasp(at)jamesmcgovern.com) | First Exam (BETA) November 1st 2008 | Second Exam (BETA) February 1st 2009 | Final Exam (BETA) March 1st 2009 | Mailing List [**To subscribe**](https://lists.owasp.org/mailman/listinfo/owasp-cert) [**To use**](mailto:owasp-cert@lists.owasp.org) |  |

Learning Outcomes

* Be concise. Each question should be one to two sentences
* Describe the behavior as a desired end product
* Focus on observable behaviors only
* Use definite terms (write, define, list, identify, predict, select, etc)
* Avoid vague terms (learn, see, realize, develop, understand, apply, etc.)

Bad Examples...

1. Develop accuracy (undefined trait)
2. Know the rules for constructing essay tests (indefinite term)
3. Define and calculate the mean and explain its uses (multiple behaviors)

Good Examples...

1. Identifies the correct definition of terms
2. Mount a USB key drive
3. Schedule a cron job

Bloom's Taxonomy of Educational Objectives

* **KNOWLEDGE** (remembering previously learned material)
  + Knowledge of specifics
    - Knowledge of terms
    - Knowledge of specific facts
  + Knowledge of ways and means of dealing with specifics
    - Knowledge of conventions
    - Knowledge of trends and sequences
    - Knowledge of classifications and categories
    - Knowledge of criteria
    - Knowledge of methodology
  + Knowledge of the universals and abstractions
    - Knowledge of principles and generalizations
* **COMPREHENSION** (grasping the meaning of the material)
  + Translation (converting one form to another)
  + Interpretation (explaining or summarizing material)
  + Extrapolation (extending meaning beyond the data)
* **APPLICATION** (using info in concrete situations)
  + *Analysis* (Breaking down material into its parts)
    - Analysis of elements (identifying the parts)
    - Analysis of relationships
    - Analysis of organizational principles (identifying the way parts are organizaned)
  + *Evaluation* (judging value of a thing using definite criteria)
    - Judgments in terms of internal evidence
    - Judgments in terms of external criteria

Content Area (Developer/Apprentice/Associate)

|  |  |  |  |
| --- | --- | --- | --- |
| **Exam One - Developer/Apprentice** | | | |
| **Subject Area** | **Questions (Target Count)** | **Content Owner (Primary)** | **Content Reviewers** |
| Basic Security Principles | 40 to 50 | [**James McGovern**](mailto:owasp(at)jamesmcgovern.com) [**Matthew Chalmers**](mailto:matthew.chalmers(at)owasp.org) | [**J. Oquendo**](mailto:sil(at)infiltrated.net) [**Paul Biciunas**](mailto:paul.biciunas(at)fmr.com) |
| OWASP Top Ten | 10 to 20 | [**Christian Wenz**](mailto:chw(at)hauser-wenz.de) | [**Matthew Chalmers**](mailto:matthew.chalmers(at)owasp.org) |
| Penetration Testing | 30 to 40 | [**J. Oquendo**](mailto:sil(at)infiltrated.net) [**Matthew Chalmers**](mailto:matthew.chalmers(at)owasp.org) | [**Josh Brown-White**](mailto:joshbw(at)analyticalengine.net) [**Bill Pankey**](mailto:bpankey(at)gmail.com) |
| Code Review | 20 to 30 | TBD | [**Mario de Boer**](mailto:njama(at)owasp.org) [**Brad Andrews**](mailto:andrews(at)rbacomm.com) |
| Logging | 10 to 20 | TBD | [**Matthew Chalmers**](mailto:matthew.chalmers(at)owasp.org) [**Nam Nguyen**](mailto:namn(at)bluemoon.com.vn) |
| Software Design Patterns | 10 to 15 | TBD | [**Andreas L. Opdahl**](mailto:andreas.opdahl(at)uib.no) |
| Network Security | 30 to 40 | [**James McGovern**](mailto:owasp(at)jamesmcgovern.com) | [**Mario de Boer**](mailto:njama(at)owasp.org) [**J. Oquendo**](mailto:sil(at)infiltrated.net) |
| XML | 20 to 30 | TBD | [**James McGovern**](mailto:owasp(at)jamesmcgovern.com) |
| Cryptography | 10 to 15 | [**Matthew Chalmers**](mailto:matthew.chalmers(at)owasp.org) [**Mario de Boer**](mailto:njama(at)owasp.org) | [**Paul Biciunas**](mailto:paul.biciunas(at)fmr.com) [**James McGovern**](mailto:owasp(at)jamesmcgovern.com) |
| Software Testing | 20 to 30 | TBD | [**James McGovern**](mailto:owasp(at)jamesmcgovern.com) |
| Threats and Vulnerabilities | 30 to 40 | [**Christian Wenz**](mailto:chw(at)hauser-wenz.de) [**J. Oquendo**](mailto:sil(at)infiltrated.net) | [**Andreas L. Opdahl**](mailto:andreas.opdahl(at)uib.no) [**Josh Brown-White**](mailto:joshbw(at)analyticalengine.net) |
| Databases | 10 to 15 | [**Christian Wenz**](mailto:chw(at)hauser-wenz.de) | [**Nam Nguyen**](mailto:namn(at)bluemoon.com.vn) |

Content Area (Architect/Journeyman/Professional)

|  |  |  |  |
| --- | --- | --- | --- |
| **Exam Two - Architect/Journeyman** | | | |
| **Subject Area** | **Questions (Target Count)** | **Content Owner (Primary)** | **Content Reviewers** |
| SDLC | 30 to 40 | [**Matthew Chalmers**](mailto:matthew.chalmers(at)owasp.org) | [**Antti Vähä-Sipilä**](mailto:avs(at)iki.fi) [**Andreas L. Opdahl**](mailto:andreas.opdahl(at)uib.no) |
| Information Security Policies | 10 to 20 | [**J. Oquendo**](mailto:sil(at)infiltrated.net) | [**Andreas L. Opdahl**](mailto:andreas.opdahl(at)uib.no) [**Matthew Chalmers**](mailto:matthew.chalmers(at)owasp.org) |
| Software Architecture | 30 to 40 | TBD | TBD |
| Economics | 20 to 30 | [**James McGovern**](mailto:owasp(at)jamesmcgovern.com) | [**Wade Mackey**](mailto:wmackey(at)comcast.net) |
| Requirements and Analysis | 10 to 20 | [**Matthew Chalmers**](mailto:matthew.chalmers(at)owasp.org) | [**Andreas L. Opdahl**](mailto:andreas.opdahl(at)uib.no) [**Wade Mackey**](mailto:wmackey(at)comcast.net) |
| Strategy | 10 to 15 | [**Wade Mackey**](mailto:wmackey(at)comcast.net) | TBD |
| SOA | 30 to 40 | Gunnar Peterson | [**Andreas L. Opdahl**](mailto:andreas.opdahl(at)uib.no) |
| Identity Management | 20 to 30 | [**Paul Biciunas**](mailto:paul.biciunas(at)fmr.com) | [**Bill Pankey**](mailto:bpankey(at)gmail.com) |
| Entitlements Management | 10 to 15 | [**James McGovern**](mailto:owasp(at)jamesmcgovern.com) | TBD |
| Privacy | 20 to 30 | [**Bill Pankey**](mailto:bpankey(at)gmail.com) | [**Antti Vähä-Sipilä**](mailto:avs(at)iki.fi) |

Content Area (Master)

The third exam will be a written essay or presentation on a topic deemed appropriate by the OWASP board. The deciding criteria will be determined by OWASP chapter leaders. Each chapter leader will receive one vote. The OWASP Certification Project Leader also gets one vote and subject area contributors also will receive one vote. If people play both roles, then they are permitted two votes. In order to pass, a candidate must receive more positive votes than negative.

Exam Details

* The first exam will consist of 100 to 120 questions (random) where the format can include:
  + Multiple-choice single answer
  + Multiple-choice multiple answer
  + Drag-and-drop
  + Fill-in-the-blank
  + Testlet
  + Simlet
  + Simulations
* Before taking the exam, candidates should become familiar with how all exam types function-especially the testlet, simlet, and the simulation tool. Such practice will allow candidates to focus their exam-taking efforts on the exam questions rather than on how to correctly use the tools.
* Candidates may only take a beta exam once.
* Candidates who fail an exam must wait a period of ninety (90) calendar days, beginning the day after the failed attempt, before they may retest for the same exam.
* Once passed, a candidate must wait a minimum of 180 days before taking the same exam with an identical exam number.

Passing scores are set by using statistical analysis and are subject to change. At the completion of the exam, candidates receive a score report along with a score breakout by exam section and the passing score for the given exam. OWASP does not publish exam passing scores because exam questions and passing scores are subject to change without notice.

Branding

You will notice that we have not landed on the branding aspects around each certification level. The headings reflect much of our current thinking. We will put out a survey to OWASP membership regarding branding aspects after we have completed item development.

In terms of names of the certification, we are currently exploring:

* Certified (Web) Application Security *(level, above)*
* Certified (Web) Application Security Professional/Practitioner
* OWASP Web Application Security Professional/Practitioner
  + [Recursive acronym](http://en.wikipedia.org/wiki/Recursive_acronym)
  + Identical to *OWASP* which could be confusing

Policies

All content, specifically questions, answers and diagrams of the certification exams are the proprietary and confidential property of OWASP. They may not be copied, reproduced, modified, published, uploaded, posted, transmitted, or distributed in any way without the express written authorization of OWASP. Candidates who sit for OWASP exams must agree they have read and will abide by the terms and conditions of the OWASP Certification and Confidentiality Agreements before beginning the certification exam. The agreement applies to all exams. Signing and adhering to this agreement is required to be officially certified and to maintain valid certification.

Conduct

Candidates must take no action to compromise the integrity or confidentiality of any OWASP certification exam or certification program. Penalties for violating the policy can include up to and including a lifetime ban on all future exams and the nullification of all previous certifications.

Correspondence

All official correspondence to certified candidates is sent to the email and/or address recorded in the OWASP Certifications Tracking System. Candidates are responsible for updating their personal information in the Tracking System to ensure receipt of official correspondence.

Other Disclaimers

* The target count for questions is the number of desired questions that are part of the exam question pool at any one time. Over time, questions will be expired and new ones will be added. The pool of questions created by the project team should be double the indicated target count.
* Each subject area will have two reviewers of which the project manager may agree to be one.
* The indicated target count should not be construed as to the number of questions that will be asked in any given exam. This will be determined based on psychometric analysis and/or other factors including but not limited to:
  + Analysis of statistics provided by initial OWASP Certification Survey
  + Detection of exam cheating (e.g. collusion, fraud, etc) by test takers
  + Feedback received from beta test takers
  + Adjustments to the exam to target first time test taker failure rate
* The Project Leader and members of the OWASP board will be the only entities that will ever see the entire question set
* No exam test taker, their employers or potential employers should assume that those who pass are suitable for any particular purpose, only that they have demonstrated sufficient knowledge of the subject areas covered by the exam
* OWASP reserves the right to revoke certification of test takers who have been validated as cheats on other IT certifications

OWASP respects your privacy and is committed to protect the personal information that you share with us. The OWASP Privacy Policy describes how we collect and use your personal information.

* OWASP reserves the right to publish the names and full contact information of any individual or party who compromises the validity of the certification process