OWASP

2013 PROJECT SUMMIT REPORT

2013 PROJECT SUMMIT REPORT

Prepared by: Samantha Groves, OWASP Projects Manager

February 2014

01 PREFACE

PREFACE

The 2013 Project Summit working session reports and outcomes were consolidated and written by the OWASP Projects Manager, Samantha Groves. If you notice anything that requires a change, please send any corrections or comments to Samantha at Samantha.Groves@owasp.org.

02 TABLE OF CONTENTS

TABLE OF CONTENTS

03 ACKNOWLEDGEMENTS

ACKNOWLEDGEMENTS

The success of the 2013 Project Summit was the culmination of months of hard work by many individuals from all parts of the OWASP Community. While I did spend the majority of our 2013 third and fourth quarter planning the logistics remotely as well as managing the on-site logistics during the 2013 AppSec USA Conference in New York City, the summit would not have been possible without the help, dedication, support, and hours of work put in by volunteers, staff, and other members of the OWASP Community. Oh behalf of all who attended and were able to benefit from the working sessions and community connections, I would like to thank all of the individuals who worked to ensure the summit was a success. Below you can find a list of key staff and volunteers who helped with the 2013 Project Summit in no particular order:

KEY VOLUNTEERS	STAFF	BOARD MEMBERS
Fabio Cerullo	Sarah Baso	Michael Coates
Larry Conklin	Kate Hartmann	Dave Wichers
Andrew van der Stock	Kelly Santalucia	Jim Manico
Matteo Meucci	Alison Shrader	Tom Brennan
Andrew Muller	Laura Grau	Eoin Keary
Bev Corwin	Matt Tesauro	Seba Deleersnyder
Robert Shullich	Jasmine Beg	
Kait Disney-Leugers		

SESSION LEADERS			
Johanna Curiel	Michael Hidalgo	Chris Schmidt	Kostas Papapanagiotou
Chuck Cooper	Abbas Naderi	Kevin Wall	Simon Bennetts
Jonathan Marcil	Rahul Chaudhary	Jack Mannino	
Abbas Naderi	John Melton	Jason Haddix	
Dinis Cruz	Dennis Groves	Martin Knobloch	

During the summit pre-planning, there were a few key individuals that I would like to personally thank as they were instrumental in ensuring the summit was a success. First, I would like to thank Dinis Cruz for his encouragement, support, and guidance both throughout the pre-planning, and during the summit working sessions. I can certainly say that the summit would not have encompassed the community environment and contributions of the previous summits if it had not been for his involvement in this year's planning process. Thank you, Dinis. I would also like to thank Tom Brennan for facilitating the summit at AppSec USA 2013, and for helping us acquire a space during the conference. If Tom hadn't suggested and pushed to have a summit during the conference, we would not have had the project progress we now have. A very special thank you to Dennis Groves for his advice, patience, and support. Dennis endured many late nights helping me edit and develop content for the summit, and I would like to thank him for his patience and dedication by helping me throughout the whole process.

I would like to extend a very special thank you to Kait Disney-Leugers, our OWASP Grants and Fundraising intern. She worked on the development of wiki pages, informative content, and marketing copy and materials that we used to promote the summit. I could not have completed the enormous amount of logistical tasks without her contributions. Thank you for helping bring order to the chaos that is planning the summit, Kait.

Additionally, a massive thank you to the OWASP Ops Team for their help and support both before and during the summit. Thank you Sarah Baso for making sure we had a space at the AppSec USA conference, and for ensuring we had enough funds to cover our expenses. I would also like to thank Kate Hartmann, Kelly Santalucia, Alison Shrader, Laura Grau, and Matt Tesauro for helping us get through the craziness that was AppSec USA and the Summit. We could not have gotten through it all without your encouragement and help throughout the pre-planning and during the working sessions. Lastly, a very big thank you to everyone, both inside and outside the OWASP Community, that made the 2013 Project Summit possible!

Samantha Groves
OWASP Projects Manager

04 ABOUT OWASP

ABOUT OWASP

The Open Web Application Security Project (OWASP) is a global, open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain software applications that can be trusted. All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security. We advocate approaching application security as a people, process, and technology problem because the most effective approaches to application security include improvements in all of these areas. We can be found at www.owasp.org.

OWASP is a new kind of organization. Our freedom from commercial pressures allows us to provide unbiased, practical, cost-effective information about application security. OWASP is not affiliated with any technology company, although we support the informed use of commercial security technology. Similar to many open-source software projects, OWASP produces many types of materials in a collaborative, open way. The OWASP Foundation is a not-for-profit entity that ensures the project's long-term success. The OWASP Foundation is a 501c3 not-for-profit charitable organization that ensures the ongoing availability and support for our work. Find out more at: www.owasp.org.

05 ABOUT OWASP SUMMITS

ABOUT OWASP SUMMITS

The OWASP Project Summits are where OWASP community members and industry experts can meet to discuss the future of application security through project collaboration and discussion. It is a neutral, commercial-free setting put together by the OWASP Foundation where attendees are free to engage with their colleagues on software security related matters.

It is important to note that OWASP Summits are NOT conferences even if they can be run alongside a conference. Typically, participants stay in shared accommodations and they are brought together to collaborate and produce a tangible result that sets the roadmap and focus for OWASP for the coming years.

All are free to attend an OWASP Summit, and OWASP will strive to raise enough funds so the majority of participants can attend without need for out of pocket expense. All attendees must come ready and willing to collaborate and work towards producing a deliverable that will advance the state of software security.

06 2013 SUMMIT OPERATIONAL DETAILS

2013 SUMMIT OPERATIONAL DETAILS

PRE-SUMMIT PLANNING

The pre-summit planning phase involved quite a bit of logistic, resource management, and team building work that had to be accomplished at a very fast pace. There were no prior plans to put together a project based summit until it was recommended by the AppSec USA 2013 planning team. Below is a more detailed account of what steps were taken to put together the 2013 summit. Please note that this is not a step-by-step account of what occurred. It is simply a summary of key events that took place, and a list of key tasks that were managed during the pre-planning of the summit.

INITIAL RECOMMENDATION

Originally, the plan was to have a series of project talks and a Project Leader Workshop at AppSec USA 2013 during the conference days. Tom Brennan suggested, during one of the planning calls with the rest of the team, that there should be a project based summit during the event. Samantha Groves agreed that this would be a challenging, but rewarding idea to pursue. She then began speaking to past summit participants/planners, and researching the logistics of past summits.

GATHERING BACKGROUND

Gathering background documentation and tacit knowledge before the event proved to be a little challenging. The documentation was not difficult to find, but it did take some time to digest all of the information in the reports from past Summits. Additionally, Samantha sought out the advice of past Summit planners and participants with the aim of acquiring some 'lessons learned' information from them. Dinis Cruz was a tremendous help during this phase of the planning process. He and Samantha had many conversations about how it was done in the past, what needed to be adapted, and what needed to be done before the event to make it successful.

LOCATION AND SPACE

The location and space were going to be a challenge to acquire from what was learned during the research phase. Past summits were much larger, had much bigger budgets, and the space required to hold all of the attendees and sessions was very large. The summit team was working with many constraints as the venue and space that was acquired for the AppSec USA conference had already been decided on. The summit would certainly be taking place at the same time as the AppSec USA conference, but a separate space large enough to accommodate all of the summit sessions and attendees would need to be found. One of the attendees on the planning calls suggested the Sky Lounge as it is a very big space that had not been allocated to anything in particular for the conference. Samantha agreed that this would be an appropriate space for the summit and proceeded to make arrangements to save the room for the summit sessions. The summit team originally had only planned to hold sessions during the conference days, but Dinis quickly let Samantha know that the sessions would need to be spread out to four days. Samantha agreed and took on the task of extending the schedule. The team ended up acquiring the Sky Lounge for the entirety of the conference.

GATHERING THE TEAM

There were many people involved in the pre-summit planning that played different roles and helped out in many different ways. Kait Disney-Leugers, OWASP's Grants and Fundraising Intern, worked on many of the wiki pages, marketing materials, promotion, page edits, and administration for the summit. Dinis Cruz was a great help as he was able to share his tacit knowledge of summit planning with Samantha. Gathering the session leaders was also a challenge. The summit team had a few sessions that were a must, but they still had to develop more sessions as they only started out with a handful of ideas. Slowly, Leaders began suggesting sessions that could be added to the summit schedule, and slowly the summit team began to grow.

MARKETING

Kait and Samantha quickly put together quite a bit of marketing and graphic content to promote the summit once the room was sorted out. Kait was immensely helpful as she put together several brilliant pieces of marketing communications material. She wrote quite a few pieces for different social media channels and several stories for the OWASP blog. Samantha created the 2013 Summit logo and other summit graphics based on the artwork created by New Way Designs as the aim was to keep visual consistency with the AppSec USA 2013 identity. She also created the wiki pages and content with Kait's assistance. Dinis Cruz helped with the wiki templates.

WORKING SESSIONS: FIXED AND DYNAMIC

During the session development process, the summit team realized that they would need space to facilitate a fixed and dynamic schedule of sessions for the summit. Fixed sessions would be decided upon before the conference, but the team would have to foster an environment that enabled dynamic sessions to serendipitously take place during the summit.

OWASP SUMMIT FUNDING

Samantha started out with zero budget resources to plan the summit with. Originally, the summit team relied on the OWASP Track budget to facilitate Leader participation as this budget is meant to be used to help pay for travel and accommodation for Leaders giving project talks at Global AppSec conferences. Since there was no budget, the summit team had to rely on the AppSec USA 2013 planning team to help them acquire the resources they would need to pull the summit together. Additionally, the summit team attempted to have a cross-collaboration between the Leaders giving project talks, and the summit session Leaders. The team asked the project talk Leaders if they would mind leading summit sessions, and they gave preference to sessions lead by Leaders who would have their travel covered by the OWASP Track budget, their individual project budgets, or their own company. A month or so before the conference, Sarah Baso let Samantha know that the AppSec USA team could give them $5,000 to cover summit expenses. That funding was quickly spent on Leader travel and room expenses. Samantha asked for an additional $5,000 as the summit team was in need of more resources, but the AppSec USA team was not able to accommodate the request when asked. However, on the first day of the conference, Tom Brennan agreed to give the summit team the additional $5,000 that was asked for which helped cover printing, shipping, office supplies, catering, and other additional expenses incurred during the event.

TRAVEL AND ACCOMMODATION FOR LEADERS

Travel and accommodation expenses were covered by the remaining OWASP Track fund, and the additional $5K given to the summit team by the AppSec USA planning team. As mentioned above, the OWASP Track fund is used to assist Leaders speaking on behalf of an OWASP project at Global AppSec conferences, with travel and accommodation expenses. Samantha manages this budget, and she divides the fund evenly by quarter as OWASP typically hosts a Global AppSec conference on each quarter of the year. If any part of the fund is not used, then the remaining budget is migrated to the next quarter. In 2013, there was approximately $6500 USD left to help with project leader travel and accommodation. This budget was used to assist key summit leaders and volunteers with their travel expenses. Every Leader shared a room unless they were coming to the conference with their spouse. In this case, these Leaders reimbursed OWASP for half of the total room cost.

REMOTE PARTICIPATION

Unfortunately, the summit team were not able to raise enough funds to facilitate remote participation for the 2013 Project Summit. It is certainly an aspect of the summits that OWASP finds incredibly important, and the summit team will work hard to make sure remote participation is an option contributors have at summits in the future. Having remote participation was made more difficult due to the need for additional AV equipment, a camera crew, and a session moderator for each event. Moreover, the shared room environment was simply not the best venue to film individual sessions as there were a handful of sessions taking place at the same time at adjacent tables.

SUMMIT LOGISTICS

The logistics during the summit were quite challenging. Samantha arrived at the venue two days before the conference was meant to start. She wanted to make sure everything was in order as the team still had quite a bit of pre-planning to work on before the event. She was joined by Dennis Groves, Dinis Cruz, Colin Watson, Jonathan Marcil, and Martin Knobloch. They all pooled together and realized that the rooms they were given were on floors separate from the Sky Lounge, which is where the summit sessions would be taking place. Dinis suggested they move the rooms to make sure they had an operational center for the planning team, and so they could have a separate filming area for Mark Miller and Jonathan that was close to the Sky Lounge. Samantha agreed as it did not make sense to have the filming room on a separate floor. Martin was able to fix the room issue for the team, and after the rooms were sorted out, they proceeded with planning the session and room logistics.

ON-SITE PLANNING TEAM

The original on-site planning team was made up of: Samantha Groves, Dennis Groves, Dinis Cruz, Jonathan Marcil, and Martin Knobloch. On Saturday, Samantha scoped out potential catering venues for the summit as it was agreed beforehand that lunch would be acquired from outside of the hotel for the first two days of the conference. Moreover, she had the last two books printed, Code Review Guide and Testing Guide, at the local print shop. On Sunday, the summit team met and began focusing on equipment set up and session organization. Dinis and Samantha worked on creating a large printed schedule, room organization, equipment inventory, equipment needs lists, and the Project Review Session logistics. Jonathan began working on getting all of the wifi and equipment set up for his media session. Setting up the wifi proved to be quite a challenge, but Jonathan managed to work his magic and had it working fairly quickly. Dennis and Colin Watson actually started discussing and working on the AppSensor project, and Martin helped manage the room changes. Additionally, Martin scoped out where the rest of the conference and comfort areas would be for the summit attendees. They were later joined by Fabio Cerullo who helped put together the summit floor plan.

SCHEDULE

The schedule was fixed before the conference, but the space allocations and printed timetable were not. The summit team began developing this information by first creating a schedule of summit sessions on the wall of the room. They separated the sessions by day and time of the day as each session was scheduled either in the morning or the afternoon. There were some sessions that were taking place on multiple days, and some that lasted the full day. That was taken into account on the schedule. Once they had a real representation of the session schedule, the summit team began to map out where the sessions would take place. They figured out how many tables were needed, where they would go, how many room dividers would be needed, and what sessions would be in what areas. This was based on the floor plan Fabio created on Sunday.

SUPPLIES

During the Sunday pre-planning activities, Samantha and Dinis took inventory of the supplies the summit team had on hand for the event. They realized that that they were in need of quite a few supplies. Inventory was taken of what was available, and what was going to arrive. This made them both aware of the supply surplus and deficit the summit team was working with. They had three printers donated to them from HP, but they would not arrive until Monday. Additionally, there were no basic office supplies such as notepads, pens, paper, staples, etc. Later that afternoon, Kate Hartmann joined the summit team in the Sky Lounge. Kate, Dinis, and Samantha then headed out to the local Office Max to purchase the supplies they would need for the summit and other event activities. It was great to source a local office supply store nearby the hotel as it proved to be very useful as supplies ran out during the event. All in all, it was a good thing Dinis suggested the purchase of a printer even if the donated HP printers were on the way. The printers did not end up arriving until Tuesday which would have put the summit team in quite a difficult position had they not purchased the printer. Well done, Dinis! Great insight.

CATERING

The catering proved to be a bit tricky. The original plan was to order lunch and have it delivered, but it turned out that the most in-expensive and healthy alternative was a bit more difficult to order from than was originally anticipated. Pret A Manger was the choice and they specialize in creating healthy sandwiches, soups, and salads. They had an online ordering system, but it seems customers have to put in their catering order 5 days in advance. This put the summit team in quite a bit of a dilemma after this was found out. Samantha visited the nearest Pret A Manger shop, which was only 3 blocks away, and talked with the staff about the predicament. She asked them if it would be ok to have her visit their shop and purchase a large bulk order of their sandwiches and drinks all at once on both Monday and Tuesday. They did not have an issue with this, and they were ready to anticipate her order for the next two days. Now, Samantha just had to figure out who would help her carry the load of sandwiches back to the conference venue. The summit team actually ended up having to order from Pret A Manger for all four days of the conference, and various volunteers helped Samantha carry the sandwiches and water bottles back to the hotel. Samantha ended up ordering water bottles from the hotel as they were far too heavy to carry, and it did not make sense to catch a cab to drive them three blocks up the road.

OVERALL SUMMIT OPERATIONAL COSTS

The table below summarizes the 2013 OWASP Summit operational costs. The costs were either covered by the OWASP Projects Track budget or by the OWASP AppSec USA operating budget.

EXPENSES: MARRIOTT FOOD & BEVERAGE

CATEGORY	COST	NOTES
Monday - Breakfast pkg for 25 ppl	$900.00	Tea and Coffee
Tuesday - Breakfast pkg for 25 ppl	$900.00	Tea and Coffee
Wednesday - Breakfast pkg for 25 ppl	$900.00	Tea and Coffee
Thursday - Breakfast pkg for 25 ppl	$900.00	Tea and Coffee
Monday - Pizza	$875.00	Dinner
Monday - Beer	$500.00	Dinner
Tuesday - Pizza	$875.00	Dinner
Tuesday - Beer	$500.00	Dinner
Tues - Coffee Break for 25 ppl	$875.00	Dinner
Mineral Water	$300.00	Lunch
Subtotal	$7,525.00	

CATEGORY	COST	NOTES
22% Service Fee	$1,655.50	
Marriott Food & Beverage Total	**$9,180.50**	

EXPENSES: ADDITIONAL FOOD AND BEVERAGE EXPENSES

CATEGORY	COST	NOTES
Lunch for Project Summit	$73.13	
Lunch for Project Summit	$204.90	
Lunch for Project Summit	$300.07	
Lunch for Project Summit	$231.27	
Lunch for Project Summit	$241.90	
Bottled Waters	$17.60	
Additional Food Expense Total	**$1,068.87**	

EXPENSES: WIRELESS, AV, SIGNAGE, EQUIPMENT

CATEGORY	COST	NOTES
16th Floor Internet	$1,964.20	
16th Floor AV	$3,665.40	
16th Floor Electrical	$1,580.00	
Signage	$277.00	
Laptops	$768.48	$384.24 each x 2
Equipment Expense Total	**$8,255.08**	

EXPENSES: MISCELLANEOUS SUPPLIES AND COSTS

CATEGORY	COST	NOTES
Gift Cards	$300.00	Coffee for Summit Session Leaders
Project Summit Supplies	$624.53	
Project Summit Supplies	$84.98	
Project Summit Supplies	$268.81	

CATEGORY	COST	NOTES
Project Summit Supplies	-$367.73	
Prints	$42.32	Reimbursement to Jonathan
Book Printing	$185.31	
Amount donated from AppSec USA	$5,000.00	To cover Summit expenses
Miscellaneous Expense Total	**$6,138.22**	

EXPENSES: TRAVEL COSTS

CATEGORY	COST	NOTES
Flights	$6,094.24	Covered by Projects Funds
Accommodation	$4,812.86	Covered by Project Funds
Flights	$3,247.10	Covered by OWASP Track Funds
Accommodation	$10,385.00	Covered by OWASP Track Funds
Travel Expense Total	**$24,539.20**	

EXPENSES: TOTALS

Subtotal Marriott Food & Beverages	$9,180.50	
Subtotal Additional Food & Beverages	$1,068.87	
Subtotal Wireless/AV, Signage, Equipment	$8,255.08	
Subtotal Miscellaneous Supplies	$6,138.22	
Subtotal Travel Costs	$24,539.20	
Total amount Spent by OWASP	**$49,181.87**	

07 LESSONS LEARNED

LESSONS LEARNED

The Lessons Learned section below was put together based on the 1st person perspective of OWASP Projects Manager, Samantha Groves. Her insight comes from being the primary planner for the 2013 Project Summit.

TACIT KNOWLEDGE

It is imperative to acquire as much tacit knowledge as possible before planning and running a summit. Tacit knowledge is very difficult to transfer as it requires going through the actual experience. I recommend attending a summit and paying attention to all of the logistical details and processes designed for the event. Reading past reports and talking to those who have planned summits before is also very important, but nothing compares to actually having planned and executed a summit despite having it be a smaller version of the much larger summits. It is also extraordinarily helpful to have a previous summit planning lead mentoring you throughout the process of running the event.

PRE-PLANNING

The pre-planning is actually a lot more work than running the summit itself. There are quite a few materials that need to be taken into consideration and managed. Not only do you have to put together sessions, encourage engagement, and create content for the event, but you have to make sure that you create promotional campaigns that inspire participation and commitment from the community and beyond. I recommend having a team of 5, but this depends on whether you are running the summit on its own or with a conference. You will need a much larger team if you are running the summit on its own. If you are running the summit with a conference, you will need a primary summit planner, a planning assistant, a wiki page editor/administrator, a session coordinator, and an on-the-ground logistics coordinator.

VENUE

The venue choice is a very key component. It is important to make sure that the attendees and summit leaders will not be disturbed or distracted; therefore, be mindful if choosing a hotel or any other well trafficked venue. Another detail to note down is that many of the 2013 Summit participants found the Times Square location a bit distracting. Having these types of events in very popular areas with many attractions for tourists, has a potential to cause a high risk for engagement decline. Be mindful of your choice of location due to this factor, as well.

FLOOR PLAN AND ROOM TYPE

I highly recommend having a communal session meeting area where an environment can be fostered to encourage a more dynamic type of working session. This is a similar type of space to what we had in the Sky Lounge at the 2013 Summit. I recommend having several round tables with a separate section with a projector. For fixed sessions, I recommend giving the session leaders their own room to work in, equipped with wifi and a projector. Additionally, if running a summit event attached to a conference, make sure your rooms are only used for summit activities only. We made the mistake of sharing the Sky Lounge with the conference bag stuffing team and it turned out to be a disaster. The bag stuffing team ended up staying in the room the entire day instead of the three hours they had originally planned, and they were a MASSIVE distraction to our sessions and Leaders. I received quite a few complaints about it. I cannot stress this enough. Make sure your session rooms are for summit activities ONLY.

SUMMITS AT A GLOBAL APPSEC

While holding the summit during the AppSec USA conference did have its benefits, it did cause quite a bit of engagement issues among attendees. Having the summit during the conference did save us money, and it allowed the summit and AppSec USA planners to consolidate their resources and save money in quite a few areas that would have otherwise cost double if they were held at separate times in separate venues. However, this savings in resources and funds had a drawback in that it caused summit and conference activities to compete with one another for attendee attention. People wanting to participate in both were forced to choose between the two, and attendees let us know they were not pleased about this. Based on this experience, I recommend either having the summit as its own event, or 2/3 days before or after a conference if it needs to be attached to an AppSec event to save on resources and funds.

CATERING

It is imperative to have a good budget for catering as this is one of the most important details that can go very wrong very quickly if not managed correctly. It is important to offer breakfast, a coffee break, lunch, afternoon coffee break, and dinner. You will receive complaints if you do not offer nourishment to your guests and session leaders at very strategic times throughout the day. Do not skimp on afternoon coffee! There will be complaints. Make sure to order catering in advance, and make sure to have a variety of options for those with different dietary needs: Vegetarian, Vegan, Gluten Free, Kosher, No Shellfish, Diabetic, Dairy Free, No Pork, etc.

BUDGET NEEDS

We most definitely need some sort of budget to pull off a summit. It is incredibly unreasonable to have no funds available to the summit planner. Thankfully, we were able to adapt, and be creative with the little funds we had. Thankfully, the AppSec USA planning team generously loaned us the resources they used to put on the conference, and we were able to piggy back off their purchases such as the venue location/costs, AV, electrical, wifi, catering, and many more items. They were also able to give us $10K at different times throughout the conference which we were in great need of even for small expenses. I recommend having at least $50,000 of seed funding available before even entertaining the idea of putting together an OWASP Summit. A big thank you to Sarah, Tom, Pete and the rest of the AppSec USA 2013 team for helping us out with our budget needs.

HUMAN RESOURCE NEEDS

When running a summit, it is imperative that you have dedicated volunteers responsible for key roles throughout the event. The principal role is the Primary Planner role. This person will be responsible for everything, making sure that all of the tasks are done, everyone knows what they need to do, and that everything is running according to plan during the event. The second most important role is that of the Session Leaders. The Session Leaders run your summit working session, and they make sure that everyone stays on point. They are ultimately responsible for making sure the session runs smoothly, and that everyone understands what the aim of the session is. Next is the Scrum Master. You will need one Scrum Master for each session. This person is responsible for making sure everyone attending the session accomplishes what was originally intended, and that all participants stay on topic. Having a room proctor for every session is also important. The Room Proctor is responsible for making sure that everyone participating in the session has everything they need throughout the working session. This includes making sure that all equipment in the room is working, and that faulty equipment is managed if anything goes wrong. I highly recommend having a Summit Assistant that will serve as the summit admin throughout the event. There were many times during the 2013 Summit where we needed additional assistance with catering, supply procurement, placement arrangement, and a general second hand in case the Primary Planner is not present. I recommend having the assistant take care of managing the printed schedule during the event, as well.

AV NEEDS

Your AV needs will certainly depend on the layout and space available. We only had one room during the 2013 Summit, but we made great use of the space with the help of some very handy dividers. We separated the space into two areas. One area had a projector hooked up to it with two round tables for guests. The other area was the main session lounge, and this area only had one projector hooked up in one of the corners of the room. This area was designated the media area. If you have individual rooms for fixed sessions, I recommend having a projector and a microphone set up in each room. Additionally, I recommend having at least 1 laptop, and 1 high quality video camera in each room to record presentations and sessions. I further recommend having a camera crew and a photographer to film and take photographs sporadically throughout the summit, as well.

WIRELESS NEEDS

It is imperative that the wireless network have a designated manager that will troubleshoot any issues throughout the entirety of the event. During the 2013 Summit, the network was down for the majority of the time causing problems for many of our attendees. The username and passwords kept changing several times a day, and this caused even more confusion. Many could not log into the network even when it was working. This issue certainly caused a loss of productivity for several of the sessions that required their attendees to be able to log into the wiki or their repositories. We need to make sure that the set up will accommodate the number of attendees estimated to participate in the sessions, and we need to make sure that the login process is streamlined and easy as well.

EQUIPMENT AND SUPPLIES

I cannot stress how important it is to have at least two printers on hand the moment the planner arrives at the venue. We made the mistake of having printers shipped to the venue, and we ended up having to purchase one at the local shop to meet our printing needs during the on-site, pre-planning days. You will need to print off an enormous amount of materials before the working sessions start, and you will need to make sure you have all of the toner necessary to print off these materials for all of your guests. The working session leaders will need to have access to these printers too. I recommend having a printer set up in every working session room if you have the space. Additionally, you will need basic office supplies such as: notepads for every attendee, pens, printer paper, tape, markers, sticky notes, highlighters, Post-It pads, sharpies, poster boards, pencils, and a sharpener at least.

08

SUMMARY OF 2013 WORKING SESSION OUTCOMES

SUMMARY OF 2013 WORKING SESSION OUTCOMES

OWASP PROJECTS REVIEW SESSION

The Projects Review Session was one of the most challenging and dynamic sessions of the entire summit. Johanna Curiel and Chuck Cooper organized and lead the session. Diniz Cruz, Dennis Groves, and Samantha Groves were key participants, as well. The original aim of the session was to review all of the current OWASP Flagship Projects based on the criteria the Technical Project Advisors put together over a period of a few months prior to the summit. As the Leaders began working on the reviews, they noticed that some of the assessment questions were redundant and did not make sense to ask for certain projects. Additionally, they realized that there was a gap in the reviews as the usability and project value were not being assessed by the criteria they currently had developed. As a result, the entire session's focus was shifted from conducting reviews, to creating a well rounded review process and criteria that would encompass not only project health and product quality, but that would measure the usability and value of project product consumers. In the end, four sets of criteria were put together, and assessment forms were created based on the criteria. This allowed the reviews to be more streamlined, and easy to use. The project health and product quality assessments were based off of the criteria developed by the Technical Project Advisors, and the usability and value assessments were developed by the session participants during the summit. The criteria are based on the OWASP OpenSAMM Framework. There were many heated discussions during this session, but in the end, the Leaders developed the foundation for a more solid OWASP Project Assessment process that can be expanded upon in 2014.

OWASP MEDIA PROJECT

The OWASP Media Project was one of the last projects to be recruited for the summit, but it proved to be one of the most valuable. Project Leader, Jonathan, Marcil, set all of the equipment up in order to showcase his ideas to potential viewers during the summit. The aim of the session was to introduce participants to the project objective which is to facilitate the recording of OWASP Project presentations, and to facilitate the organization of video and audio based material into one consolidated, easy to find location. Jonathan only had one participant that he showcased his project too, but the more valuable outcome was the community and support he gathered from the attendees. He was able to capture forty three (43) videos online for a total of 34.5 hours of content. Due to his hard work, he was able to increase our OWASP YouTube Channel views from 245 to 11,289 views in one month alone. He was also able to capture that we were watched by 114 different countries across the globe. Overall, the success of the session was due to Jonathan's keen organizational skills, the quick posting of our video and audio recordings, and his ability to adapt to the ever changing environment of an OWASP AppSec.

MOBILE SECURITY SESSION

The OWASP Mobile Security Session was one of our most popular working sessions at the conference. The group was small, but the attendees were very engaged. The majority were there to discuss the project's progress with the attending Project Leaders. Jack Mannino and Jason Haddix were both leading the session. The working session group had a great discussion about identifying classes of mobile vulnerabilities specifically in the Mobile Top Ten. The working session group went over quite a few ideas, but they decided on minimal changes to the categories as some places have already established a standard. Additionally, the group were able to identify some new issues and potential new projects to add to the overall Mobile Security Project. Overall, Jason and Jack were able to accomplish what they set out to do with the working session. They were able to discuss category changes, and they were able to talk to actual users of the project and discuss some of their "pains". The primary concern was project completion according to the Leader report. The next steps are to finish updating the project wiki content, create a PDF guide for the project, and update some of the categories. The Mobile Security Project team hoped to unveil the finished wiki at the AppSec Cali Conference in January 2014.

OWASP PCI TOOLKIT SESSION

Johanna Curiel lead the OWASP PCI Toolkit Session, and it was one of our most popular working session at the summit. There were about 20 attendees that all contributed to the working session in great detail. They ranged from recent graduates to experienced PCI-QSA auditors. The aim of the session was to gather feedback from the sector to gauge the need for the project, and to better formulate requirements and a roadmap to move forward in 2014. The working session focused on explaining the project purpose and gathering feedback before beginning the programming work on the toolkit. The session attendees all agreed that this tool will be very beneficial to organizations wishing to understand the PCI-DSS requirements; as a result, Johanna has decided to move the project forward. She has now completed her PCI training, and she was able to become a PCI professional late last year. She hopes to deploy the tool by mid February with the first beta version with 2 modules.

OPENSAMM SESSION

The OpenSAMM Session was another one of our popular working sessions during the summit. There were eleven attendees, and Seba Deleersnyder and Pravir Chandra lead the team. The session took on the form of a workshop where the focus was to establish the current state of the project and future action items in an effort to move the project forward. The team took an inventory of the current tools and templates, and this was followed by a discussion on shared experiences or case studies. Next, they talked about what currently needs improvement and they prioritized their set of goals for the coming year. This was followed by the collaborative development of a rough plan for future activities aimed at moving the project forward. Overall, it was a very successful working session as the team was able to discuss what items need improvement, and they were able to put together a plan of action for 2014.

OWASP O2 DOCUMENTATION SESSION

The OWASP O2 Guide was one of the books created for the 2013 Project Summit. It was a very alpha stage version of the guide that nailed down the foundation for the more robust project book. Michael Hidalgo and Dinis Cruz lead the working session, and they had several attendees contribute to the discussion about the content's direction. Everyone agreed that the O2 Platform is a very powerful tool, but the primary concern is that the user learning curve is quite high. "How To" documentation can be incredibly useful to potential consumers of the tool, and the team worked on developing a few key chapters. The solid outline still needs to be defined, but the primary outcome is the development of the roadmap goal to work on and complete the guide in 2014.

WRITING AND DOCUMENTATION REVIEW SESSION

The Writing and Documentation Review Session was lead my Michael Hidalgo. One of the challenging aspects of this session is that it only lasted four hours, and Michael reported that the time limit was simply not enough. Contributors really needed to come prepared to discuss each book having already read the materials beforehand. The contributors were only able to skim the sections of the majority of the books, and they gave feedback based on their assessment of the material. The only book that was able to get solid feedback from the contributors was the Code Review Guide as Larry Conklin was in attendance. Larry was able to sit down with Michael and the other contributors, and they were able to discuss the content in more detail. Larry was also able to provide a good roadmap for the content that still needed to be completed for the guide. Overall, this session had many learned lessons to be recorded. If we are to have another writing and documentation review working session at future summits, it is imperative that all contributors come prepared to discuss the content having already read the materials. Additionally, it is incredibly helpful to have the Project Leader on hand to discuss the documentation with the reviewing contributors as it helps to have in-person discussions about the content.

OWASP PHP SECURITY AND RBAC PROJECT SESSIONS

Abbas Naderi and Rahul Chaudhary headed up both of these sessions. They are working together on these projects; however, Abbas focused more on presenting the PHP Security Project and Rahul focused on presenting the RBAC Project. The primary aim for both Leaders was to promote both projects, and to potentially get attendees to contribute to both projects. They each prepared a presentation to give to attendees, but unfortunately very few attendees came to their sessions. The projects are fairly new to the inventory so they were not surprised at the turnout, but both Leaders were able to use this to their advantage. They collaborated with Jonathan Marcil from the OWASP Media Project, and they both did a full recording of their presentation for the OWASP YouTube Channel. They were the first summit participants to record their presentations, and they were both happy to have the promotional opportunity. The primary outcome for these two sessions was an increase in outreach. Both Abbas and Rahul were able to promote their project, establish what they need from the community, and what they would like to accomplish going forward.

ESAPI HACKATHON SESSION

Kevin Wall and Chris Schmidt lead the ESAPI Hackathon during the summit. The working session lasted all four days of the AppSec USA conference, and there were quite a few interested participants that sat down with both Leaders to discuss the Hackathon. It was the first time Chris and Kevin were able to meet in person, and this sparked a great debate on what aspects of ESAPI should be focused on for 2014. Overall, ESAPI received two bug fixes from the ESAPI Google Issues, and one contributor wrote implementations for the proposed interfaces. One of the biggest challenges the Hackathon faced was that the venue's Wifi access kept dropping for hours on end. This created a huge barrier to contribution as all contributions required online access to the repositories. However, despite this set back, Chris and Kevin were able to make valuable connections and contacts with attendees. They were able to meet with DHS representatives who expressed interest in funding their initiatives, and they met with several organizations that were interested in volunteering some human resources to work on the project. Both Leaders were able to adapt to the unfortunate Wifi set backs, and create value from the connections made at the summit. Moreover, the Hackathon was extended to mid-January. The aim was to run the Hackathon remotely and award prizes to the individuals with the best contributions to the project.

OWASP ZAP HACKATHON SESSION

The ZAP Hackathon had a very good attendee turnout. The session was lead by Project Leader, Simon Bennetts, and it was adapted based on attendee need. Simon had originally wanted to have contributions added to ZAP; however, the attendee discussion dynamically changed the nature of the session. In the end, Simon took over the back room of the summit hall, and gave more of a training session on ZAP. Overall, Simon was very happy with the result as the attendees were happy to be involved in the session. Additionally, Simon collaborated with Jonathan Marcil and the OWASP Media Project. He was able to record his OWASP ZAP presentation which has received a total of 4,490 views to date. Simon has no plans for a future Hackathon, but stresses that there are always things to do when it comes to the OWASP ZAP Project.

APPSENSOR 2.0 HACKATHON SESSION

The AppSensor 2.0 Hackathon working session was lead by John Melton and Dennis Groves. The aim of the session was to review the current AppSensor Guide documentation for version 2 of the book and give initial feedback on the content to the team. The AppSensor team was able to meet in person for the very first time to discuss the goals and timeline for the second version of the book. They specifically focused on presenting the initial design and code, and they were able to get feedback from the rest of the team and other session attendees. The AppSensor team members were also able to meet with various other conference attendees and present AppSensor to them. They were also able to showcase other OWASP Projects that would meet their needs, during the summit. Overall, the team's goals were met for the working session. They were able to meet in person, gain some potential new contributors, and discuss the current progress of the AppSensor book project. Additionally, John plans to complete V2 of the code and release it by Q1 of 2014. Current progress can be seen here: https://github.com/jtmelton/appsensor

TRAINING AND ACADEMIES DEVELOPMENT SESSION

The OWASP Training and Academies sessions were one of the most successful working groups at the summit. A good number of Leaders and participants attended the sessions, and the meeting ended up lasting the full day. Attendees decided that since both sessions were very related, it would be best to merge them into one longer working session. Martin Knobloch and Dr. Kostas Papapanagiotou lead both sessions together. The primary outcome was the establishment of a new project type for all of the educational projects within the OWASP Project infrastructure. The attendees identified two primary issues the projects are currently facing: too many projects, and unreachable targets for each project. To solve these issues, the group decided to merge all education projects into one, much larger project, with all other projects treated as sub-projects of the much larger entity. The umbrella project will be called the OWASP Education Project, and participants hope it will eliminate one of the biggest issues with project development. Additionally, the team developed a roadmap on how to proceed with the educational projects in 2014. For a detailed roadmap, please see pg.41 of this report.

09

WORKING SESSION OUTCOMES: LEADER REPORTS

WORKING SESSION OUTCOMES: LEADER REPORTS

The working session outcomes below are the direct reports sent to the OWASP Projects Manager from the participating Project Leaders. They outline, in greater detail, what their session deliverables were, and list their roadmaps for future work to be completed. Please note, that some sentence structure, and spelling was corrected before implementation of each report to this document.

OWASP PROJECTS REVIEW SESSION

SESSION DESCRIPTION: During the OWASP Projects Review working session, attendees will be able to participate in the review of the entire inventory of OWASP Projects using the new assessment criteria developed by our team of Technical Project Advisors. The aim of this session is to establish a more accurate representation of OWASP project health and product quality. The session outline is as follows:

- Overview of new assessment criteria to conduct reviews.
- Team in small groups (2 to 3 max) based on experience and background to asses a set of Projects (Code, Tool or Documentation)
- Fill in the Questionnaire (Google Forms) to complete assessment of Projects and provide the review with a final score and results (Project defined as Incubator, Lab or Flagship)
- Review results of questionnaire with your team.
- Present results and conclusions of assessment session.

OUTCOMES

1. We were able to present the project quality and health assessments that the team had worked on over the prior few months, get some good feedback from OWASP leaders, and have a number of OWASP members use the assessment to rate some of the existing projects so we could see what worked well and what didn't work.

2. Yes, we were able to take everyone's input to further improve both assessments. We removed a couple of questions that were well-intentioned, but problematic for reviewers. Since it wasn't clear if a project passed a health assessment and should be promoted or not, we made sure all of the questions on the overall project health questions were knock-out questions, meaning that if they did not satisfy the criteria they weren't ready to be promoted since these are all key principles fundamental to the goals of all OWASP projects.. To accomplish this, more subjective questions were moved to the quality assessment which uses a numeric scale to rank the project, rather than being ‘Yes’ or ‘No’ questions. We also created a standard scoring scale for all project types, which works with a single rating range if users assign full credit if a question is not applicable. There were also some cosmetic changes made regarding the instructions to make it easier to focus on the question, and yet still easily get guidance on how to answer each question.

The bottom line is that I believe that the time spent talking with OWASP Leaders and Members directly resulted in the biggest improvement to the project assessments, which exceeded my expectations of what we wanted to accomplish at the summit.

3. The follow-up items were to create an online form that reviewers could use to rate projects, ask project leaders to rate their own project (partly as a process to weed out inactive projects, so we don't spend time reviewing dormant projects), get 10 quality reviews for each project from OWASP members who use the projects (especially the tool and library code projects since good health assessments are predicating on having reviews from those most familiar with those project that have an environment to use them in and projects to apply them to), and perform health assessments on all of the projects (focusing first on projects who have requested a review or to be promoted and flagship projects, then lab projects, and finally incubator projects).

OWASP MEDIA PROJECT SESSION

SESSION DESCRIPTION: The OWASP Media Project is an infrastructure project that gathers, consolidates, and promotes OWASP content in video format on a central appealing hub. The first and main instance of the project will be a YouTube channel.

The session will be used in order bring project leaders up to speed on how video sharing and live streaming can help promote your project and reach people. We will do that by presenting Google Hangout, and the official OWASP YouTube channel.

Then, we will gather potential sources and existing videos in order to populate the OWASP channel. This summit experience will not just be about promoting the Media Project itself, but also about the exposure of any other projects with video content.

OUTCOMES

1. What were the outcomes of the Sessions?

I can't speak for the other project leaders really, but on my part I did meet a lot of them and briefly exchanged contacts. I'd say the session brought us together, not only to see the people within one project, but to also see other project leaders and volunteers and this should be encouraged regularly.

2. Did you accomplish what you set out to accomplish before the summit?

In our cases we just presented the project to one interested person, so it was not that good on this part. I think it's hard for a project that isn't flagship level to motivate people to go one day only for that. However we wanted to accomplish something else with the Media Project: record other people from other project, and in that regards we succeeded.

3. What is there left to do?

Do more stuff in order to promote the project leader's presentations online and do working session.

4. Roadmap for accomplishing what is left to do.

That would be added to the roadmap of Media Project; however, we have many more priorities and this would be down on the list. That could change if we get more volunteers.

OWASP MOBILE SECURITY SESSION

SUMMIT DESCRIPTION: Just as the mobile security landscape has changed, so has the OWASP Mobile Project. Join us as we discuss the major milestones of 2013 and what is in store for the projects future. We will also go deeper in to the Mobile Top Ten project where we will discuss the decisions made on categories, vulnerability information, and look at some surprising vulnerability trends in mobile applications.

During this session, we will cover:

- OWASP Top 10 Mobile Risks, 2014 Refresh.

- Mobile project 2013 achievements and the 2014 roadmap.

- Increasing industry collaboration within the mobile security space.

OUTCOMES

1. What were the outcomes of the Sessions?
a. Our small group spent time trying to identify classes of mobile vulnerabilities. The mobile top ten in specific. We went over a lot of ideas but ended up deciding on minimal changes to the current categories. This was for a few reasons. Some places have already instated a standard for one. We did identify some new issues arising and new potential projects to add to the overall mobile security project, such as criteria for MDM type solutions since they are not cover in the mobile project but companies want some security guidance when they test or evaluate them.

2. Did you accomplish what you set out to accomplish before the summit?
a. We did. We decided on a few category changes. We talked to users of the mobile top ten and addressed some pain points (mostly project incompletion).

3. What is there left to do?
a. We are finishing the wiki content this month and "unveiling" it at Appsec California. We are also aiming at re-categorization for 2014, but we are unsure if we can make the next week deadline.

4. Roadmap for accomplishing what is left to do.
a. Wiki content is our top priority at the moment.
b. Followed by restructuring the categories and evaluating data from 2013
c. A PDF guide would be awesome after all that

OWASP PCI TOOLKIT SESSION

SUMMIT DESCRIPTION: Join us and learn how to help organizations achieve PCI-DSS compliance with OWASP tools & Documentation by creating an interactive scope toolkit app.

OUTCOMES

1. What were the outcomes of the Sessions?

At APPSEC we had one session with a group of 20 persons approx., ranging from recent graduates in security engineering to experienced PCI-QSA auditors. The session focused on explaining the purposes of the project and their feedback before embarking into fully programming the toolkit. All agreed that such a tool will be very beneficiary to companies looking to understand the PCI-DSS requirements and how OWASP guides fits into all of that.

2. Did you accomplish what you set out to accomplish before the summit?

Yes. The idea was to get feedback from the sector to understand and adapt the toolkit requirements to their needs and what kind of information are they looking for to comprehend. Before the summit I had a defined idea , but after speaking to the assistants, it was clearer and better to focus in certain areas, which helped to define a better plan that fits their needs.

3. What is there left to do?

Right now, I'm programming the different sectors. End December I had a PCI_training and I was able to become PCI professional which took time from my development, but I think this all adds to better understanding and the credibility of the project. I'm happy that now that people can verify my credentials as a PCI professional through the PCI council website. This achievement was also part of my project

https://www.pcisecuritystandards.org/approved_companies_providers/verify_pcip.php

Name: Johanna Curiel

PCIP Certificate #: 1001-533

PCIP Certified From: 23 Dec 2013

PCIP Certified Through: 23 Dec 2015

4. Roadmap for accomplishing what is left to do.

Right now, I'm focusing to deploy by mid February the first beta version with 2 modules (APPS & NETWORK0) I need to adapt the Wiki, and the idea is that by May to have the other modules completed. A simple draft is available already as a google app on: http://pci-toolkit.appspot.com/

This app will be updated an later on available through GitHUb. I have 2 potential contributors but again, after I'm back from the Netherlands I'll check with them to get some work done on this part.

OPEN SAMM SESSION

SESSION DESCRIPTION: OWASP Software Assurance Maturity Model (SAMM) is an open framework to help organizations start and implement a secure software development lifecycle that is tailored to the specific risks facing the organization. During the AppSec USA conference, the SAMM project team organizes this workshop for you to influence in which direction SAMM evolves. The workshop is also an excellent opportunity to exchange experiences with your peers.

We will cover the following agenda:

- Introduction / getting to know each other
- Project status and goals
- OpenSAMM inventory of tools and templates
- Case studies / sharing experiences
- What do we need (thinking about improvements, can be anything ranging from translations over tools to model improvements)
- What do we need next (prioritization)
- Call for involvement (responsibilities), identity teams for specific topics
- Rough planning for the future
- Extra topic: source/build control

OUTCOMES

Thursday November 21, 2013 1:00pm - 5:00pm

Location: Sky Lounge (16th Floor) (NY Marriott Marquis)

During the AppSec conferences, the SAMM project team organizes workshops for you to influence the direction SAMM evolves. This is an excellent opportunity to exchange experiences with your peers. Understanding of SAMM is a prerequisite for participation in this OWASP summit session.

Present:

A. Stephanie Tan

B. David Felio

C. Aaron Estes

D. Adam Langford

E. Martin Knobloch

F. Seba Deleersnyder

G. Yan Kravchenko

H. Qinglin Jiang

I. Colin Watson

J. Matteo Meucci

K. Jonathan Carter

Agenda:

1. Introduction / getting to know each other - 10 mins.
2. Project status and goals
3. OpenSAMM inventory of tools and templates
4. Case studies / sharing experiences
5. What do we need (thinking about improvements, can be anything ranging from translations over tools to model improvements)
6. What do we need next (prioritization)
7. Call for involvement (responsibilities), identity owners / teams for specific topics
8. Rough planning for the future
9. Source/build control

Meeting notes:

Latest OpenSAMM presentation done as project talk: https://www.owasp.org/images/4/47/OpenSAMM_-_OWASP_USA_2014_-_Seba-Pravir.pptx

Resources from the wiki/opensamm.org website / mailing list will all be consolidated online in https://www.owasp.org/index.php/Category:Software_Assurance_Maturity_Model#tab=Tools__26_Templates

The Quick Start draft is created and can be commented on online:

https://docs.google.com/document/d/1WNCcoYg1-PYli5DNQZKLxwzibmwpNawacloH-8ZAlUc/edit?usp=sharing

Metrics:

Some overall SAMM score calculation options were discussed, with weighing the 4 business functions (possibly slider based).

With the latest SAMM-BSIMMv5 mapping it should be possible to produce statistics on implemented SAMM activities in different verticals.

Latest mapping by Lius Service is uploaded to the mailing list on http://lists.owasp.org/pipermail/samm/2013-November/000528.html

Operational Enablement:

Request to update the name for security practice "operational enablement" as this title is too "fuzzy" and interpreted in different ways.

Suggestions during the meeting were: "DevOps", Operations, Production Support.

Action decided: start thread on the mailing list to gather input on new name with a timing towards selection of a new name (or keep the existing one) (Seba)

Improvement for next SAMM version: More guidance to add on how to manage/prioritize fixing found vulnerabilities during verification/production phases.

Yan - Experiences and examples were shared on how to implement SAMM on a portfolio of applications, measuring "static/dynamic" risk for applications.

Yan will share a template on this.

Matteo showed how they guide prioritization of SAMM security activities based on estimated effort and expected impact. This nicely complements the prior portfolio view.

Matteo will share the template.

Action: combine the demonstrated templates to one SAMM application portfolio dashboard to guide people on implementation priorities and reporting.

Aaron showed a secure development implementation guideline as used by Lockheed Martin, based on SAMM with extra metrics, resources, tips and tricks. The final document (with a how-to) will be donated to the SAMM project.

Action: Aaron to share final document

David has mapped SAMM on PCI (v2) and Microsoft SDL and will share these mappings with the SAMM projects. Kuai to coordinate the PCI mapping (also started with this).

Jonathan proposed to put focus on how to handle code modification / reverse engineering in hosting environments and mobile apps. During the meeting it was suggested to first create a paper to discuss of this specific topic should be integrated in the SAMM model.

SAMM Version 1.1 priorities are confirmed to be:

1. Add quick start guide
2. Add tools & OWASP resources

3. Add use cases , experience.
4. Revamp SAMM wiki

All SAMM model related changes are to be implemented in SAMM v2.

A full day SAMM summit will be organized in Cambridge (AppSec Europe 2014).

Action points:

1. Use the BSIMM Mapping to create an overview of SAMM activities that are done by organisations? (Seba?)
2. Start thread on the mailing list to gather input on new name to replace “Operational Enablement” with a timing towards selection of a new name (or keep the existing one). (Seba)
3. Share SAMM portfolio view of applications, measuring "static/dynamic" risk for applications. (Yan)
4. Share how to prioritize SAMM security activities based on estimated effort and expected impact. (Matteo)
5. Create a unified SAMM application portfolio dashboard (owner : TBD)
6. Share the secure development implementation guideline as used by Lockheed Martin, based on SAMM with extra metrics, resources, tips and tricks (Aaron)
7. Create / share a PCI v3 mapping on SAMM activities (Kuai / David)
8. Create / share separate paper on how to handle code modification / reverse engineering in hosting environments and mobile apps and propose how this could be integrated in SAMM. (Jonathan)

OWASP O2 DOCUMENTATION SESSION

SUMMIT DESCRIPTION: The objective of this session is to discuss the development of a Book about the O2 Platform Web Automation capabilities. Join us during our initial discussion, and get your ideas heard.

OUTCOMES

During the O2 Session we were looking at the O2 book and we were able to distribute several copies. The initial book can be found at GiHub https://github.com/o2platform/Book_WebAutomation.

We had an interesting conversation about it and the main idea is to continue writing the book and add an introductory chapter about the O2 platform to reduce the learning curve. We also are adding a chapter for the already created applications available at O2 so developers and security consultants can consume them.

For the O2 book we will be working on adding more chapters about how to use the O2 Platform and reducing the learning curve. Basically is to continue developing the book in a way that more developers and security consultants can take advantage of the framework already created. We need to define the outline and then start to write the content. The roadmap here is to define/discuss the outline of the chapters, we defined some sections that are a must to include in the next version of the book.

WRITING AND DOCUMENTATION REVIEW SESSION

SUMMIT DESCRIPTION: OWASP Documentation Projects are a key element in the industry. They are broadly adopted and used. This session aims to review the below documents, and give recommendations on where they can be improved.

Books to be Reviewed:

- OWASP AppSensor Project.
- OWASP Development Guide Project.
- OWASP Code Review Guide Project.
- OWASP Testing Guide Project.
- OWASP Code of Conduct.

During this session, the objectives we will be covering are:

1. Figure out what needs to be done for each project.

2. Assign sections to each participant

3. Finish various sections assigned to you.

4. Consolidate all finished sections.

OUTCOMES

Larry Conklin, the Project Manager, participated during the session which was really good because we had the chance to discuss about the book and the sections that need improvement.

We received feedback about the organization of the content and also about completing the chapter that requires more content. Pretty much the feedback received was about organization. For the Code Review Guide, there are some content that needs to be finished and we are expecting to finished it soon. Larry defined a nice goals to be completed and we are working on them :

I am need for authors to sign up for the following….

1. Manual Review - Pros and Cons (https://www.owasp.org/index.php/CRV2_ManualReviewProsCons)
2. 360 Review: Coupling source code review and Testing / Hybrid Reviews (https://www.owasp.org/index.php/CRV2_360Review)
3. Code Review Approach (https://www.owasp.org/index.php/CRV2_CodeReviewApproach) I am not sure about this subject. It seems to me it would be covered in the above section under Code Review Introduction.

4. Application Threat Modeling (https://www.owasp.org/index.php/CRV2_AppThreatModeling) Update this section. I am going to take this one.

5. Understanding Code layout/Design/Architecture (https://www.owasp.org/index.php/CRV2_CodeLayoutDesignArch)

6. SDLC Integration (https://www.owasp.org/index.php/CRV2_SDLCInt) Update this section

7. Secure Deployment Configuration (https://www.owasp.org/index.php/CRV2_SecDepConfig)

8. Metrics and Code Review (https://www.owasp.org/index.php/CRV2_MetricsCodeRev) Update this section

9. Source and sink reviews (https://www.owasp.org/index.php/CRV2_SourceSinkRev)

10. Code Review Coverage (https://www.owasp.org/index.php/CRV2_CodeRevCoverage) Update this section

11. Risk based approach to Code Review (https://www.owasp.org/index.php/CRV2_RiskBasedApproach) I am not sure about this subject. It seems to me it would be covered in the above section under Coder Review Introduction.

12. Code Review and Compliance (https://www.owasp.org/index.php/CRV2_CodeRevCompliance) Update this section

OWASP PHP SECURITY AND RBAC PROJECTS SESSION

SESSION DESCRIPTION: The aim of this session is to introduce attendees to both projects, and to get them working on project related activities.

OWASP PHP Security Project

1. To demonstrate and introduce the OWASP PHP Security Project, have people contribute to it and have people contribute it to their own projects!

2. The project is developed, we're going to show sample usages and have people try to hack them (which should be impossible). We also introduce the libraries and discuss what future works are needed on the project.

3. The project is really interesting and has a cool aim, and this will help get a lot more people in its community.

OWASP RBAC PROJECT

1. OWASP RBAC is a new cutting-edge technology that can revolutionize the authorization domain. Unfortunately because its rigorous and complex, we haven't been very successful in expanding its usage.

2. Get the people know how awesome this is, and get them use it in their applications. This is a pretty mature project and is one of those things that you don't know exists, but when you do you can't get enough of. We also like to get contributors porting it to other programming languages.

3. We've done 85% of the job. There is a website, API, full code with tests, all we need is people to go ahead and use it, and some people who want to use it in another programming language so that we get the community to port it!

OUTCOMES

The outcome of our sessions were only outreach. We expected more participants and project promotion, but due to limited audience we were unable to achieve that. We planned to have an audience, intrigue them, and get them to support the project by promotion, using the product, coding, and testing. However, we were not really able to accomplish what we set out to accomplish before the summit due to limited participants.

Most of the team working on these projects are students, so we will do a promotion kick-start after the Fall semester. We will start coding and contributing to the project after they are out of school. I want to add a whole new section to project as well. We plan to develop the full roadmap for 2014 after the exams and Rahul's graduation.

ESAPI HACKATHON SESSION

SESSION DESCRIPTION: Take part in building the next generation of the Enterprise Security API. In this hackathon we will focus on building modular security controls that can be plugged in to the brand new ESAPI 3.0 framework allowing developers to quickly and easily integrate the security controls they need into their projects. During the hackathon, the ESAPI leaders will be on-site to get the effort kicked off, join in the coding fun, and to present awards for submitted components on the final day! Join us to leave your mark on one of the most visible OWASP Code Projects in our arsenal, and help make tomorrow's applications more secure!

OUTCOMES

1. What were the outcomes of the Hackathon?

We got two bugs from the ESAPI Google Issues fixed. We received a fix from a Maven pom.xml problem I was on one of the SVN branches (kww-java-html-sanitizer). One person wrote some implementations of the proposed interfaces. We met Kevin Greene from DHS SWAMP project that may be a source of grants. Most importantly, we discussed 3 companies (Akamai, Oracle, and LivePerson) about dedicating some of their developer time to ESAPI.

2. Did you accomplish what you set out to accomplish before the summit?

Well, I was hoping that more coding would have been accomplished there, but meeting Kevin Greene, and discussing companies that could dedicate some of their developers to the project more than makes up for it if those people follow through. I had hoped for more submissions of controls for new ESAPI, but I think that we got the word out, sparked a bunch of interest and it was extremely well received.

3. What is there left to do?

We need to finish up the proposed interfaces for ESAPI 3.0. Chris said he will try to get those finished by year end 2013. Additionally, to summarize, some of the most important pieces are:

a) Move from Google Code to GitHub

b) Stand up new esapi.org website

c) Work on CloudBees integration

d) Solidify ESAPI 3.0 interfaces before end of year.

e) T-Shirts (I have good contacts for this and some great artists already working on the full design)

f) Sync up on ESAPI Book Status

g) Schedule and plan next years (Q2) and (AppSecUSA) Hackathons

ZAP HACKATHON SESSION

SESSION DESCRIPTION: This session is a chance for people to learn how to work on ZAP from the ZAP Project Leader. ZAP is a community project, and as such participation is actively encouraged. Simon will explain the numerous ways in which individuals and companies can contribute to ZAP. He will also explain how the code is structured and explain how any part of the project can be changed. Working on ZAP is a great way to learn more about web application security.

Being able to change the code means that you can add and change any features you want, either just for you own benefit or to contribute back to the community. There will be time set aside for hacking ZAP, with Simon on hand to answer any questions and give any guidance required. This is a great opportunity to be part of the fastest growing and most active OWASP project.

During this session, Simon will:

- Explain how people can contribute to ZAP.
- Demonstrate how to set up a ZAP development environment.
- Explain ZAP code structure.
- Show people how to code scripts, active/passive scan rules, add-ons, core changes and improve the docs and localization.
- Let people hack the ZAP code and docs with full support and guidance.

Please note that if you want to work on ZAP source code (including add-ons) then you should set up a ZAP development environment prior to attending this session.

You will need to download and install Eclipse and import the main ZAP project as well as the ZAP extension projects - for more details see http://code.google.com/p/zaproxy/wiki/Building

You will not need to set up a development environment if you just plan to work on scripts, documentation or translation.

OUTCOMES

The hackathon ended up being more of a training event than a session for enhancing ZAP. My goals were fairly flexible. I was primarily interested in getting a dozen or so people along who seemed to be very happy with how it went. Since I was able to do that it means that I'm happy with the outcome. For the hackathon, there is nothing left to do; however, for ZAP, there are always more things to do. I do not have plans for future work related to a ZAP Hackathon.

OWASP APPSENSOR 2.0 HACKATHON

SUMMIT DESCRIPTION: Take part in building the next generation of AppSensor. In this hackathon we will focus on building the code for AppSensor 2.0, which will involve moving to a services (both REST and SOAP) model for event detection and response. During the hackathon, the AppSensor development leaders will be designing and coding side-by-side with you. Come join us and help make the AppSensor idea available to all!

OUTCOMES

1. What were the outcomes of the Sessions?

- Reviewed documentation for V2 of the book and gave initial feedback.
- Met with team members in person and discussed V2 book timeline and goals
- Presented initial V2 design/code and got feedback from internal team and session visitors
- Met with various folks new to OWASP and presented AppSensor along with other projects based on their needs

By the way, Dennis, could you send me an e-copy of the new doc - I shared the paper copy with someone at the conference who was interested and didn't get it back. I want to give you better feedback over the intro section in particular.

2. Did you accomplish what you set out to accomplish before the summit?

Yes. Goal for me was to review V2 book intro and discuss V2 design / code

3. What is there left to do?

For me:
- Send more detailed feedback on V2 book intro section to Dennis / Colin
- Complete V2 code and release - progress is happening! https://github.com/jtmelton/appsensor

4. Roadmap for accomplishing what is left to do.

- For V2 book review, when Dennis gets me the e-copy of the book, I'll try to get detailed feedback to him within a week or so - definitely by end of year.
- For V2 code, I'm looking at a release in Q1 2014. Things are going well at the moment, so we may get some code from other folks as well. Looks like we have 1 or maybe 2 people who are actively jumping in, so I'm hopeful.

OWASP EDUCATION INITIATIVES SESSION

TRAINING DEVELOPMENT SUMMIT DESCRIPTION: Training is an important part of OWASP's mission as it helps not only in increasing the awareness around application security but also in actually improving the security of applications. In the past, we have tried several training models (e.g. Training Days, Tours, etc.) and dozens of ideas have been put on the table. Nevertheless, we are still missing a viable training model that will be easy to reproduce and will provide added value to attendees.

During the Project Summit, we will discuss various training models, and the experience we have gained over the past years in order to build a model that will be subsequently used to train developers and anyone involved in securing applications.

ACADEMIES DEVELOPMENT SUMMIT DESCRIPTION: The OWASP Academies program aims to bring together academic institutions from all over the world in order to collaborate towards increasing awareness on application security. The OWASP Academy Portal is the actual deliverable of this process: a portal that will provide various types of content (presentations, labs, etc.) to students and faculty who wish to learn or teach application security.

During the Projects Summit we intend to kick start the Academy Portal, complete the initial design and add some actual content. The OWASP Academy Portal will then serve as the meeting point for application security in academia. Moreover, the Projects Summit will serve as a meeting point for several members of the academic community and a unique opportunity to exchange ideas and experience.

OUTCOMES

The OWASP Educational Initiatives have suffered from a stall for development. During the project summit, we came together to solve the two main problems that cause this in our opinion:

- splintering into many projects / initiative

1. Some of the educational projects / initiatives even competed for volunteers and visibility.
2. Goals and purpose of each educational project / initiative was not defined with clear boundaries.
3. Some of the educational projects / initiatives suffered form lack of visibility, being overrun (not to say ignored) by "yet another great idea.

- Unreachable targets for each project / initiative

1. The project targets where set high, to high, what seemed to cause a stall in progress as the targets where unreachable.

During the project summit at the AppSec-US 2013, the following was achieved. The volunteers who came together for the Education Project during the summit agreed on:

- One major project, leading the sub projects that are mainly supporting or implementing projects / initiatives.

1. The OWASP EDU project is created and nominated to be the leading OWASP educational initiative.

2. Smaller targets, as reachable first target of the EDU project, the creation of "Instructor Lead Courses" has been defined.
3. During the Summit, we defined the setup / lay-out of what we understand as "Instructor Lead Course”.
    - We defined the context and building blocks of a "Instructor Lead Course”.
    - We defined first to implement courses.

OWASP Instructor Lead Course outcome. Using a mind map tool, we defined the framework and some implementation ideas for the ILC (instructor Lead Courses):

- Mission

1. Produce Training Material.
2. The material can be delivered in a consistent manner by an experienced professional.
3. Delivery mechanism agnostic.

- Available Resources
- Framework
- Mechanisms

1. Lecture
2. Demo
    - Mutillidae (vulns)
    - WebGoat (coding)
    - ZAPBodgeIT (coding)
3. Hands-on Labs
    - attack
    - coding

- Precompiled courses

1. OWASP Top10 for development teams
2. OWASP Secure Development
3. Testing security in software

- Topics

1. OWASP TopTen
    - SQLi
    - Broken Authentication
    - XSS
    - Insecure Direct Object Reference
    - Security Misconfiguration
    - Sensitive data exposure
        1. Information leakage
        2. Improper Error Handling
        3. Insecure Crypto Storage
        4. Insufficient Transport Layer Protection
    - Missing function level Access Control
    - CSRF
    - Known Vulnerabilities

- Unvalidated redirects and forwards
- Malicious file execution

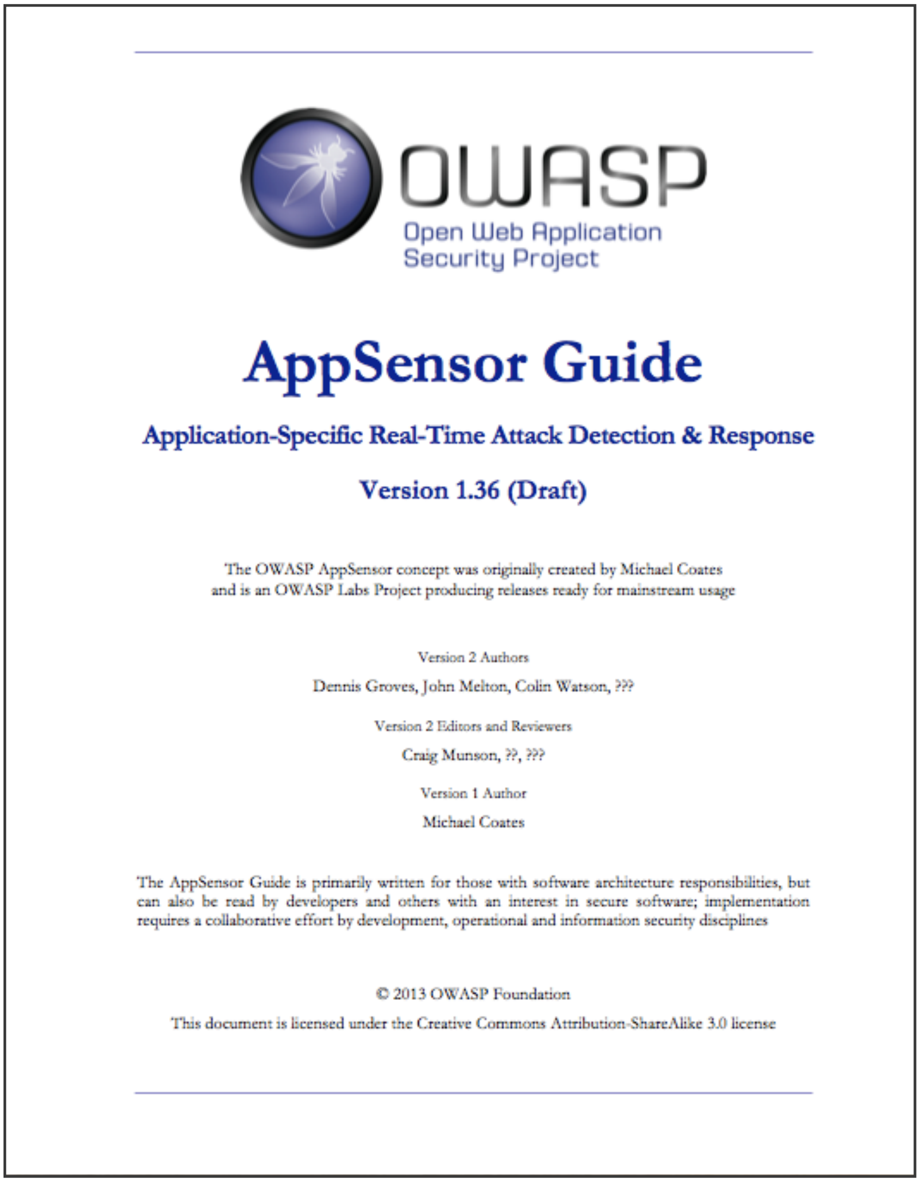
2. Secure Development
    - Secure Design Principles
        1. least privileges
        2. defense in depth
        3. secure by default
        4. security / obscurity
        5. fail securely
        6. keeping it simple
        7. default deny
        8. complete mediation
        9. minimize attack surface
        10. Trust no-one
        11. proportional acceptable to risk
    - Secure Development principles
        1. input validation
        2. output encoding
        3. authentication & autorisation
        4. session management
        5. error handling
        6. logging and auditing
    - Secure Testing
    - SDLC
3. Passwords
4. Basic Risk Classification
    - How to tell your manager he can be hacked?

10 PRODUCTS: BOOKS PRODUCED FOR THE SUMMIT

PRODUCTS: BOOKS PRODUCED FOR THE SUMMIT

Below you can find a summary of the books that were produced for the 2013 Project Summit. The books produced were in various stages of development as the aim was to showcase the work completed thus far by our Project Leaders and contributors. You can find a link to the full copies of the books produced by clicking on the URL under the respective book title.

OWASP APPSENSOR PROJECT



OWASP
Open Web Application
Security Project

AppSensor Guide

Application-Specific Real-Time Attack Detection & Response

Version 1.36 (Draft)

The OWASP AppSensor concept was originally created by Michael Coates
and is an OWASP Labs Project producing releases ready for mainstream usage

Version 2 Authors
Dennis Groves, John Melton, Colin Watson, ???

Version 2 Editors and Reviewers
Craig Munson, ??, ???

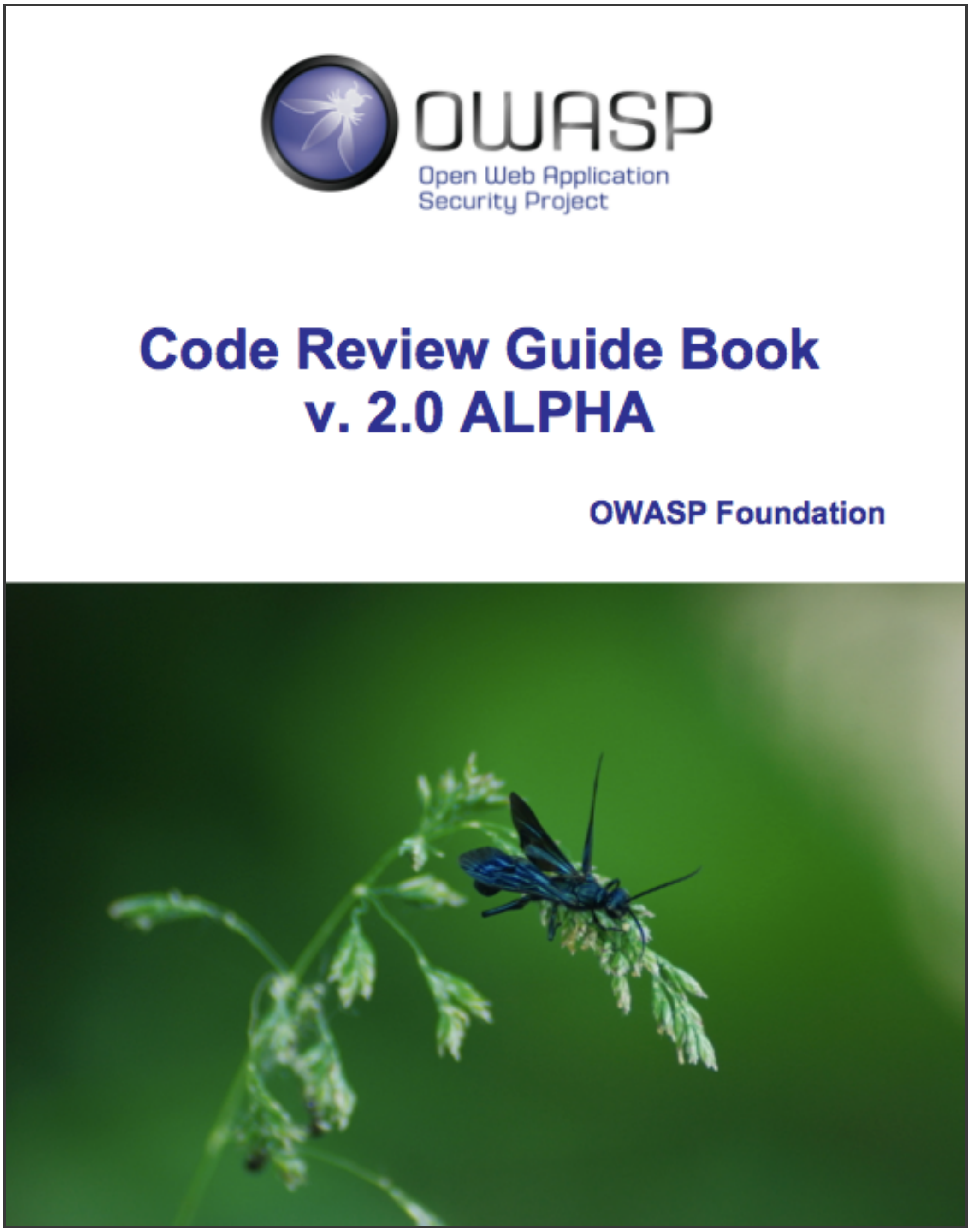
Version 1 Author
Michael Coates

The AppSensor Guide is primarily written for those with software architecture responsibilities, but can also be read by developers and others with an interest in secure software; implementation requires a collaborative effort by development, operational and information security disciplines

© 2013 OWASP Foundation
This document is licensed under the Creative Commons Attribution-ShareAlike 3.0 license

https://www.owasp.org/images/2/20/Owasp-appsensor2-1v36-cc.pdf

OWASP CODE REVIEW GUIDE PROJECT: V2.0 PRE-ALPHA



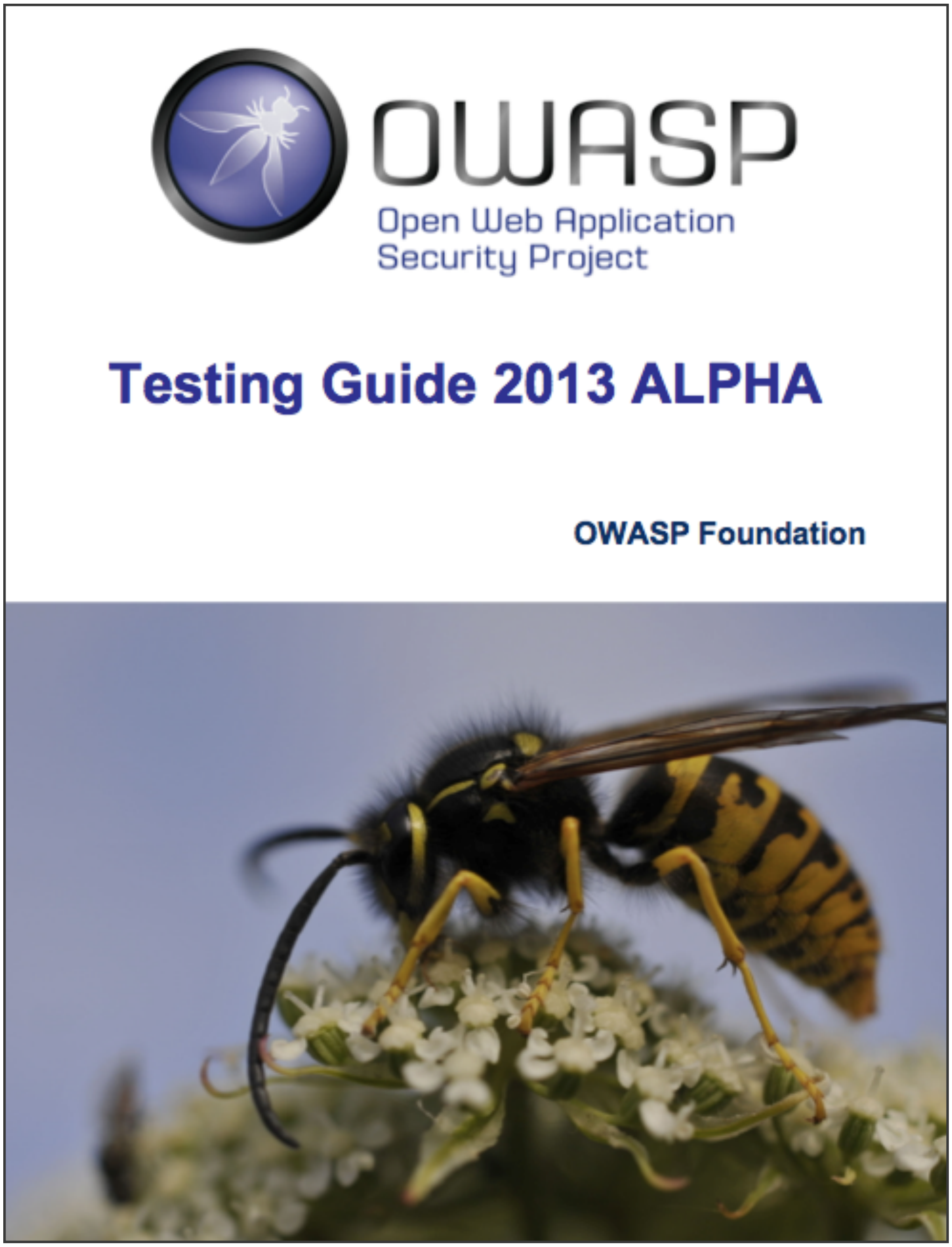
OWASP
Open Web Application
Security Project

Code Review Guide Book
v. 2.0 ALPHA

OWASP Foundation

https://www.owasp.org/images/f/fa/Code_Review_Guide_Pre-AlphaV2_%281%29.pdf

OWASP TESTING GUIDE PROJECT: ALPHA



OWASP

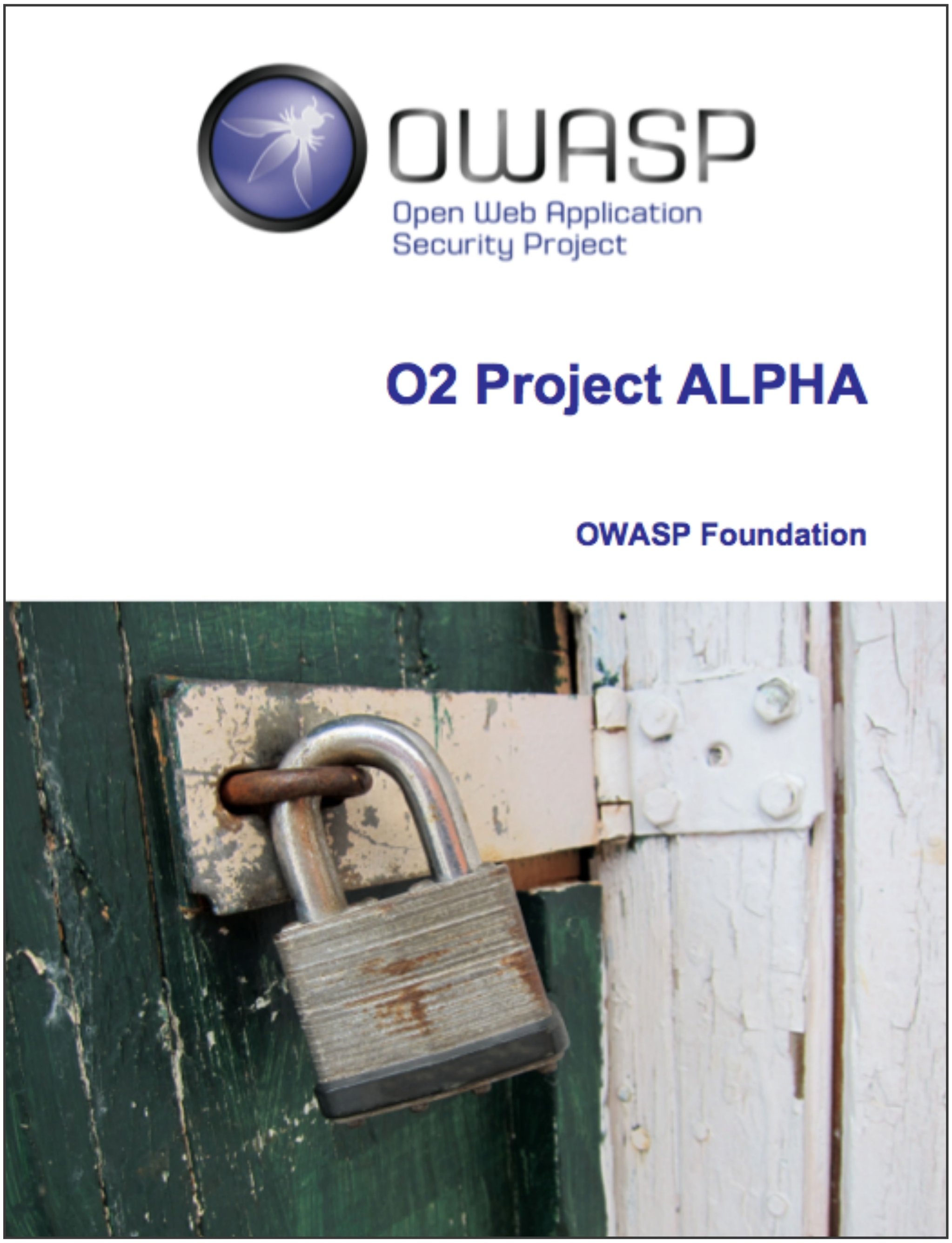
Open Web Application Security Project

Testing Guide 2013 ALPHA

OWASP Foundation

https://www.owasp.org/images/9/91/TestingGuide.pdf

OWASP O2 HANDBOOK: ALPHA



OWASP

Open Web Application Security Project

O2 Project ALPHA

OWASP Foundation

https://www.owasp.org/images/b/be/O2Documentation.pdf

11 APPENDIX

APPENDIX

In this section, you will find various reports, tables, slides, forms, and other materials produced for and at the summit. You will also find historical summit information such as previous summit budgets and funds spent. Finally, you will find a list of primary summit contributors with a short bio for each individual. Please contact Samantha Groves (Samantha.Groves@owasp.org) if you have any questions about anything in the report or the Appendix section specifically.

2008 SUMMIT FINANCIAL DETAILS

CATEGORY	COST	NOTES
Travel - Diplomata Tours	$54,325.84	Includes flights for 65 attendees
Other Travel Costs	$12,563.72	Flights and other expenses submitted for reimbursement
Grande Real Santa Eulalia Hotel	$58,018.12	Includes accommodations for 74 and food for 76 attendees
AV Expenses - Eurologistix	$5,222.61	
Advertising - Generator	$1,261.50	
Summit Personnel	$960.00	
FedEx	$3,080.37	
Miscellaneous	$6,337.91	
Banking & Currency Corrections	$498.90	
SUBTOTAL	$142,268.97	
Income - Reimbursements/ Donations	-$6,290.04	
TOTAL	$135,978.93	

Almost all OWASP participants (OWASP Project Leaders, Reviewers, and Contributors) at the 2008. Summit had their trip sponsored, at least in part, by the OWASP Foundation. To be considered a relevant. OWASP participant, and, consequently, to qualify to have the Summit attendance expenses partially paid, attendees needed to fall into of the following categories:

1. OWASP Summer of Code 2008 project leaders & reviewers,

2. OWASP Summer of Code 2008 special project contributors,

3. OWASP Spring of Code 2007 project leaders & reviewers,

4. OWASP Autumn of Code 2006 project leaders & reviewers,

5. Active Project Leaders (not currently participating on SoC 08),

6. Active Chapter Leaders,

7. Member with significant past OWASP Contribution.

A list of OWASP sponsored attendees to the 2008 Summit as well as the reason for the sponsorship (i.e. the category from the above list that they fall into) can be found at: http://spreadsheets.google.com/pub?key=pAX6n7m2zaTVLrPtR07riBA

Additionally, the following rules were established by the 2008 Summit planning committee to clarify which expenses and how much would be paid for by the OWASP Foundation:

1. With exceptions noted below, all accommodation and meals during the four-day event will be paid.

2. As we are still seeking out financial sponsorship support, until further notice, none of the dinners will be paid.

3. The meals consist of a pre-negotiated menu and only this menu will be paid.

4. The accommodation will consist in a place in a shared T1 (3 people) or T2 (5 people) apartment. Therefore, even though one can choose an individual room, OWASP will pay only for the cost associated with a shared stay. At the cost of +/- 60 Euros per night, there is the option to stay in an individual room (or in a double-room, in the cases where the partner - wife / husband - is also present).

5. Please note that the nights of 3 and 7 of Nov will be included in the paid accommodation for those individuals attending the whole event.

6. Regarding the flight expenses, OWASP will pay a maximum of 1000 US dollars for all non-European attendees and 600 US dollars for the European ones.

Please Note: The 2008 Summit financial details information was taken from the 2011 Project Summit Report prepared by Sarah Baso.

2011 SUMMIT FINANCIAL DETAILS

EXPENSES: SUMMIT VENUE

CATEGORY	COST	NOTES
Alentejo Room	$2,502.00	450€/day x 4 days = 1,800€
Campo Real 1	$3,614.00	650€/day x 4 days = 2,600€
Campo Real 2, 3 & 4	$3,614.00	650€/day x 4 days = 2,600€
Catering Supplement - dinners served in villas	$1,056.40	1.50€/person/day = 760€
Catering Supplement	$354.45	85€/day x 3 days = 255€
ASDL	$1,997.75	€1,437.23
Printer	$2,085.00	€1,500
Suite	$1,390.00	200€day x 5 days = 1,000€
AV Equipment	$16,853.75	€12,125
Drink Tickets	$2,636.83	7€/drink x 271 tickets = 1,897€
Cocktail Hour	$708.90	€510
Nuno Marco	$7,051.88	5,066.10€ (Optimus, Projector, PCs, Labor)
Food & Beverage Extras	$7,717.38	For Summit Team/Early Arrival 5,552.07€
CampoReal Total	$51,572.34	€37,107.40

EXPENSES: SUMMIT GIVEAWAYS

CATEGORY	COST	NOTES
Podcast CD & Book	$1,800.00	
Attendee Misc.	$5,254.17	Stickers, Passports & Compasses

EXPENSES: SUMMIT EQUIPMENT & SERVICES

CATEGORY	COST	NOTES
Operational Expenses	$1,384.22	Disposable cell phones, SIM cards, Netgear hub, baggage fees, ipad
OWASP Band Equipment Rental	$1,500	€1,100
Apparel - LX Studios & Polo Shirts	$2,858.96	

EXPENSES: SUMMIT EQUIPMENT & SERVICES

CATEGORY	COST	NOTES
Marketing – Hackers News Network	$250.00	
PR - Generator Beyond the Brand	$2,760.00	€2,000
SAPO (Additional Internet Connectivity)	$2,175.00	€1,577
Baltazar Martins (Summit Design/ Marketing)	$3,210.00	€2,327

EXPENSES: SUMMIT SUPPORT STAFF

CATEGORY	COST	NOTES
Sarah Baso (Summit Logistical Support)	$4000	
Marta Pergorelli (Brazilian Delegation)	$5,000	
Sarah Cruz (Design)	$2,100	
Sandra Paiva (Working Session Editor)	$2,000	
Deb Brewer (Summit – On-site Event Planner)	$3,915.77	

EXPENSES: TOTALS

Summit Expenses Subtotal	$89.780.46	
Summit Travel Subtotal	$152,855.58	http://sl.owasp.org/summit2011_travelcosts
TOTAL EXPENSES	$242,636.04	

INCOME: OWASP BUDGET ALLOCATION - BOARD APPROVED

CATEGORY	COST	NOTES
OWASP Funds for Operational Expenses	$50,000	$50,000 allocated by Board – Aug 2010
Summit Attendee Travel Budget	$50,000	$50,000 approved by Board in Dec 2010
$15,000 for Operational Costs and $25,000 for Summit Travel Expenses	$40,000	Approved by Board 23-Jan-2011

INCOME: INTERNAL SPONSORSHIPS

CATEGORY	COST	NOTES
Local Chapter Sponsorships	$44,095.65	Direct chapter donations & OSTR funds
Project Sponsorships	$2,000.00	Funds donated from project budgets

INCOME: EXTERNAL SPONSORSHIPS

CATEGORY	COST	NOTES
Wiki Donations	$1,310.11	
Praetorian	$1,942.14	$5000 Corporate membership with 40% ($2000 less fees) allocated to sponsor summit attendee
Security Innovation	$1,942.14	$5000 Corporate membership with 40% ($2000 less fees) allocated to sponsor summit attendee
(ISC)2	$1,947.09	Lunch Sponsorship ($2,000 less fees)
Trustwave	$1,975.00	Wireless Sponsorship ($2,000 less fees)

INCOME: ACCOMMODATION CREDIT

CATEGORY	COST	NOTES
Accommodation Credit	$8,860.36	Credit from Diplomata Tours

EXPENSES: TOTALS

Subtotal Internal Income	$186,095.65	
Subtotal External Income	$16,029.75	
TOTAL INCOME	**$202,125.40**	
PROFIT/LOSS	**-$40,510.64**	Total amount “over budget”
Total amount Spent by OWASP	**$226,606.29**	

The above details on the 2011 Summit Expenses and Income can be found at: http://sl.owasp.org/summit2011_finalbudget

More details on Summit Travel and Accommodation costs, broken down by attendee can be found at: http://sl.owasp.org/summit2011_travelcosts

Please Note: The 2011 Summit financial details information was taken from the 2011 Project Summit Report prepared by Sarah Baso.

MARKETING MATERIALS: ACADEMIES AND TRAINING INVITATION TO THE COMMUNITY

Education and training is an important part of OWASP's mission as it helps not only in increasing the awareness around application security but also in actually improving the security of applications.

The OWASP Academies program aims to bring together academic institutions from all over the world in order to collaborate towards increasing awareness on application security. The OWASP Academy Portal is the actual deliverable of this process: a portal that will provide various types of content (presentations, labs, etc.) to students and faculty who wish to learn or teach application security.

We would like to invite you to join us in the OWASP 2013 Projects Summit which is organized during OWASP AppSec USA 2013, in New York City from November 18th to November 21st.

During the Projects Summit we intend to kick start the Academy Portal, complete the initial design and add some actual content. The OWASP Academy Portal will then serve as the meeting point for application security in academia. Moreover, we will discuss various training models and the experience we have gained over the past years in order to build a model that will be subsequently used to train developers and anyone involved in securing applications.

The OWASP 2013 Projects Summit will serve as a meeting point for several members of the educational and academic community and a unique opportunity to network, collaborate, exchange ideas and experience.
The OWASP Project Summit is a smaller version of the much larger OWASP Summits. This year’s summit aims to give our project leaders the opportunity to have attendees sit down and work on project related activities during AppSec USA. It is an excellent opportunity to engage with active OWASP Project Leaders, and it gives project leaders the chance to move forward on their project milestones while meeting new potential volunteers that can assist with future milestones.

To participate in the Projects Summit Register for FREE for the “Expo and Career Fair Only Pass” and use the following discount code at checkout: NYC13_SUMMIT.

Looking forward to working with you during the OWASP 2013 Projects Summit,

Dr. Kostas Papapanagiotou
Martin Knobloch

MARKETING MATERIAL: OWASP REVIEW CRITERIA AND 2013 PROJECT ASSESSMENTS

I am happy to report that the Technical Project Advisors team has completed the final version of the our project assessment criteria. This criteria grades our project quality based on the overall project health and the overall quality of the product each project is producing. The aim of developing this criteria was to help guide OWASP Project Leaders toward the successful completion and development of their overall project deliverable. Moreover, this criteria will be used to establish the appropriate stage the reviewed project is in, basing the decision on overall project health and product quality. I encourage all Project Leaders to please take a bit of time and review the 2013 Project Assessment Criteria.

2013 PROJECT SUMMIT REVIEWS

As many of you know, attendees will be able to participate in the review of the entire inventory of OWASP Projects using the new assessment criteria developed by our team of Technical Project Advisors, during the OWASP Projects Review working session at AppSec USA. The aim of this session is to establish a more accurate representation of OWASP project health and product quality.

Leaders are encouraged to review the 2013 Project Assessment Criteria, and make certain that their project fulfills all of the guidelines outlined in the criteria. Please note, that it is not mandatory to work towards fulfilling all of the criteria for this round of reviews. However, passing the assessment is a requirement if you wish to graduate from an Incubator to a Lab and Lab to a Flagship Project. We do encourage all current Lab and Flagship project leaders to ensure that they are in alignment with the new 2013 project assessment criteria.

NEW OWASP PROJECT WIKI TEMPLATES

The new project wiki templates were created to make adding content to a project wiki page, a much easier task for Leaders. A big thank you to Colin Watson for creating these for us.
We are encouraging all Leaders to switch over to these templates starting in 2014. Please note that Leaders are not required to use these templates, but the use of this wiki template is a requirement for graduation for Incubator projects starting in 2014. Below you will see an example of what we would like to see from an OWASP Project in regard to their wiki content and links.

If you have any questions about any of the topics above, or if you want to be involved, please reach out to me at Samantha.Groves@owasp.org. See you all at the Project Summit in New York City!

MARKETING MATERIAL: 2013 PROJECT SUMMIT IS ONLY 2 WEEKS AWAY: SIGN UP NOW!

The Project Summit taking place in tandem with this year's AppSec USA in New York City, is only two weeks away! Unfortunately, we were not able to raise enough funds to facilitate remote participation for the 2013 Project Summit. It is certainly an aspect of our summits that we find incredibly important, and we will work hard to make sure remote participation is an option our contributors have in 2014. As a result, we recommend attending the summit in person, and signing up for the sessions you are interested in. We now have 18 sessions scheduled. The list includes:

Monday: Nov 18th

1. OWASP Project Review Session
2. ESAPI Hackathon Session
3. OWASP Media Project
4. OWASP PHP Security and RBAC Projects: An Introduction
5. AppSensor 2.0 Hackathon
6. Bug Bounty Hack Session

Tuesday: Nov. 19th

1. OWASP Training Development Session
2. OWASP Academies Development Session
3. Mobile Security Session
4. ESAPI Hackathon Session
5. Bug Bounty Hack Session

Wednesday: Nov. 20th

1. Writing and Documentation Review Session
2. ESAPI Hackathon Session
3. Bug Bounty Hack Session

Thursday: Nov. 21st

1. ZAP Hackathon Session
2. Open SAMM Session
3. ESAPI Hackathon Session
4. Bug Bounty Hack Session

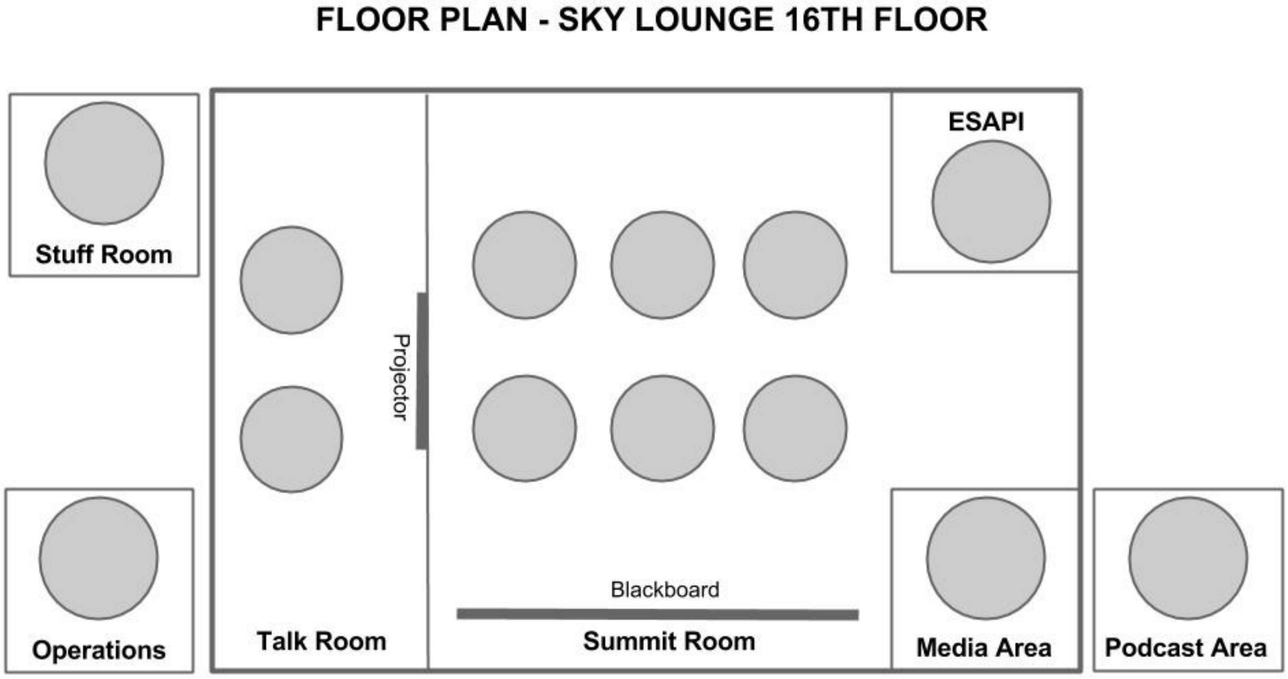
For more information on the 2013 Project Summit, please contact Samantha Groves (Samantha.Groves@owasp.org), or visit the Project Summit wiki page.

MARKETING MATERIAL: INDIVIDUAL SUMMIT TWEETS BY KAIT DISNEY-LEUGERS

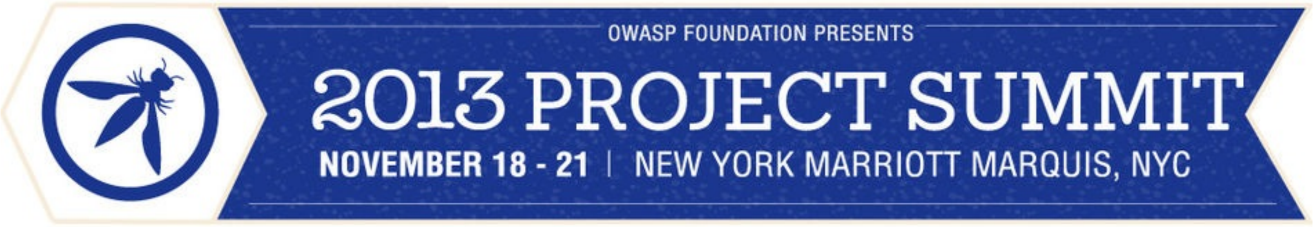
1. Those OWASP Projects are not going to review themselves, maybe you should help. https://www.owasp.org/index.php/Projects_Summit_2013/Working_Sessions/003
2. The ESAPI Hackathon is going on throughout the four days of the Projects Summit. Sign up to participate here: https://www.owasp.org/index.php/Projects_Summit_2013/Working_Sessions/001
3. A 'live-hacking' event in a controlled environment. Get your hack on at the Bug Bounty Session, sign up here: https://www.owasp.org/index.php/Projects_Summit_2013/Working_Sessions/0013
4. Help to define the standards and guidelines on training material. Sign up for the Training Development Session here: https://www.owasp.org/index.php/Projects_Summit_2013/Working_Sessions/008
5. OWASP is going back to school to get the youth involved. Help create the guidelines for the Academies Initiatives:https://www.owasp.org/index.php/Projects_Summit_2013/Working_Sessions/009
6. Build and maintain secure mobile applications at the Mobile Security Session. Sign up here: https://www.owasp.org/index.php/Projects_Summit_2013/Working_Sessions/0012
7. Release your inner wordsmith at the Project Guide Review Writing Session. https://www.owasp.org/index.php/Projects_Summit_2013/Working_Sessions/005
8. Wrap up your week at the OWASP Projects Summit by participating in the ZAP Hackathon. Sign up here: https://www.owasp.org/index.php/Projects_Summit_2013/Working_Sessions/007

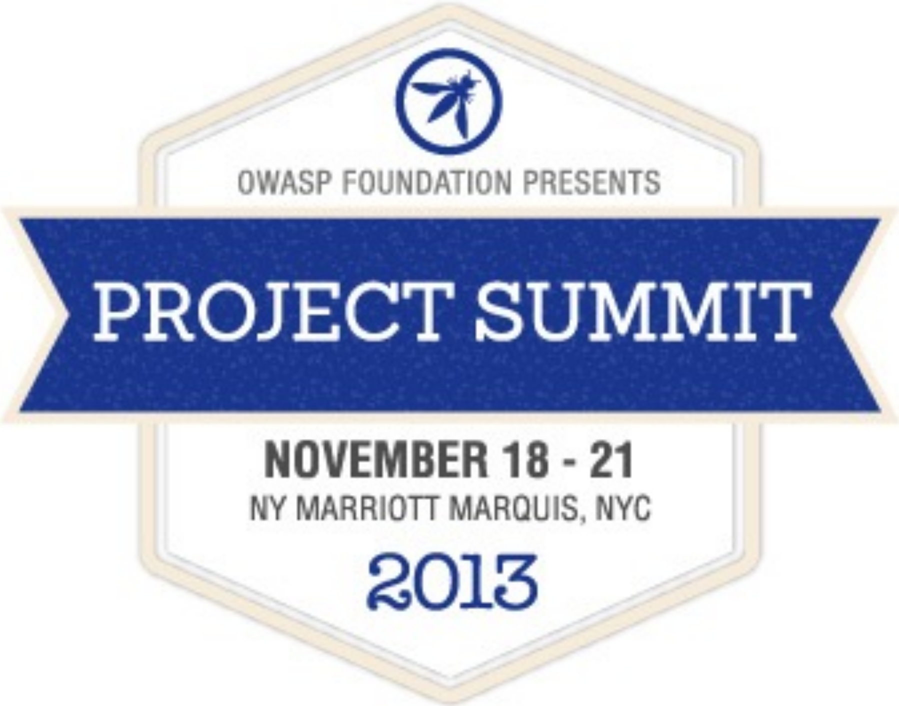
2013 SUMMIT: SKY LOUNGE FLOOR PLAN

The floor plan below was put together by Fabio Cerullo after the planning team were able to assess the space in person. The space allocation was organized based on the space needs of each session Leader. Mark Miller had a suite to himself for filming in the Podcast area, and the talk room area was created by using a room divider and a projector. The ESAPI and Media areas were separated out as they required more space for more expected contributors. The Media area was given a projector and media equipment, as well. Overall, the spaces worked well, but it is important that the summit area not be shared with any other conference happenings if taking place with a conference. Sharing the space simply did not work, and it caused many distractions for contributors.



SUMMIT LOGOS AND IMAGES


OWASP FOUNDATION PRESENTS
2013 PROJECT SUMMIT
NOVEMBER 18 - 21 | NEW YORK MARRIOTT MARQUIS, NYC



USPA
sunglass hut

OWASP Application Security
Codes of Conduct
Aggregated Booklet
Version 1.17 (27th March 2013)

PLANNING TEAM, WORKING SESSION LEADERS, AND KEY SUMMIT VOLUNTEERS

PRIMARY PLANNING TEAM

SAMANTHA GROVES

Samantha Groves is the Project Manager at OWASP. Samantha has led many projects in her career, some of which include website development, brand development, sustainability and socio-behavioral research projects, competitor analysis, event organization and management, volunteer engagement projects, staff recruitment and training, and marketing department organization and strategy implementation projects for a variety of commercial and not-for-profit organizations. She now works to help our OWASP Project leaders, aiding them in starting and running their OWASP based projects.

KAIT DISNEY-LEUGERS

Kait was the Grants and Fundraising Intern for the fall of 2013. Kait received her B.A. in history from Ohio University and plans to pursue her masters in technical writing and communication sometime next year. She has previously worked with non-profits groups and museums doing fundraising and research. She operates out of the Bay Area/Silicon Valley and has been indirectly involved with OWASP since 2012.

WORKING SESSION LEADERS

JOHANNA CURIEL

Johanna is one of OWASPs Technical Project Advisors responsible for creating our new project assessment criteria and grading process. Johanna has mainly worked in the area of C# and ASP.NET development, Testing and Quality Control. She is an experienced developer and understands different types of programming languages such as Java and PHP and different types of scripting languages. Johanna has ample experience in Microsoft Technologies and Security Engineering.

CHUCK COOPER

Chuck has been developing and/or managing several award winning software products for over 25 years including working on Great Plains Property Management, Borland Paradox, Acuity Projects, CA Clarity, and Paylocity Web Pay. For the past 8 years he has been working as the CIO at Paylocity, and recently he earned his CISSP certification and became the CISO and Sr. VP of Enterprise Architecture. Now he can focus primarily on network and application security for Paylocity's Software-as-a-Service Payroll, HR, Time & Labor Management, and Online Benefits products.

JONATHAN MARCIL

As the chapter leader of OWASP Montreal, Jonathan manages most of the events and do the online community management. He is filling up the 2013 chapter's agenda with continuous events and bring new activities than just presentations the way we are used to: Workshops on OWASP projects, community mash-up with other programming related user groups, doing talks in various venues and online events using YouTube and Google Hangouts. He is also Advisor of the security track of ConFoo, a Web techno conference held each year in Montreal that gathers over 600 Web developers and enthusiasts.

ABBAS NADERI

Information security, cryptography, computer science, and all sorts of geeky stuff make up my life. I spend considerable time in OWASP, and deem myself one of the people who is pushing OWASP forward in every direction. I am also currently chapter leader of Iran in OWASP and have participated in OWASP Projects for more than 5 years. I'm leading OWASP PHP Security Project, OWASP RBAC Project, and a handful of others and have plans for a lot more to come! On top of that I take part in other open source communities, trying to improve the security aspects of every software.

RAHUL CHAUDHARY

I like security and algorithms. I like the codes and logic combined to form something that makes your daily work so easy. Just think of all the money in the banks...they are just numbers in computers dancing around in super speed, all numbers, all algorithms....and they need to be SAFE!

DINIS CRUZ

Dinis Cruz is a Developer and Application Security Engineer focused on how to develop secure applications. A key drive is on 'Automating Application Security Knowledge and Workflows' which is the main concept behind the OWASP O2 Platform and Security Innovation's TeamMentor (Dinis is the main developer and architect of both Applications). Current day job is with Security Innovation where Dinis tries to promote openness, quality and sharing as part a core tenet of TeamMentor's application development environment. After many years (and multiple roles) Dinis is still very active at OWASP, currently leading the O2 Platform project and helping out other projects and initiatives. Additionally, Dinis provided essential mentorship, and was a key contributor in the pre-planning and execution of the 2013 Summit.

MICHAEL HIDALGO

Software Developer Engineer based on San José, Costa Rica. With more than 6 years of experience building financial applications and with his high sense of responsibility and quality, Michael always work hard to do things better. Currently Michael works as a Software Developer Engineer for one of the best Application Security company in the market. He also leads the OWASP Chapter in Costa Rica and he is always writing about software, testing, quality and application security.

JOHN MELTON

John specializes in the design, development and security analysis of secure J2EE web-based applications.

Goal: Help other J2EE developers grow in knowledge with regards to building secure applications.

KEVIN WALL

Kevin is an experienced Application Security developer, and he is the OWASP ESAPI project co-leader / committer.

DENNIS GROVES

Dennis Groves's work focuses on a multidisciplinary approach to risk management. He is particularly interested in risk, randomness, and uncertainty. He holds an MSc in Information Security from the University of Royal Holloway where his thesis received a distinction. He is currently a UK expert for the UK mirror of ISO subcommittee 27, IT Security Techniques, working group 4, Security Controls and Services at the British Standards Institute. He is most well known for co-founding OWASP. His contributions to OWASP include the ‘OWASP Guide (v1)’ downloaded over 2 million times; now a reference document in the PCI DSS standard, and the de-facto standard for securing web applications. He is a thought leader in the web application security space, where he has spent the last decade of his career. Dennis Groves has been an Security Architect, Ethical Hacker, Web Application Security Consultant, IT Security Consultant, System Administrator, Network Administrator, and a Software Engineer. He has taught various courses on information security and is best known for his ability to bring fresh insight to difficult security problems.

CHRIS SCHMIDT

Chris is currently the Project Leader for the OWASP ESAPI Projects and also served on the OWASP Global Projects Committee. He has been involved with OWASP for 6 years and has spoken at many OWASP events about the benefits of the Enterprise Security API as well as participated in Leadership discussions amongst the organization. During the day, Chris is Chief Architect for Contrast Security where he has been since fall 2010. Prior to joining the team at Contrast Security he spent 5 years as 'Black Ops Beef' for ServiceMagic Inc with the official title of Software Engineer. Before getting involved in software professionally, Chris worked in hardware as a Senior Field Service Engineer providing hardware and software support for PC’s, Servers, Midrange Systems and Peripherals for 9 years.

KONSTANTINOS PAPANAGIOTOU

Dr Konstantinos Papapanagiotou has more than 10 years of experience in the field of Information Security both as a corporate consultant and as a researcher. Currently he is leading the information security services practice at OTE, the largest telco in Greece. In the past he has provided information security services to large organizations in Greece, Cyprus, Balkans and the Middle East. He has been involved with OWASP for several years now, leading the OWASP Greek Chapter and lately the Hackademic Challenges Project. He also organized the OWASP AppSec Research 2012 conference. Konstantinos hold a BSc and PhD from the University of Athens and an MSc in Information Security from Royal Holloway, University of London.

JACK MANNINO

Jack Mannino is a Partner at nVisium, a DC area firm specializing in application security. At nVisium, he helps to ensure that large corporations, government agencies, and software startups have the tools they need to build and maintain successful security initiatives. He is an active Android security researcher/tinkerer, and has a keen interest in identifying security issues and trends on a large scale. Jack is a leader and founder of the OWASP Mobile Security Project. He is the lead developer for the OWASP GoatDroid project, and is the chairman of the OWASP Northern Virginia chapter.

JASON HADDIX

I currently facilitate information security consulting at HP which includes developing test plans for Fortune 100 companies and competing in "bake-offs" against other top tier consulting vendors. My strengths are web, network, and mobile assessments. I write for my own infosec website (www.securityaegis.com) that reviews industry training, interviews security professionals, and provides anecdotal/practical advice related to offensive security. I also write articles for security publications and speak at security conferences whenever possible. I am a semi-regular player on the capture the flag team Shellphish, an academic hacking group based out of the University of California, Santa Barbara.

MARTIN KNOBLOCH

Martin is an independent security consultant and owner of PervaSec (http://www.pervasec.nl). His main working area is (software) security in general, from awareness to implementation. In his daily work, he is responsible for education in application security matters, advise and implementation of application security measures.

Martin got involved in OWASP in 2006. He became a member of the OWASP Netherland Chapter board in 2007. He has contributed to several OWASP projects and is co-organizer of the OWASP BeNeLux-Day conference since 2008. Martin has been chair of the Global Education Committee from 2008 until the ending of the Global Committees.Martin is a frequent speaker at universities, hacker spaces and various conferences.

SIMON BENNETTS

Simon Bennetts has been developing web applications since 1997, and strongly believes that you cannot build secure web applications without knowing how to attack them. He is the OWASP Zed Attack Proxy Project Leader and works for Mozilla as part of the Security Team.

KEY SUMMIT VOLUNTEERS

FABIO CERULLO

Fabio has over 10 years of experience in the information security field gained across a diverse range of industries. As CEO & Founder of Cycubix, he helps customers around the globe by assessing the security of applications developed in-house or by third parties, defining policies and standards, implementing risk management initiatives, as well as providing training on the subject to developers, auditors, executives and security professionals. As a member of the OWASP Foundation, Fabio is part of the Global Education Committee whose mission is to provide training and educational services to businesses, governments and educational institutions on application security, and has been appointed OWASP Ireland Chapter Leader since early 2010. He holds a Msc in Computer Engineering from UCA and has been granted the CISSP & CSSLP certificates by (ISC)2.

LARRY CONKLIN

Larry is the co-project leader of the OWASP Code Review Guide. His current emphasis is in Microsoft .NET technologies including C#, VB.NET, and SQL Server. Recent project experiences include converting legacy VB software to .NET, creating and maintaining operational support web sites to help QuikTrip manage it’s 600+ stores. Larry is currently a Senior Software Developer for QuickTrip.

ANDREW VAN DER STOCK

Andrew is a seasoned web application security specialist and enterprise security architect. He leads the Technical Security Service line at KPMG Australia, performing security architecture, security architecture reviews, coding guidelines, PCI DSS technical remediation, secure code reviews, penetration tests, and developer training. Andrew has worked in the IT industry for over 20 years. Andrew has researched and developed the web application security and architecture fields since 1998, based in Melbourne, Sydney, and the USA for Fortune 50 clients here in Australia, Asia-Pacific, Europe, and the USA.

Andrew currently leads the OWASP Developer Guide 2013, the forthcoming OWASP Proactive Security Controls, and has contributed a significant revision of the Application Security Verification Standard 2.0. He has previously lead the OWASP Top 10 2007 and ESAPI for PHP projects.

ANDREW MULLER

I have a drive to improve the security and efficiency of business processes through innovative solutions to perennial problems. Currently I am developing security management through security automation and redefining the security testing process through work with Standards Australia and OWASP.

MATTEO MEUCCI

Matteo Meucci is the CEO and a cofounder of Minded Security, where he is responsible for strategic direction and business development for the Company. Prior to founding Minded Security, Matteo had several consultancy experiences from BT Global Services, INS, Business-e and CryptoNet. Matteo has more than 13 years of specializing in information security and collaborates from several years at the OWASP project: he founded the OWASP-Italy Chapter in 2005 and leads the OWASP Testing Guide from 2006. Matteo is invited as speaker at many events all around the world talking about Web Application Security. Matteo has undergraduate degrees in Computer Science Engineering from the University of Bologna.

BEV CORWIN

Bev was one of our room proctors at the 2013 Summit at AppSec USA. She helped manage the room on several days, making sure all of the leaders had everything they needed during their working sessions. Bev is a consultant and the Member Representative for the IDESG Identity Ecosystem for the OWASP Foundation.

ROBERT SHULLICH

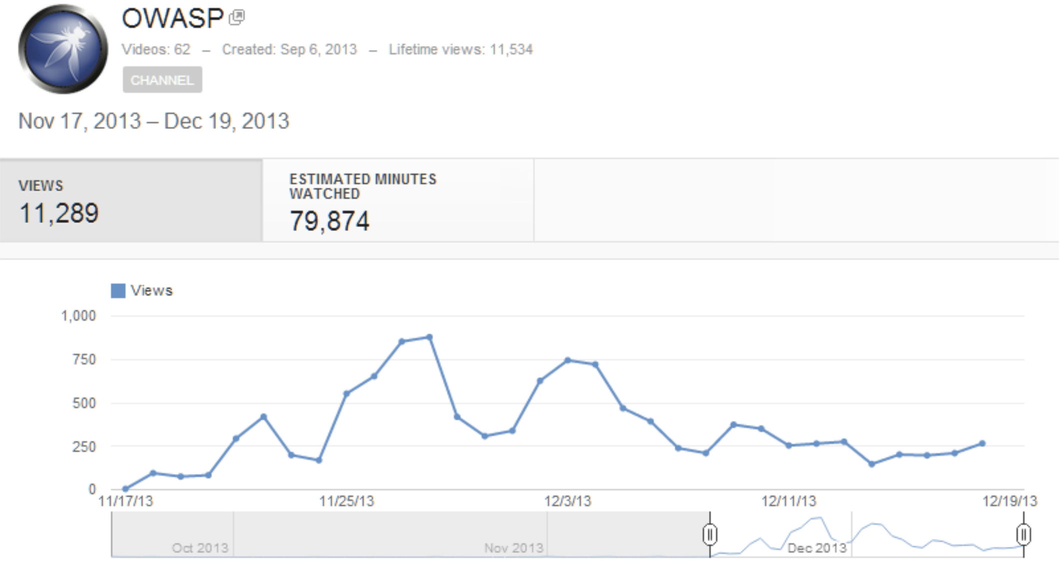
Robert is a Senior IT Specialist in Administration and Information Security of computer systems. He works in areas of IT Security Governance, Security Review, Security Audit, and Incident Response. Specializing in GRC and ITRM. Robert was another one of our room proctors. He made sure all of our leaders had everything they needed during their working sessions.

OWASP MEDIA PROJECT REPORT AFTER APPSEC USA 2013

OWASP Media Project after AppSecUSA 2013

At last AppSecUSA, OWASP Media Project has put 43 videos online for 32 hours for the talks, and also 6 videos from the Project Summit for 2.5 hours of content. All of that was online live for the summit and less than 24 hours after for the first talks, then the rest was published in one week just after the conference.

Now for some stats, covering from November 17th 2013 to December 19th 2013.



OWASP

Videos: 62 – Created: Sep 6, 2013 – Lifetime views: 11,534

CHANNEL

Nov 17, 2013 – Dec 19, 2013

VIEWS	ESTIMATED MINUTES WATCHED
11,289	79,874

We are at 11,289 views and 79,874 of estimated watched minutes.

Let me remind you that before that, we where at 245 views for 1,312 minutes, mainly from the OWASP Global Meetup live hangouts.
As for the subscribers, we are at 438 and we gained 442 of them with AppSecUSA efforts. We lost 4 hence the numbers.

The average view duration is 7:04 minutes, so 16% of the total times of videos. Since we have mostly one hour long videos, this is normal and in fact is probably a great number for YouTube.

Notables popular videos are:

OWASP Zed Attack Proxy - Simon Bennetts
2,126 views 17,712 minutes watched 8:19 avg
http://youtu.be/pYFtLA2yTR8

Top Ten Proactive Controls - Jim Manico
Jim Manico
@manicode
OWASP Volunteer
Global OWASP Board Member
OWASP Cheat-Sheet Series Project Manager and Contributor
VP Sec Architecture, WhiteHat Security
16 years of web-based, database driven software development and analysis experience
Secure coding educator/author
Kama'aina Resident of Kauai, Hawaii
Aloha!
00:00 / 49:55

Top Ten Proactive Controls - Jim Manico
845 views 8,293 minutes watched 9:48 avg
http://youtu.be/Cg5dN8Pyn_c

What You Didn't Know About XML External Entitie...
APPSEC USA
2013
What You Didn't Know About
XML External Entities Attacks
Timothy D. Morgan
VSR
00:00 / 38:40

What You Didn't Know About XML External Entities Attacks - Timothy Morgan
790 views 5,857 minutes wathced 7:24 avg
http://youtu.be/eHSNT8vWLfc

Finally, the countries with the top viewership:

United States	37%
Canada	12%
India	4.5%
United Kingdom	4.0%

I must point out that we were watched in 114 countries in total. That's amazing and shows the power of OWASP worldwide.

With that big first step done, we will continue with our Roadmap and the next thing on the table is to present a Webinar on how to use Google Hangout with live YouTube streaming. We will also shake things with the Chapters by inciting them to use Hangout and YouTube in order to get more into the Global Chapter Meetings Project. This has great potential but is not really used right now for helping smaller chapters to get contents.

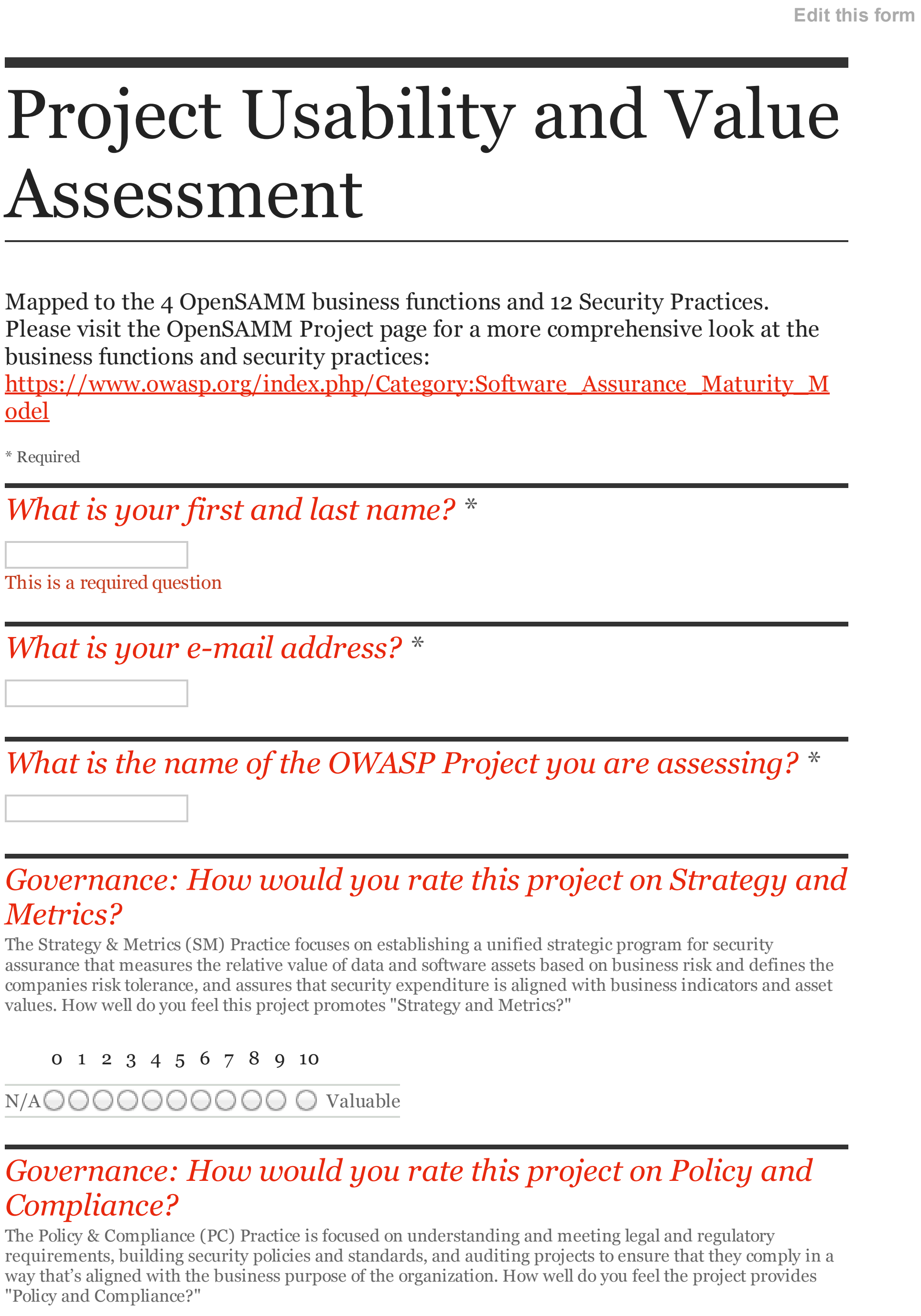
And and last, but not least, we are officially on the https://www.owasp.org home page and we can control what is shown without having to edit the Wiki.

One thing that is sure, is that we need more people in OWASP Media project. The good news is, unlike most other OWASP projects, you don't need to be an application security specialist to be really useful, you just need to be motivated to share knowledge with the world. If you want to join us, contact Jonathan Marcil the project leader.

Thanks to all who contributed and helped with OWASP Media Project!

PROJECT REVIEWS: USABILITY ASSESSMENT

http://sl.owasp.org/assessment_project_usability



Edit this form

Project Usability and Value Assessment

Mapped to the 4 OpenSAMM business functions and 12 Security Practices. Please visit the OpenSAMM Project page for a more comprehensive look at the business functions and security practices: https://www.owasp.org/index.php/Category:Software_Assurance_Maturity_Model

* Required

What is your first and last name? *

This is a required question

What is your e-mail address? *

What is the name of the OWASP Project you are assessing? *

Governance: How would you rate this project on Strategy and Metrics?

The Strategy & Metrics (SM) Practice focuses on establishing a unified strategic program for security assurance that measures the relative value of data and software assets based on business risk and defines the companies risk tolerance, and assures that security expenditure is aligned with business indicators and asset values. How well do you feel this project promotes "Strategy and Metrics?"

	0	1	2	3	4	5	6	7	8	9	10	
N/A	○	○	○	○	○	○	○	○	○	○	○	Valuable

Governance: How would you rate this project on Policy and Compliance?

The Policy & Compliance (PC) Practice is focused on understanding and meeting legal and regulatory requirements, building security policies and standards, and auditing projects to ensure that they comply in a way that's aligned with the business purpose of the organization. How well do you feel the project provides "Policy and Compliance?"

	0	1	2	3	4	5	6	7	8	9	10	
N/A	○	○	○	○	○	○	○	○	○	○	○	Valuable

Governance: How would you rate this project on Education and Guidance?

The Education & Guidance Practice is focused on educating personnel involved in the software development life-cycle with technical security awareness training, and defining and maintaining technical guidelines on security development best practices. Starting with role-specific training on application security, training should proliferate through the organization and culminate in role-based certification to verify comprehension of the materials. With improved access to information, project teams will be better able to proactively identify and mitigate the specific security risks that apply to their organization. How well do you feel this project promotes "Education and Guidance?"

	0	1	2	3	4	5	6	7	8	9	10	
N/A	○	○	○	○	○	○	○	○	○	○	○	Valuable

Construction: How would you rate this project on its Security Requirements?

The Security Requirements Practice focuses on explicitly considering security during design by specifying the expected behavior of software with respect to security. An access control matrix for resources and capabilities should be used, and security requirements should be derived from business logic and known risks. Furthermore, security requirements should be mandated for all projects and third parties, and these requirements should be audited. How well do you feel this project provides "Security Requirements?"

	0	1	2	3	4	5	6	7	8	9	10	
N/A	○	○	○	○	○	○	○	○	○	○	○	Valuable

Construction: How would you rate this project on its Threat Assessment?

The Threat Assessment Practice is centered on identifying and understanding high-level threats to the organization and individual projects using threat modeling, attacker profiling, abuse-case models per project that uses a weighting system for measuring threats. Threat models should evaluate the effectiveness of compensating controls for each threat as well as evaluating the risk from third party components How well do you feel this project promotes "Threat Assessment?"

	0	1	2	3	4	5	6	7	8	9	10	
N/A	○	○	○	○	○	○	○	○	○	○	○	Valuable

Construction: How would you rate this project on its Security Architecture?

The Secure Architecture Practice is focused on explicitly applying security principles to design, directing the software design process towards known-secure services and secure-by-default designs. And Secure Architecture involves formally controlling the design process and validating the usage of through frameworks, patterns, and platforms as secure components. How well do you feel this project provides "Security Architecture?"

0 1 2 3 4 5 6 7 8 9 10

N/A ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ Valuable

Verification: How would you rate this project on its Design Review?

The Design Review Practice involves identifying software attack surfaces, analyzing the design against security requirements. Assessment services should be provided to review software design against comprehensive best practices for security. Artifacts should be required to provide a detailed understanding of protection mechanisms, and formal assessments should be required at appropriate stages. How well do you feel this project provides "Design Review?"

	0	1	2	3	4	5	6	7	8	9	10	
N/A	○	○	○	○	○	○	○	○	○	○	○	Valuable

Verification: How would you rate this project on its Code Review?

The Code Review Practice is focused on inspection of software at the source code level in order to find security vulnerabilities. Security checklists should be created from existing security requirements and detailed inspections performed on high-risk code. Code reviews should include automated code analysis tools that are integrated into the development process. And formal code reviews should be mandated at appropriate stages to discover application-specific and language-specific risks. How well do you feel this project provides "Code Review?"

	0	1	2	3	4	5	6	7	8	9	10	
N/A	○	○	○	○	○	○	○	○	○	○	○	Valuable

Verification: How would you rate this project on its Security Testing?

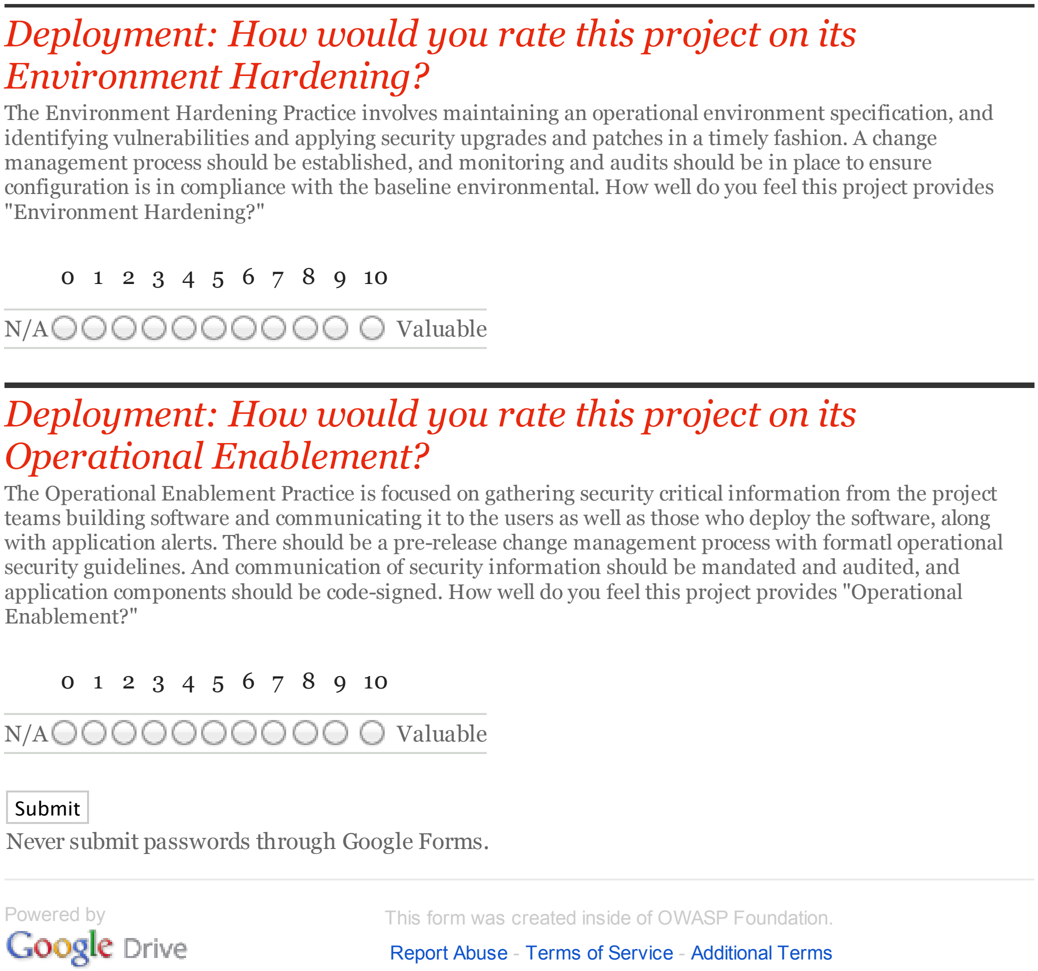
The Security Testing Practice is focused on performing penetration tests on software releases to find security problems. Penetration testing should be automated and integrated into the development process. And penetration testing should be application-specific. How well do you feel this project provides "Security Testing?"

	0	1	2	3	4	5	6	7	8	9	10	
N/A	○	○	○	○	○	○	○	○	○	○	○	Valuable

Deployment: How would you rate this project on its Vulnerability Management?

The Vulnerability Management Practice should include a high-level plan for responding to reported security incidents and identify a point of contact and response teams. An incident response process should be defined, along with a security incident disclosure process. Each security incident should include root cause analysis and document the impact of the incident through appropriate metrics. How well do you feel this project provides "Vulnerability Management?"

	0	1	2	3	4	5	6	7	8	9	10	
N/A	○	○	○	○	○	○	○	○	○	○	○	Valuable



Deployment: How would you rate this project on its Environment Hardening?

The Environment Hardening Practice involves maintaining an operational environment specification, and identifying vulnerabilities and applying security upgrades and patches in a timely fashion. A change management process should be established, and monitoring and audits should be in place to ensure configuration is in compliance with the baseline environmental. How well do you feel this project provides "Environment Hardening?"

	0	1	2	3	4	5	6	7	8	9	10	
N/A	○	○	○	○	○	○	○	○	○	○	○	Valuable

Deployment: How would you rate this project on its Operational Enablement?

The Operational Enablement Practice is focused on gathering security critical information from the project teams building software and communicating it to the users as well as those who deploy the software, along with application alerts. There should be a pre-release change management process with formatl operational security guidelines. And communication of security information should be mandated and audited, and application components should be code-signed. How well do you feel this project provides "Operational Enablement?"

	0	1	2	3	4	5	6	7	8	9	10	
N/A	○	○	○	○	○	○	○	○	○	○	○	Valuable

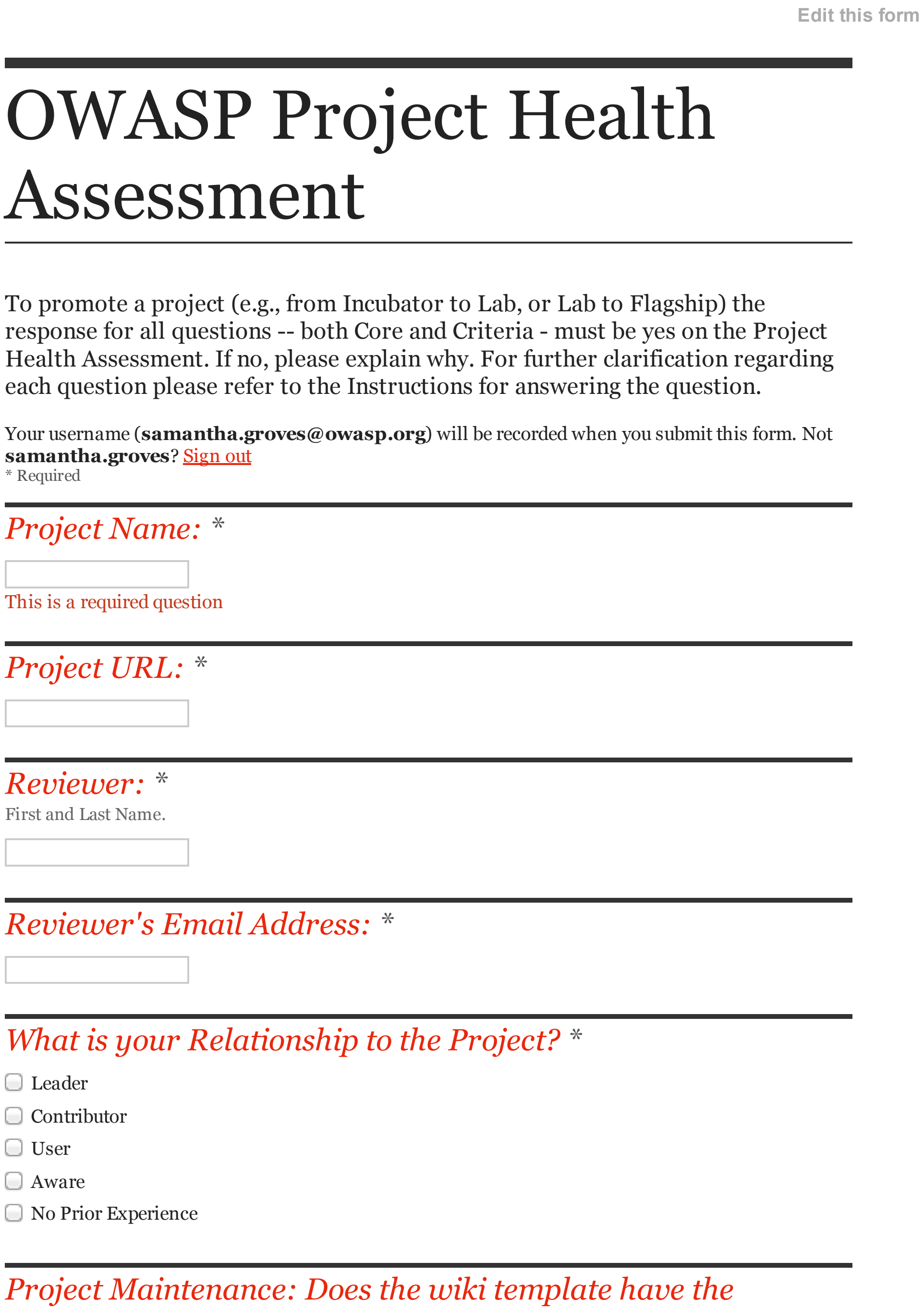
Never submit passwords through Google Forms.

This form was created inside of OWASP Foundation.

Report Abuse - Terms of Service - Additional Terms

OWASP PROJECT HEALTH ASSESSMENT

http://sl.owasp.org/assessment_project_health



Edit this form

OWASP Project Health Assessment

To promote a project (e.g., from Incubator to Lab, or Lab to Flagship) the response for all questions -- both Core and Criteria - must be yes on the Project Health Assessment. If no, please explain why. For further clarification regarding each question please refer to the Instructions for answering the question.

Your username (**samantha.groves@owasp.org**) will be recorded when you submit this form. Not **samantha.groves**? Sign out

* Required

Project Name: *

This is a required question

Project URL: *

Reviewer: *

First and Last Name.

Reviewer's Email Address: *

What is your Relationship to the Project? *

□ Leader

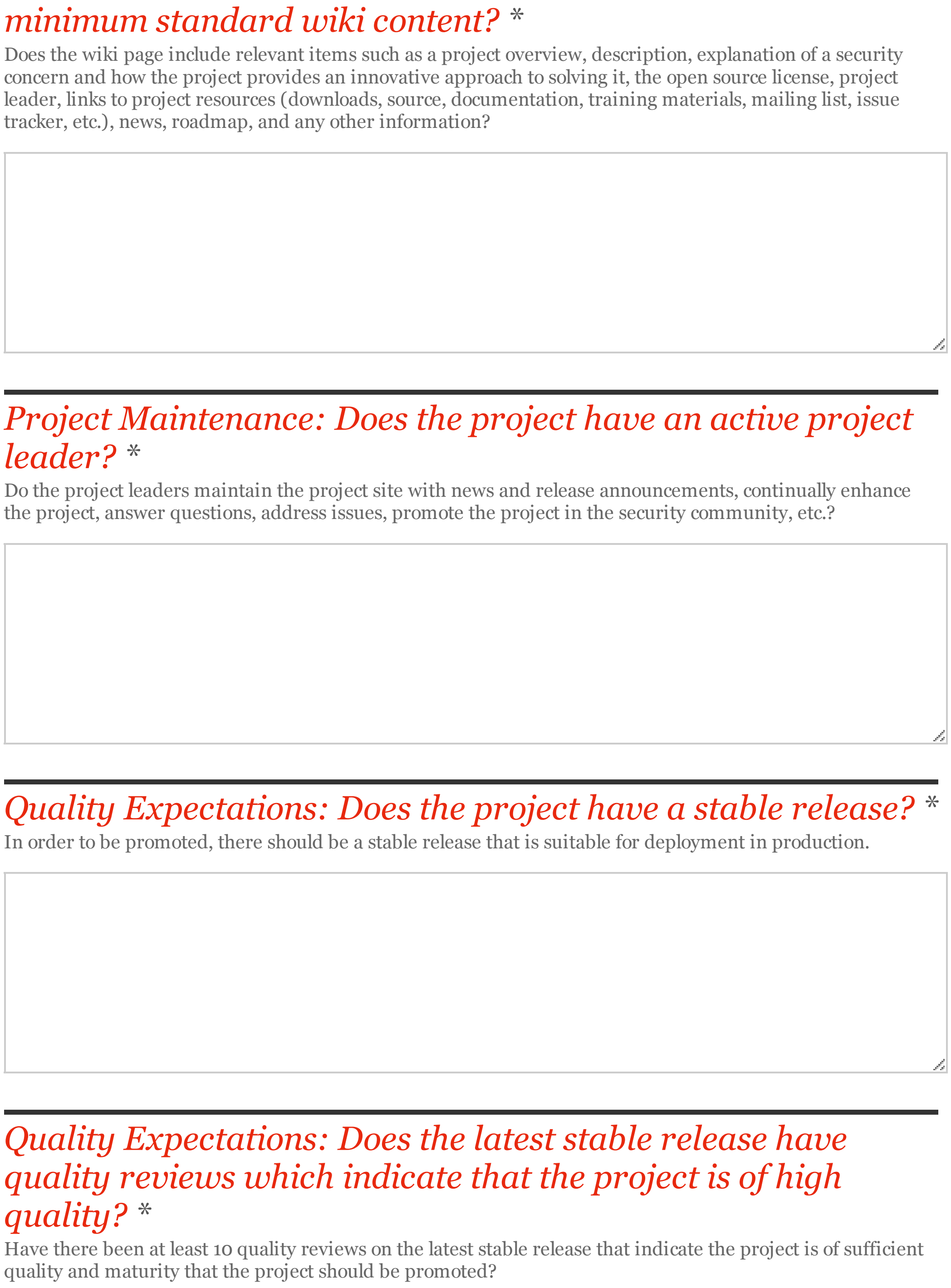
□ Contributor

□ User

□ Aware

□ No Prior Experience

Project Maintenance: Does the wiki template have the



minimum standard wiki content? *

Does the wiki page include relevant items such as a project overview, description, explanation of a security concern and how the project provides an innovative approach to solving it, the open source license, project leader, links to project resources (downloads, source, documentation, training materials, mailing list, issue tracker, etc.), news, roadmap, and any other information?

Project Maintenance: Does the project have an active project leader? *

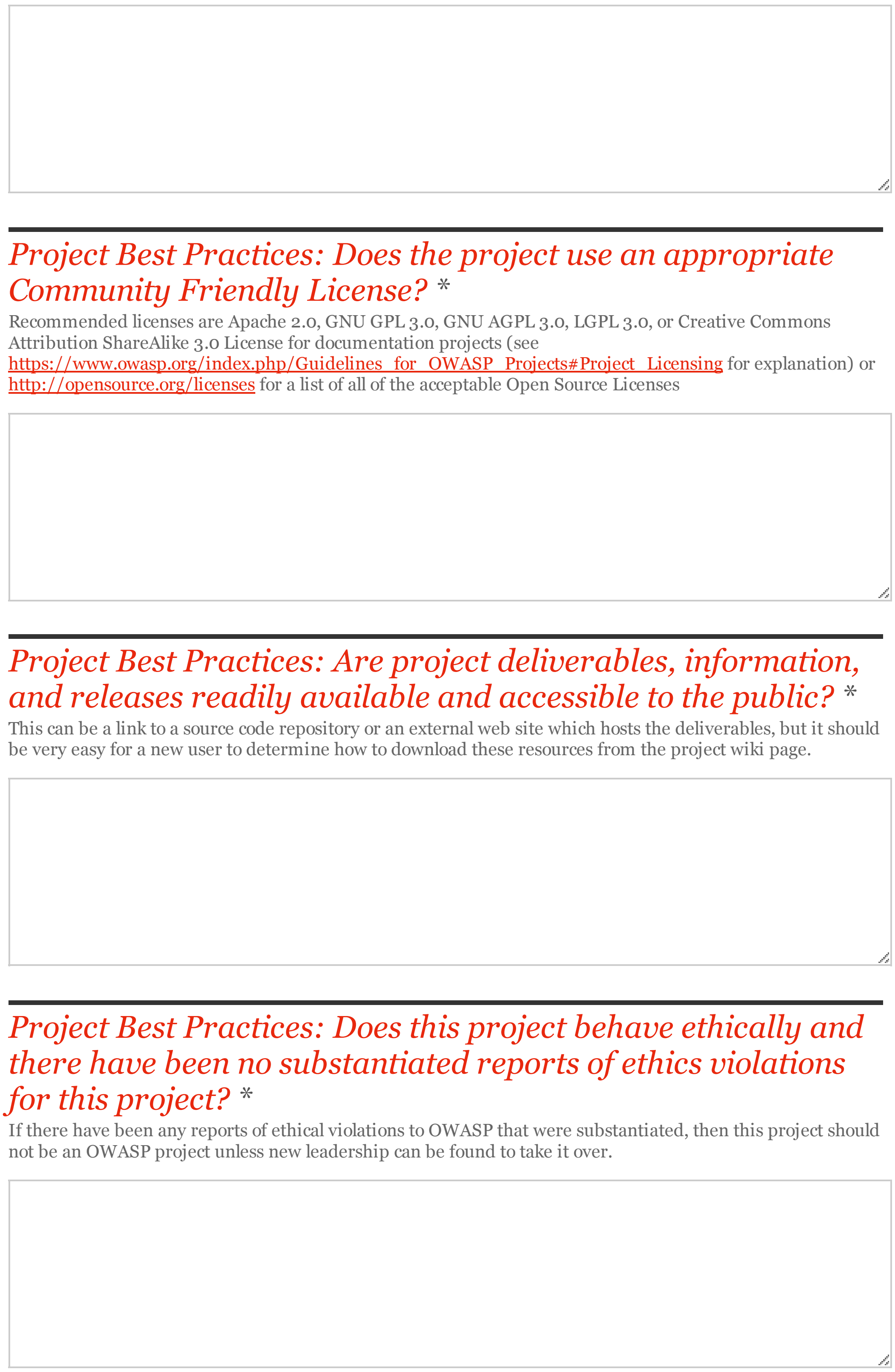
Do the project leaders maintain the project site with news and release announcements, continually enhance the project, answer questions, address issues, promote the project in the security community, etc.?

Quality Expectations: Does the project have a stable release? *

In order to be promoted, there should be a stable release that is suitable for deployment in production.

Quality Expectations: Does the latest stable release have quality reviews which indicate that the project is of high quality? *

Have there been at least 10 quality reviews on the latest stable release that indicate the project is of sufficient quality and maturity that the project should be promoted?



Project Best Practices: Does the project use an appropriate Community Friendly License? *

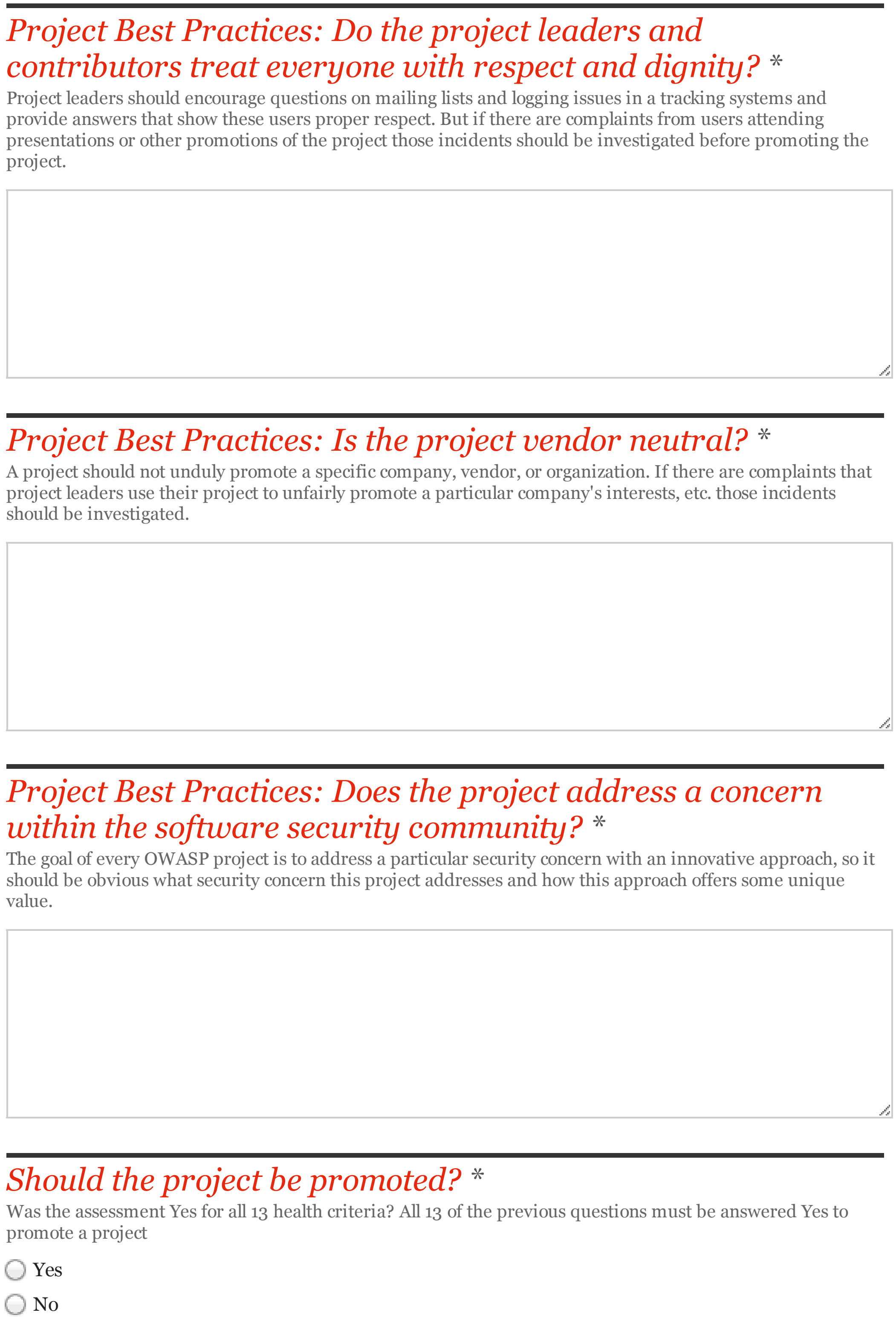
Recommended licenses are Apache 2.0, GNU GPL 3.0, GNU AGPL 3.0, LGPL 3.0, or Creative Commons Attribution ShareAlike 3.0 License for documentation projects (see https://www.owasp.org/index.php/Guidelines_for_OWASP_Projects#Project_Licensing for explanation) or http://opensource.org/licenses for a list of all of the acceptable Open Source Licenses

Project Best Practices: Are project deliverables, information, and releases readily available and accessible to the public? *

This can be a link to a source code repository or an external web site which hosts the deliverables, but it should be very easy for a new user to determine how to download these resources from the project wiki page.

Project Best Practices: Does this project behave ethically and there have been no substantiated reports of ethics violations for this project? *

If there have been any reports of ethical violations to OWASP that were substantiated, then this project should not be an OWASP project unless new leadership can be found to take it over.



Project Best Practices: Do the project leaders and contributors treat everyone with respect and dignity? *

Project leaders should encourage questions on mailing lists and logging issues in a tracking systems and provide answers that show these users proper respect. But if there are complaints from users attending presentations or other promotions of the project those incidents should be investigated before promoting the project.

Project Best Practices: Is the project vendor neutral? *

A project should not unduly promote a specific company, vendor, or organization. If there are complaints that project leaders use their project to unfairly promote a particular company's interests, etc. those incidents should be investigated.

Project Best Practices: Does the project address a concern within the software security community? *

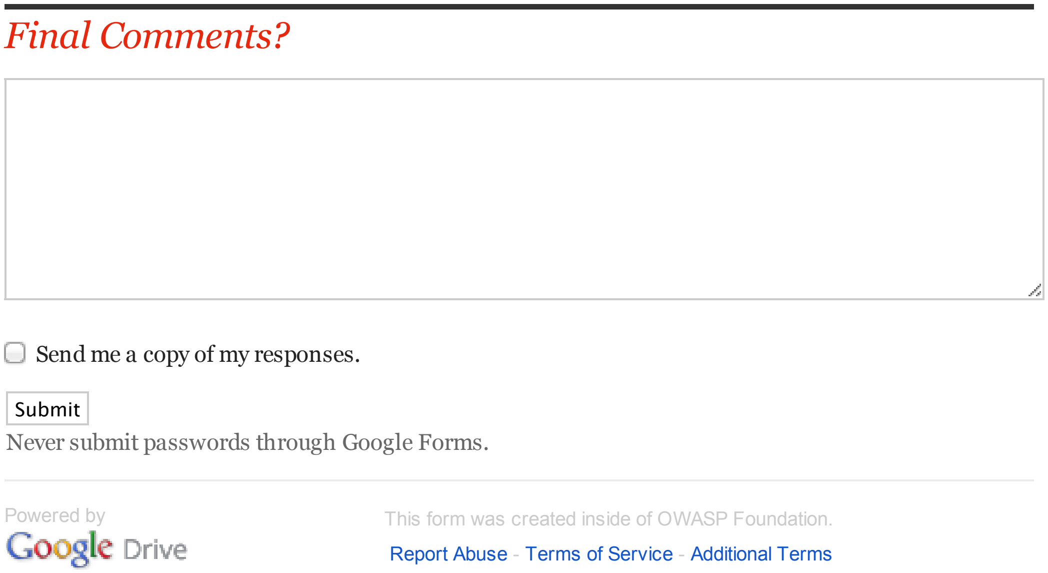
The goal of every OWASP project is to address a particular security concern with an innovative approach, so it should be obvious what security concern this project addresses and how this approach offers some unique value.

Should the project be promoted? *

Was the assessment Yes for all 13 health criteria? All 13 of the previous questions must be answered Yes to promote a project

○ Yes

○ No



Final Comments?

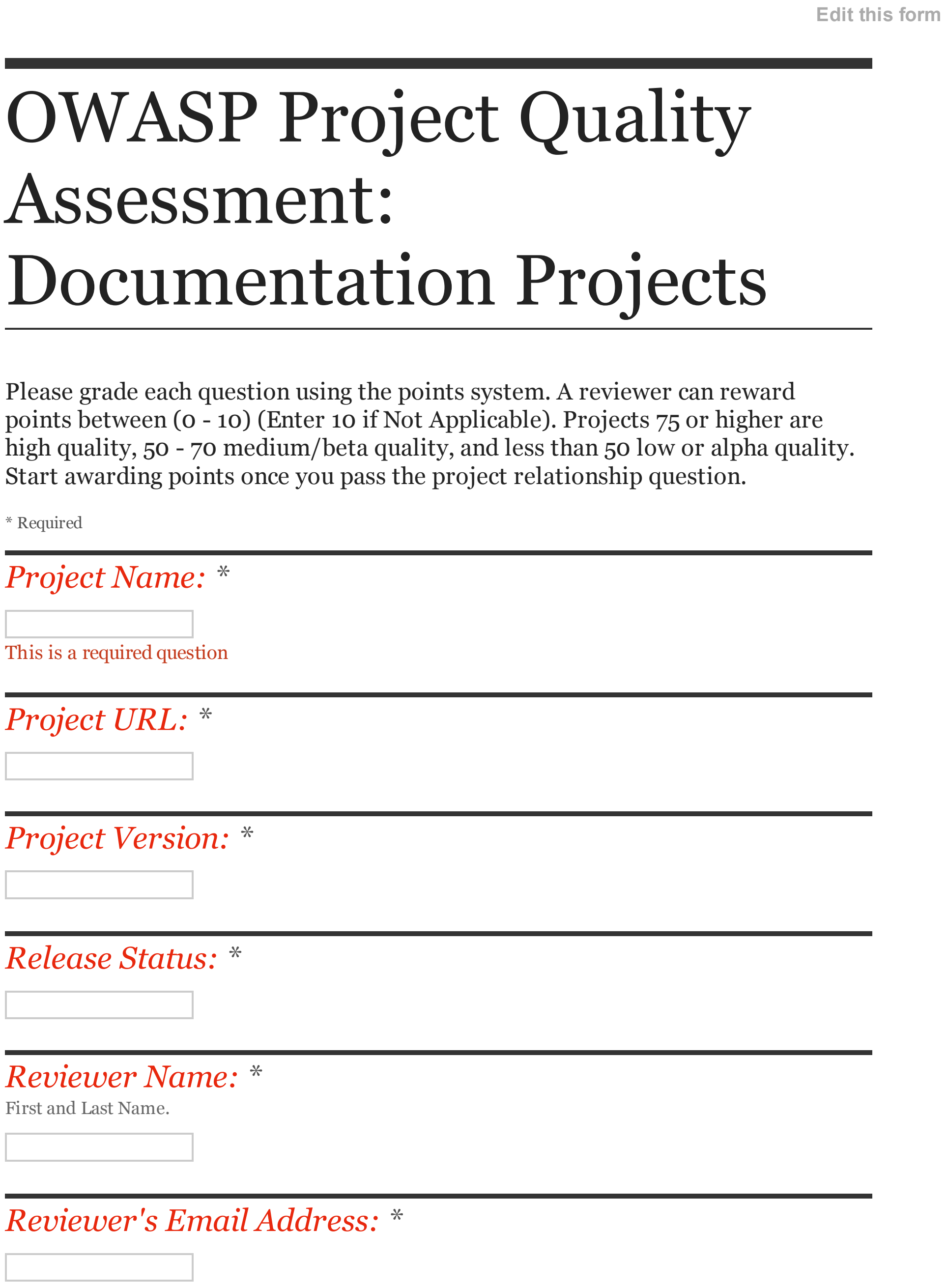
□ Send me a copy of my responses.

Never submit passwords through Google Forms.

This form was created inside of OWASP Foundation.

PROJECT QUALITY ASSESSMENT: DOCUMENTATION PROJECTS

http://sl.owasp.org/assessment_project_quality_documentation



Edit this form

OWASP Project Quality Assessment: Documentation Projects

Please grade each question using the points system. A reviewer can reward points between (0 - 10) (Enter 10 if Not Applicable). Projects 75 or higher are high quality, 50 - 70 medium/beta quality, and less than 50 low or alpha quality. Start awarding points once you pass the project relationship question.

* Required

Project Name: *

This is a required question

Project URL: *

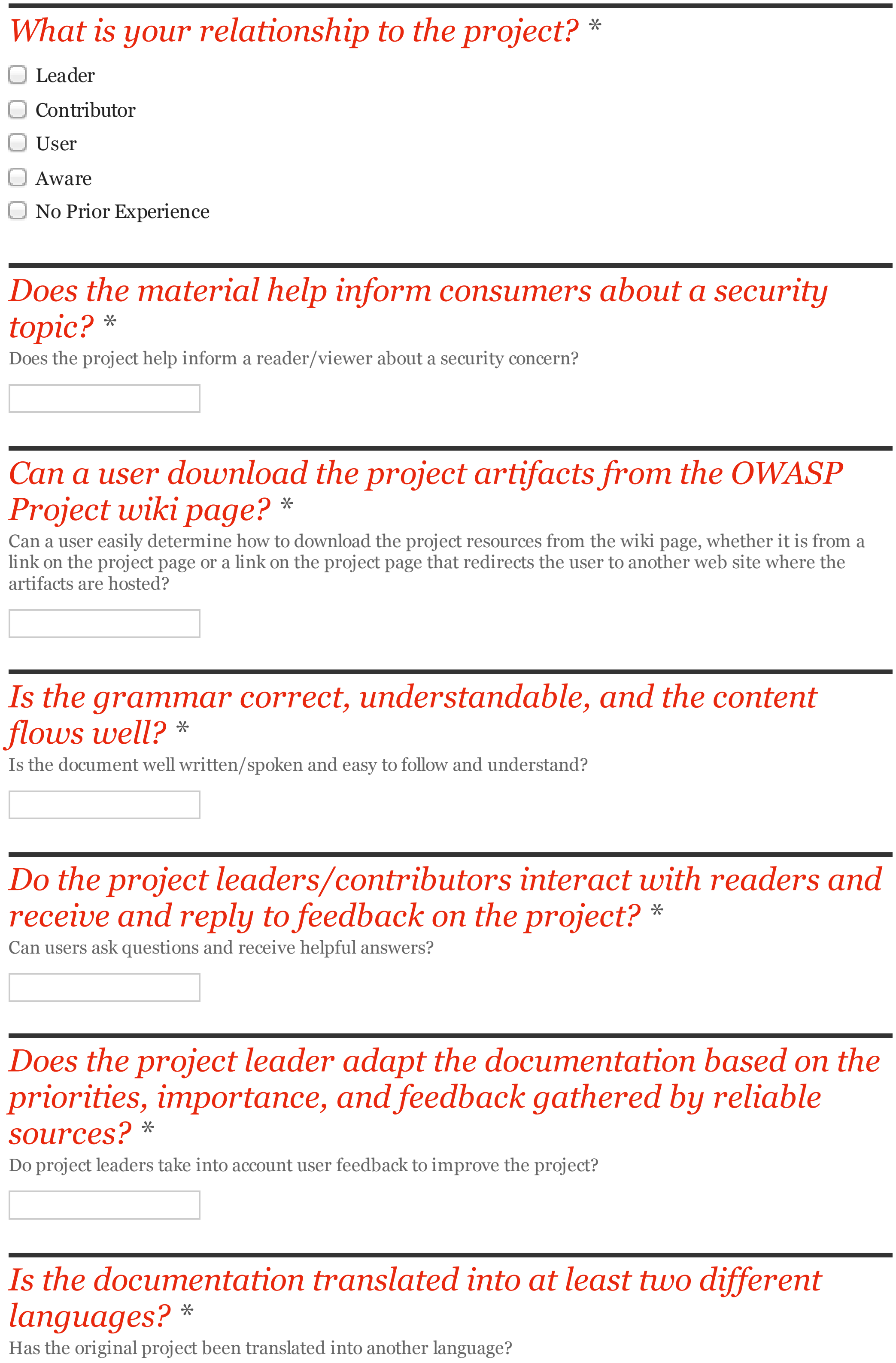
Project Version: *

Release Status: *

Reviewer Name: *

First and Last Name.

Reviewer's Email Address: *



What is your relationship to the project? *

- ☐ Leader
- ☐ Contributor
- ☐ User
- ☐ Aware
- ☐ No Prior Experience

Does the material help inform consumers about a security topic? *

Does the project help inform a reader/viewer about a security concern?

Can a user download the project artifacts from the OWASP Project wiki page? *

Can a user easily determine how to download the project resources from the wiki page, whether it is from a link on the project page or a link on the project page that redirects the user to another web site where the artifacts are hosted?

Is the grammar correct, understandable, and the content flows well? *

Is the document well written/spoken and easy to follow and understand?

Do the project leaders/contributors interact with readers and receive and reply to feedback on the project? *

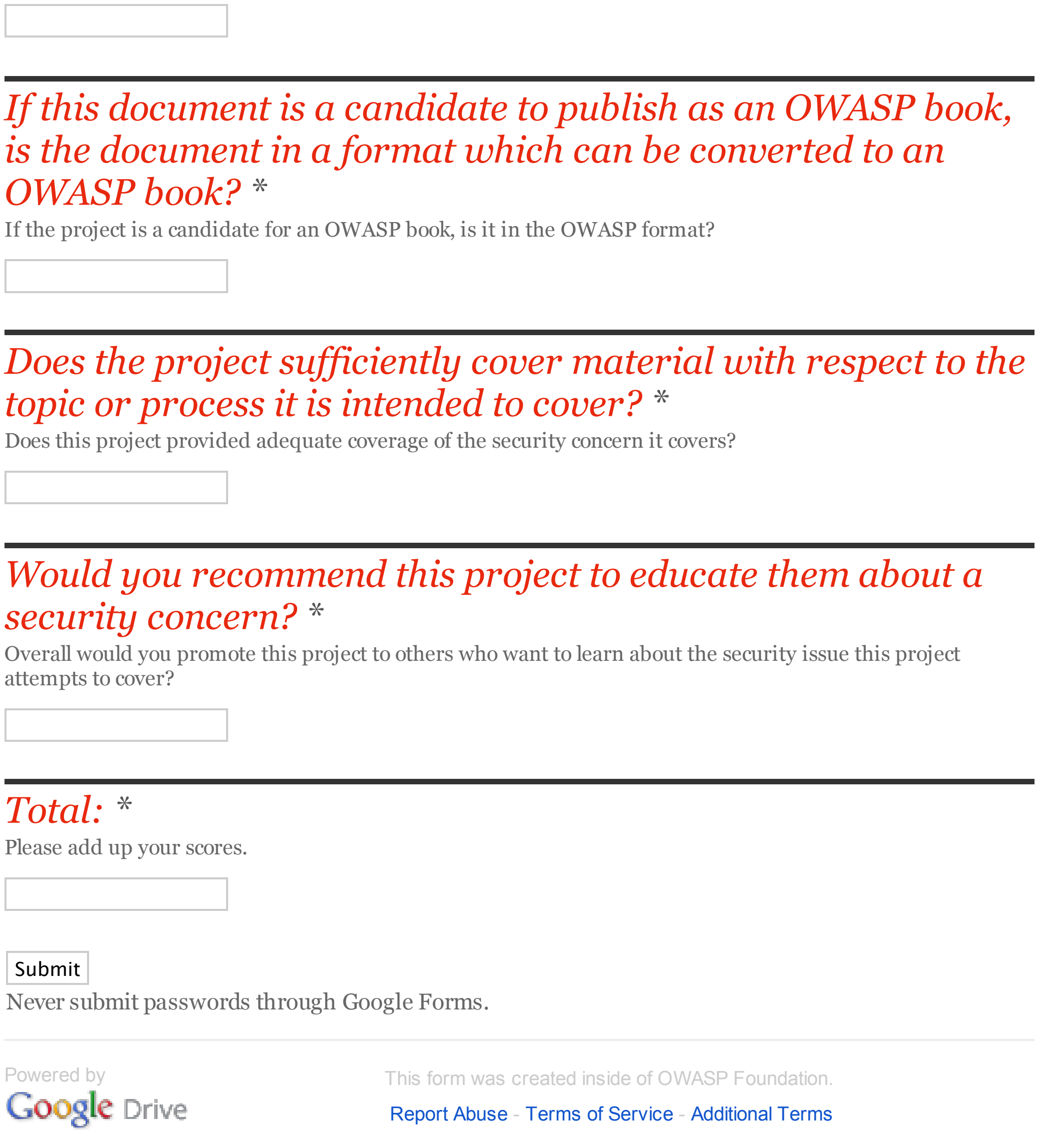
Can users ask questions and receive helpful answers?

Does the project leader adapt the documentation based on the priorities, importance, and feedback gathered by reliable sources? *

Do project leaders take into account user feedback to improve the project?

Is the documentation translated into at least two different languages? *

Has the original project been translated into another language?



If this document is a candidate to publish as an OWASP book, is the document in a format which can be converted to an OWASP book? *

If the project is a candidate for an OWASP book, is it in the OWASP format?

Does the project sufficiently cover material with respect to the topic or process it is intended to cover? *

Does this project provided adequate coverage of the security concern it covers?

Would you recommend this project to educate them about a security concern? *

Overall would you promote this project to others who want to learn about the security issue this project attempts to cover?

Total: *

Please add up your scores.

Never submit passwords through Google Forms.

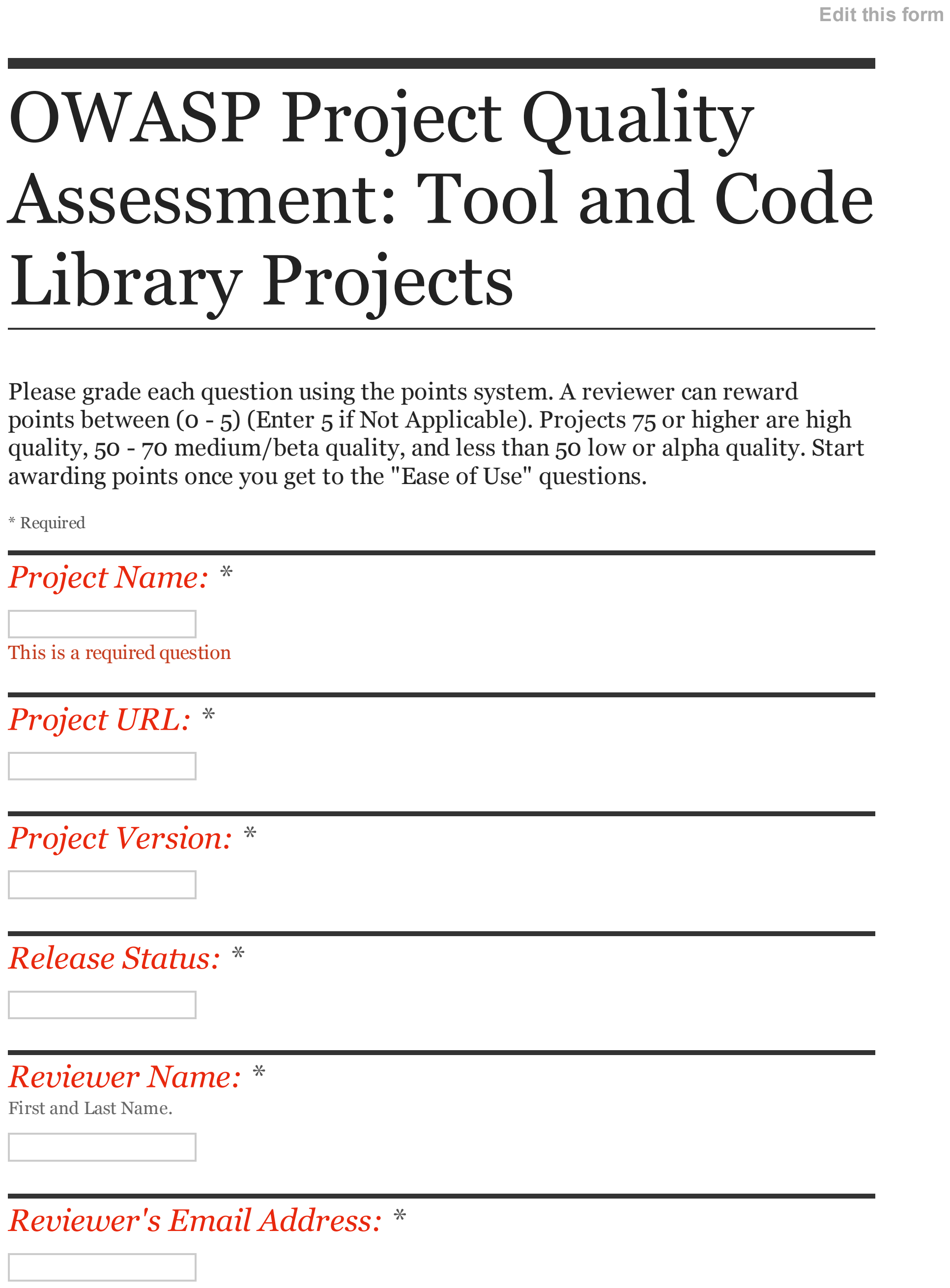
Powered by Google Drive

This form was created inside of OWASP Foundation.

Report Abuse - Terms of Service - Additional Terms

PROJECT QUALITY ASSESSMENT: CODE AND TOOL PROJECTS

http://sl.owasp.org/assessment_project_quality_tool_code



OWASP Project Quality Assessment: Tool and Code Library Projects

Please grade each question using the points system. A reviewer can reward points between (0 - 5) (Enter 5 if Not Applicable). Projects 75 or higher are high quality, 50 - 70 medium/beta quality, and less than 50 low or alpha quality. Start awarding points once you get to the "Ease of Use" questions.

* Required

Project Name: *

This is a required question

Project URL: *

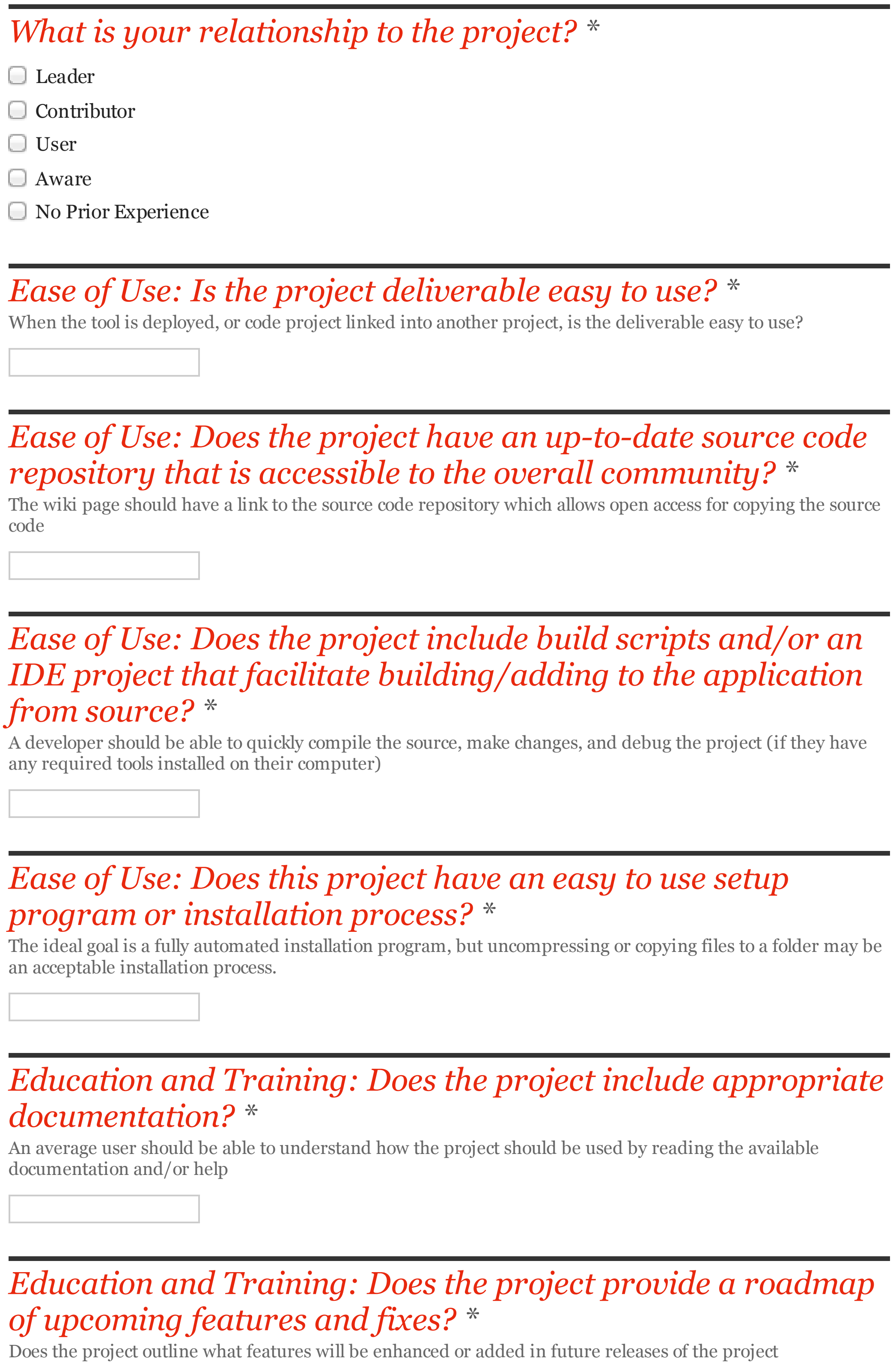
Project Version: *

Release Status: *

Reviewer Name: *

First and Last Name.

Reviewer's Email Address: *



What is your relationship to the project? *

□ Leader

□ Contributor

□ User

□ Aware

□ No Prior Experience

Ease of Use: Is the project deliverable easy to use? *

When the tool is deployed, or code project linked into another project, is the deliverable easy to use?

Ease of Use: Does the project have an up-to-date source code repository that is accessible to the overall community? *

The wiki page should have a link to the source code repository which allows open access for copying the source code

Ease of Use: Does the project include build scripts and/or an IDE project that facilitate building/adding to the application from source? *

A developer should be able to quickly compile the source, make changes, and debug the project (if they have any required tools installed on their computer)

Ease of Use: Does this project have an easy to use setup program or installation process? *

The ideal goal is a fully automated installation program, but uncompressing or copying files to a folder may be an acceptable installation process.

Education and Training: Does the project include appropriate documentation? *

An average user should be able to understand how the project should be used by reading the available documentation and/or help

Education and Training: Does the project provide a roadmap of upcoming features and fixes? *

Does the project outline what features will be enhanced or added in future releases of the project

Education and Training: Does the Project leader identify the development stage a release is in (e.g., Alpha, Beta, Stable, etc.)? *

Since different users have different levels of risk and tolerance for early beta releases, project leaders should identify the current development stage to indicate if a release should only be deployed in test environments and if they are seeking user input on a beta release versus a stable release that is appropriate to deploy in production.

Education and Training: Does the project contain a release document explaining the new features and fixes? *

When there is a new release are new features and fixes identified?

Education and Training: Does the project include training materials (e.g., tutorials, slide shows, videos, etc.)? *

Have the project leaders provided training materials that someone implementing this project could use to train other developers within their organization?

Education and Training: Is there a way for developers to ask questions or engage in discussions about the project? *

Can users ask questions through a mailing list, a forum, etc. that result in meanginful discussions with the project leaders?

Maintaining Quality: Is the project being maintained with current operating systems and other technology? *

If this project has been out for a while, is it being updated as new Operating Systems come out, or any libraries and tools that are used by the project are updated

Maintaining Quality: Does the project include Unit tests which provide sufficient code coverage? *

To ensure high quality, and make it easier for developers to make changes with confidence that they don't break existing code they are unfamiliar with, the project leaders should provide sufficient unit test code coverage

Maintaining Quality: Does the project maintain a prioritized list of open issues and allow users to report issues which are added to this list? *

Does the project maintain a public prioritized list of known issues which incorporates issues reported by end users?

Maintaining Quality: Are major issues quickly addressed? *

Are high priority issues addressed within a reasonable period of time?

Internationalization Support: Are all text strings displayed to the end user loaded from a resource file, and the appropriate language resource file is used based on user settings (if available). *

If text strings are displayed in the tool or returned as error messages from code projects, are the text strings externalized into resource files and the appropriate resource file is used based on the user's language settings when their language is available?

Internationalization Support: Does the program support international date and number/currency formats (if applicable)? *

If the program uses dates, numbers, or currency does the project handle different international formats appropriately?

Overall: Does this project provide a unique or innovative approach to address a security concern? *

The Project Leader(s) should explicitly state what security concern they are addressing and explain how this project offers a unique or innovative approach so it is clear to all users why they should be interested in downloading this project versus other projects which may attempt to address a similiar security concern

Overall: Would you recommend this project to a friend to solve their security concern? *

Overall would you promote this project to others who face the security issue this project attempts to address?

Total: *

CONTACT INFORMATION

If you would like more information regarding anything in this report, please contact the OWASP Projects Manager, Samantha Groves via e-mail at (Samantha.Groves@owasp.org).

OWASP

OWASP is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted. All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security. We urge approaching application security as a people, process, and technology problem because the most effective approaches to application security include improvements in all of these areas.

All content is ©2013 OWASP Foundation. This document is released under the CC Attribution-ShareAlike 3.0 license. For any reuse or distribution, you must make clear to others the license terms of this work.