# OER Revisions and Ancillary Materials Creation Mini-Grant Application

Affordable Learning Georgia aims to support the sustainability of previous Textbook Transformation Grants implementations through revisions of created open educational resources or the creation of new ancillary materials for existing OER. Individuals or teams who would like to apply for an OER Revisions or Ancillary Materials Creation. Mini-grant participants do not need to be the original creators of the resource(s). While we welcome original authors to revise their original materials, the nature of open licenses allows for the revision and remixing of OER materials by anyone as long as the terms of the license are adhered to.

The final deliverable for this category is the revised or newly-created materials as proposed in the application, which will be hosted through GALILEO Open Learning Materials. All revised or newly-created materials will be made available to the public under a Creative Commons Attribution License (CC-BY), unless the original materials were under a more restrictive license such as the inclusion of SA (Share-Alike) or NC (Non-Commercial).

For the purposes of this grant, we define revision as the major improvement of a resource through updates for accuracy, accessibility, clarity, design, and formatting. We define ancillary materials as any materials created to substantially support the instruction of a course using an existing open educational resource(s).

## Applicant Name *

Hossain Shahriar

## Applicant Position *

Associate Professor of Information Technology

## Applicant Institution *

Kennesaw State University

## Applicant Email Address *

Please use your institutional email address.

hshahriar@kennesaw.edu

## Other Team Members

Individuals can apply for mini-grants; a team is not required. If you do want to add team members to your grant, please provide the names and email addresses here.

## Type of Project *

- ○ Revision of pre-existing OER
- ◉ Creation of ancillaries for pre-existing OER
- ○ Other:

## Final Semester of the Project *

This is the semester in which the materials created/revised will be completed.

- ○ Fall 2019
- ○ Spring 2020

## Proposed Grant Funding Amount: *

This is the total (in a dollar amount) of funding you are requesting for the mini-grant. There is a maximum of $4800, with a maximum of $2000 per team member and $800 for project expenses.

$2,444

## Currently-Existing Resource(s) to be Revised / Ancillaries Created *

Please provide a title and web address (URL) to each of the currently-existing resources that you are either revising or creating new ancillary materials for below.

IT4843 - Ethical Hacking For Effective Defense,
http://ksuweb.kennesaw.edu/~hshahria/IT4843/IT4843.html

Module 6- Enumeration, http://ksuweb.kennesaw.edu/~hshahria/IT4843/module6/Module6-Lab.docx
Module 10- Hacking web servers,
http://ksuweb.kennesaw.edu/~hshahria/IT4843/module10/Module10-Lab.docx
Module 12- Hacking wireless networks,
http://ksuweb.kennesaw.edu/~hshahria/IT4843/module11/Module11-Lab.docx

## Project Description *

In at least one paragraph, describe your project's goals and deliverables.

a) Project goals:
In this project, we aim to develop additional hands-on lab materials for three existing modules of Ethical Hacking (IT4843) course. This course was originally developed as part of ALG Round 8 (see current course page, http://ksuweb.kennesaw.edu/~hshahria/IT4843/IT4843.html).
In particular, we plan to leverage existing programs available at Kali Linux [1], tools available as open source [2] [3] for enumeration of computers, vulnerability detection of web applications, and probing of IoT devices connected with Bluetooth wireless.

The Ethical Hacking (IT4843) course currently has 13 modules and each module comes with hands-on instruction covering a limited number of tools. For example, Nessus tool [4] is to enumerate computers in a network in Module 6, Webgoat application [5] for hands-on experience of attacking a web application (e.g., SQL injection) in Module 10, and aircrack-ng tool [6] is used to crack password of wifii and decrypt traffic to discover information in Module 12. However, there are further tools out there. Learners who wish to develop advanced skills on enumerating and vulnerability scanning of applications and computers in a network, currently have no availability of organized resources to use the advanced tools. Therefore, additional hands-on lab instructions increase the availability of the ancillary resources in the form of hands on lab instructions.

Our goal is to add the following resources for the three current modules:
a) Module 6 - Enumeration: We will add hands-on instructions how to install, configure and apply Sparta [7] and Inguma [8] tools to enumerate computers in a network that include identifying risky ports that may be open in computers.
b) Module 10 - Hacking Web Server: We will add hands-on instructions for Skipfish [9] and Dirbuster [11] tool to reconnaissance web application that include discovering vulnerabilities in application, and finding hidden directories.
c) Module 12 - Hacking Wireless Network: Using Blue Hydra program [10], we plan to provide hands-on instruction how to configure Blue Hydra application in Kali Linux, and look for IoT devices connected to Wifii with Bluetooth under discoverable and non-discoverable modes.

For all three modules, we are planning to use available manuals from Kali, tool websites, blogs where others may have shared experience (currently scattered on the web), available videos from Youtube (e.g., [12]), and trial and error run of these tools on Kali Linux computers.

b) Project Deliverables:
The end outcome will be three hands-on lab instructions for the three modules in the current course. Each of the module will provide detailed hands-on instructions showing how to install

and configure in Kali Linux, how to apply commands to gather information and use for attacks. The materials will include sufficient screenshots so learners having basic knowledge are able to follow the instructions. The developed materials would increase the availability of the ancillary resources in the form of hands on lab instructions that any interested learners can follow to develop advanced skills to enumerate and discover vulnerabilities in computers, applications and within IoT devices.

References

[1] Kali Linux, 2018, https://www.kali.org/
[2] Enumeration tools, 2018, http://tools.kali.org/tag/enumeration
[3] OWASP Testing Took, 2018, https://www.owasp.org/index.php/Appendix_A:_Testing_Tools
[4] Nessus, 2018, https://www.tenable.com/products/tenable-io/web-application-scanning/
[5] Webgoat, 2018, https://www.owasp.org/index.php/WebGoat_Getting_Started
[6] Aircrack-ng, 2018, https://www.aircrack-ng.org/
[7] Sparta, 2018, https://tools.kali.org/information-gathering/sparta
[8] Inguma, 2018, http://tools.kali.org/tag/enumeration/
[9] Skipfish, 2018, https://code.google.com/archive/p/skipfish/
[10] Blue Hydra, 2018, https://github.com/pwnieexpress/blue_hydra
[11] Dirbuster, 2018, https://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
[12] How to list Directories and Files of a Website using DirBuster in Kali Linux. 2017, https://www.youtube.com/watch?v=3xlMIEN_XvU

## Timeline and Personnel *

Provide a project timeline with milestones below, keeping in mind your selected Final Semester above. Provide a short description of the roles any additional team members will take on during the activities in your timeline.

Timeline

| | |
|---|---|
| 10/1/2018 – 11/30/2018 | Development of resources - Sparta, Inguma |
| 12/1/2018 – 1/31/2019 | Development of resources - Skipfish, Dirbuster |
| 1/2/2019 – 4/30/2019 | Development of resources - Blue hydra, IoT |
| 5/1/2019 – 5/30/2019 | Hosting materials into website |
| 5/31/2019 – 7/25/2019 | Teaching IT4843 with ancillary materials |
| 7/26/2019 – 8/14/2019 | Gather feedback, update materials, Final report |

Personnel (1)

1. Dr. Hossain Shahriar

## Budget *

Please enter your project's budget below. Include personnel and projected expenses. The maximum amounts for the award are as follows: $4,800 maximum award, $2,000 maximum per team member, $800 maximum for overall project expenses. Unlike standard-scale and large-scale transformations, the maximum of $800 is not a required element of the budget, but rather meant primarily for the purchase of specific tools and software which would help with improving resources.

The tools used in Module 6 (Enumeration) and Module 10 (Web Server Hacking) are available for free. However, in Module 12 (Wireless security), the IoT devices discovery with bluehydra will require to have us to obtain sample devices. We plan to use two popular household items: an Amazon Echo [1] and Altec [2]. We also need wireless network adapter to allow Kali Linux to discover the devices from Blue Hydra in discoverable mode. To discover devices in non-discoverable mode, we need additionally Ubertooh One gadget to work with Kali Linux. Below are the estimated costs of these devices.

| Item | Qty | Unit price($) | Total($) |
|---|---|---|---|
| Amazone Echo [1] | 1 | $100 | $100 |
| Altec Lansing [2] | 1 | $30 | $30 |
| TP-Link -Adapter [3] | 2 | $10 | $20 |
| Ubertooth One [4] | 2 | $127 | $254 |
| NooElec-Enclosure [5] | 2 | $20 | $40 |
| Total | | | $444 |

## Creative Commons Terms *

- [x] I understand that any new materials or revisions created with ALG funding will, by default, be made available to the public under a Creative Commons Attribution License (CC-BY), with exceptions for modifications of pre-existing resources with a more restrictive license.